Elmi Əsərlər

PROCEEDINGS *of* Science

Cild 22, № 2, 2024

Volume 22, № 2, 2024

Milli Müdafiə Universiteti
Heydər Əliyev adına
HƏRBİ İNSTİTUT

Milli Müdafiə Universiteti

Heydər Əliyev adına
HƏRBİ İNSTİTUT

Elmi Əsərlər

jurnalı

Cild 22, № 2, 2024

National Defence University

MILITARY INSTITUTE
named after Heydar Aliyev

Proceedings of Science

Volume 22, Number 2, 2024

www.mod.gov.az
www.mmu.edu.az
harbiinstitut@gmail.com

Hərbi İnstitutun nəşri
Bakı – 2024

Heydər Əliyev adına Hərbi İnstitutun nəşri

Jurnal 2003-cü il tarixində Azərbaycan Respublikası Ədliyyə Nazirliyində qeydə alınıb. Qeydiyyat nömrəsi: 535.
"Elmi Əsərlər" jurnalı elmi tədqiqatların əsas müddəalarının nəşr edilməsi üçün Azərbaycan Respublikası Prezidenti yanında Ali Attestasiya Komissiyası tərəfindən tövsiyə olunan nəşrlər siyahısına daxil edilmişdir.

Çap olunma tarixi: 28.09.2024
Şərti ç.v. 8.1 Kağız formatı $60*84^{1/16}$
Sifariş № 22. Tiraj 50 nüsxə

(AZ1018) Bakı şəhəri, Zığ qəsəbəsi, Polad Həşimov küçəsi 9
Telefon: (012) 479-78-43, mob. (050) 454 23 35
www.mod.gov.az, www.mmu.edu.az E-mail: harbiinstitut@gmail.com

Press of Military Institute named after Heydar Aliyev

The journal was registered in the Ministry of Justice of the Republic of Azerbaijan in 2003. Registration number: 535.
The "Proceedings of Science" has been included in the list of recommended publications by the Higher Attestation Commission under the President of the Republic of Azerbaijan for the publication of the main provisions of scientific research.

Date of publication: 28.09.2024
Conditional print sheet 8.1 Paper format 60*84 $^{1/16}$
Order № 22. Circulation 50 copy

(AZ1018) Baku city, Zigh settlement, Polad Hashimov street 9
Telefon: (012) 479-78-43; mob. (050) 454 23 35
www.mod.gov.az, www.mmu.edu.az E-mail: harbiinstitut@gmail.com

MÜNDƏRİCAT

CONTENTS

Elmi Əsərlər
Proceedings of Science

Heydər Əliyev adına Hərbi İnstitutun **Elmi Əsərlər** jurnalı, Cild 22, № 2, 2024 / 6-13
Proceedings of Science of the Military Institute named after Heydar Aliyev, Volume 22, № 2, 2024 / 6-13

Daxilolma tarixi / Received date: 10.05.2024
Qəbulolma tarixi / Accepted date: 16.09.2024

DOI: 10.30546/8967.2024.22.2.1001

CYBER WARFARE: NEW BATTLEFIELD

Nuran Mahmudov
lieutenant colonel
National Defense University, Military Scientific Research Institute, Baku
E-mail: mahmudovnuran@outlook.com
ORCID ID: 0009-0002-0103-9612

Abstract

Cyber warfare has emerged as a pressing concern in the modern era, posing significant threats to national security, critical infrastructure, and global stability. This article provides a comprehensive examination of the phenomenon of cyber warfare, exploring its definition, forms, motivations, and actors. Through the analysis of notable case studies such as "Stuxnet", "WannaCry", and "NotPetya", the article delves into the strategies employed and the impact of these incidents on affected entities. Additionally, the article discusses the legal and ethical considerations surrounding cyber warfare and evaluates international efforts to establish norms and regulations for cyberspace. The research aims to deepen understanding of the challenges posed by cyber warfare and identify strategies for enhancing cybersecurity resilience and mitigating risks. The obtained results underscore the importance of cybersecurity measures in safeguarding against cyber threats and highlight the need for increased international cooperation and collaboration to address the complexities of cyber warfare in an interconnected world.

Keywords: cyber warfare, security, threats, cyber-attacks, cyber resilience.

KİBERMÜHARİBƏ: YENİ DÖYÜŞ MEYDANI

Nuran Mahmudov
polkovnik-leytenant
Milli Müdafiə Universiteti, Hərbi Elmi Tədqiqat İnstitutu, Bakı

Xülasə

Kibermüharibə müasir dövrdə milli təhlükəsizliyə, kritik infrastruktura və qlobal sabitliyə ciddi təhdidlər yaradan aktual problemə çevrilib. Bu məqalə kibermüharibə fenomeninin hərtərəfli tədqiqini, onun tərifini, formalarını, motivlərini və aktyorlarını araşdırır. "Stuxnet", "WannaCry" və "NotPetya" kimi kiber hücumların təhlili vasitəsilə məqalədə istifadə olunan strategiyalar və bu hadisələrin təşkilatlara təsiri ətraflı şəkildə nəzərdən keçirilir. Bundan əlavə, məqalədə kibermüharibə ilə bağlı hüquqi və etik mülahizələr müzakirə edilir və kiber məkan üçün normativ hüquqi akt və qaydaların yaradılması üzrə beynəlxalq əməkdaşlığın əhəmiyyəti vurğulanır. Tədqiqatın məqsədi kibermüharibənin təbiətini anlamaq, kiber dayanıqlılığı artırmaq və riskləri azaltmaq üçün strategiyaları müəyyən etməkdir. Nəticə olaraq, məqalədə kiber təhdidlərdən qorunmaq məqsədilə kibertəhlükəsizlik tədbirlərinin vacibliyi və qloballaşan dünyada kibermüharibənin mürəkkəb təbiətindən irəli gələn problemləri həll etmək üçün beynəlxalq əməkdaşlığın zəruriliyini vurğulanır.

Açar sözlər: kibermüharibə, təhlükəsizlik, təhdidlər, kiber hücumlar, kiber dayanıqlıq.

КИБЕРВОЙНА: НОВОЕ ПОЛЕ БОЯ

Нуран Махмудов
подполковник
Национальный Университет Обороны, Военный Научно Исследовательский Институт, Баку

Аннотация

Кибервойна стала насущной проблемой в современную эпоху, создавая серьезные угрозы национальной безопасности, критической инфраструктуре и глобальной стабильности. В этой статье

проводится всестороннее исследование феномена кибервойны, исследуется его определение, формы, мотивации и действующие лица. Благодаря анализу таких известных тематических исследований, как “Stuxnet”, “WannaCry” и “NotPetya”, в статье подробно рассматриваются используемые стратегии и влияние этих инцидентов на пострадавшие организации. Кроме того, в статье обсуждаются правовые и этические соображения, связанные с кибервойной, и оцениваются международные усилия по установлению норм и правил для киберпространства. Исследование направлено на углубление понимания проблем, связанных с кибервойной, и определение стратегий повышения устойчивости кибербезопасности и снижения рисков. Полученные результаты подчеркивают важность мер кибербезопасности для защиты от киберугроз и подчеркивают необходимость расширения международного сотрудничества и взаимодействия для решения сложностей кибервойны во взаимосвязанном мире.

Ключевые слова: кибервойна, безопасность, угрозы, кибератаки, кибер устойчивость.

Introduction

In the digital age, where technology permeates nearly every aspect of society, the battlefield has expanded beyond traditional borders into the realm of cyberspace. Cyber warfare, the strategic use of digital attacks to disrupt, damage, or destroy computer systems or networks, has emerged as a potent tool in the arsenal of nations and non-state actors alike. Its significance in the modern world cannot be overstated, as the interconnected nature of the internet has rendered virtually every sector vulnerable to cyber threats.

At its core, cyber warfare encompasses a wide range of activities, from espionage and sabotage to propaganda and disinformation campaigns. Nation-states, criminal organizations, hacktivists, and even lone individuals can all engage in cyber operations, leveraging the anonymity and accessibility afforded by the internet to achieve their objectives. Whether motivated by political, economic, or ideological reasons, the potential impact of cyber-attacks on critical infrastructure, financial systems, and national security is profound.

The evolution of cyber warfare has mirrored the rapid advancement of technology, with each new innovation opening up new avenues for exploitation and disruption. Initially relegated to the realm of espionage and intelligence gathering, cyber warfare has evolved to encompass more aggressive tactics, including the use of malware, phishing, and distributed denial-of-service (DDoS) attacks. The proliferation of sophisticated cyber weapons and the emergence of state-sponsored cyber warfare units have further escalated tensions in cyberspace.

The impact of cyber warfare extends far beyond the digital realm, exerting significant influence on geopolitics and international relations. State-sponsored cyber-attacks have been employed as tools of coercion, espionage, and even warfare, blurring the lines between traditional and unconventional forms of conflict. From targeted cyber espionage campaigns aimed at stealing sensitive information to disruptive cyber-attacks targeting critical infrastructure, the consequences of cyber warfare can reverberate across borders and have far-reaching implications for global stability.

Moreover, the interconnectedness of the modern world means that no nation is immune to the effects of cyber warfare. A cyber-attack launched against one country's infrastructure or financial system can have cascading effects that ripple across the globe, underscoring the interconnected nature of cyberspace and the need for international cooperation in addressing cyber threats. As the frequency and sophistication of cyber-attacks continue to escalate, cybersecurity has become a paramount concern for governments, businesses, and individuals alike.

In this article, we will delve into the multifaceted landscape of cyber warfare, exploring its various forms, motivations, and actors. Through a series of case studies, we will examine notable examples of cyber-attacks and their implications for cybersecurity policy and defense strategies. Additionally, we will discuss the challenges posed by the militarization of cyberspace and the urgent need for international norms and regulations to mitigate the risks of cyber warfare. Ultimately, our aim is to shed light on this complex and evolving phenomenon and its significance in shaping the modern world.

1. Understanding cyber warfare

Cyber warfare, a term that encapsulates the strategic use of digital attacks to disrupt, damage, or destroy computer systems or networks, manifests in various forms, each with distinct objectives and methodologies. One prominent facet is espionage, where actors infiltrate targeted systems to gather

sensitive information for intelligence or competitive advantage. From state-sponsored cyber espionage campaigns aimed at stealing military secrets to corporate espionage targeting proprietary data, espionage represents a cornerstone of cyber warfare. Sabotage, another form of cyber warfare, involves the deliberate disruption or destruction of critical infrastructure or systems. Whether through the deployment of malware to cripple energy grids or the manipulation of financial systems to sow chaos, sabotage can inflict widespread damage and destabilize societies. Additionally, cyber warfare encompasses propaganda and disinformation campaigns, which aim to manipulate public opinion, sow discord, and undermine trust in institutions. By disseminating fake news, amplifying divisive narratives, and exploiting social media platforms, actors can wage information warfare to achieve their objectives [1, s. 12].

The motivations driving cyber-attacks are as varied as the forms they take, reflecting a complex interplay of political, economic, and ideological factors. Political motivations often underpin state-sponsored cyber-attacks, where nations seek to advance their strategic interests, exert influence, or retaliate against perceived adversaries. Economic motives drive cyber-attacks aimed at financial gain, whether through the theft of valuable intellectual property, the extortion of ransom payments, or the disruption of competitors' operations. Ideological considerations also play a role, with hacktivist groups leveraging cyber-attacks to promote their beliefs, advocate for social change, or protest perceived injustices. From ideological hackers targeting government websites to criminal organizations orchestrating ransomware attacks for financial profit, the motivations behind cyber-attacks are diverse and multifaceted.

The actors involved in cyber warfare span a wide spectrum, ranging from nation-states with vast resources and sophisticated capabilities to decentralized groups of individuals operating on the fringes of society. Nation-states represent the most powerful and influential actors in cyberspace, possessing the resources, expertise, and legal authority to conduct cyber operations on a global scale. From intelligence agencies conducting espionage to military units launching offensive cyber-attacks, nation-states wield significant influence in the digital domain [2]. However, non-state actors also play a significant role in cyber warfare, with criminal organizations leveraging cyber-attacks for financial gain and hacktivist groups employing them to advance their agendas. From cybercriminal syndicates orchestrating large-scale data breaches to hacktivist collectives launching distributed denial-of-service (DDoS) attacks against targeted organizations, the landscape of cyber warfare is populated by a diverse array of actors with varying capabilities and motivations. Understanding the motivations and actors behind cyber-attacks is crucial for developing effective cybersecurity strategies and mitigating the risks posed by cyber warfare in an increasingly interconnected world.

2. Methods and techniques

In the ever-evolving landscape of cyber warfare, adversaries employ a plethora of techniques and tactics to achieve their objectives, ranging from stealthy infiltration to overt disruption. Malware stands as one of the most pervasive and versatile tools in the cyber arsenal, encompassing a wide array of malicious software designed to infiltrate, damage, or control computer systems or networks. From viruses and worms to trojans and ransomware, malware poses a significant threat to organizations and individuals alike, capable of causing widespread disruption and financial losses. Phishing, another prevalent tactic in cyber warfare, involves the use of deceptive emails, websites, or messages to trick recipients into divulging sensitive information or downloading malware. By impersonating trusted entities or exploiting human vulnerabilities, phishing attacks can facilitate data breaches, identity theft, and other malicious activities. Furthermore, distributed denial-of-service (DDoS) attacks represent a formidable weapon in the cyber arsenal, leveraging a network of compromised devices to overwhelm targeted servers or networks with a flood of traffic, rendering them inaccessible to legitimate users. By disrupting essential services and causing downtime, DDoS attacks can inflict significant economic and reputational damage on targeted entities [3].

Advanced technologies such as artificial intelligence (AI) and machine learning are increasingly being integrated into cyber warfare operations, enabling adversaries to enhance the speed, scale, and sophistication of their attacks. AI-powered cyber tools can automate various aspects of the attack lifecycle, from reconnaissance and vulnerability scanning to malware creation and evasion. Machine

learning algorithms can analyse vast amounts of data to identify patterns, detect anomalies, and adapt attack strategies in real-time, making them invaluable assets for both offensive and defensive cyber operations. However, the proliferation of AI in cyber warfare also raises concerns about the potential for autonomous, self-learning cyber weapons that could evade detection and countermeasures, exacerbating the challenges faced by defenders [4].

In the murky world of cyber warfare, attribution the process of identifying the perpetrators behind cyber-attacks presents a significant challenge. Adversaries often employ tactics such as routing attacks through multiple proxies, using false flag operations, or exploiting compromised infrastructure to obfuscate their identities and evade detection. The use of cyber proxy's third-party entities or botnets enlisted to carry out cyber-attacks on behalf of a sponsor further complicates attribution efforts, as attackers can distance themselves from their actions and obscure their true intentions. Moreover, the global nature of cyberspace and the lack of international norms and regulations governing cyber operations make it difficult to hold perpetrators accountable for their actions. As a result, attribution in cyberspace remains an elusive and often contentious endeavour, hampering efforts to deter malicious actors and respond effectively to cyber threats [5, s. 28].

In conclusion, the methods and techniques employed in cyber warfare continue to evolve in response to advancements in technology and changes in the geopolitical landscape. From malware and phishing to DDoS attacks and AI-powered cyber tools, adversaries leverage a diverse array of tactics to achieve their objectives in cyberspace. However, the challenges of attribution and the use of cyber proxies underscore the need for enhanced cybersecurity measures, international cooperation, and the development of norms and regulations to mitigate the risks posed by cyber warfare in an increasingly interconnected world.

3. Case studies

In the annals of cyber warfare, several notable incidents have left an indelible mark on the digital landscape, showcasing the power and potency of cyber-attacks in today's interconnected world. Among these incidents, "Stuxnet", "WannaCry", and "NotPetya" stand out as exemplars of the diverse tactics and far-reaching consequences associated with cyber warfare.

"Stuxnet", a sophisticated computer worm discovered in 2010, is widely regarded as one of the most groundbreaking cyber weapons ever deployed. Designed to sabotage Iran's nuclear enrichment facilities, "Stuxnet" targeted industrial control systems (ICS) used in centrifuge operations, causing physical damage and delaying Iran's nuclear program. Its highly targeted nature and unprecedented level of complexity marked a significant escalation in cyber warfare tactics, demonstrating the potential for cyber-attacks to cause real-world damage and disrupt critical infrastructure [6].

"WannaCry", a ransomware attack that struck global systems in 2017, exploited a vulnerability in Microsoft Windows to encrypt data and demand ransom payments in Bitcoin. Targeting organizations across multiple sectors, including healthcare, finance, and transportation, "WannaCry" caused widespread chaos and financial losses, highlighting the vulnerability of unpatched systems and the interconnected nature of cyberspace. The incident underscored the importance of cybersecurity hygiene and the need for organizations to prioritize patch management and vulnerability remediation to mitigate the risks of cyber-attacks [7].

"NotPetya", another ransomware attack that emerged in 2017, targeted organizations primarily in Ukraine but quickly spread to infect systems worldwide. Disguised as a software update for accounting software used by Ukrainian businesses, "NotPetya" employed sophisticated propagation techniques to rapidly propagate across networks, causing widespread disruption and financial losses. Although initially believed to be a ransomware attack, "NotPetya's" destructive capabilities and lack of a feasible decryption mechanism led experts to conclude that its primary goal was to cause chaos and destruction rather than financial gain. The incident highlighted the dangers of indiscriminate cyber-attacks and the potential for collateral damage in cyberspace [8].

The strategies employed in these cyber warfare incidents varied widely, ranging from targeted sabotage to indiscriminate disruption. "Stuxnet" demonstrated the effectiveness of precision targeting and the exploitation of vulnerabilities in critical infrastructure to achieve strategic objectives. "WannaCry" and "NotPetya", on the other hand, leveraged widespread propagation and ransom demands

to maximize impact and financial gain. However, all three incidents shared common themes, including the exploitation of known vulnerabilities, the use of malware to achieve objectives, and the disruption of essential services and operations.

The impact of these cyber warfare incidents on affected entities was profound, causing significant financial losses, reputational damage, and operational disruptions. Stuxnet's sabotage of Iran's nuclear program set back its enrichment efforts and highlighted the vulnerability of critical infrastructure to cyber-attacks. “WannaCry” and “NotPetya” disrupted businesses, government agencies, and critical infrastructure worldwide, causing billions of dollars in damages and eroding trust in digital systems. The incidents also exposed the interconnected nature of cyberspace and the need for coordinated international responses to cyber threats.

In the aftermath of these cyber warfare incidents, numerous lessons have been learned, and their implications for cybersecurity policy and defense strategies have become increasingly apparent. Organizations have recognized the importance of proactive cybersecurity measures, including patch management, vulnerability scanning, and incident response planning, to mitigate the risks of cyber-attacks and minimize their impact. Governments have sought to enhance collaboration and information sharing to improve cyber threat intelligence and attribution capabilities, enabling more effective responses to cyber threats. Additionally, the incidents have underscored the need for international norms and regulations to govern cyberspace and deter malicious actors from engaging in cyber warfare. By learning from past incidents and adapting cybersecurity policies and defense strategies accordingly, organizations and governments can better defend against the evolving threats posed by cyber warfare in an increasingly digitized world.

4. International law and governance

In the complex realm of cyber warfare, navigating the legal and ethical landscape presents formidable challenges, as the traditional frameworks of international law struggle to keep pace with the rapidly evolving nature of cyber threats. At the heart of the matter lie profound questions surrounding sovereignty, jurisdiction, and accountability in cyberspace, where the boundaries between state and non-state actors blur, and the rules of engagement remain largely undefined. As a result, the legal and ethical considerations surrounding cyber warfare are subject to intense debate and scrutiny, with divergent interpretations and competing interests shaping the discourse.

One of the central tenets of international law applicable to cyber warfare is the principle of sovereignty, which asserts the right of states to exercise exclusive control over their territory and cyberspace. However, the transnational nature of cyberspace complicates matters, as cyber-attacks can originate from anywhere in the world and traverse multiple jurisdictions before reaching their intended targets. This raises thorny questions about attribution, responsibility, and the applicability of traditional legal norms to cyber operations conducted across borders. Moreover, the absence of clear rules governing cyber warfare leaves room for ambiguity and exploitation by malicious actors, further complicating efforts to establish accountability and deterrence in cyberspace.

In response to these challenges, international efforts have been underway to establish norms and regulations for cyberspace, aimed at promoting stability, predictability, and responsible behavior among states and other actors. One such initiative is the Tallinn Manual, a comprehensive study of how existing international law applies to cyber operations, conducted by a group of legal experts convened by the NATO Cooperative Cyber Defence Centre of Excellence. The Tallinn Manual seeks to clarify key legal principles and provide guidance on issues such as the use of force, sovereignty, and state responsibility in cyberspace, offering valuable insights into the legal framework governing cyber warfare [9].

Additionally, the United Nations Group of Governmental Experts (UN GGE) has played a pivotal role in advancing international dialogue and cooperation on cybersecurity issues. Through a series of reports, the UN GGE has examined the applicability of international law to cyberspace, identified norms of responsible state behaviour, and proposed confidence-building measures to enhance cybersecurity and reduce the risk of conflict in cyberspace. However, despite these efforts, significant challenges remain, including the lack of consensus among states on key issues such as the definition of cyber warfare, the scope of permissible cyber operations, and the appropriate responses to cyber-attacks [10].

The effectiveness of existing frameworks in addressing the challenges of cyber warfare is a subject of ongoing debate and scrutiny. While initiatives such as the Tallinn Manual and the UN GGE reports have made important contributions to the development of international norms and regulations for cyberspace, their impact remains limited by the voluntary nature of compliance and the absence of enforcement mechanisms. Moreover, the proliferation of state-sponsored cyber-attacks, the emergence of non-state actors as significant players in cyberspace, and the increasing weaponization of information and communication technologies pose formidable challenges to the stability and security of cyberspace.

In conclusion, the legal and ethical considerations surrounding cyber warfare are complex and multifaceted, reflecting the unique challenges posed by the interconnected nature of cyberspace. International efforts to establish norms and regulations for cyberspace have made progress in clarifying key legal principles and promoting responsible behavior among states and other actors. However, significant gaps and ambiguities persist, highlighting the need for continued dialogue, cooperation, and innovation to address the challenges of cyber warfare and safeguard the integrity and stability of cyberspace in an increasingly digitized world.

5. Future trends and challenges

As we peer into the future of cyber warfare, a landscape fraught with emerging technologies and evolving threats unfolds before us, presenting both opportunities and challenges for defenders and adversaries alike. Among the emerging trends in cyber warfare, quantum computing looms large as a game-changer, promising unprecedented computational power and the ability to break conventional encryption schemes. Quantum computers could render existing cryptographic protocols obsolete, exposing sensitive data to interception and manipulation by malicious actors. Moreover, the advent of quantum-resistant encryption algorithms and the race to develop quantum computing capabilities herald a new era of cyber warfare, where the rules of engagement are reshaped by the quantum revolution.

Another emerging trend in cyber warfare is the rise of cyber-physical attacks, where digital intrusions target physical systems and infrastructure, with potentially catastrophic consequences. From attacks on critical infrastructure such as power grids and transportation networks to the manipulation of internet-connected devices in the Internet of Things (IoT), cyber-physical attacks blur the boundaries between cyberspace and the physical world, amplifying the potential impact of cyber warfare on society and national security. As the integration of digital technologies into critical infrastructure accelerates, the vulnerabilities exposed by cyber-physical attacks become increasingly pronounced, highlighting the urgent need for robust cybersecurity measures and resilience strategies to mitigate the risks.

The militarization of cyberspace and the proliferation of cyber weapons pose significant challenges to global security and stability, as nations invest heavily in building offensive cyber capabilities and conducting cyber operations to advance their strategic interests. The attribution problem, exacerbated by the use of cyber proxies and false flag operations, further complicates efforts to hold perpetrators accountable for their actions and deter malicious behaviour in cyberspace. Moreover, the lack of internationally accepted norms and regulations governing cyber warfare leaves room for ambiguity and miscalculation, increasing the risk of conflict escalation and unintended consequences.

In the face of these emerging trends and challenges, strategies for enhancing cyber resilience and mitigating the risks of cyber warfare are imperative. One approach is to prioritize investment in cybersecurity research and development, fostering innovation in areas such as quantum-resistant encryption, threat intelligence, and secure software development. By staying ahead of emerging threats and vulnerabilities, organizations and governments can bolster their defences and adapt to the evolving threat landscape. Additionally, enhancing international cooperation and information sharing is crucial for building collective resilience and responding effectively to cyber threats. Initiatives such as the establishment of cyber defense alliances, the sharing of best practices and threat intelligence, and the development of incident response frameworks can help coordinate responses to cyber attacks and build trust among nations [11].

Furthermore, integrating cybersecurity into broader national security and defense strategies is essential for addressing the challenges posed by the militarization of cyberspace and the proliferation of cyber weapons. By adopting a comprehensive approach that combines deterrence, resilience, and diplomacy, governments can effectively manage cyber risks and safeguard their interests in an

increasingly digitized world. Moreover, promoting a culture of cybersecurity awareness and education among businesses, governments, and the general public is crucial for building a cyber-resilient society capable of withstanding the challenges of cyber warfare. Ultimately, by embracing innovation, cooperation, and resilience, we can navigate the future of cyber warfare with confidence and ensure the security and stability of cyberspace for generations to come.

Conclusion

In conclusion, the exploration of cyber warfare reveals a multifaceted landscape characterized by diverse actors, evolving tactics, and profound implications for global security and stability. Throughout this article, we have delved into the various dimensions of cyber warfare, from its definition and forms to its impact on geopolitics, legal considerations, and emerging trends. We have examined notable case studies such as “Stuxnet”, “WannaCry”, and “NotPetya”, which illustrate the complexity and potency of cyber-attacks in today's interconnected world. Furthermore, we have explored the challenges posed by the militarization of cyberspace, the proliferation of cyber weapons, and the need for enhanced cybersecurity measures to mitigate the risks of cyber warfare.

Central to our discussion is the recognition of the paramount importance of cybersecurity measures in safeguarding against cyber threats. As the frequency and sophistication of cyber-attacks continue to escalate, organizations and governments must prioritize investment in cybersecurity research, technology, and workforce development to stay ahead of emerging threats and vulnerabilities. By adopting a proactive approach to cybersecurity, organizations can enhance their resilience and minimize the potential impact of cyber-attacks on their operations, reputation, and bottom line.

Moreover, the evolving landscape of cyber warfare underscores the critical need for increased international cooperation and collaboration to address shared challenges and threats. Cyber-attacks transcend national borders and require coordinated responses and collective action to effectively mitigate risks and enhance cybersecurity posture. Initiatives such as information sharing, capacity building, and the development of international norms and regulations can help build trust among nations and promote responsible behaviour in cyberspace. By working together to address the root causes of cyber threats and vulnerabilities, the international community can create a safer and more secure digital environment for all.

In summary, the phenomenon of cyber warfare represents a complex and dynamic challenge that requires a comprehensive and collaborative approach to address effectively. By embracing innovation, resilience, and cooperation, we can navigate the evolving landscape of cyber warfare with confidence and safeguard the integrity and stability of cyberspace for future generations. The stakes are high, but by working together, we can rise to the challenge and build a more secure and resilient digital world for all.

References

1. Whyte, C. Understanding cyber-warfare: Politics, policy and strategy / C.Whyte & B.Mazanec. – London: Routledge, – 2023. – 364 p.

2. Dato’Abd, N. A. A. B., Habib, E. A. B. E., & Saudi, M. M. The Integration of Cyber Warfare and Information Warfare // OIC-CERT Journal of Cyber Security, – 2021. vol. 3, № 1, – pp. 7-20.

3. Eliyan, L. F., & Di Pietro, R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges // Future Generation Computer Systems, – 2021. vol. 122, – pp. 149-171.

4. Johnson, J. Artificial intelligence & future warfare: implications for international Security // Defense & Security Analysis, – 2019. vol. 35, № 2, – pp. 147-169.

5. Jasper, S. Russian Cyber Operations: Coding the Boundaries of Conflict / S.Jasper. – Washington, DC, USA: Georgetown University Press, – 2020. – 214 p.

6. Baezner, M., & Robin, P. Stuxnet: [Electronic resource] / research-collection.ethz.ch – 2017. URL: https://www.research-collection.ethz.ch/handle/20.500.11850/200661

7. Kaspersky. What is WannaCry ransomware? [Electronic resource] / kaspersky.com – 2024. URL: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

8. Greenberg, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History: [Electronic resource] / wired.com – August 22, 2018. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

9. Arnold, R. The Tallinn manual 2.0 on the international law applicable to cyber operations // International Criminal Law Review, – 2020. vol. 20, № 1, – pp. 155-159.

10. Pauletto, C. Information and telecommunications diplomacy in the context of international security at the United Nations // Transforming Government: People, Process and Policy, – 2020. vol. 14, № 3, – p. 351-380.

11. Yaacoub, J. P. A. Cyber-physical systems security: Limitations, issues and future trends / O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, [et al.] // Microprocessors and microsystems, – 2020. vol. 77, – p. 103201.

Elmi Əsərlər
Proceedings of Science

Heydər Əliyev adına Hərbi İnstitutun **Elmi Əsərlər** jurnalı, Cild 22, № 2, 2024 / 14-23
Proceedings of Science of the Military Institute named after Heydar Aliyev, Volume 22, № 2, 2024 / 14-23

Daxilolma tarixi / Received date: 24.07.2024
Qəbulolma tarixi / Accepted date: 17.09.2024

DOI: 10.30546/8967.2024.22.2.1003

DEMOKRATİK DÖVLƏTİN BƏRQƏRAR OLMASI PROSESİ: RASİONAL SİYASİ ŞÜURUN İNKİŞAFI

Ramid Hüseynov
siyasi elmlər üzrə fəlsəfə doktoru, dosent
Heydər Əliyev adına Hərbi İnstitut, Bakı
E-mail: ramidhuseynov82@gmail.com
ORCİD ID: 0000-0002-6473-8165

Xülasə

Dövlətlərin necə və hansı usulla idarə olunması, hansı rejimin daha effektiv olması ilə bağlı mübahisələr hazırki dövrümüzə qədər davam etməkdədir. Xüsusən də demokratik dövlətlə bağlı məsələlər bir çox alimlərin və siyasətçilərin müzakirə obyekti olaraq qalmaqdadır. İlk baxışda aydın və sadə izah olunan demokratik sistem əslində bir o qədər də mürəkkəb və abstrakt mahiyyət kəsb edir. İllər əvvəl qərbdə yaranmasına, bərqərar olmasına və cəmiyyətin daha yaxşı, ədalətli idarə olunması üçün effektiv əhəmiyyət kəsb etməsinə baxmayaraq, dünyanın əksər yerlərində özünə tam olaraq yer tapa bilməmişdir. Bu yerlərdə mövcud dövlətlər üzdə demokratik olduqlarını bəyan etsələr də, hətta hüquqi baxımdan bunu numayiş etdirsələr də əslində rejimin mahiyyətində totalitar və avtoritar amillər üstünlük təşkil edir. Siyasi institutların icra mexanizminin buna adekvat olmaması və cəmiyyətin rasional siyasi şüurunun, siyasi mədəniyyətinin kifayət qədər inkişaf etməməsi demokratiyanın tam bərqərar olmasına maneçilik törədir. Göründüyü kimi, qeyd olunan vəziyyət özündə böyük araşdırma tələb edən bir problemi birləşdirir. Bu məqsədlə, müəyyənləşdirilmiş vəzifələrə uyğun olaraq, ilk öncə demokratiya fenomeninə təkrar nəzər yetirilmiş və alimlərin, klassik və müasir mütəfəkkirlərin fikirləri müqayisələndirilmişdir. Daha sonra demokratiyanı üstün edən mühüm amillər, prinsiplər qeyd olunmaqla izahlar verilmişdir. Demokratiyanın inkişafında beynəlxalq əməkdaşlıq və qarşılıqlı siyasi mübadilənin roluna diqqət yetirilmiş və bu məsələnin vacibliyi göstərilmişdir. Elmi işdə əsas diqqət isə demokratik idarəetməyə keçid zamanı həlli zəruri olan problemlər və rasional siyasi şüurun inkişafına yönəldilmiş və bu məqamlar əsaslı və ətraflı tədqiq olunmuşdur. Belə nəticəyə hasil olmuşdur ki, demokratik dövlətin bərqərar olmasında qanunvericilik bazasının və siyasi idarəetmə mexanizminin təkmilləşdirilməsi, inteqrasiyası və cəmiyyətin rasional siyasi şüurunun formalaşması mütləq vacibdir.

Açar sözlər: demokratik dövlət, demokratiya fenomeni, demokratik idarəetməyə keçid, rasional siyasi şüur, demokratiyanın bərqərar olması.

THE PROCESS OF ESTABLISHING A DEMOCRATIC STATE: THE DEVELOPMENT OF RATIONAL POLITICAL CONSCIOUSNESS

Ramid Huseynov
PhD in political sciences, associate professor
Military Institute named after Heydar Aliyev, Baku

Abstract

Debates about how and in what way states are managed, which regime is more effective, continue to this day. In particular, the issues related to the democratic state remain the subject of discussion by many scientists and politicians. At first glance, the democratic system, which is clearly and simply explained, actually has an equally complex and abstract nature. Although it was created in the west many years ago, established and effective for the better and fair management of society, it has not fully found a place for itself in most parts of the world. Even if the existing states in these places declare that they are democratic on the face, even if they demonstrate it from a legal point of view, in reality totalitarian and authoritarian factors prevail in the essence of the regime. The inadequacy of the executive mechanism of political institutions and the insufficient development of the society's rational political consciousness and political culture prevent the full establishment of democracy. As it can be seen, the mentioned

situation combines a problem that requires a great deal of research. In accordance with the tasks defined for this purpose, first of all, the phenomenon of democracy was reviewed and the opinions of scientists, classical and modern thinkers were compared. Then the important factors and principles that make democracy superior were explained. The role of international cooperation and mutual political exchange in the development of democracy was emphasized and the importance of this issue was shown. In the scientific work, the main attention was focused on the problems that need to be solved during the transition to democratic governance and the development of rational political consciousness, and this point was thoroughly and thoroughly studied. It was concluded that the improvement and integration of the legislative framework and the political management mechanism and the formation of the rational political consciousness of the society are absolutely essential for the establishment of a democratic state.

Keywords: democratic state, phenomenon of democracy, transition to democratic management, rational political consciousness, establishment of democracy.

ПРОЦЕСС СТАНОВЛЕНИЯ ДЕМОКРАТИЧЕСКОГО ГОСУДАРСТВА: РАЗВИТИЕ РАЦИОНАЛЬНОГО ПОЛИТИЧЕСКОГО СОЗНАНИЯ

Рамид Гусейнов
доктор философии по политических наук, доцент
Военный Институт имени Гейдара Алиева, Баку

Аннотация

Споры о том, как и каким образом управляются государства, какой режим более эффективен, продолжаются и по сей день. В частности, вопросы, связанные с демократическим государством, остаются предметом обсуждения многих ученых и политиков. На первый взгляд демократическая система, которую объясняют ясно и просто, на самом деле имеет столь же сложную и абстрактную природу. Хотя она была создана на Западе много лет назад, создана и эффективна для лучшего и справедливого управления обществом, она не нашла себе в полной мере места в большинстве частей мира. Даже если существующие государства в этих местах заявляют, что они демократичны на первый взгляд, даже если они демонстрируют это с юридической точки зрения, на самом деле в сути режима преобладают тоталитарные и авторитарные факторы. Полному установлению демократии препятствуют неадекватность исполнительного механизма политических институтов, недостаточное развитие рационального политического сознания и политической культуры общества. Как видно, указанная ситуация объединяет в себе проблему, требующую большого исследования. В соответствии с поставленными для этой цели задачами, прежде всего, был рассмотрен феномен демократии и сопоставлены мнения ученых, классических и современных мыслителей. Затем были объяснены важные факторы и принципы, которые делают демократию превосходящей. Была подчеркнута роль международного сотрудничества и взаимного политического обмена в развитии демократии и показана важность этого вопроса. В научной работе основное внимание было сосредоточено на проблемах, которые необходимо решить в ходе перехода к демократическому управлению и развития рационального политического сознания, и этот момент тщательно и всесторонне изучался. Сделан вывод, что совершенствование и интеграция законодательной базы и механизма политического управления, формирование рационального политического сознания общества абсолютно необходимы для становления демократического государства.

Ключевое слова: демократическое государство, феномен демократии, переход к демократическому управлению, рациональное политическое сознание, установление демократии.

Giriş

Yaşadığımız dövrdə ən yaxşı siyasi idarəetmə forması olmasına baxmayaraq, demokratiya hələ də bütün dövlətlərdə təşəkkül tapmamışdır. Əksər hallarda ən azğın və mürtəce şovinizm, yaxud dini təməlçiliklə qovuşan müxtəlifyönlü totalitar və avtoritar ideologiya və hərəkatlar hələ də yaşamaqdadırlar. Demokratik hökumətlər dünya ölkələrinin yalnız yarısından azında hakimiyyət başındadır və bu ölkələrin vətəndaşları sayca Yer kürəsinin bütün sakinlərinin güclə yarısını təşkil edir. Son zamanlar demokratiyaya keçid mərhələsində olan bir çox dövlətlərdə də hələ də çoxlu problemlər qalmaqda davam edir. Bununla belə demokratik cəhətdən inkişaf etmiş ölkələrin özlərində hər şey xalqın istədiyi kimi deyil. Orada hələ də işsizlik, yoxsulluq, korrupsiya, kasıbların sosial təminatı və s. problemlər qalmaqdadır. Lakin bir sıra çatışmazlıqların olmasına baxmayaraq, demokratiya digər siyasi sistemlərdən daha mütərəqqidir.

Araşdırmanın tamamilə demokratiyanın nəzəri tədqiqi ilə bağlı olmadığını əsas götürərək, həmçinin demokartiyanın nəzəri cəhətdən araşdırılmasının ayrıca, geniş bir tədqiqat işi olduğunu nəzərə alaraq, biz sadəcə olaraq, demokratik dövlətin bərqərar olmasında inteqrasiya və rasional siyasi şüurun inkişafı məsələlərini məqaləmizdə öyrənməyə çalışmışıq. Belə ki, qarşıya qoyulan məqsədə uyğun olaraq göstərilmişdir ki, demokratiya ideyasının əsasını insanların azadlığı və bərabərliyi kimi sosial dəyərlərin dərk edilməsi və zəruriliyinin qiymətləndirilməsi təşkil edir. Demokratik idarəetmə sisteminin ən üstün tərəflərindən biri və ən başlıcası, məhz hüquqi dövlətin formalaşması, qanunun aliliyinin hökm sürməsi və hər şeyin qanun çərçivəsində olmasıdır. Bu idarəetmə formasının, sisteminin formalaşması, bərqərar olması üçün mühüm amillərdən biri inteqrasiya prosesinin sürətləndirilməsi, dünyanın bu sahədə inkişaf etmiş dövlətləri ilə münasibətlərin dərinləşdirilməsi və insanların rasional siyasi şüurunun, siyasi mədəniyyətinin inkişaf etdirilməsidir. Yalnız demokratik dəyərlərin, prinsiplərin cəmiyyətin siyasi şüurunda, təfəkküründə öz əksini tapması ilə ümumilikdə demokratiyanın bərqərar olmasına əmin olmaq olar.

1. Demokratiya fenomeni: demokratiyanı üstün edən mühüm faktorlar

Demokratiyanın eramızdan əvvəl yaranmasına və bu günə kimi böyük inkişaf yolu keçməsinə baxmayarq, o, hələ də tam, lazımi səviyyədə bərqərar olmamışdır. Demoratik cəhətdən yüksək inkişaf etmiş dövlətlərdə belə, müxtəlif problemlər, nöqsanlar qalmaqdadır. Həmçinin bu gün dünyaya nəzər yetirsək, görərik ki, heç də bütün dövlətlər demokratik idarəetmə yolunu tutmamışlar, onlarda hələ də qeyri-demokratik siyasi vəziyyət qalmaqdadır.

Demokratiya fenomeninin qarşısında duran başlıca məsuliyyət onun xalq tərəfindən bütün aspektlərilə birlikdə tam mənada başa düşülməsidir. Lakin digər tərəfdən bunun tam başa düşülməsi də mümkün görünmür. Başqa sözlə, bunun bütünlükdə dərk edilməsi reallıqdan bir qədər uzaqdır.

Hazırki dünyada fərdlərin əksəriyyəti demokratik sistemin nə olduğunu bilmədiklərinə və ya çox kiçik bir qisminin məlumatlı olmasına baxmayaraq, uzun müddət bu sistemin əsası qoyulmuş ölkələrdə də bu tam anlamlı deyil və olsa da belə bir çox hallarda qüsurlu olur [1, s. 4]. Bir çox hallarda dünyada demokratiya ilə bağlı müşahidə olunan ciddi problemlərin səbəbləri də buradan qaynaqlanır.

Belə ki, qloballaşan dünyada hər insan tam azad, bərabərhüquqlu vətəndaş kimi yaşamağa çalışır. Çünki bu, onların insan və mənsub olduqları ölkələrin vətəndaşları kimi ayrılmaz hüquqlarıdır. Bu hüquqların ən yaxşı qorunduğu, təmin olunduğu cəmiyyət, idarəetmə forması heç şübhəsiz ki, demokratiyadır. Bu baxımdan da dünyanın bütün vətəndaşları öz ölkələrində demokratiyanın bərqərar olması uğrunda mübarizə aparırlar.

Diqqət yetirsək görərik ki, idarəetmənin bu formasının ən mühum prinsipi: hakimiyyətin xalqa məxsus olması, vaxtaşırı, mütəmadi seçkilərin keçirilməsidir.

Hakimiyyətin yalnız və yalnız seçkilər, xalqın iradəsi əsasında formalaşması demokratiyanın digər idarəetmə usullarından fərqləndirən ən başlıca cəhətdir. Demokratiyanın tanınmış tədqiqatçısı Robert Dahl demokratiyanın üstün cəhətlərini göstərmişdir:

- tiraniyadan qurtulma;
- əsas hüquq və azadlıqlara riayət etmə;
- şəxsi toxunulmazlıq hüququ;
- öz müqəddəratını təyin etmə;
- mənəvi muxtariyyət;
- şəxsiyyətin inkişafetmə imkanları;
- şəxsiyyətin təməl mənafelərinin qorunması;
- siyasi bərabərlik.

Bunlardan əlavə, müasir demokratiyalar nəzərdə tutur:

- sülhə can atma;
- firavan yaşama [2, s. 43-83].

Ümumilikdə mütəxəssislər demokratiyanın əsas 14 prinsipini qeyd edirlər:

1. Vətəndaşların iştirakı;
2. Bərabərlik;
3. Məsuliyyət;

4. Şəffaflıq;
5. Siyasi tolerantlıq;
6. Çoxpartiyalı sistem;
7. Hakimiyyətdən sui-istifadəyə nəzarət;
8. Azad iqtisadiyyat;
9. Hüquq sistemi;
10. İnsan hüquqları;
11. Azad və ədalətli seçkilər;
12. Ədalətli məhkəmə;
13. Seçki nəticələrinin qəbul edilməsi;
14. Qanunun aliliyi [3].

Düzdür təməl prinsiplər qalmaq şərtilə, digər prinsiplər zaman ötdükcə forma və məzmunca dəyişikliyə və əlavələrə ehtiyac duya bilir.

Bu gün mövcud dövlətlərin və onları idarə edən şəxslərin də qarşısında duran ən başlıca məsələ öz vətəndaşlarının azadlığını, hüquqlarını və təhlükəsizliyini təmin etməkdən ibarət olmalıdır. Əks halda, həmin ölkə vətəndaşlarının seçdikləri hakimiyyəti digərləri ilə əvəz etməyə haqları vardır [4]. Yəni bu haqların olması hakimiyyətin qeyri-məhdud olmasının (daimi olmasının) qarşısını alır və onun xalq qarşısında məsuliyyətini artırır. Başqa sözlə, siyasətçilər (hakimiyyət) xalq qarşısında cavabdehdirlər, onların iradəsinə uyğun hərəkət etməyə, özlərinin və yaxınlarının varlanması üçün səlahiyyətlərindən sui-istifadə etməməyə borcludurlar.

Məhz burdan irəli gələrək, müasir demokratiyanın yuxarıda qeyd etdiyimiz prinsiplərinə əlavələr etmək zərurəti yaranır: avtoritar təzyiqlərə qarşı həmrəylik; media azadlığı və dezinformasiyaya müqavimət; korrupsiyaya qarşı müdafiə tədbirləri; vətəndaş həmrəyliyi; hamı üçün bərabər iqtisadi imkan (azad rəqabət mühiti) və s. [5].

Təbii ki, bu hal yalnız demokratiyanın mövcud olduğu, demokratik dəyər və prinsiplərin təşəkkül tapdığı ölkələrdə rast gəlinə bilər. Avtoritarizmin, totalitarizmin mövcud olduğu və ya demokratiyanın formalaşmadığı, ona qarşı ciddi təzyiqlərin olduğu siyasi sistemlərdə, rejimlərdə insan hüquq və azadlıqlarının qorunmasından və onların reallaşdırılması üçün hər hansı bir təşəbbüsdən danışmaq doğru olmaz. Belə cəhdlərin qarşısı ən sərt formada alınmaqla, digərlərinə qorxu olsun deyə, həmin fərdlərə qarşı rejimin ən ağır cəzası tətbiq olunur. Bu zaman azad kütləvi informasiya vasitələrinin olmaması da korrupsiya və hakimiyyətdən sui-istifadə hallarını ictimaiyyətin gözündən yayındırmağa şərait yaradır və nəticədə xalqın nəzarət imkanlarını məhdudlaşdırır.

Amma qeyd etmək lazımdır ki, əsrlər boyu mövcud olmuş imperiyalar, despotik tiraniyalar sonda dağılmağa məruz qalmış/qalmaqdadır. Tarix boyu belə imperiyalar çox olduğundan, onların necə yaranmasına və ümumiyyətlə, hansı inkişaf yolu keçərək sonda nə səbəbə görə dağılması daha geniş araşdırma tələb etdiyindən bu məsələlərə ətraflı toxunmuruq. Qısaca olaraq, onu demək olar ki, imperiyalar geniş əraziyə, çoxlu müstəmləkələrə malik olduqları üçün və burada müxtəlif xalqların numayəndələri yaşadıqlarına görə bu dövlətdə despotik hakimiyyətin olması zəruri idi. Bu tip rejimlərdə yaşayan əhali öz iradələrinə görə deyil, zor gücünə, işgəncələr hesabına idarə olunurdu/olunur. Təbii ki, əhali də mövcud hakimiyyətdən razı ola bilməzdi və həmişə də ona qarşı mübarizə aparmağa cəhd edirdi. İnsanların hüquq və azadlıqları olduqca kobud formada pozulur, fərdin sosial varlıq olaraq rolu heçə enirdi. Heç şübhəsiz ki, zor və işgəncə ilə hakimiyyətin uzun müddətə davam etdirilməsi, əhalinin nəzarətdə saxlanılması, hakimiyyətin idarə olunması olduqca çətinlik törədirdi. Bu səbəbdən də imperiyalar sonda dağılmağa məruz qalırdılar. Digər səbəb kimi daxildən əhalinin azadlıq mübarizəsi və digər imperiyalarla aparılmış müharibələr də bu hakimiyyətlərə son qoyurdu.

Bu onu göstərir ki, sabitlik olmayan şəraitdə demokratiya və vətəndaş cəmiyyəti barədə hər hansı söhbətin mənası yoxdur. Qeyri-sabitliyin olduğu, Aristotelin dediyi "dövlət vətəndaşların xoşbəxt yaşamaları üçün yaradılmışdır" həqiqətini vətəndaşların başa düşmədiyi ölkədə hüquq bərabərliyinə və şəffaflığa istiqamətlənmiş ictimai şüur formalaşdırmaq çətin məsələdir [6, s. 38].

XX əsrin ikinci yarısında və üçüncü minilliyin başlanğıcında demokratik ölkələrin sayının artması nəticəsində Qərbdə, xüsusilə də Avropa ölkələrində demokratiya fenomeninin elmi araşdırılmasına olan maraq yenidən artdı. Müasir demokratiya nəzəriyyələri meydana gəlməyə, demokratiya sahəsində çoxlu elmi-tədqiqat işləri yazılmağa başladı. Demokratiya fenomeni xüsusi olaraq diqqət mərkəzinə keçdi.

Bu baxımdan, Oksford Universitetinin professoru Larri Zidentopun A.Tokvilin "Amerikada demokratiya" adlı əsərinin adı ilə səsləşən "Avropada demokratiya" əsəri diqqəti daha çox cəlb edir. L.Zidentop öz əsərində müasir dövrdə demokratiyanın yüksək inkişaf etdiyi ölkələrin çoxluq təşkil etdiyi Avropa dövlətlərində demokratiyanın inkişafında baş verən mürəkkəb proseslərlə bağlı dərin mühakimələrinin əsasını Avropa milli dövlətlərinin vahid Avropa İttifaqına keçməsi prosesinin analizi təşkil edir [7].

Bütün yuxarıda qeyd olunanlar bu və ya digər dərəcədə siyasi sistemin fəaliyyətinin nəticələrini əks etdirir. Ancaq biz sistemin demokratikliyi haqqında danışarkən, nəticələr haqqında fikirləşmirik, proses haqqında, qərarların necə qəbul edilməsi haqqında fikirləşirik. Demokratiyanın hakimiyyətin cəmiyyətdə daha geniş cəmlənməsi imkanlarını nəzərdə tutduğunu nəzər alsaq, belə qənaətə gəlirik ki, siyasətin başlıca məqsədlərindən biri hər bir vətəndaşın "siyasi çəkisinin" artması, onun muxtariyyətinin, şəxsi azadlığının hədlərinin genişləndirilməsi olmalıdır. J.J.Russonun və C.Millin klassik demokratiya nəzəriyyəsindən başlayaraq insanın azadlığı, avtonomiyası həmişə həm siyasətin ən yüksək məqsədi, həm də bu məqsədə çatmanın ən mühüm vasitəsi kimi dərk edilmişdir [8; 9].

Demokratiyanın inkişaf tarixinə nəzər salaraq görürük ki, bu uzun bir inkişaf yolu tələb edən prosesdir. Bu həm idarəetmə strukturunda, qanunvericlik bazasında və ən əsası da cəmiyyətin siyasi şüurunda, təfəkküründə formalaşması və inkişaf etməsi vacib olan amilləri əhatə edir. Onu da nəzərə almaq lazımdır ki, zaman keçdikcə bu formalar da dəyişikliyə uğrayır, təkmilləşir və yeni çalarlar əldə edir. İlkin demokratiya ilə müasir dövrümüzdəki demokratiya idarəetmə formalarının müqayisəsi nəticəsində çox böyük fərqlərin olduğunu da müəyyən edirik. Əgər qədim Yunanıstanda və Romada mövcud olmuş demokratiyanın birbaşa forması üstünlük təşkil edirdisə, hazırki dövrdə nümayəndəli və ya plüralist demokratiyaya üstünlük verilir [10, s. 324-335]. Hazırki şərait və reallıqlar birbaşa demokratiyanın gerçəkləşməsinə mane olur və ən uyğun forma olaraq nümayəndəli demokratiya çıxış edir.

Bu gün belə hesab edilir ki, sistemin demokratikliyi az və ya çox dərəcədə nümayəndəli demokratiyanın mexanizmləri – ümumi seçki hüququ, gizli səsvermə, təminatlı seçkilərlə daha etibarlı təmin edilir. Beləliklə, biz bu gün demokratiyadan söhbət açarkən demokratiyanın birbaşa olmayan formasını deyil, məhdudlaşdırılmış formasını – daha çox liberal demokratiyanı nəzərdə tuturuq. Amma unutmaq olmaz ki, mövcud vəziyyətdə (vaxt, effektivlik və səmərəlilik) birbaşa demokratiyalardan fərqli olaraq, nümayəndəli demokratiyada insanların birbaşa deyil, nümayəndələri vasitəsilə olsa da belə qanunların qəbul olunmasında, hakimiyyətin idarə olunmasında iştirak etməsi, dolayısı ilə fikirlərini, arzularını ifadə etməkdə azad səsə sahib olması demokratiyanı güclü edən təməldir.

Onu da etiraf etmək lazımdır ki, müasir demokratiyanın problematikası özündə həm də özünəməxsus, daxili dilemmaları və ziddiyyətləri daşıyır. Bunlardan ən başlıcası da yuxarıda göstərdiyimiz əsas amildir: *"xalqın iştirakı vasitəsilə idarəetməni xalqın maraqları naminə idarəetmə arasındakı mümkün olan balansı necə müəyyən etmək olar"*. Çünki siyasi iştirak (bununla birlikdə birbaşa demokratiya) ideyasını daha çox yeganə bir səbəbdən tənqid edirlər ki, vətəndaşların əksəriyyətinin siyasətdə tam iştirak etməsi üçün nə vaxtları, nə bilikləri, nə də siyasi yetginlikləri yoxdur. Burdan çıxış edərək, Platon belə hesab edirdi ki, dövləti aristokratlar idarə edərək demosu (xalqı) öz hakimiyyətində saxlamalıdır [11]. Təbii ki, bu cür yanaşma dövlət idarəçiliyində xalqın iştirakını bütünlükdə inkar edir, onu müdrikliyə yad olan, həqiqətdənkənar baxışlara xas olan kütlə kimi qiymətləndirir. Bir çox hallarda kütləni hətta dağıdıcı qüvvə kimi xarakterizə edirlər.

Elita nəzəriyyəsinin tərəfdarı olaraq Nitsşe də xalq üzərində aristokratiyanın hakimiyyətini daha məqsədəmüvafiq hesab edirdi. Habelə xalqın hakimiyyətinin arzuolunmaz və mümkünsüz olduğunu düşünərək Hamilton bir qədər də irəli gedərək deyirdi ki, *"Çoxluğa imkan versəniz, onlar azlıqları məhv edərlər"* [12].

Göründüyü kimi, Elita nəzəriyyəsinin qeyd olunan və digər nümayəndələri birmənalı olaraq, hakimiyyətin idarə olunmasında xalqın (onların ifadə etdiyi kimi kütlənin) rolunu qeyri-rasional hesab edərək hər bir halda elitaya etibar olunmasına üstünlük verirdilər. Belə bir yanaşma sərgiləyən bu nəzəriyyəçilərin baxışında hakimiyyətin sadə xalq (dünyagörüş, təfəkkür baxımdan yetkin, rasional olmayan) tərəfindən idarə oluna bilməsi, bir qədər qeyri-real görünməsi normal hesab edilməlidir. Çünki idarəetmənin kifayət qədər mürəkkəb və çətin olmasını nəzərə aldıqda, onun intellektual, yüksək

təfəkkürlü, idarəetmə bacarığına malik şəxs və ya şəxslər tərəfindən həyata keçirilməsini mümkün hesab edirdilər. Heç şübhəsiz ki, bu cür yanaşmanı doğru hesab etmək olar.

Amma demokratiya üçün vacib prinsip xalqın maraqlarının nəzərə alınması, onların əksəriyyətinin fikir və düşüncəsinin, hüquq və azadlıqlarının mütləq qaydada qorunmasıdır. Sistem elə təşkil olunmalıdır ki, ədaləti, qanunçuluğu qorumaq mümkün olsun. Hətta Platon da demokratiyaya qarşı olmuş olsa da idarəetmədə yaranan problemin həlli üçün həm də ən ləyaqətli filosof-hökmdarların idarəetməsinin təmin olunmalı olduğunu da qeyd edirdi. Yəni xalqın maraqları naminə idarəetmənin tamamilə hansısa maarifçi despotizmə oxşar bir idarəetməyə çevrilə biləcəyini də doğru hesab etmirdi.

Deməli, əsas dilemma fərdlə cəmiyyət arasında balansın yaradılmasıdır: necə etmək olar ki, vətəndaşın siyasi mövqeyinin gücləndirilməsi xalq hakimiyyətinin zəifləməsinə və yaxud əksinə çevrilməsin. Bütün bunların altında bir çox problem gizlənir ki, praktikada bunların həlli olduqca çətindir. Bundan başqa, bir çox nəzəriyyəçilər belə hesab edirlər ki, məhz bu problem – fərdlə cəmiyyət arasındakı mümkün olan nisbət məsələsi doğrudan da siyasi nəzəriyyələrin mərkəzi problemidir.

Bütün bunlara baxmayaraq, müqayisəli formada götürmüş olsaq, o qənaətə gələ bilərik ki, demokratik idarəetmə sistemi insan hüquq və azadlıqlarının hüquqi çərçivədə qorunması, hüququn aliliyi, vətəndaşların sosial rifah halının yaxşılaşdırılması və s. müasir idarəetmə sistemində ən yaxşısı hesab edilir. Sosial ədalətin, qanun qarşısında bərabərliyin, fərdi azadlığın təminatı baxımından da ən effektli idarəetmə forması kimi üstünlük təşkil edir [13, s. 91-95]. Qeyd etmək lazımdır ki, demokratiyada bütün insanlara bərabər münasibətin olması, təkcə vacib deyil, həm də zəruridir.

2. Demokratiyanın inkişafında beynəlxalq əməkdaşlıq və qarşılıqlı siyasi mübadilə

Demokratik idarəetmə forması Qərbdə təşəkkül taparaq dünyanın müxtəlif regionlarına tərəf genişlənməkdə və inkişaf etməkdədir. Yarandığı ilkin formasından fərqli olaraq, bu idarəetmə forması zaman ötdükcə müxtəlif dəyər və prinsipləri özündə cəmləməklə böyük bir təkmilləşmə yolu keçmişdir. Müasir dövrümüzdə demokratik idarəetmə formasının ilkin mərhələsi ilə müqayisədə böyük fərqlər vardır. Həmçinin müxtəlif regionlarda yaşayan xalqların özünəməxsus düşüncə tərzinin, dünyagörüş səviyyəsinin, dövlətlərin fərqli milli-mənəvi dəyərlərinin, spesifik idarəetmə ənənələrinin olması demokratik idarəetmə üsulunun tətbiqi zamanı öz təsirini göstərir. Heç şübhəsiz ki, bir idarəetmə formasının bütün mövcud prinsiplərini eynilə başqa bir dövlətin idarə olunması üçün tətbiq olunması məqbul sayıla bilməz və ya bu prinsiplərlə idarəetmə effektiv ola bilməz.

Müxtəlif dövlətlərdə bərqərar olmuş demokratik idarəetmə forması üçün ümumi qəbul olunmuş klassik prinsiplərlə yanaşı, həmçinin təşəkkül tapdığı dövlətin, ərazinin, əhalinin keçdiyi tarixi inkişaf yolu, özünəməxsus idarəetmə ənənələri də müvafiq olaraq spesifik əhəmiyyət kəsb edir. Başqa sözlə desək, demokratiyanın ilkin formasından fərqli olaraq, müasir idarəetmədə tətbiq olunan forması hər bir dövlətdə mövcud tarixi ənənələri, xalqların milli təfəkkür tərzini, mövcud hakimiyyətlərin xarakterini, sosial-iqtisadi-siyasi vəziyyətini özündə ehtiva etməklə nəzərəçarpacaq müxtəlifliyi ilə seçilir. Məhz bu müxtəliflik, dünyanın bir çox dövlətlərini siyasi, iqtisadi, mədəni və s. sahədə bir-biri ilə əməkdaşlıq etməyə, qarşılıqlı münasibətlər yaratmağa və daha uyğun idarəetmə prinsiplərini mənimsəməyə sövq edir. Beynəlxalq təşkilatların (*beynəlxalq təşkilatlar* – suveren dövlətlərin əməkdaşlığı və razılığı, müəyyən məqsədlərin və vəzifələrin birgə, kollektiv şəkildə həlli üçün müqavilə əsasında yaratdıqları müxtəlif siyasi-inzibati, iqtisadi və s. xarakterli daimi orqanlardır) [14, s. 329] əsas fəaliyyət istiqamətlərindən biri kimi dünya dövlətləri arasında qarşılıqlı mübadilənin təşkil olunması üçün əlaqələrin yaradılmasıdır. Bu baxımdan, demokratik idarəetmə formasının tətbiq olunduğu gənc ölkələrin dünyaya inteqrasiya etməsi, beynəlxalq hüququn norma və prinsiplərindən faydalanması zəruridir.

Düzdür, dövlətlər bəzən buna ikitərəfli formada qarşılıqlı əlaqələr qurmaqla, yəni bir-birinin təcrübəsindən istifadə etməklə nail olmağa çalışırlar. Bu zaman proses daha uzunmüddətli dövrü əhatə edir.

Lakin bu istiqamətdə təkmilləşmiş və geniş imkanları olan təşkilata üzv olmaq eyni anda bir çox qabaqcıl təcrübəyə, böyük potensiala malik dövlətlərlə əməkdaşlıq fürsəti yaradır. Belə olan təqdirdə, siyasi-iqtisadi cəhətdən geri olan və ya demokratik-sivil idarəetmə sahəsində hələ yenicə addımlar atmış dövlətin şansları artmış olur. Məsələn, Avropa Şurasına üzvlük keçmiş postsovet dövlətləri üçün belə bir əlverişli imkanlar yaratmış oldu. İnkişaf edən, demokratiya yolunda çox irəli getmiş Qərb dövlətləri ilə

eyni təşkilatda olmaq, onların təkliflərdən, tövsiyələrindən yararlanmaq və daha səmərəli və effektiv idarəetmə modelini seçmək, bu istiqamətdə irəliləmək həqiqətən də böyük perspektivlər vəd edir.

Baxmayaraq ki, keçmiş SSRİ-dən ayrılmış dövlətlərin bir çoxu avrointeqrasiya xəttini prioritet seçmişlər və 25 ilə yaxın müddətdə Avropa Şurasının üzvüdürlər, amma hələ də bu ölkələrdə demokratik idarəetmə prinsiplərini və dəyərlərini tətbiq etmək mümkün olmur. Görünən odur ki, bu bir tərəfdən sovet düşüncəsinin (qeyri-demokratik) və bu düşüncəyə malik şəxslərin hələ də idarəetmə strukturunda çoxluq təşkil etmələri, digər tərəfdən cəmiyyətin rasional siyasi şüurunun, siyasi mədəniyyətinin istənilən səviyyədə inkişaf edə bilməməsi (maarifləndirmə işinin lazımi səviyyədə aparılmaması) ilə əlaqədar ola bilər. Başqa bir səbəb kimi, SSRİ-nin varisi kimi çıxış edən Rusiyanın postsovet respublikalarına təsir imkanlarının hələ də, kifayət qədər üstünlük təşkil etməsini, avrointeqrasiyaya və demokratik idarəetmənin inkişafına mane olmasını göstərmək olar. Çünki prosesin demokratiyaya doğru istiqamətlənməsi, dövlətlərin iqtisadi-siyasi azadlıqlarının, habelə gücünün artması, suverenliyinin daha da möhkəmlənməsi qeyd olunan dövlətlərin Rusiyanın nəzarətindən çıxmasına və onun təsir imkanlarının zəifləməsinə şərait yarada bilər.

3. Demokratiyaya keçid zamanı həlli zəruri olan problemlər: rasional siyasi şüurun inkişafı

Yuxarıda qeyd etdiymiz kimi, demokratik idarəetməyə keçid heç şübhəsiz ki, asanlıqla başa gəlmir. Bu bir proses olduğundan bunu qısa zamanda həyata keçirmək bir qədər mümkünsüzdür. Obyektiv və subyektiv faktorlar, daxili və xarici təsirlər burda mühüm rol oynayır. Məsələnin aydınlaşdırılması üçün geniş təhlilə, səbəblərin izahına ehtiyac var.

Belə ki, totalitar, avtoritar siyasi rejimlərin və ya imperiyanın nəzarətindən azad olmaq, suveren, müstəqil dövlət olmaq hələ demokratiyanın formalaşması, bərqərar olması anlamına gəlmir. Düzdür qeyd olunduğu kimi, bu dövlətlərə görə dəyişə bilər. Amma ümumilikdə bunu qısa zamanda, problemsiz və asanlıqla keçmək də imkansızdır.

İlk öncə demokratik idarəetmə sisteminə keçid və onun bərqərar olması üçün aşağıda qeyd edilmiş vacib problemləri həll etmək tələb olunur:

1. Beynəlxalq aləmdə tanınmaq və dünya dövlətləri tərəfindən dövlət müstəqilliyinin qəbul olunması;
2. Siyasi rejimlərin mahiyyətinin, xüsusiyyətlərinin dəyişmək istəklərinin olması;
3. Hakimiyyətdə təmsil olunan şəxslərin demokratik düşüncəyə malik olub-olmaması;
4. İnsanların rasional siyasi şüur, siyasi mədəniyyət səviyyəsinin yüksək olmaması;
5. İdarəetmə mexanizmlərinin həyata keçirilməsində yeni qanunvericilik bazasının hazırlanması zərurəti;
6. İnstitusional idarəetmə institutlarının formalaşdırılması vacibliyi;
7. İqtisadi inkişafın zəif olması, inflyasiya və sosial problemlərin mövcudluğu [15, s.168].
8. Ölkənin yerləşdiyi coğrafi mövqeyi, potensialı və qonşuların təsir imkanları;
9. Qonşu dövlətlərdə mövcud olan siyasi rejimlərin xarakteri və s.

Ümumilikdə, demokratik idarəetmənin bərqərar olması böyük bir prosesdir, amma yuxarıda sadaladığımız faktorlar bu prosesin ləngiməsinə, yeni idarəetmə sisteminin formalaşmasına ciddi çətinlik yaratmış olur. Totalitar rejimlərin siyasi və iqtisadi təsirindən azad olmuş, müstəqil olaraq demokratik idarəetmə sisteminə keçid prosesində olan dövlətlərin qarşısında şübhəsiz müəyyən çətinliklərin olması labüddür. Xüsusilə də müstəqilliyə gedən bir yolda müharibə faktoru, ölkə ərazisinin işğalı, qaçqın-köçkün problemi, iqtisadi problemlər, inflyasiya, siyasi qeyri-sabitlik, ölkədaxili münaqişə - bütün bunlar keçid prosesinin başa çatmasına öz mənfi təsirini göstərmiş olur.

Belə olan təqdirdə heç şübhəsiz ki, dövlətin qarşısında duran başlıca hədəf mövcud vəziyyəti ən qısa vaxtda və səmərəli formada müsbətə doğru dəyişmək, sabit, dayanıqlı və inkişafa yönəlik bir sistem formalaşdırmaqdır. Bunun üçün ən optimal çıxış yolu və uğurlu addım dünyanın inkişaf edən dövlətlərinə inteqrasiya etmək, münasibətlər qurmaq, əməkdaşlığı həyata keçirməkdir.

Nəzərə almaq lazımdır ki, iqtisadi və mədəni əlaqələr, xalqların və dövlətlərin beynəlxalq münasibətləri sahəsində daim mühüm rol oynamışdır. Müasir beynəlxalq hüquq dinc yanaşı yaşamaq prinsipləri əsasında bütün dövlətlərin, o cümlədən də müxtəlif ictimai quruluşlu dövlətlərin iqtisadi əməkdaşlığını, nəinki mümkün, hətta olduqca vacib hesab edir. Həmçinin hər bir xalqın inkişaf edərək sivil bir toplum halında formalaşması, özünün milli-mənəvi dəyərləri ilə bərabər, beynəlxalq aləmə

inteqrasiya edərək, qloballaşan dünya ilə əməkdaşlıq etmək, daha mütərəqqi hüquq normalarını, idarəetmə prinsiplərini mənimsəməyi və onlardan faydalanmağı da əhəmiyyətli hesab edir.

Xüsusilə geostrateji və geopolitik baxımdan həssas bir bölgədə yerləşən dövlətlər üçün beynəlxalq təşkilatlara inteqrasiya olunmaq, dünya müstəvisində tanınmaq, özünə partnyor tapmaq müstəqilliyinin möhkəmləndirilməsi baxımından mühüm əhəmiyyət kəsb edir [16, s. 261-275]. Ölkənin yerləşdiyi çoğrafi şərait ona mühüm üstünlüklər verməklə yanaşı, eyni zamanda onu bir sıra təhlükəsizlik problemləri ilə də üzləşdirir [17, s. 331]. Demokratik və hüquqi dövlət qurmağı məqsəd seçmiş bir dövlət üçün dünyanın inkişaf etmiş demokratik dövlətləri ilə əməkdaşlıq etmədən, beynəlxalq təşkilatların köməyindən faydalanmadan mövcud imkanlarla idarəetmə strukturunu qurub yaratmaq, siyasi və iqtisadi tərəqqiyə nail olmaq bir sıra çətinliklər yaradır. Belə dövləti qurub yaratmaq, inkişaf etdirmək zamanla bərabər həm də mövcud təcrübədən faydalanmağı tələb edir. Bu nöqteyi-nəzərdən inkişaf etmiş dövlətlərin mütərəqqi təcrübəsindən faydalanmaqla yeni idarəetmə sistemini yaratmaq və onu inkişaf etdirmək prosesi sürətləndirir, mövcud strukturdan, prinsiplərdən daha yaxşısını formalaşdırmağa fürsət qazandırır.

Totalitar rejimdən demokratik idarəetmə sisteminə keçid, təkcə strukturun qurulması, qanunvericilik bazasının yaradılması ilə kifayət etmir, mühüm olan məsələ demokratik prinsiplərin, ideyaların, normaların insanların şüurunda, təfəkküründə formalaşması və bərqərar olmasıdır [18, s. 309-311]. Əgər bu proses baş vermirsə, idarəetmə sisteminin tam olaraq formalaşması da mümkünsüz görünür. Bu mənada totalitarizmdən ayrılmış dövlətlərdə struktur, qanunvericilik bazasının müəyyən vaxt çərçivəsində qurulması yekunlaşsa da, amma əhalinin təfəkküründə bu ideyaların tam olaraq bərqərar olmasını söyləmək doğru olmazdı (cəmiyyətin siyasi şüurunda, təfəkküründə keçid prosesinin bütünlüklə başa çatması hələ bir qədər vaxt tələb edir).

Yəni demokratiyanın istənilən səviyyədə formalaşması və inkişafı üçün bütün vətəndaşların siyasi proseslərdə rasional iştirakı, seçkilərdə aktivlik göstərmələri olduqca vacibdir. Hər bir vətəndaş bu fəallığı ilə demokratik sistemin bərqərar olmasında iştirak edir. Nəticə etibarilə, özünün azad, ədalətli və sosial bərabərliyin təmin olunduğu cəmiyyətdə yaşamasını təmin etmiş olur. Bu zaman demokratiya daha yaxşı işləyir.

Beləliklə, uğurlu demokratiya üçün yerinə yetirilməli olan iki vacib şərt var – vətəndaşlar kifayət qədər intellektli, rasional olmalıdır ki, onlar yaxşı kollektiv qərarlar qəbul edə bilsinlər və kifayət qədər etik motivasiyaya malik olmalıdırlar ki, vaxt sərf etməyə hazır olsunlar [19, s.1-2].

Rasional davranışın əsasında isə rasional təfəkkür dayanır. Rasional siyasi davranışa gəlincə isə o, rasional fərdin və ictimai davranışın bir elementidir. Fərd və ya institusional vahid ən faydalı siyasi davranışa sahib olmaq üçün öncə ümumilikdə özünün fərdi və ictimai davranışını rasionallaşdırmalıdır. Bunun üçün isə o, rasional təfəkkürə malik olmalıdır.

Rasional təfəkkürə gəlincə o, davranışa təkan verən niyyət, məram, məqsəd kimi ön amilin ən doğrusunun seçilməsi qabiliyyətidir. Daha geniş formada izah etsək, təfəkkür fikrən araşdırılan məlumatlar əsasında hər hansı bir nəticə çıxartmaq, qiymət vermək, müqayisə etmək, başa düşmək qabiliyyətidir. Təfəkkür idraki proses olaraq məlumatlar əsasında işləyir, fikir, anlayış, düşüncədən istifadə edir, anlayışları, ifadələri müəyyən edir.

Bu mənada rasional təfəkkür fərdin xarakteri ilə əksər halda bağlı məsələdir. Lakin tam da ondan asılı deyildir. Çünki rasional təfəkkür fərdin xarakterindən daha geniş anlayışdır. Buna görə də rasional təfəkkür hətta fərdin xarakterini dəyişmək imkanına malikdir.

İzahlardan və təhlillərdən belə nəticə hasil olur ki, həqiqətən də insanın hər şeyin ölçüsü ola biləcəyinə olan bu inam demokratiyanın təməl prinsipini təşkil edir. Yəni hər bir xalq insanın bu tələbləri yerinə yetirmək qabiliyyətinə güvənməlidirlər. Deməli, təfəkkürü düzgün inkişaf edən hər bir fərd heç şübhəsiz ki, rasional qərar vermək imkanına da malik ola bilər/malikdir. Xüsusilə də o, dərk etməlidir ki, məhz onun tərəfindən bu qərarın verilməsi özünün daha yaxşı gələcəyi üçün vacibdir.

Digər tərəfdən, dərketmənin baş verməsi üçün həm də hakimiyyət iradəli və yeniliyə açıq olmalı, cəmiyyətin inkişafına yönəlik daxili siyasəti düzgün qurmalı, hüquqi bazanı, hüququn aliliyini, müstəqil məhkəməni, azad və sərbəst mühiti, maarifləndirmə işlərini məqsədyönlü və ardıcıl həyata keçirməlidir. İkinci önəmli amillərdən biri də xarici siyasətin düzgün qurulması, beynəlxalq cəmiyyətə inteqrasiya prosesinin sürətləndirilməsi, müasir təcrübənin öyrənilməsi və tətbiqidir.

Nəzərə almaq lazımdır ki, əksər ölkələrdə insanların iştirakı üçün sosial, iqtisadi və mədəni amillərin rolu böyükdür. Yoxsulluğun çoxluq təşkil etməsi, təhsilin aşağı səviyyəsi, iqtisadi, sosial və mədəni sahədə ciddi nöqsanlar, insan hüquqlarına cüzi hörmət və onların həyata keçirilməsinə maneələr və s. ciddi təsiredici faktorlardır. Bu baxımdan, göstərilən amillər cəmiyyətin rasional siyasi iştirakçılığına mənfi təsir göstərir və nəticədə demokratiyanın genişlənməsinə, güclənməsinə imkan vermir.

Təsadüfi deyil ki, demokratiyanın inkişaf göstəricilərindən biri də iqtisadiyyatın, cəmiyyətin sosial durumunun yüksək səviyyədə olmasıdır. Sosial durumu yaxşı vəziyyətdə olmayanla müqayisədə iqtisadi azadlığını, tələbatlarını təmin etmiş fərd fikirlərini, düşüncələrini daha sərbəst, daha rasional ifadə etmək bacarığına malik olur.

Burdan belə qənaətə gəlmək olur ki, həqiqətən də sosial-iqtisadi inkişaf öz-özlüyündə iştirakçılığı artırır və ya ən azı iştiraka şərait yarada bilir. Aşağı sosial durumda olan insanların iştirakı vaxt çatışmazlığı ilə məhdudlaşır, çünki onlar gündəlik yaşamaq üçün çalışmalıdırlar. Onların səmərəli kollektiv fəaliyyətinin təşkili üçün maddi resursları və texniki bacarıqları kifayət qədər olmadığından siyasi proseslərdə, hakimiyyətin təşkilində və ona nəzarətin həyata keçirilməsində də effektiv ola bilmirlər. Bu zaman irq, din, dil, qeyri-adekvat ünsiyyət və dağınıq məskunlaşma da öz rolunu oynayır.

Eyni zamanda bir çox fərdlər (sosial durumu aşağı olanlar) siyasi hüquqlarını həyata keçirməklə qərar qəbulunun rəsmi kanallarında iştirakın iqtisadi və sosial hüquqlarını əldə etməyin çətin və səmərəsiz bir yol olduğunu da düşünürlər [20, s. 161].

Nəticə

Belə bir nəticəyə gəlmək olar ki, demokratik dövlət quruculuğu uzun surən bir prosesdir. Belə ki, Avropa dövlətləri 300 ildən çoxdur ki, bu yolda addımlamalarına baxmayaraq, hələ də mükəmməl (mütləq formada) vahid idarəetmə dəyərləri, prinsipləri yarada bilməyiblər (bəşər cəmiyyəti inkişaf etdikcə, insanların dünyagörüşləri dəyişdikcə idarəetmə mexanizmlərinin, prinsiplərinin yenilənməsinə hər zaman ehtiyac yaranır). Son dövrlərdə Qərbdə cərəyan edən siyasi proseslər bir daha demokratiyanın hələ də təkmilləşməyə ehtiyac olduğunu göstərir. Bəzən geosiyasi, geoiqtisadi maraqlar, yeni dünya düzəni istiqamətində dövlətlərin daha çox istiqamətlənmələri demokratik dəyərlərin bir qədər arxa plana düşməsi təəssüratını yaratmışdır. Amma əslində isə yeni dünya düzənində həm də demokratik cəmiyyətin totalitarizmə, avtoritarizmə qarşı durması, onu sıxışdırmağa çalışması da müşahidə olunur.

Belə olan təqdirdə, beynəlxalq təsirlərin artması nəticəsində qeyri-demokratik idarəetmənin hakim olduğu dövlətlərdə vəziyyətin dəyişməsi, daha sağlam, sivil siyasi sistemin formalaşması, cəmiyyətin rasional siyasi şüurunun inkişaf etməsi baş vermiş ola bilər. İnteqrasiya prosesinin sürətlənməsi mövcud olan dəyərlərin mənimsənilməsində, tətbiq və inkişaf etməsində daha səmərəli ola bilər. Qarşılıqlı mübadilə nəticəsində mütərəqqi dəyərlərdən bəhrələnmək dövlətin daha qısa zamanda idarəetmədə, insan hüquq və azadlıqlarının formalaşmasında böyük üstünlük qazandırmış olar.

Hadisə və proseslər göstərir ki, inteqrasiyanın sürətli getməsi tez bir zamanda istər iqtisadi, istərsə siyasi və istərsə də digər sahələrdə böyük nailiyyətlərin əldə olunmasına effektiv təsir göstərir.

Bütün uğurlu demokratiyalar oxşar şərtlərin yerinə yetirilməsini tələb edir. Bütün vətəndaşlar eyni ictimai əmtəə və xidmətlər toplusunu istehlak etdikləri üçün sivil dövlətlərin/hakimiyyətlərin məqsədləri ilə razılaşırlar. Fərdi üstünlüklər diametral şəkildə ziddiyyət təşkil edərsə, hamının xeyrinə olan kollektiv qərarlar qeyri-mümkün ola bilir. Bütün uğurlu demokratiyalar tələb edir ki, vətəndaşlar seçici kimi prosesdə iştirak etməklə öz vəzifələrini ciddi qəbul etsinlər, həm də cəmiyyətin düzgün qərarlar qəbul etməsinə töhfə vermək üçün kifayət qədər məlumatlı olsunlar.

Ədəbiyyat

1. Ronald, O. W. Lessons in democracy. tərc. ed.: redaktorlar: Nurullayev, R. Gülalıyev, O. / Bakı: Demokratik İslahatlar Uğrunda Cəmiyyət, – 2015. – 53 s.

2. Robert, A. Dahl. On democracy. tərtibat, redaktə və şərhlər: Hikmət Hacızadə / New Haven & London: Yale University Press, – 2004. – 127 s.

3. Jonathan, Day. 14 Principles of Democracy [Electronic resource], 12 april, 2022. URL: https://www.liberties.eu/en/stories/principles-of-democracy/44151

4. Melvin, İ.Urofski. ABŞ demokratiyası haqqında əsas mətnlər. tər. ed. red. Hacızadə, H. / Bakı: Far Center, – 2005. – 487 s.

5. Mccain İnstitute. A civil society declaration of democratic principles on the occasion of the 2023 summit for democracy: [Electronic resource], 24 March, 2023. URL: https://www.mccaininstitute.org/resources/in-the-news/a-civil-society-declaration-of-democratic-principles-on-the-occasion-of-the-2023-summit-for-democracy/

6. Mehdiyev, R. Gələcəyin strategiyasını müəyyənləşdirərkən: modernləşmə xətti / R.Mehdiyev. – Bakı: "Şərq-Qərb", – 2008. – 216 s.

7. Зидентон, Л. Демократия в Европе / Л.Зидентон. – Москва, – 2001. – 360 с.

8. John, Stuart Mill. Considerations on representative goverment / J.S.Mill. – New York: Liberal Arts Press, – 1958. – 230 p.

9. Ross, S.R. American National Coverment: institutions, policy and participation. Fourth edition / S.R.Ross. – Chico: California State University, – 1996. – 394 p.

10. Hüseynov, R. Siyasi iştirak və müasir demokratiya nəzəriyyələri // – Bakı: "Dirçəliş-XXI əsr", – 2008. – № 126-127, – s. 324-335.

11. Platon. Dövlət. tərc. edən: Araz Gündüz / Bakı: Qanun, – 2024. – 448 s.

12. Manafova, M. Mədəniyyət tarixi və nəzəriyyəsi. Ali məktəblər üçün dərslik / M.Manafova, N.Əfəndiyeva, S.Şahhüseynova, – Bakı: Sabah nəşriyyatı, – 2010. – 876 s.

13. Huseynov, R. Polıtıcal mechanısms of democracy: establıshment of Polıtıcal Instıtutıons // – Praha: "Sciences of Europe" journal, – 2023, № 114 (1), – pp. 91-95, https://doi.org/10.5281/zenodo.7811562

14. Əsgərov, Ə. Beynəlxalq hüquq. Dərslik / Ə.Əsgərov. – Bakı: Maarif, – 1979. – 443 s.

15. Hüseynov, R. Demokratik dəyərlərin inkişaf yolu // – Bakı: "Dirçəliş – XXI əsr", – 2007. – № 108-109, – s. 228-239.

16. Həsənov, Ə. Geosiyasət. Dərslik / Ə.Həsənov. – Bakı: Aypara-3, – 2010. – 604 s.

17. Həsənov, Ə. Azərbaycan Respublikasının milli inkişaf və təhlükəsizlik siyasəti / Ə.Həsənov. – Bakı: Letterpress, – 2011. – 440 s.

18. Hüseynov, R. Azərbaycanda iştirak demokratiyasına keçidin xüsusiyyətləri // – Bakı: "Dirçəliş – XXI əsr", – 2009. № 133-134, – s. 299-313.

19. Mueller, Dennis C. Democracy, rationality and morality / Dennis C. Mueller. – Jena: Papers on Economics and Evolution, No. 0615, Max Planck Institute of Economics, – 2006. – 57 p.

20. Robinson, M., White, G. ed. The Democratic developmental state. political and institutional design / M.Robinson, G. White. – Oxford Univ. Press. – 1999. – 368 p.

Elmi Əsərlər
Proceedings of Science

Heydər Əliyev adına Hərbi İnstitutun **Elmi Əsərlər** jurnalı, Cild 22, № 2, 2024 / 24-31
Proceedings of Science of the Military Institute named after Heydar Aliyev, Volume 22, № 2, 2024 / 24-31

Daxilolma tarixi / Received date: 27.06.2024
Qəbulolma tarixi / Accepted date: 19.09.2024

DOI: 10.30546/8967.2024.22.2.1011

MÜASİR DÖVRDƏ HƏRBİ-ELMİ TƏDQİQAT METODLARINDAN İSTİFADƏ: YENİ TENDENSİYALAR KONTEKSTİNDƏ

Bahadur Qəmbərov
polkovnik-leytenant

Sevda Hüseynova
fəlsəfə üzrə fəlsəfə doktoru, dosent
Heydər Əliyev adına Hərbi İnstitut, Bakı
E-mail: huseynova.sevda@outlook.com
ORCID ID: 0000-0002-1627-4386

Xülasə

Məqalə müasir dövrdə hərbi-elmi tədqiqat metodlarından istifadə məsələsinə həsr olunmuşdur. Məlumdur ki, müvəffəqiyyətli hərbi fəaliyyət prosesində obyektiv elmi araşdırma çox mühüm rol oynayır. Bunun əsasında isə doğru seçilmiş hərbi-elmi tədqiqat metodları dayanır. Eyni zamanda dünyanın hadisə və proseslərinin dəyişkən, dinamik xarakteri, o cümlədən onların təsiri ilə müharibələrin xarakterində baş verən dəyişikliklər hərbi-elmi tədqiqat metodlarının da bu çağırışlarına uyğun olaraq daim yenilənməsini tələb edir. Belə şəraitdə hərbi-elmi biliklərin əldə edilməsi üçün istifadə olunan hərbi-elmi tədqiqat metodlarının özünün araşdırma obyekti olaraq öyrənilməsi xüsusi əhəmiyyət kəsb edir. Əsasən də 44 günlük Vətən Müharibəsindən sonra yaranmış yeni geosiyasi reallıqla əlaqədar ordu quruculuğu işinə daha böyük diqqət yetirilən Azərbaycanda bu məsələ xüsusilə vacib faktora çevrilmişdir. Hazırki araşdırmanın da məqsədi, məhz hərbi-elmi tədqiqat metodlardan istifadənin müasir dövrdə yeni tendensiyalar kontekstində öyrənilməsidir. Bunun üçün məqalədə müasir dövrdə öyrənilən tədqiqat metodlarına təsir göstərən qloballaşma, sosial, siyasi, iqtisadi dəyişikliklər kimi faktorlar, bu faktorların təsiri ilə ənənəvi metodlardakı yenilənmə və yeni metodların meydana gəlməsi zərurəti araşdırılır, bu sahədə qarşıda dayanan vəzifələr vurğulanır. Məqalədə, həmçinin Azərbaycanda hərbi-elmi tədqiqatın müasir dövr üçün xarakterik xüsusiyyətləri və xarici təcrübədən istifadənin zəruriliyi məsələsinə diqqət yetirilir. Problemlə bağlı elmi ədəbiyyatın və faktoloji materialın məntiqi analiz vasitəsi ilə araşdırılması, təhlili, ümumiləşdirilməsi ilə belə bir yekun fikrə gəlinir ki, Azərbaycanda bu sahədə qarşıda dayanan əsas vəzifə müasir dövrün təsiri və inkişaf tendensiyaları nəzərə alınmaqla, hərbi-elmi tədqiqat sahələrinə, hərbi biliyin əldə edilməsi metodlarına yenidən baxılması, hərbi sahədə olan yeni texnologiyaların inkişaf dinamikasına paralel getdikcə artan insan faktorunun rolunun araşdırılması və zamanı qabaqlayacaq hərbi elm üzrə mütəxəssislərin hazırlığı mühüm əhəmiyyət daşıyır.

Açar sözlər: hərbi elm, hərb sənəti, hərbi-elmi idrak, hərbi-elmi tədqiqat metodları, hərbi təhlükəsizlik.

USE OF MILITARY-SCIENTIFIC RESEARCH METHODS IN THE MODERN PERIOD: IN TERMS OF NEW TRENDS

Bahadur Gambarov
lieutenant colonel

Sevda Huseynova
PhD in philosophy, associate professor
Military Institute named after Heydar Aliyev, Baku

Abstract

The article is devoted to the issue of using military-scientific research methods in modern times. It is known that objective scientific research plays a very important role in the process of successful military activity. This is based on correctly selected military-scientific research methods. At the same time, the changing, dynamic nature of world events and processes, including changes in the nature of wars due to their influence, require constant

updating of military-scientific research methods in accordance with these challenges. In such conditions, the study of the military-scientific research methods used for obtaining military-scientific knowledge as an object of investigation is of particular importance. This issue has become an especially important factor in Azerbaijan, where more attention is paid to the work of building the army, mainly due to the new geopolitical reality that arose after the 44-day Patriotic War. The purpose of the current study is to study the use of military-scientific research methods in the context of new trends in modern times. For this, the article examines factors such as globalization, social, political, and economic changes affecting the research methods studied in the modern era, the necessity of updating traditional methods and the emergence of new methods under the influence of these factors, and the tasks ahead in this field are emphasized. The article also focuses on the characteristic features of military-scientific research in Azerbaijan for the modern era and the necessity of using foreign experience. Researching, analyzing and summarizing the scientific literature and factual material related to the problem with the help of logical analysis leads to the conclusion that the main task ahead in this field in Azerbaijan, taking into account the influence and development trends of the modern era, is to focus on military-scientific research areas and methods of obtaining military knowledge. revising, examining the role of the human factor, which is increasing in parallel with the dynamics of the development of new technologies in the military field, and the training of specialists in military science who will be ahead of the times are of great importance.

Keywords: military science, military art, military-science cognition, methods of military-scientific research, military security.

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ВОЕННО-НАУЧНЫХ ИССЛЕДОВАНИЙ В СОВРЕМЕННЫЙ ПЕРИОД: В КОНТЕКСТЕ НОВЫХ ТЕНДЕНЦИЙ

Бахадур Гамбаров
подполковник

Севда Гусейнова
доктор философии по философии, доцент
Военный Институт имени Гейдара Алиева, Баку

Аннотация

Статья посвящена вопросу использования военно-научных методов исследования в современное время. Известно, что объективные научные исследования играют очень важную роль в процессе успешной военной деятельности. В основе этого лежат правильно выбранные военно-научные методы исследования. В то же время меняющийся, динамичный характер мировых событий и процессов, в том числе изменение характера войн под их воздействием, требуют постоянного обновления методов военно-научных исследований в соответствии с этими вызовами. В таких условиях особое значение приобретает изучение военно-научных методов исследования, используемых для получения военно-научных знаний как объекта исследования. Этот вопрос стал особенно важным фактором в Азербайджане, где работе по строительству армии уделяется больше внимания, главным образом, в связи с новой геополитической реальностью, возникшей после 44-дневной Отечественной войны. Целью настоящего исследования является изучение использования военно-научных методов исследования в контексте новых тенденций современности. Для этого в статье рассматриваются такие факторы, как глобализация, социальные, политические и экономические изменения, влияющие на методы исследования, изучаемые в современную эпоху, необходимость обновления традиционных методов и появление новых методов под влиянием этих факторов, а также задачи приоритеты в этой области подчеркнуты. В статье также акцентируется внимание на характерных особенностях военно-научных исследований в Азербайджане для современной эпохи и необходимости использования зарубежного опыта. Исследование, анализ и обобщение научной литературы и фактического материала, связанного с проблемой, с помощью логического анализа приводит к выводу, что основной задачей, стоящей перед Азербайджаном в этой области, с учетом влияния и тенденций развития современной эпохи, является сосредоточить внимание на пересмотре военно-научных направлений исследований и методов получения военных знаний, рассмотрении роли человеческого фактора, возрастающей параллельно с динамикой развития новых технологий в военной сфере, и подготовке специалистов в этой области. большое значение имеет военная наука, которая будет опережать время.

Ключевые слова: военная наука, военное искусство, военно-научное познание, методы военно-научного исследования, военная безопасность.

Giriş

Ölkəmizin təhlükəsizliyinin qorunması problemi uzun illər hərbi təcavüzə məruz qalmış və hazırda da bu təhlükənin keçmədiyi bir dövrdə gündəmimizi zəbt edən prioritet məsələlərdəndir. Buna görə də bu təhlükəsizliyi təmin edən ən mühüm vasitələrdən biri olan hərbi işin öyrənilməsi məsələsinin aktuallığı şübhə doğurmur. Bu məsələyə dair bizə məlum olan ən qədim mənbədən – Çin sərkərdəsi Sun Tuzunun "Savaş sənəti" əsərindən başlayaraq, Karl fon Klauzevitsin məşhur "Müharibə haqqında" traktına qədər və ondan sonrakı dövrdə problemə toxunan müəlliflər hərbi işin özünün bir sənət olduğunu sübut etmiş, bu sənətin öyrənilməsinin, yəni müasir terminlə prosesi daha dəqiq ifadə etsək, tədqiqinin əhəmiyyətini vurğulamışlar. Hazırki dövrdə dünyada bu problem üzərində bir çox elmi müəssisə çalışır və qeyd etmək yerinə düşərdi ki, Azərbaycanın apardığı Vətən Müharibəsinin, Şuşanı işğaldan azad edən qəhrəmanlarımızın igidliyi də dünyanın aparıcı tədqiqat müəssisələrinin və o cümlədən azərbaycanlı müəlliflərin tədqiqat obyektinə çevrilmişdir.

Bütövlükdə hərbi fəaliyyətin, hərb sənətinin və onun ayrı-ayrı aspektlərinin öyrənilməsi məsələsi bir sıra tədqiqatçılar tərəfindən həyata keçirilsə də zaman dəyişiklikləri və tarixi inkişaf faktoru hər dəfə yeni bir elmi problemlər ortaya çıxarır. Bu baxımdan, müasir dövrdə dünyada baş verən dəyişikliklər, o cümlədən, sosial-iqtisadi və bütövlükdə ictimai proseslərdəki dəyişikliklər, elm və texnikanın inkişafı, siyasi həyatın yenilənməsi ilə bağlı olan dəyişikliklər hərbi işin öyrənilməsi və xüsusilə də öyrədilməsi sahəsinə yenidən, dövrün tələbləri aspektində baxılmasını vacib edir. Göründüyü kimi, hərbi-elmi tədqiqat sahəsində hələ toxunulmamış problemlər və görüləcək işlər çoxdur. Lakin ən vacibi isə hərbi fəaliyyətdə elmin nüfuzuna söykənilməsi məsələsidir. Çünki bəzi tədqiqatçıların sözləri ilə desək, elmin inkar edilməsi hərb sənətində xaosa gətirib çıxarır. Hərb sənətinin dərki nə qədər dərin olarsa, bu sahədə fəaliyyət bir o dərəcədə təsirli olar. Bu sahədə fəaliyyət qeyri-elmi ilkin şərtlərə, sistemsiz yanaşmaya deyil, mötəbər elmi metodun nüfuzuna əsaslanmalıdır [1].

Hərbi işin dərindən öyrənilməsi baxımından yanaşılarsa, dövrümüzün spesifikliyinin insan fəaliyyətinin bütün sahələrinə olduğu kimi, hərbi-elmi tədqiqata və o cümlədən onun metodlarına da ciddi şəkildə təsir göstərməsinin şahidi olarıq. Azərbaycanda da hərbi-elmi tədqiqat işi müasir dünyada gedən proseslərdən kənarda götürülə və öyrənilə bilməz. Bu tədqiqat işlərinin lokal deyil, ümumdünya kontekstində həyata keçirilməsi zəruridir.

1. Müasir dövrdə hərbi-elmi tədqiqat sahəsinə və metodlarına təsir göstərən faktorlar

Qeyd edilən faktorlardan ən mühümlərini aşağıdakı şəkildə xarakterizə edə bilərik:

Dövrün fəlsəfəsindəki dəyişikliklər. Əgər əvvəllər hər hansı konkret fəlsəfi sistemi ümumi bir metod kimi götürərək hadisələrə dialektik və ya metafizik aspektdən yanaşılırdısa, hazırki dövrdə hərbi işin tədqiqi zamanı bir tərəfdən sinergetik, yəni sistem yanaşma, digər tərəfdən insanyönümlü yanaşmanın üstünlük təşkil etməsinin şahidi oluruq. Əgər sistemli yanaşma hərbə qarşılıqlı əlaqədə olan elementlərdən ibarət bütöv bir sistem və ya qarşılıqlı təsirdə olan, xarici mühitlə təsir-əks-təsir əlaqələrində olan elementlərin məcmusu kimi yanaşmanı müəyyən edirsə, insanyönümlü yanaşma hərbi tədqiqatçının, nəinki hadisələri kənar müşahidəçi kimi izləməsini, yalnız lokal baxımdan yanaşılmasını, həm də hərbi fəaliyyəti müəyyən istiqamətə - qloballaşma, insani birlik, insanın mənafeyi, onun mühafizəsi istiqamətinə dəyişilməsini müəyyən edir. Bəşəriyyət hərbi zorakılığın qarşısını almaq üçün vasitələr axtarır.

1.1. Dünyanın sosial-siyasi mənzərəsindəki dəyişikliklər

Bu, bilavasitə dövlətlərin demokratikləşməsi, qloballaşma ilə bağlı olaraq cəmiyyətlərin müharibəyə, hərbi proseslərə təsir gücünün artması ilə, eyni zamanda bu təsir gücü beynəlxalq təşkilatların fəaliyyətinə cəmiyyətin bilavasitə təsiri ilə də bağlıdır. Demokratik cəmiyyətlər müharibə və təhlükəsizlik, hərbi fəaliyyətlərlə bağlı dövlətin idarəetmə proseslərinə təsir göstərə bilirlər. Qloballaşma şəraitində milli təhlükəsizlik, dövlət təhlükəsizliyi bütövlükdə dünyada və ya onun ayrı-ayrı regionlarında təhlükəsizlikdən asılı olur və bu da tədqiqatın əhatə dairəsini daha da genişləndirməyi tələb edir. Yəni öyrənilən proseslərə qlobal yanaşma zərurəti meydana gəlir.

1.2. Bəşəriyyətin maddi-rifah halında, iqtisadiyyatda dəyişikliklər

Bütövlükdə bir çox dövlətlərin maddi-rifah halı yüksəlmişdir ki, bu da həm hərbi fəaliyyət və həm də onun öyrənilməsi üçün böyük miqdarda vəsaitin ayrılmasını mümkün edir. Başqa tərəfdən, bu maddi rifahın daha da yüksəldilməsi istəyi dövlətlər arasında rəqabəti, qarşıdurmanı, o cümlədən, hərbi qarşıdurmanı artıran faktora çevrilir. Müharibəyə ayrılan maliyyə vəsaitləri artır. Yeni texnologiyalara nəzarət və onların tədqiqinin maliyyələşdirilməsi xərclərinin ödənilməsi imkanları yaranır. Digər tərəfdən tədqiqatçıların qeyd etdiyi kimi simulyasiyativ müharibə modelləri və hərbi oyunlardan istifadə hərbçi hazırlığına ayrılan xərcləri azaldır [2]. Buna görə də belə modellərin, virtual hazırlığın elmi tədqiqinin yeni metodlarının axtarışı stimullaşdırılır.

Silah istehsal edən korporasiyaların hərbi proseslərə təsiri ciddi şəkildə artmışdır. 2024 -cü ilin fevral ayında ABŞ Konqresində yeni hərbi texnologiyalar ilə bağlı keçirilmiş dinləmələrdə yeni texnologiyaların son dövrdə inkişafı və yayılması, ilk növbədə kommersiya sektorundakı nailiyyətlərlə izah olunur [3]. Bu baxımdan, hərbi iqtisadi metodların tətbiqi hərbi fəaliyyətin elmi araşdırılmasında böyük rol oynayır.

1.3. Elmi-texniki inkişaf prosesindəki sürətlənmə

Müasir dövr kəsiyini götürsək, bu sürətlənmə həm silahların təkmilləşməsi, həm də hərbi idarəetmə sistemindəki dəyişikliklərin xarakterində özünü daha çox göstərir. Ən mühüm faktor isə bütövlükdə müharibənin xarakterinin dəyişməsidir. 2024-cü ilin fevral ayında ABŞ Konqresindəki yuxarıda qeyd edilən müzakirələrdə yeni texnologiyaların özünə "böyük miqdarda informasiyanın" təhlilini, süni intellekti, avtonom idarəetməni, robot texnikaları, istiqamətlənmiş enerji, hidrosəs və biotexnologiyaları daxil etdiyi vurğulanır. Qeyd edilir ki, yalnız bunlar vasitəsilə gələcəkdə döyüşmək və gələcəyin müharibələrində qələbə qazanmaq mümkündür [3].

Qeyd edilən elmi-texniki inkişaf həm də hərbi-elmi tədqiqat metodlarının arealını genişləndirir və göstərilən sahələrlə bağlı yeni tədqiqat metodlarının meydana gəlməsini müəyyən edir.

Elmi-texniki tərəqqinin nəticəsi olaraq, hazırki dövrdə hərbi münaqişələr zamanı həm döyüşçülərin, həm də dinc əhalinin qorunması üçün şəraitin yaradılmasına yeni imkanlar açılır. Yüksək dəqiqlikli silahların meydana gəlməsi ilə mülki şəxslər arasında itkilərin azaldılması imkanlarının yaranması ilə bərabər, avtomatik idarəetmə sistemlərinin meydana gəlməsi, bu silahların fəaliyyətinin nəticələri üçün məsuliyyəti kimin daşıması və s. kimi bir sıra ümumbəşəri mənəvi problemləri də ortaya qoyur ki, bu da mütləq şəkildə hərbi elmin tədqiqat obyektinə çevrilir və özü ilə subyektiv və mənəvi faktoru daxil edən yeni tədqiqat metodları gətirir.

1.4. Azərbaycanda hərbi elmin inkişafı, tədqiqi metodlarına təsir göstərən spesifik faktorlar

Bütövlükdə hərbi-elmi tədqiqata, o cümlədən onun metodlarına təsir göstərən bu ümumi faktorlarla bərabər müasir dövrdə Azərbaycanda hərbi elmin inkişafına, onun tədqiqat metodlarına təsir göstərən spesifik faktorlar da mövcuddur ki, bu faktorlar və onların araşdırılma metodları da tədqiqat zamanı nəzərə alınmalı və tədqiqat obyektinə çevrilməlidir. Bu faktorlardan ikisinin, xüsusilə, diqqət mərkəzində saxlanması vacibdir:

1. Azərbaycan qalibiyyətli Vətən Müharibəsindən böyük hərbi, döyüş təcrübəsi ilə çıxmışdır. Bu təcrübənin qısa zamanda öyrənilməsi həm hərbi işin tədqiqi, həm də gələcək nəsillər üçün qəhrəmanlıq salnaməmizin qorunub saxlanılması baxımından əhəmiyyət daşıyır;
2. Azərbaycan üçün hərbi təhlükə hələ sovuşmamışdır. Bu da hərbi sahədə tədqiqatların genişləndirilməsini, bu sahədə dünya təcrübəsinin öyrənilməsini və problemin öyrənilmə effektivliyinin artırılması üçün ən yeni üsul və metodlardan istifadəni zəruri edir.

Müasir dövrdə hərbi-elmi tədqiqata təsir göstərəcək bütün bu yeni tendensiyalarla bərabər, problemin öyrənilməsi üçün bu tədqiqatın uzun illərin sınağından çıxmış metodlarına yenidən baxış, onların müasir dövr baxımından tətbiqi xüsusiyyətləri də nəzərə alınmalıdır.

2. Ənənəvi hərbi-elmi tədqiqat metodları müasir tendensiyalar baxımından

Bilindiyi kimi, hərbi elmi bilik ümumi biliklərin altsistemini təşkil edir. Bütövlükdə müharibə fenomeni və digər silahlı mübarizə formaları, hərbi qüvvələrin qurulması və döyüşə hazırlığı, hərbi təhlükəsizliyin təmin edilməsi prinsipləri, dövlətin hərbi gücü və müharibəyə hazırlığı məsələlərini

öyrənən hərbi-elmi tədqiqat prosesi qeyd olunanlar haqqında əldə edilmiş bütün biliklərdən istifadə edir, digər tərəfdən, tədqiqat obyektləri barədə spesifik məsələləri də öyrənir. Bununla, hərbi-elmi idrak prosesində spesifik bilik əldə olunur. Beləliklə, hərbi elmi bilik həm tədqiqat obyektinə görə, həm də bu obyektin öyrənilməsi zamanı istifadə edilən xüsusi metodlara görə fərqlənir.

Mütəxəssislər qeyd edirlər ki, hərbi tədqiqat metodlar sistemi üfüqi və şaquli xarakterli əlaqələr yaradan struktura malikdir və bu metodların təsnifatını aşağıdakı şəkildə verirlər:

- ✓ ən ümumi fəlsəfi metodlar;
- ✓ ümumelmi xüsusi metodlar;
- ✓ yalnız hərbi-elmi tədqiqat zamanı və ya digər elmlərin hərblə bağlı problemlərinin tədqiqi zamanı istifadə olunan xüsusi metodlar [4, s.188].

Müasir dövrün fəlsəfəsində baş verən dəyişikliklərdən danışarkən ən ümumi fəlsəfi metodlar məsələsinə toxunmuşduq. Ümumi dialektik, metafizik, sinergetik (sistem), intuitiv, hermenevtik (anlama) və s. metodları bir qayda olaraq tədqiqatçının dünyagörüşünün əsasını təşkil edir və tədqiqat fəaliyyətində nümayiş etdirdiyi düşüncəyə öz təsirini göstərir. Bu, bəzən şüurlu deyil kortəbii şəkildə də ola bilər.

Hərbi-elmi tədqiqat zamanı istifadə olunan ümumelmi metodlardan danışarkən qeyd etməliyik ki, bunlardan istifadə əksər hallarda hərbi-elmi tədqiqatın bazasını təşkil edir. Hazırki dövrdə hərbi-elmi tədqiqatda bu metodların daha çox empirik və nəzəri bilik səviyyəsi üzrə bölgü təsnifatından istifadə olunur. Buna müvafiq olaraq, hərbi-elmi tədqiqat metodları üç formada özünü göstərir:

1. **Hərbi praktik metodlar.** Bu metodlar, həmçinin empirik metodlar da adlanır. Hərbi praktiki metodlar müharibə və ya sülh şəraitində bilavasitə praktiki hərbi fəaliyyətin gedişində elmi tədqiqatçının (əksər hallarda hərbi qulluqçu, komandir) iştirakı ilə həyata keçirilir. Konkret şəraitlə bağlı olur və bu şəraitlə şərtlənir;
2. **Hərbi-nəzəri metodlar.** Bu metodlar alimlər tərəfindən həyata keçirilən xüsusi elmi tədqiqat zamanı istifadə olunur və mahiyyətcə hərbi praktikanın elmi-nəzəri təminatını təşkil edir. Bu metodlardan istifadənin nəticəsi olaraq hərbi elmi bilik formalaşır.
3. **Həm empirik, həm də nəzəri səviyyədə istifadə edilən metodlar** da mövcuddur ki, analiz və sintez, induksiya və deduksiya, modelləşdirməni və s. bura aid edə bilərik.

Hərbi-elmi tədqiqatda empirik metodlar ya bilavasitə hiss üzvləri vasitəsilə, ya da cihazlar vasitəsilə hissi olaraq qəbul edilən gerçəklik obyekti, onun ayrı-ayrı hissələri, xüsusiyyətləri, fəaliyyətinin öyrənilməsinə əsaslanır. Burada, ilkin olaraq silahlı mübarizə vasitələri və onların fəaliyyəti təsvir olunur. Empirik tədqiqat zamanı qarşıya qoyulan vəzifələr empirik metodların spesifik formalarını müəyyən edir. Hərbi-elmi tədqiqat zamanı istifadə edilən əsas empirik metodlar kimi müşahidə, eksperiment, ölçü, konkret sosioloji tədqiqat metodları (ilk növbədə sorğu-söhbət, müsahibə, anketləşdirmə, sosiometrik sorğu) qeyd edilə bilər.

Mütəxəssislər hərbi tədqiqatın empirik metodlarına hərbi müşahidə (operativ-praktiki, hərbi-elmi), hərbi kəşfiyyat, hərbi eksperiment (hərbi-texniki, sosial-pedaqoji, operativ taktiki və s. aid edirlər [4, s.193]. Bir də qeyd etmək yerinə düşərdi ki, bu metodlardan istifadə zamanı tədqiqatçı prosesə sadəcə müşahidəçi kimi yanaşmır, özü üçün vacib olanları seçir, ümumiləşdirir, təsnifatını verir və s.

Empirik metodlardan danışarkən, onların subyektivliyi məsələsi də diqqət mərkəzində dayanmalıdır. Əgər söhbət hərbi-elmi tədqiqatdan gedirsə, burada hərbi gücün, silahların, cihaz və digər maddi vasitələrin standart ölçü vahidləri mövcuddur. Lakin insan fəliyyətinin bu şəkildə ölçü etalonu yoxdur. Heç bir yerdə "vətən sevgisi", "qəhrəmanlıq", "şücaət" və s. kimi keyfiyyətlərin statistik ölçüsünü təyin edə biləcək standartlar yoxdur. İş o yerə gəlib çatıb ki, erməni ekspertlər 12 min fərarisi olan ordularının "qəhrəmanlığından" danışırlar. Yəni hərbidə insan faktorundan danışarkən, burada tədqiqatın subyektiv ölçü vahidlərindən – bu vahidin subyektiv təyinindən söhbət gedə bilər. Bununla belə, müasir dövrdə hərbi fəaliyyətdə insana təsirin bir sıra yeni forma və metodları meydana gəldiyi, psixoloji mübarizə formalarının təkmilləşdiyi bir zamanda empirik tədqiqatın bu faktorları diqqət mərkəzində saxlayacaq yeni tədqiqat metodlarının meydana gəlməsi, mövcudların təkmilləşdirilməsi vacibdir.

İdrakın nəzəri səviyyəsinin qarşısında dayanan əsas vəzifə silahlı mübarizə vasitələri barədə yeni, daha dərin bilik əldə etməkdir. Bu zaman empirik metodlarla əldə edilən bilik şərh və izah edilir, elmi biliyin sintezi həyata keçirilir. Nəzəri tədqiqat zamanı daha mötəbər bilik əldə edilir, tədqiq olunan hərbi

hadisələr ümumi təsvirlə izah olunur, ümumi qanun və qanunauyğunluqlar açılır, bütövlükdə empirik tədqiqat zamanı əldə edilən biliklər sistemləşdirilir, yeni nəzəriyyə və konsepsiyalar meydana gəlir, hələ öyrənilməmiş faktlar aşkarlanır və s.

Hərbi nəzəri tədqiqat zamanı istifadə edilən nəzəri metodlar ümumi elmi tədqiqatın nəzəri metodları ilə üst-üstə düşür və buraya, ilk növbədə aşağıdakıları daxil edə bilərik:

- ✓ həm empirik, həm də nəzəri metod kimi istifadə edilən, yuxarıda qeyd olunan induksiya və deduksiya, analiz və sintezi, modelləşdirməni və s. kimi metodları;
- ✓ yalnız nəzəri tədqiqat metodu kimi istifadə olunan ideallaşdırma, abstraktlaşdırma, ümumiləşdirmə, formallaşdırma, məntiqi yanaşma və s. kimi metodları.

Nəzəri metodlar da daim bir sıra dəyişikliklərə uğrayır. Bu, həm dövrün xarakterindəki dəyişikliklər, tədqiqat obyekti və predmetinin dəyişməsi, onun sırasına yenilərinin daxil edilməsi, həm bununla əlaqəli şəkildə yeni nəzəri metodların formalaşması, həm də elmi-texniki inkişafdan qaynaqlanan yeni riyazi, kibernetik üsulların meydana gəlməsi ilə bağlıdır.

Hərbi elmi idrak bir qayda olaraq, hərbi praktika əsasında həyata keçirilir və ondan kənarda mövcud ola bilməz. Lakin lazımi nəzəri bilik olmadan da, xüsusən müasir dövrdə, praktiki hərbi fəaliyyətdə müvəffəqiyyətin əldə edilməsi mümkünsüzdür. Bu bilik, təkcə konkret hərb sahəsindəki nəzəri biliklərə deyil, uyğun elmi biliklərin nailiyyətlərinə də söykənir. Buna görə də nəzəri metodlardan danışarkən, hərbi-elmi tədqiqatın bütün elm sahələri ilə əlaqəli şəkildə aparılmasını, nəzəri biliklərin sintezinin əldə edilməsini də qeyd etməyi vacib bilirik. Məsələn, dəqiq elmlər hərbi sistemin fiziki predmet və hadisələrinin xarakteristikalarını öyrənməyə imkan verirsə, humanitar və sosial elmlər təsir və qarşılıqlı təsirin obyekti və subyekti kimi bütövlükdə insan və kollektiv, cəmiyyət haqqında təsəvvür almağa imkan verir. Təbiət elmləri insanın bioloji mahiyyəti haqqında məlumat verir. Tədqiqatçıların fikrincə, bu biliklər hərbi-elmi tədqiqatların aparılmasında məcmu şəkildə böyük rol oynayır. Məsələn, bütövlükdə bir çox sahələrin, o cümlədən, hərbi-texniki, hərbi-elmi biliklərin öyrənilməsi hərbi-pedaqoji prosesi, hərbi qulluqçular və hərbi kollektivlərin təlim tərbiyəsi, onların uğurlu hərbi əməliyyatlar aparılmasına və hərbi-peşə fəaliyyətinə psixoloji hazırlığı təmin edən hərbi pedaqoji prosesləri və onların elementlərini modelləşdirmə imkanı verir [5, s. 41].

Qeyd etdiyimiz kimi, yalnız hərbi tədqiqatda istifadə olunan xüsusi metodlar da mövcuddur. Müasir dövrdə hərbi tədqiqatda istifadə edilən elmi metodlarından danışarkən, onların tətbiq sahəsinə görə aşağıdakı təsnifatını qeyd edə bilərik:

- ✓ hərbi-tarixi;
- ✓ hərbi-pedaqoji;
- ✓ hərbi-strateji;
- ✓ hərbi-taktiki və s. [6, s. 127].

Tədqiqatçılar xüsusi hərbi metodlara misal olaraq vəziyyətin operativ-taktiki təsviri, döyüş şəraitinin hərbi analizini, operativ-taktiki hesablamaları və s. qeyd edirlər [4, s. 192].

Beləliklə, hərbi elmi biliyin digər bilik növləri ilə ümumilik təşkil etməsi ilə bərabər onu iki bənd üzrə digər bilik növlərindən fərqləndirə bilərik:

- ✓ spesifik tədqiqat obyektinə görə;
- ✓ tədqiqat zamanı istifadə olunan metodların spesifikliyinə görə.

Dünyanın sosial, iqtisadi, siyasi mənzərəsi dəyişildikcə, müharibənin yeni metod və vasitələri meydana gəldikcə, müharibə, silahlı toqquşmalar zamanı istifadə olunan texnologiyalar və silahlar daha da təkmilləşdikcə hərbi elmin obyekt və predmeti, bununla əlaqəli şəkildə elmi tədqiqatının metodları da dəyişikliyə uğrayır. Fikrimizcə, ümumi baza metodlarının nisbi sabitliyi şəraitində hərbi elmi tədqiqatda istifadə olunan xüsusi metodlar daha dəyişkən xarakter daşıyır ki, bu da hərbi işin müasir dövrlə ayaqlaşan sürətli təkamülü ilə bağlıdır.

Hipersəs, lazer texnologiyalarının təkmilləşdirilməsi, silahlı münaqişələr zamanı daha çox süni intellektdən istifadə, digər texnoloji yeniliklər, informasiya və kiber təhlükəsizlik məsələlərinin daha da aktuallaşması onların tədqiqinin yeni metodlarının axtarışını vacib edir.

Müasir dövrdə diqqət yetirilən və dövlətlərin hərbi gücünün ölçülməsində, miqyasının təyinində mühüm rol oynadığı güman edilən yeni texnologiya sahələri aşağıdakılardır:

- ✓ süni intellekt;
- ✓ öldürücü avtonom silahlar;

- ✓ hipersəs silahları;
- ✓ yönləndirilmiş enerji silahları;
- ✓ biotexnologiyalar;
- ✓ Kvant texnologiyaları [3].

Bu sahələrin konkretləşdirilməsi, həm də hərbi-elmi tədqiqatın inkişaf istiqaməti, onun obyekti və predmeti, buradan çıxış edərək elmi tədqiqat metodlarını müəyyən edir.

Vurğulamaq istədiyimiz digər məsələ böhranlı vəziyyətlərdən istifadə edərək rəqibə iqtisadi, maliyyə, diplomatik təsir, birbaşa vətəndaşlara informativ-psixoloji təsir vasitələri geniş yayılmasıdır ki, regionumuzun timsalında bunun şahidi oluruq. Hadisələrin inkişaf tendensiyasına diqqət yetirsək gələcəyin silahlı münaqişə və müharibələrinin, təkcə klassik formada deyil, assimetrik və hibrid şəkildə aparılacağını proqnozlaşdıra bilərik. Deməli, mübarizə, təkcə hərbi sahə ilə məhdudlaşmayacaq. Bu da hərbi elmi biliyin tədqiqat dairəsinin genişləndirilməsini tələb edir. Buna görə kibernetik, koqnitiv və mental mübarizənin öyrənilməsi metodları da təkmilləşdirilməlidir. "Vestpoint" hərbçi hazırlığı proqramına nəzər salınarsa, burada ayrı-ayrı kurslar çərçivəsində hərbi sahədə müasir texnologiyalar, onların beynəlxalq şəraitlə qarşılıqlı təsirdə müharibələrin xarakterində dəyişiklik yaratması, yeni texnologiyaların gələcək komandirlərin fəaliyyətinə təsiri, hərbi-elmi tədqiqatın, o cümlədən strateji tədqiqatın müxtəlif metodlarının tədrisinin, kursant yaradıcılığının, onun ayrı-ayrı problemlərə fərdi yanaşmasının təşviqinin şahidi ola bilərik [7]. Fikrimizcə, bu qabaqcıl təcrübənin Azərbaycanda istifadəsi gələcək zabitlərimizin sürətlə dəyişən innovativ xarakterli hərbi hadisələrə, o cümlədən hərbi-elmi tədqiqatın yeni metodlarının tətbiqinə hazır olmasını təmin edər.

Bütün elm sahələrində olduğu kimi, hərbi-elmi tədqiqatda da empirik və nəzəri tədqiqat metodları bir-birini müəyyən edir və tamamlayır. Bu metodlar arasında inkişaf baxımından həmişə bərabərlik olmur. Silahlı mübarizə vasitələrinin inkişafının müəyyən mərhələsində empirik metodların nəzəri metodları önləməsi və əksi mümkündür. Adətən yeni nəzəriyyənin meydana gəlməsi zamanı empirik, artıq mövcud olan nəzəriyyələrin təşəkkülü prosesində nəzəri metodlar daha çox üstünlük təşkil edir. Müasir dövrdə silahlı mübarizənin forma və metodlarının sürətli dəyişkənliyini nəzərə alsaq, bununla bağlı empirik metodların üstünlüyünü qeyd edə bilərik. Eyni zamanda müasir dövrdə kibernetik, riyazi, fiziki modelləşdirmə ilə bağlı empirik əsası olmayan tədqiqatlara da tez-tez təsadüf olunur. Bu, nəzəri konstruksiyalar, fikrimizcə, tətbiqindən əvvəl praktiki verifikasiyaya uğramalıdır. Belə ki, məhz hərbi tədqiqat sahəsində buraxılan səhvlər sonradan ağır nəticələrə gətirib çıxara bilər. Bu, mürəkkəb məntiqi konstruksiyaların praktiki yoxlama metodları da çox güman ki, zamanla yenilənərək daha mürəkkəb xarakter alacaq. Eyni zamanda qeyd etmək lazımdır ki, humanitar xarakterli məsələlərin mövcudluğu bu praktiki metodların məzmununun daha da mürəkkəbləşdirilməsi məcburiyyətinə gətirib çıxarır.

Fikrimizcə, müasir dövrün xarakterini nəzərə alsaq, hazırda hərbi-elmi tədqiqat metodlarının effektivliyinin aşağıdakı faktorlardan asılı olduğunu deyə bilərik:

- ✓ müxtəlif bilik sahələrinin öyrənilən obyekt və predmetlə bağlı tədqiqatlarını əhatə edən sistem modelləşdirmənin həyata keçirilməsi;
- ✓ qarşıda dayanan vəzifələr nəzərə alınmaqla, bütövlükdə istifadə olunacaq metodlar kompleksinin təyini. Diqqət yetirilməlidir ki, hərbi-elmi idrak metodologiyası hərbi-nəzəriyyə və hərbi-praktikanın konkret məsələlərinə deyil, hərbi məsələlərin öyrənilməsinin əsas yolları və üsullarına istiqamətlənmişdir və tədqiqatçını idraki fəaliyyətin prinsipləri ilə silahlandırır;
- ✓ istifadə olunan metodların funksiyası, rolu, xüsusiyyətləri, istifadə zamanı həyata keçirilən prosedurların müasir bilik baxımından elmi araşdırılması, effektivliyinin təyini;
- ✓ hər bir konkret obyektin öyrənilməsi üçün metodun və ya metodlar qrupunun düzgün seçilməsi;
- ✓ metodların doğru tətbiqi;
- ✓ metodlardan kompleks istifadə;
- ✓ nəticələrin qeyri-müəyyənliyinin təyini, verifikasiyasının həyata keçirilməsi, səhvlərin düzəldilməsi;
- ✓ hərbi fəaliyyətin inkişaf perspektivi meyilləri nəzərə alınmaqla, mümkün gələcəyin proqnozlaşdırılması üçün yeni metodların axtarışı;
- ✓ hələlik mövcud olmayan, gələcəkdə yarana biləcək yeni problemlərin həlli yollarının axtarışı.

Nəticə və təkliflər

Gördüyümüz kimi, müasir dövrü xarakterizə edən bir sıra mühüm faktorların təsiri ilə hərbi- elmi tədqiqat və onun metodlarında yeni inkişaf tendensiyaları meydana gəlmişdir. Bu, həm mövcud empirik və nəzəri tədqiqat metodlarının təkmilləşdirilməsi, həm də bu sahədə yeni metodların meydana gəlməsində özünü göstərir. Tədqiqat zamanı bütün ümumi elmi nailiyyətlərdən istifadə olunaraq, biliklərin qovşağında olan hərbi tədqiqatın genişləndirilməsi və dərinləşdirilməsi dövrün tələbidir. Azərbaycanda da hərbi-elmi tədqiqat göstərilən bütün tendensiyaları özündə əks etdirməklə bərabər, həm də müdafiə təhlükəsizliyimizlə əlaqədar qarşıya ciddi vəzifələr qoyur. Bu vəzifələr, birinci növbədə hərbi-elmi tədqiqatın dinamik bir proses kimi inkişaf etdirilməsi, onun bilik metodlarının təkmilləşdirilməsi ilə bağlıdır. Bunun üçün diqqət yetirilməsi ən vacib olan istiqamətlər aşağıdakılardır:

– müasir dövrün tələblərinə və çağırışlarına uyğun olaraq, hərbi-elmi tədqiqatın əsas sahə və istiqamətlərinin müəyyənləşdirilməsi;

– hərbi sahədə yeni elmi tədqiqat texnologiyalarından istifadənin öyrənilməsi və tətbiqi. O cümlədən:

– yeni texnika və texnologiyaların tətbiqi nəticəsində müharibələrin xarakteri, üsul və vasitələrində baş verən dəyişikliklərin elmi tədqiqi metodlarının araşdırılması;

– müasir müharibələrdə insan faktoru rolunun hərtərəfli öyrənilməsi, dinamik müasir texniki inkişafa münasibətdə insan faktorunun doğru dəyərləndirilməsi üçün yeni metodların tətbiqi, bu məsələdə yeni informasiya texnologiyalarından istifadə;

– hərbi-elmi tədqiqat və onun metodlarının inkişaf dinamikası öncədən müəyyən edilərək, bu sahələr üzrə gələcək mütəxəssislərin hazırlanması.

Bugünkü şəraitdə qarşıda dayanan ən mühüm vəzifə hərbi-elmi tədqiqatın zamanla ayaqlaşmasını, gələcəyin proqnozlaşdırılmasını təmin etməkdir. Hərbi nəzəriyyənin müasir hərbi praktikadan ləngiməsinə yol vermək olmaz. Eyni zamanda hərbi nəzəriyyənin praktiki verifikasiyası ilə bağlı yeni metodların işlənib hazırlanması vacib şərtdir.

Ədəbiyyat

1. Xiyao, Hong. Advantages and methods of military sciences [Electronic resource] / URL: https://www.longdom.org/open-access/advantages-and-methods-of-military-sciences-97708.html

2. Kurtay, K.G., Dağistanli, H. A., Altundaş, A. Simülasyon, muharebe modelleme ve harp oyunu teknolojileri // Genişletilmiş gerçeklik teknolojileri ve güvenlik uygulamaları. Editör Doç. Dr. Hamit Erdal. Birinci Baskı, – 2022. – İstanbul. Chapter: 7 Publisher: Kriter Yayınevi (pp.211-265). [Elektronik kaynak] URL: //https://www.researchgate.net/publication/364845706_simulasyon_muharebe_modelleme_ve_harp_oyunu_teknolojileri

3. Emerging Military Technologies: background and issues for congress – FAS Project on Government Secrecy [Electronic resource] / URL: https://sgp.fas.org/crs/natsec/R46458.pdf

4. Философия: Учебник для военных вузов (Под ред. О.Ю. Ефремова). – Санкт Петербург: Питер, – 2021. – 464 с.

5. Военная педагогика: Учебник для вузов / И.А.Алехин [и др.]; под общей редакцией И.А.Алехина. – Москва: Издательство Юрайт, – 2024. – 414 с.

6. Hüseynova, S. Fəlsəfədən mühazirələr konspekti. Dərs vəsaiti / S.Hüseynova – Bakı: "Təknur" nəşriyyatı, – 2019. – 204 s.

7. Department of Military Instruction Course Catalog.29 Courses [Electronic resource] / URL: https://courses.westpoint.edu/crse_dept_catalog.cfm?str_sub_div_ofc_sym_cd=MACC-Q

Elmi Əsərlər
Proceedings of Science

Heydər Əliyev adına Hərbi İnstitutun **Elmi Əsərlər** jurnalı, Cild 22, № 2, 2024 / 32-42
Proceedings of Science of the Military Institute named after Heydar Aliyev, Volume 22, № 2, 2024 / 32-42

Daxilolma tarixi / Received date: 20.07.2024
Qəbulolma tarixi / Accepted date: 15.09.2024

DOI: 10.30546/8967.2024.22.2.1014

DRONUN TƏHLÜKƏSİZLİK SİSTEMİNDƏ SÜNİ İNTELLEKT VƏ MAŞININ ÖYRƏNİLMƏSİ

Manafəddin Namazov
texnika elmləri namizədi, dosent
Azərbaycan Texniki Universiteti, Bakı
E-mail: manafeddin.namazov@aztu.edu.az

Xülasə

Bu məqalə, müasir təhlükəsizlik sistemlərində dronların rolunu və bu sistemlərdə süni intellekt (AI) və maşın öyrənməsi (ML) alqoritmlərinin effektivliyini geniş miqyasda araşdırır. Dronlar, müxtəlif sahələrdə geniş tətbiq edildiyindən, onların təhlükəsizliyi böyük önəm kəsb edir. Məqalədə əsas diqqət, DDoS (Distributed Denial of Service) hücumları kimi ən çox yayılmış kiberhücum növlərinə yönəldilmişdir. DDoS hücumları zamanı çoxlu sayda zərərli cihaz bir hədəfə qarşı eyni anda hücum edir və bu, sistemin işini iflic edir. Dronlar da belə hücumlara qarşı həssasdır, çünki onlar uzaqdan idarə olunan və internet şəbəkəsinə qoşulu cihazlar olduğuna görə potensial təhlükələrə daha çox açıqdırlar. Məqalədə bu kimi hücumları vaxtında aşkarlamaq və onlara qarşı mübarizə aparmaq üçün xüsusi süni intellekt və maşın öyrənməsi modellərinin tətbiqi təsvir edilmişdir. Burada xüsusilə dərin öyrənmə və qərar ağacları kimi maşın öyrənməsi metodlarından istifadə edilərək DDoS hücumlarını aşkarlayan alqoritmin işləmə mexanizmi və prinsipləri izah edilmişdir. Bu alqoritm şəbəkə trafiki və digər məlumat axınlarını analiz edərək zərərli fəaliyyəti aşkar edir və dronların təhlükəsizliyini qorumaq üçün vaxtında tədbirlər görməyə imkan verir. Məqalənin son bölməsində isə bu alqoritmin Matlab mühitində necə realizə olunması geniş izah olunur. Nəticədə, bu araşdırma süni intellekt və maşın öyrənməsi texnologiyalarının dronların təhlükəsizliyində necə mühüm rol oynadığını göstərir və bu sahədə gələcək inkişaflar üçün yeni istiqamətlər təqdim edir.

Açar sözlər: dron təhlükəsizliyi, süni intellekt (AI), maşın öyrənməsi (ML), DDoS hücumları, MATLAB simulyasiyası.

SECURITY SYSTEMS FOR DRONES WITH ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Manafeddin Namazov
candidate of technical sciences, associate professor
Azerbaijan Technical University, Baku

Abstract

This article extensively examines the role of drones in modern security systems and the effectiveness of artificial intelligence (AI) and machine learning (ML) algorithms within these systems. Since drones are widely used in various fields, their security is of great importance. The article focuses primarily on Distributed Denial of Service (DDoS) attacks, which are among the most common types of cyberattacks. During DDoS attacks, a large number of malicious devices simultaneously target a single system, causing it to malfunction. Drones are vulnerable to such attacks because they are remotely controlled and connected to the internet, making them more susceptible to potential threats. The article describes the application of specific AI and ML models to detect and prevent these types of attacks in a timely manner. In particular, deep learning and decision tree methods are utilized to explain the mechanism and principles of the algorithm that detects DDoS attacks. This algorithm analyzes network traffic and other data flows to identify malicious activities and enables timely action to protect the security of drones. The final section of the article provides a detailed explanation of how this algorithm is implemented in the Matlab environment. The stages of simulation and application of the algorithm using Matlab are described step by step, along with the technical details regarding its integration into drone systems. Ultimately, this study highlights the crucial role of AI and ML technologies in drone security and presents new directions for future developments in this field.

Keywords: drone security, artificial intelligence (AI), machine learning (ML), DDoS attacks, MATLAB simulation.

СИСТЕМЫ БЕЗОПАСНОСТИ ДРОНОВ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ

Манафеддин Намазов
кандидат технических наук, доцент
Азербайджанский Технический Университет, Баку

Аннотация

В данной статье подробно рассматривается роль дронов в современных системах безопасности и эффективность алгоритмов искусственного интеллекта (AI) и машинного обучения (ML) в этих системах. Поскольку дроны широко используются в различных областях, их безопасность имеет большое значение. Основное внимание в статье уделяется распределенным атакам типа отказа в обслуживании (DDoS), которые являются одними из самых распространенных видов кибератак. Во время DDoS-атак большое количество вредоносных устройств одновременно атакуют одну систему, что вызывает ее сбой. Дроны уязвимы к таким атакам, так как они дистанционно управляются и подключены к интернету, что делает их более подверженными потенциальным угрозам. В статье описывается применение конкретных моделей AI и ML для своевременного обнаружения и предотвращения подобных атак. В частности, методы глубокого обучения и деревьев решений используются для объяснения механизма и принципов работы алгоритма, который обнаруживает DDoS-атаки. Этот алгоритм анализирует сетевой трафик и другие потоки данных для выявления вредоносной активности и позволяет своевременно предпринять меры по защите безопасности дронов. В заключительной части статьи подробно объясняется, как этот алгоритм реализован в среде Matlab. Шаг за шагом описаны этапы симуляции и применения алгоритма с использованием Matlab, а также технические детали его интеграции в системы дронов. В конечном итоге данное исследование подчеркивает важную роль технологий AI и ML в обеспечении безопасности дронов и представляет новые направления для будущего развития в этой области.

Ключевые слова: безопасность дрона, искусственный интеллект (AI), машинное обучение (ML), атаки DDoS, симуляция MATLAB.

Giriş

Dron texnologiyaları müasir dünyada müxtəlif sahələrdə geniş şəkildə tətbiq olunur. Bu cihazlar nəqliyyat, kənd təsərrüfatı, təhlükəsizlik və hətta hərbi əməliyyatlar kimi bir çox sahədə istifadə edilir. Dronların geniş yayılması ilə onların təhlükəsizliyi də əsas prioritetlərdən birinə çevrilib.

Bu məqalədə dronların təhlükəsizlik sistemlərində istifadə olunan əsas xüsusiyyətləri təsvir edilir. Eyni zamanda süni intellekt və maşın öyrənməsi alqoritmlərinin bu xüsusiyyətlər vasitəsilə potensial təhdidlərin aşkar edilməsi və onların qarşısının alınması məqsədilə necə tətbiq olunduğu araşdırılır. Dronlar müxtəlif məqsədlər üçün geniş istifadə edildikcə, onların kibertəhlükəsizlik riskləri də paralel olaraq artır.

Məlumat toplama modulu dronun fəaliyyətinin əsas hissəsidir və onun təhlükəsizliyini təmin etmək üçün müxtəlif kibertəhlükəsizlik tədbirləri görülməlidir. Bu tədbirlər olmadan dronların topladığı məlumatların sızdırılması və ya manipulyasiyası ciddi nəticələrə səbəb ola bilər. Dronların təhlükəsizlik sistemlərində süni intellekt və maşın öyrənməsi alqoritmləri əsasən anomaliyaların aşkarlanması və potensial təhdidlərin proqnozlaşdırılması məqsədilə istifadə olunur. Məlumat toplama modulu dronun işləməsi üçün vacib məlumatları topladığı üçün kibercinayətkarlar üçün hədəf ola bilər. Aşağıda bu modulu inkar etmənin (müdaxilə olunmanın mümkünlüyünün) bəzi üsulları göstərilib:

GPS Saxtalaşdırılması (GPS Spoofing): GPS Spoofing hücumları zamanı kibercinayətkarlar dronun GPS modulu tərəfindən qəbul edilən siqnalları saxtalaşdıraraq, onu səhv mövqelərə yönləndirir. Bu, dronun yanlış mövqeyə getməsinə və ya planlaşdırılmamış marşrut izləməsinə səbəb ola bilər. Bundan müdafiə olunmaq üçün GPS siqnallarının şifrələnməsi və əlavə doğrulama sistemləri ilə bu cür hücumların qarşısını almaq mümkündür [5].

Sensor Manipulyasiyası: Dronun akselerometr, giroskop və barometr kimi sensorları manipulyasiya edilə bilər. Kibercinayətkarlar dronun sensorlarına saxta siqnallar göndərərək, onun sürətini, hündürlüyünü və ya dönmə sürətini səhv oxumağa məcbur edə bilərlər. Bundan müdafiə

olunmaq üçün sensorların siqnallarını yoxlayan və doğrulayan sistemlər quraraq, bu hücumların qarşısını almaq mümkündür.

Məlumat Axınının Dinlənməsi (Data Sniffing): Dronun məlumat toplama modulu ilə idarəetmə mərkəzi arasında olan məlumat axını ələ keçirilə bilər. Bu hücum növü ilə kibercinayətkarlar dronun topladığı həssas məlumatları əldə edə bilər. Bundan müdafiə olunmaq üçün məlumat axınlarının şifrələnməsi və təhlükəsizlik protokollarının tətbiqi ilə məlumat axınının dinlənməsinin qarşısını almaq mümkündür.

Proqram təminatı zəifliklər: Dronun sensorlarını idarə edən proqram təminatı zəifliklərindən istifadə edərək, kibercinayətkarlar bu sensorları manipulyasiya edə və ya onların fəaliyyətini tamamilə dayandıra bilərlər. Bundan müdafiə olunmaq üçün proqram təminatını mütəmadi olaraq yeniləmək və təhlükəsizlik yamalarını tətbiq etmək bu cür hücumların qarşısını almağa kömək edir [1-3].

DDoS (Distributed Denial of Service) hücumları, dronların təhlükəsizliyinə təhdid yaradan başqa bir hücum növüdür və xüsusilə dronun idarəetmə və rabitə sistemlərinə qarşı yönəldilir. Bu hücumlar məlumat axınının dinlənməsi və bloklanması (data sniffing və blocking) sinfinə daxildir. Bu zaman DDoS hücumları zamanı kibercinayətkarlar dronun idarəetmə mərkəzi ilə olan rabitəsini məhdudlaşdırmaq və ya tamamilə bloklamaq üçün böyük həcmdə yükləmə (trafik) göndərirlər. Bu, dronun idarəetmə siqnallarını qəbul etməməsinə, fəaliyyətini dayandırmasına və ya əlaqəni itirməsinə səbəb ola bilər. Bu hücumların qarşısını almaq üçün bir neçə müdafiə yolu mövcuddur [3]:

- **Şəbəkə trafiki monitorinqi və süzgəclənməsi:** Dronun rabitə kanalları üzərində şəbəkə trafikinin monitorinqi və zərərli trafiklərin süzgəclənməsi DDoS hücumlarının qarşısını ala bilər;
- **Redundant rabitə kanalları:** Dron üçün birdən çox rabitə kanalı qurularaq, biri hücuma məruz qalarsa, digərləri vasitəsilə idarəetmə davam etdirilə bilər;
- **Şifrələmə və autentifikasiya:** Güclü şifrələmə və autentifikasiya mexanizmləri istifadə edilərək, dronun yalnız etibarlı mənbələrdən siqnallar almasına imkan verilir.

DDoS hücumları ilə mübarizə aparmaq, dronun təhlükəsiz və etibarlı fəaliyyətini təmin etmək üçün mühüm bir addımdır, xüsusən də geniş miqyaslı hücumların qarşısını almaq və dronun idarəetməsini itirməmək üçün istifadə edilir. Bunun qarşısını almaq üçün süni intellekt (AI) və maşın öyrənməsi (ML) bu təhlükəsizlik sistemlərinin daha effektiv və dayanıqlı olmasını təmin edən əsas texnologiyalardır [3].

1. Dronun struktur sxemində əsas bloklar

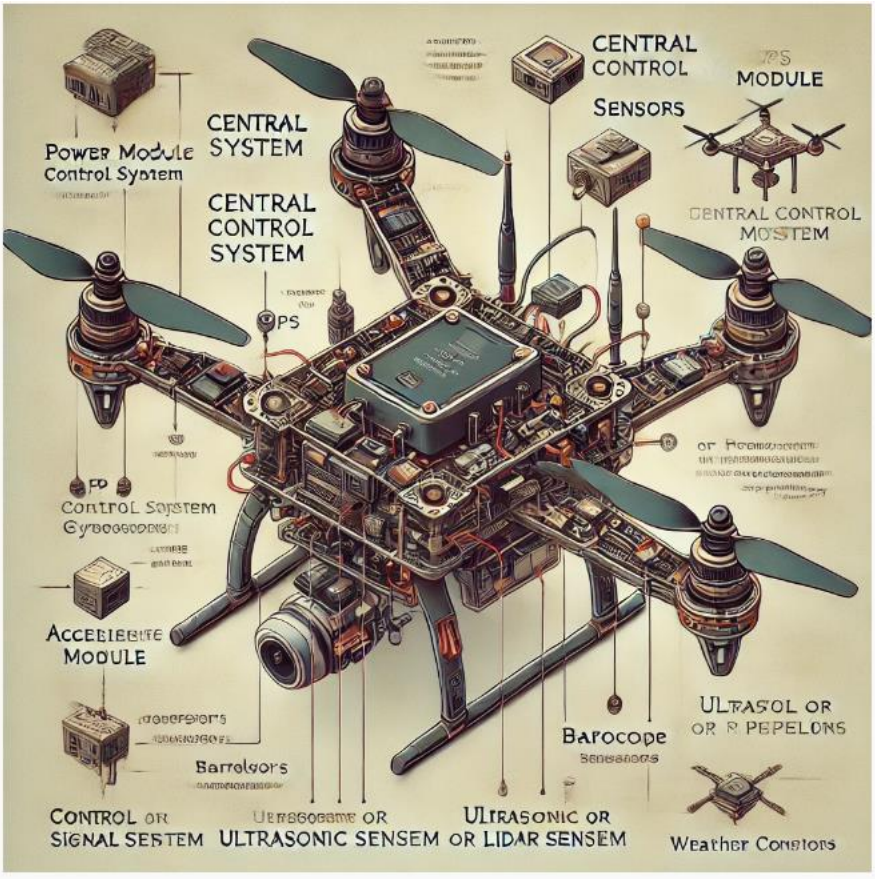
Dronun struktur sxemi, onun əsas komponentlərinin bir-biri ilə necə əlaqəli olduğunu və necə işlədiyini göstərən vizual təmsildir. Bu sxem dronun müxtəlif sistemlərini və alt-sistemlərini təsvir edir və onların birgə işləmə prinsipini izah edir. Dronun struktur sxemində əsas bloklar aşağıdakılardır: Güc modulu (power module) - dronun enerji təminatını təşkil edir. Akkumulyator (batareya) dronun müxtəlif komponentlərinə enerji verir. Mərkəzi idarəetmə sistemi (Central Control System) - Dronun bütün fəaliyyətini idarə edir. Buraya uçuşa nəzarət, stabilizasiya və bütün digər alt-sistemlərin koordinasiyası daxildir. GPS Modulu - dronun mövqeyini təyin edir və marşrutun izlənməsini təmin edir. GPS siqnalları əsasında dronun istiqaməti və hündürlüyü müəyyənləşdirilir.

- **Sensorlar**:
- Akselerometr: Dronun sürətlənməsini ölçür və sabitliyi təmin edir;
- Giroskop: Dronun dönmə sürətini ölçür və istiqaməti stabil saxlayır;
- Barometr: Dronun hündürlüyünü ölçür və uçuş zamanı sabit hündürlük təmin edir;
- Ultrasonik və ya lidar sensorlar: Maneə aşkarlanması üçün istifadə olunur və dronun toqquşmasının qarşısını alır.

Motorlar və propellerlər: Dronun uçuşunu təmin edir. Mərkəzi idarəetmə sistemi bu motorları koordinasiya edərək dronun hərəkətini istiqamətləndirir.

1. **Kamera və görüntü sistemi:** Dronun uçuşu zamanı real vaxt rejimində görüntüləri qeyd edir. Bu sistem dronun müşahidə və nəzarət işlərində istifadə edilir.
2. **İdarəetmə və siqnal gücü modulu:** Dron ilə idarəetmə mərkəzi arasında əlaqəni təmin edir. Bu modul dronun idarə olunması üçün lazım olan siqnalları alır və ötürür.

3. Hava şəraiti modulu: Uçuş zamanı hava şəraitini monitorinq edir və bu məlumatları mərkəzi idarəetmə sisteminə ötürür.



Şəkil 1. Dronun əsas blokları

Bu blok diaqramı dronun müxtəlif funksiyalarını və bu funksiyaların dronun əsas sisteminə necə bağlı olduğunu göstərir. Bu sistemin işləmə prinsipi aşağıdakı kimidir:

- **Enerji təminatı:** Güc modulu (akkumulyator) dronun bütün sistemlərinə enerji verir;
- **Nəzarət:** Mərkəzi idarəetmə sistemi bütün sensorlardan və modullardan məlumat alır, onları emal edir və uçuş zamanı qərarları qəbul edir;
- **Uçuş:** Motorlar və propellerlər mərkəzi idarəetmə sistemindən gələn siqnallara əsasən dronu havada saxlayır və hərəkətini təmin edir;
- **Məlumat toplama:** Sensorlar və görüntü sistemi dronun mövqeyi, sürəti, hündürlüyü və ətraf mühiti haqqında məlumatları toplayır;
- **Maneələrin aşkarlanması:** Ultrasonik və lidar sensorlar ətrafdakı obyektləri aşkarlayır və toqquşmaların qarşısını almaq üçün dronu yönləndirir;
- **Geri bildiriş:** Dron idarəetmə mərkəzindən gələn siqnallara cavab verir və lazım olduqda uçuşu dayandırır və ya təlimatlara uyğun hərəkət edir.

Bu struktur sxemi dronun əsas funksiyalarını və onların bir-biri ilə necə əlaqəli olduğunu izah edir. Məlumat toplama modulu, dronun mövqeyi, sürəti, hündürlüyü və ətraf mühiti haqqında məlumatları toplamaq üçün müxtəlif sensorlar və görüntü sistemlərindən ibarətdir. Bu modul dronun əsas strukturunda, adətən mərkəzi idarəetmə sistemi ilə birbaşa əlaqədə olan bir yerdə yerləşir. Məlumat toplama modulu aşağıdakı komponentləri əhatə edir:

1. **GPS modulu:** Dronun mövqeyini və marşrutunu təyin edir;
2. **Akselerometr və giroskop sensorları:** Sürət və dönmə sürətini ölçür;
3. **Barometrik sensor:** Hündürlüyü ölçür;

4. **Kamera və görüntü sistemi:** Ətraf mühit haqqında vizual məlumatları toplayır;
5. **Ultrasonik və ya lidar sensorları:** Maneələri aşkar edir.

Bu alqoritmlər dronun normal fəaliyyətinə dair böyük həcmdə məlumatları təhlil edir və istənilən anormallıqları müəyyən edir. Bu məqsədlə, istifadə olunan əsas alqoritmlər aşağıdakılardır [4]:

1. Süni neyron şəbəkələri (artificial neural networks): Bu alqoritm dronun müxtəlif sensor məlumatlarını təhlil edərək, təhdidlərin aşkarlanmasında istifadə olunur. Məsələn, DDoS hücumları zamanı sistemin normal davranışından sapmalar aşkar edilir.

2. Dərin öyrənmə (deep learning): Daha mürəkkəb məlumatların təhlili üçün dərin öyrənmə metodlarından istifadə olunur. Bu alqoritmlər, xüsusilə kamera görüntülərindən potensial təhdidlərin aşkarlanmasında çox effektivdir.

3. Qaydalara əsaslanan sistemlər (rule-based systems): Bu alqoritmlər müəyyən qaydalara əsaslanaraq dronun normal və anormal vəziyyətlərini müəyyən edir. Məsələn, müəyyən sürət həddini keçmək dron üçün təhlükə ola bilər və belə bir vəziyyət qaydalara əsaslanaraq aşkar edilir.

Maşın öyrənməsi və süni intellektin dron təhlükəsizlik sistemlərində tətbiqi, potensial təhdidlərin əvvəlcədən aşkarlanmasını və qarşısının alınmasını təmin edir. Bu texnologiyalar dronların idarəetmə sistemlərinin daim öyrənməsini və təhdidlərə qarşı adaptasiya olunmasını mümkün edir. Süni intellekt əsaslı sistemlər təhdidləri daha sürətli və dəqiq müəyyən edə bilir, bu da dronların təhlükəsizliyini artırır. Bunun üçün o, əsas xüsusiyyətləri təsbit etmək və toplamaq lazımdır.

2. Dronların təhlükəsizlik sistemlərində istifadə olunan əsas xüsusiyyətləri

Dronların təhlükəsizlik sistemlərində süni intellekt və maşın öyrənməsi alqoritmlərinin effektiv işləməsi üçün müxtəlif xüsusiyyətlərə malik məlumatlar istifadə olunur. Aşağıda bu xüsusiyyətlər və onların ölçü vahidləri haqqında məlumat verilir:

- **Sürət (speed):** Dronun hazırki uçuş sürəti, metr/saniyə (m/s) və ya kilometr/saat (km/s) ilə ölçülür. **Necə ölçülür:** Dronun GPS sistemləri və ya daxili sürət sensorları (akselerometr) vasitəsilə uçuş sürəti təyin olunur. GPS verilənləri istifadə edilərək, müəyyən bir zaman aralığında dronun keçdiyi məsafə hesablanır və bu məsafə zamana bölünərək sürət təyin edilir;
- **Yüksəklik (altitude):** Dronun dəniz səviyyəsindən olan yüksəklik dərəcəsi, metr (m) və ya fut (ft) ilə ölçülür. Dronun barometrik sensorları və ya GPS sistemi vasitəsilə dəniz səviyyəsindən olan yüksəklik təyin edilir. Barometrik sensorlar atmosfer təzyiqinə əsaslanaraq hündürlüyü ölçür, GPS isə peyklərdən alınan məlumatlara əsaslanır.
- **GPS koordinatları (GPS coordinates):** Dronun yerini təyin edən enlik və uzunluq dərəcələr (°) ilə ölçülür. Dronun GPS modulu vasitəsilə yer üzərindəki mövqeyi təyin edilir. GPS peyklərindən alınan siqnallar dronun yerini dəqiq təyin etməyə imkan verir.
- **Akkumulyatorun gərginliyi (battery voltage):** Dronun akkumulyatorunun cari gərginlik səviyyəsi, volt (V) ilə ölçülür. Dronun daxili Enerji İdarəetmə Sistemi (Power Management System) vasitəsilə akkumulyatorun cari gərginliyi ölçülür. Bu sistem akkumulyatorun vəziyyətini və enerji səviyyəsini monitorinq edir.
- **Hava şəraiti (weather conditions):** Temperatur və rütubət göstəriciləri, dərəcə Selsi (°C) və faiz (%) ilə ölçülür. Temperatur və rütubət sensorları dronun üzərində quraşdırılaraq uçuş zamanı havanın vəziyyətini ölçür. Məsələn, DHT22 və ya BMP180 kimi sensorlar hava şəraitini təyin etmək üçün istifadə edilə bilər.
- **Akselerometr göstəriciləri (accelerometer readings):** Dronun üç ox üzrə sürətlənmələri**,** metrlər/saniyə kvadrat (m/s²) ilə ölçülür. Akselerometr sensorları dronun üç ox üzrə (x, y, z) sürətlənməsini ölçür. Bu sensorlar dronun hərəkətinin hər bir istiqamətdə nə qədər sürətlənib-yavaşladığını göstərir.
- **Giroskop göstəriciləri (gyroscope readings):** Dronun bucaq sürətləri, dərəcə/saniyə (°/s) ilə ölçülür. Giroskop sensorları dronun bucaq sürətini (yəni dronun öz oxları ətrafında fırlanma sürəti) ölçür. Bu sensorlar dronun dönmə hərəkətlərini təyin etmək üçün istifadə olunur.
- **Siqnal gücü (signal strength):** Dron və idarəetmə mərkəzi arasındakı siqnalın gücü, desibel-milliwatt (dBmW) ilə ölçülür. Dron və idarəetmə mərkəzi arasında əlaqənin siqnal gücü radiomodullar vasitəsilə ölçülür. Siqnal gücü dronun nə qədər güclü və stabil əlaqəyə sahib olduğunu göstərir.

• **Kamera görüntüsü (camera feed):** Dronun kamerasından gələn görüntülərə əsaslanan təhlillər, piksel (pixels) ilə ölçülür. Dronun üzərində quraşdırılmış kamera vasitəsilə əldə edilən görüntülər - kamera modulu real vaxt rejimində video və ya fotoqrafik məlumatları toplayır.

• **Maneə aşkarlama (obstacle detection):** Dronun qarşısındakı maneələri müəyyən edən sensor məlumatları, metr (m) ilə ölçülür. Ultrasəs, lidar, ya da infraqırmızı sensorlar vasitəsilə dronun qarşısındakı maneələrin məsafəsi ölçülür. Bu sensorlar dronun ətrafındakı obyektləri aşkar edərək dronun həmin obyektlərdən təhlükəsiz məsafədə qalmasına kömək edir.

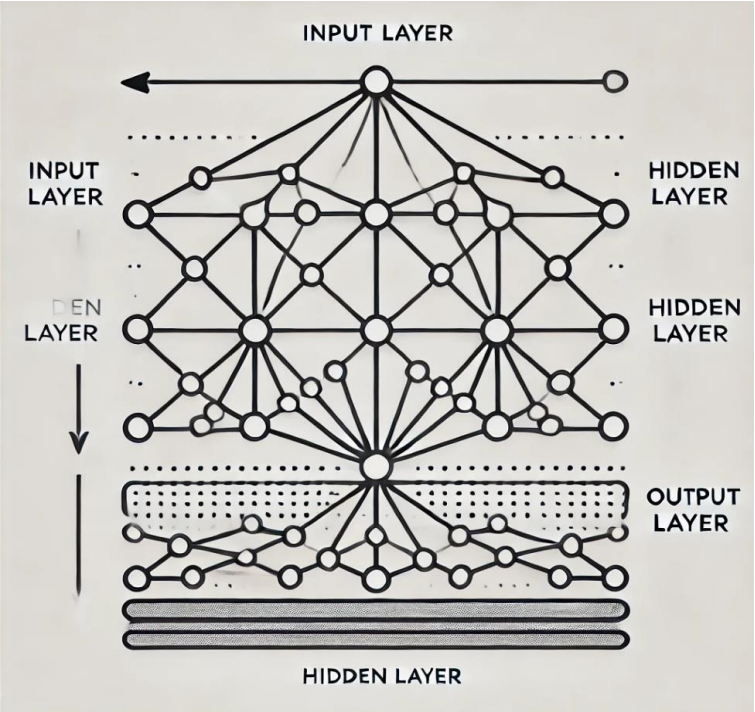
3. Süni neyron şəbəkəsinin (ANN) arxitekturası

Bu qrafik, süni neyron şəbəkəsinin (ANN) arxitekturasını təsvir edir və dronun təhlükəsizlik sistemlərində tətbiqini izah edir. Şəbəkə üç əsas qatdan ibarətdir: Giriş qatı (input layer), gizli qatlar (hidden layers) və çıxış qatı (output layer).

Bu məqalədə, dronların təhlükəsizlik sistemində təhdidlərin aşkarlanması üçün süni neyron şəbəkələrindən (artificial neural networks - ANN) istifadə olunması təhlil ediləcəkdir. Süni neyron şəbəkələri, dronun müxtəlif sensorlarından toplanan məlumatların analizində güclü bir vasitədir. Giriş qatı (input layer), gizli qatlar (hidden layers) və çıxış qatı (output layer) olmaqla üç əsas qatdan ibarət olan bu şəbəkə, məlumatların emal edilməsi və nəticələrin çıxarılması prosesini həyata keçirir.

Giriş qatı (input layer) dronun mövqeyi, sürəti, yönü və digər fiziki parametrlər kimi müxtəlif sensorlardan toplanan məlumatları təhlil edir. Gizli qatlar (hidden layers) isə məlumatları bir neçə mərhələdə emal edir, nümunələri analiz edir və kompleks əlaqələri öyrənir. Bu mərhələdə sensorlardan gələn məlumatlar arasındakı əlaqələr araşdırılır və hər hansı bir anormallıq müəyyən edilə bilər. Nəticə etibarilə, çıxış qatı (output layer) bu məlumatlara əsasən təhdidlərin mövcudluğunu və ya olmamasını müəyyən edir.

Süni neyron şəbəkələri, DDoS hücumları zamanı dronun idarəetmə sistemində və ya şəbəkə trafikində normal davranışdan sapmaları vaxtında aşkar etməyə imkan verir. Belə sapmaların erkən mərhələdə müəyyən edilməsi, potensial hücumların qarşısını almaq üçün vacibdir. Bu yanaşma, dronun təhlükəsizlik sistemlərinin effektivliyini artıraraq, onları kiber təhdidlərə qarşı daha dayanıqlı edir. Süni neyron şəbəkələrinin tətbiqi, dronların təhlükəsizliyini təmin etmək üçün əsaslı və inkişaf etmiş bir texnologiya kimi önə çıxır.



Şəkil 2. Süni neyron şəbəkəsinin arxitekturası

Bu qrafik, DDoS hücumlarını aşkar etmək üçün istifadə olunan sadə bir süni neyron şəbəkəsinin arxitekturasını təsvir edir. Şəbəkə üç əsas qatdan ibarətdir:

4. DDoS hücumlarını aşkar etmək üçün alqoritmin layihələndirilməsi

4.1. Məlumatların yığılması

Süni neyron şəbəkəsinin təlim prosesi üçün bir dataset (verilənlər çoxluğu) nəzərdə tutulur. Bu verilənlər çoxluğu, X matrisindən və Y etiket vektorundan ibarətdir:

- **X (verilənlər matrisi):** X matrisi n×m ölçülüdür. Burada, n=1000 nümunə sayını, m=10 isə hər bir nümunənin xüsusiyyətlərinin (feature) sayını təmsil edir. Bu o deməkdir ki, hər bir nümunə 10 fərqli xüsusiyyətdən ibarətdir.
  - $X \in R^{n \times m}$ X matrisi verilən nümunələrdən ibarətdir və burada hər bir sıra fərqli bir nümunəni, hər bir sütun isə bir xüsusiyyəti təmsil edir. Bu matrisin hər bir sətri X_i bir nümunəyə uyğun gəlir, hər bir sütunu isə bir xüsusiyyətə aiddir. Beləliklə, X matrisinin ümumi forması aşağıdakı kimi təyin olunur:

$$X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{pmatrix}$$

Burada hər bir x_{ij} elementi, i-ci nümunənin j-ci xüsusiyyətini təmsil edir. Bu matris, süni neyron şəbəkəsinin giriş qatında istifadə olunan məlumatları təşkil edir və bu verilənlər əsasında şəbəkə təyin olunur.

Y (hədəf etiketləri vektoru): Y vektoru, hər bir nümunənin uyğunluq etiketlərini təmsil edir. Burada Yi=0 normal trafiki, Yi=1 isə DDoS hücumunu təmsil edir.

- $Y \in \{0,1\}^n$: Hədəf etiketləri vektorudur və burada Y_i hər bir nümunə üçün ya normal trafiki (0) ya da DDoS hücumunu göstərir.

Bu verilən çoxluğu süni neyron şəbəkəsi tərəfindən təlim üçün istifadə edilir. Şəbəkə, DDoS hücumlarını aşkar etmək məqsədilə verilən nümunələri və anormallıqları öyrənir və son nəticə olaraq hücum ehtimalını müəyyən edir. Bu qrafik, sinir şəbəkəsinin necə qurulduğunu və neyronlar arasındakı əlaqələri sadə və aydın şəkildə göstərir, beləliklə DDoS hücumlarının aşkarlanması prosesini başa düşməyi asanlaşdırır. Bu məlumatları əldə etmək üçün **Matlabdan** istifadə edərək sintetik məlumatlar generasiya edilmişdir. Bu verilənlər, süni sinir şəbəkəsi modelinin təlimi üçün istifadə olunacaq. Nümunələrin yarısı (n/2) normal trafik, qalan yarısı isə DDoS hücumlarını təmsil edir.

4.2. Süni neyron şəbəkəsinin qurulması

Süni neyron şəbəkəsinin arxitekturasına və onun fərqli qatlarının funksiyalarına baxaq. Giriş qatında (input layer) 20 neyron yerləşir və bu neyronlar dronun sensorlarından gələn müxtəlif xüsusiyyətləri təmsil edir. Bu xüsusiyyətlər, şəbəkəyə daxil olan məlumatların əsas elementlərini təşkil edir. Gizli qat (hidden layer) isə bu məlumatları emal etmək üçün məsuliyyət daşıyır. Gizli qatda neyronların sayı h olaraq təyin olunur, məsələn, h=20 olaraq seçilə bilər. Gizli qat məlumatları emal edir, nümunələri tanıyır və daha yüksək səviyyəli xüsusiyyətləri çıxarmaq üçün məlumatları hazırlayır.

Çıxış qatı (output layer) şəbəkənin nəticəsini təmsil edir və burada yalnız bir neyron var. Bu neyron, DDoS hücumunun ehtimalını göstərən çıxış dəyərini, yəni $\hat{Y}$ verir. Şəbəkənin hər bir qatı arasında məlumatların necə emal edildiyini və nə nəticələr verdiyini müəyyənləşdirən aktivasiya funksiyaları da mövcuddur. Gizli qatda, ReLU (Rectified Linear Unit) funksiyası istifadə olunur. ReLU funksiyası, mənfi dəyərləri 0-a çevirir və müsbət dəyərləri isə olduğu kimi saxlayır, bu da şəbəkənin qeyri-xətti davranışlarını modelləşdirmək üçün geniş istifadə olunan bir texnikadır. Bu süni neyron şəbəkəsi, DDoS hücumlarını aşkar etmək üçün nəzərdə tutulmuşdur və şəbəkənin müxtəlif qatlarında məlumatların emalı prosesini və alınan nəticələri göstərir.

DDoS hücumlarının aşkarlanması üçün qurulan süni neyron şəbəkəsi (ANN) üç əsas qatdan ibarətdir: giriş qatı (input layer), gizli qat (hidden layer) və çıxış qatı (output layer). Bu qatlardakı neyronlar bir-biri ilə əlaqəlidir və məlumatın işlənməsi bu qatlar arasında həyata keçirilir. Aşağıda bu qatlardan hər biri daha geniş şəkildə izah olunur: Süni neyron şəbəkəsi riyazi olaraq çox qatlı funksiyalardan ibarətdir. Modelin riyazi modeli aşağıdakı kimi verilə bilər:

- **Giriş qatı (input layer):** Giriş verilənləri X matrisində toplanır, burada $X \in R^n$ xüsusiyyətdən ibarət i-ci nümunəni təmsil edir.
- **Gizli qat (hidden layer):** Gizli qatda hər bir neyronun çıxışı aşağıdakı kimi hesablanır:

$$Z^{(1)} = W^{(1)}X + b^{(1)}$$

Burada $W^{(1)}$ gizli qatın ağırlıqlar matrisi, $b^{(1)}$ isə öyrənilən meyl vektorudur. Bu əməliyyatdan sonra aktivasiya funksiyası tətbiq olunur:

$$A^{(1)} = \mathrm{ReLU}(Z^{(1)})$$

Çıxış qatı (output layer): Çıxış qatında sonuncu neyronun çıxışı aşağıdakı kimi hesablanır:

$$Z^{(2)} = W^{(2)}A^{(1)} + b^{(2)}$$

Bu çıxış, adətən bir kvadratik funksiya vasitəsilə ehtimal dəyərinə çevrilir:

$$\hat{Y} = \sigma(Z^{(2)}) = \frac{1}{1 + e^{-Z^{(2)}}}$$

Burada Y^ çıxış dəyəri, yəni DDoS hücumunun ehtimalıdır.

Zərər funksiyası (loss function):

Modelin çıxışını öyrətmək üçün zərər funksiyası istifadə olunur. Zərər funksiyası, modelin nə dərəcədə düzgün proqnoz verdiyini ölçən bir metrikdir. İki sinifli təsnifat üçün ən çox istifadə olunan zərər funksiyası logistik itki (binary cross-entropy) funksiyasıdır:

$$L(Y, \hat{Y}) = -\frac{1}{n}\sum_{i=1}^{n}\left[Y_i \log(\hat{Y}_i) + (1 - Y_i)\log(1 - \hat{Y}_i)\right]$$

Burada:

- Y_i real etiketdir (0 və ya 1);
- $\hat{Y}_i$ modelin proqnozlaşdırdığı ehtimal dəyəridir.

Təlim prosesi

- Modelin öyrədilməsi üçün irəli ötürmə (forward propagation) və geri yayılma (backpropagation) üsulları istifadə olunur;
- İrəli ötürmə (forward propagation): Modelin riyazi tərifində göstərildiyi kimi giriş verilənləri gizli qatlar vasitəsilə ötürülür və çıxış dəyəri (proqnoz) hesablanır;
- Zərər funksiyasının hesablanması: Proqnozlaşdırılan çıxış ilə real etiketlər arasındakı fərq zərər funksiyası ilə hesablanır.

Geri yayılma (backpropagation): Geri yayılma prosesi zamanı zərər funksiyasının hər bir ağırlığa və meylə görə törəmələri hesablanır və bu qiymətlər əsasında modelin ağırlıqları yenilənir. Yenilənmə aşağıdakı şəkildə aparılır:

$$W^{(l)} \leftarrow W^{(l)} - \alpha\frac{\partial L}{\partial W^{(l)}}$$

Burada, α - öyrənmə sürəti (learning rate), $\frac{\partial \dot{w}(1)}{\partial L}$ isə zərər funksiyasının həmin ağırlığa görə törəməsidir.

Təkrarlama: Bu proses təkrarlanaraq, modelin ağırlıqları təlim verilənləri üzərində optimallaşdırılır. Nəticədə model daha dəqiq proqnozlar verə bilir.

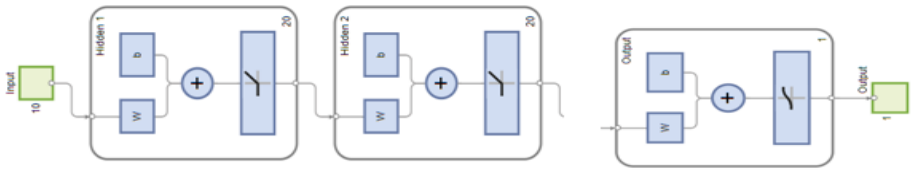
Bu riyazi model, zərər funksiyası və təlim prosesi neyron şəbəkəsinin öyrədilməsini və nəticədə DDoS hücumlarını aşkar etmək üçün istifadə edilən bir modelin necə qurulacağını təsvir edir.

5. DDoS hücumlarını aşkar etmək üçün süni neyron şəbəkəsinə (SNŞ) əsaslanan alqoritmin MATLAB -da realizə olunması

Qeyd olunan alqotimi reallaşdırmaq üçün Matlabın uyğun skript yazılmışdır. Bu şəkil, süni neyron şəbəkəsinin arxitekturasını göstərir və üç əsas qatdan ibarət olan modelin quruluşunu əks etdirir. Şəbəkə iki gizli qat (hidden layers) və bir çıxış qatından (output layer) ibarətdir. İlk gizli qat (hidden layer 1) 20 neyronu ehtiva edir və hər bir neyron ağırlıq (W) və meyl (b) vektorlarına malikdir. Bu qatın sonunda aktivasiya funksiyası tətbiq olunur, bu da neyronların çıxışını hesablayaraq onları növbəti qata ötürür. Aktivasiya funksiyası olaraq ReLU (Rectified Linear Unit) istifadə edilə bilər. İkinci gizli qat (hidden layer 2) də 20 neyronu ehtiva edir və yenə hər bir neyron ağırlıq və meyl vektorlarına malikdir. Bu qatın sonunda da aktivasiya funksiyası tətbiq edilir, bu funksiyalar əvvəlki qatın çıxışlarını transformasiya edərək sonrakı qata ötürür. Bu proses, şəbəkənin daha mürəkkəb nümunələri öyrənməsinə və təsnifat qabiliyyətini artırmasına kömək edir.

Çıxış qatı (output layer) isə tək bir neyronu ehtiva edir. Bu qatın neyronu da ağırlıq və meyl vektorlarına malikdir. Çıxış qatında tətbiq olunan aktivasiya funksiyası, nəticəni ehtimal dəyərinə çevirir.

Ümumilikdə, bu süni neyron şəbəkəsi iki gizli qatdan və bir çıxış qatından ibarət olub, hər bir gizli qatda 20 neyron yerləşdirilmişdir. Bu arxitektura, modelin məlumatları emal etməsini və son nəticəni proqnozlaşdırmasını təmin edir. Model, DDoS hücumlarını aşkarlamaq üçün verilənlər üzərində təlim keçir və nəticədə hücum ehtimalını proqnozlaşdırır. Bu quruluş, əsasən klassifikasiya məsələlərində istifadə olunan tipik bir süni neyron şəbəkəsi arxitekturasıdır.



Şəkil 3. DDoS hücumlarının aşkarlanması üçün neyron şəbəkəsinin Matlab-da qurulan arxitekturası

Bu məsələdə, DDoS hücumlarının aşkarlanması üçün süni neyron şəbəkəsinin qurulması, təlimi və qiymətləndirilməsi mərhələləri həyata keçirilmişdir. İlk addımda, 1000 nümunədən ibarət bir verilənlər toplusu generasiya edilmiş, hər bir nümunə 10 xüsusiyyətə malik olmuşdur. Verilən nümunələrdən ilk 500-ü normal trafik, son 500-ü isə DDoS hücumu kimi etiketlənmişdir. Verilənlər daha sonra təsadüfi olaraq qarışdırılmışdır.

İkinci addımda, modelin gücünü artırmaq üçün iki gizli qat əlavə edilmiş və hər bir qata 20 neyron təyin edilmişdir. Gizli qatlarda ReLU (Rectified Linear Unit) aktivasiya funksiyası, çıxış qatında isə sigmoid funksiyası istifadə edilmişdir. Üçüncü mərhələdə, verilənlər 80% təlim və 20% test üçün bölünmüşdür.

Dördüncü mərhələdə, modelin təlim prosesi həyata keçirilmişdir. Şəbəkə təlim verilənləri üzərində öyrədilmişdir. Beşinci mərhələdə isə model test verilənləri üzərində sınaqdan keçirilmiş, proqnozlar yaradılmış və nəticələr qiymətləndirilmişdir.

Altıncı mərhələdə, modelin performansı qarışıq matrisi və dəqiqlik kimi metriklərlə qiymətləndirilmişdir. Precision, recall və F1 skoru kimi əlavə metriklər də modelin dəqiqliyini və səhvlərini təhlil etmək üçün hesablanmışdır. Yeddinci mərhələdə, təlim və test dəstlərindəki dəqiqlik müqayisə edilərək modelin overfitting (həddən artıq uyğunlaşma) və ya underfitting (çox az uyğunlaşma) problemi olub-olmadığı təhlil edilmişdir.

Son mərhələdə, model k-fəld (k-fold) kros-valiadasiya ilə sınanmış və orta dəqiqlik və F1 skoru təyin olunmuşdur. Nəticələr göstərmişdir ki, model təlim dəstində nisbətən yaxşı nəticələr versə də, test dəstində dəqiqlik aşağıdır və model overfitting problemi ilə üzləşmişdir. Bu da modelin daha geniş təlim verilənləri və ya parametrlərin optimallaşdırılması ilə yaxşılaşdırılmasının vacibliyini vurğulayır. Proqram işlədikdən sonra aşağıdakı performans göstəriciləri də nəticə olaraq verilmişdir. Bu nəticələr modelin performansını təhlil etmək üçün vacib məlumatlar verir və müəyyən problemlərə işarə edir:

- **Dəqiqlik:** Modelin test dəstində əldə etdiyi dəqiqlik 88.00% olaraq qeyd edilmişdir. Bu, modelin ümumi olaraq düzgün təsnifat etmə qabiliyyətinin nisbətən yüksək olduğunu göstərir. Lakin, digər metriklərə nəzər saldıqda, bu yüksək dəqiqliyin modellə bağlı bəzi problemləri gizlədə biləcəyini görə bilərik;
- **F1 skoru:** F1 skoru 0.86 olaraq verilir ki, bu da təsnifat balansının və modelin düzgün işləmə qabiliyyətinin yaxşı olduğunu göstərir. F1 skoru, modelin pozitiv və neqativ təsnifatlar arasındakı dəqiqliyini ölçdüyü üçün, bu dəyər modelin müəyyən hallarda yaxşı performans göstərdiyini ifadə edir;
- **Təlim dəqiqliyi:** Modelin təlim dəsti üzərində əldə etdiyi dəqiqlik 92.12%-dir. Bu, modelin təlim verilənləri üzərində çox yaxşı öyrəndiyini göstərir, lakin bu da potensial overfitting problemi göstəricisi ola bilər;
- **Test dəqiqliyi:** Test dəstindəki dəqiqlik 51.00% olaraq ölçülmüşdür. Bu, test dəstində modelin performansının ciddi şəkildə azaldığını göstərir və onun ümumiləşdirmə qabiliyyətində böyük çatışmazlıqlar olduğunu bildirir;
- **Həddindən artıq uyğunlaşma (overfitting)-:** Təlim dəsti üzərində yüksək dəqiqlik (92.12%) və test dəsti üzərində çox aşağı dəqiqlik (51.00%) modelin ciddi şəkildə həddindən artıq uyğunlaşdığını **(overfitting)** göstərir. Bu, modelin təlim verilənlərindəki nümunələri əzbərlədiyini, lakin yeni verilənlər üzərində zəif performans göstərdiyini nümayiş etdirir;
- **Orta dəqiqlik:** Kros-valiadasiya nəticələrinə görə, modelin orta dəqiqliyi 59.50%-dir. Bu, modelin müxtəlif bölmələrdəki performansının stabil olmadığını və yaxşı ümumiləşdirmə qabiliyyətinə malik olmadığını göstərir;
- **Orta F1 skoru:** Orta F1 skoru 0.62 olaraq verilmişdir, bu da modelin müxtəlif bölmələrdə balanslı təsnifat nəticələri göstərməkdə çətinlik çəkdiyini göstərir.

Proqramın işləməsi nəticəsində hücum ehtimalının hesablanması baş verir. Test dəstində hər bir nümunənin ehtimal dəyəri çıxış olaraq verilir. Bu dəyərlər 0.5-dən böyükdürsə, DDoS hücumu aşkar edilmiş sayılır və hücum indexi Ypred =1 qiymətini alır. Bundan başqa, birbaşa **hücum ehtimalının qiymətləri də hesablanır (**Y_pred_probs).

Nəticə

Nəticə göstərir ki, model təlim verilənləri üzərində yüksək performans göstərir, lakin test verilənlərində bu performansı təkrarlaya bilmir. Bu, modelin ciddi şəkildə həddindən artıq uyğunlaşdığını (overfitting) və təlim verilənlərini əzbərlədiyini, lakin yeni verilənlər üzərində zəif performans göstərdiyini nümayiş etdirir. F1 skoru nisbətən yüksək olsa da test dəsti üzərindəki aşağı dəqiqlik, modelin ümumiləşdirmə qabiliyyətinin zəif olduğunu təsdiqləyir. Bu problemi aradan qaldırmaq üçün modelin təlim prosesi optimallaşdırılmalı, requlərizasiya üsulları tətbiq edilməli və verilənlər üzərində daha effektiv bir analiz aparılmalıdır.

Ədəbiyyat

1. Akram, R. N., Markantonakis, K., Mayes, K. Secure and trusted execution in mobile devices: Using Public-Key Cryptography in Drones // Mobile Security and Privacy, – 2014. – pp. 245-267. Springer.

2. Hooper, A. Securing Drone Data: The Need for End-to-End Encryption // Journal of Information Security, – 9(2), – 2018. – pp. 63-72.

3. Hayajneh, T., Mohd, B.J., & Almashaqbeh, G.A. Secure control of drones: protecting wireless communications from hijacking attacks // IEEE Communications Magazine, – 2016, – 54(5), – pp.75-81.

4. Shafique, K., Khawaja, B. A., Khurram, M., & Qazi, S. Internet of drones (IoD): threats, vulnerabilities, and security challenges // Elsevier Ad Hoc Networks, 83, – 2018. – pp. 96-111.

5. Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., & Kintner, P.M. Assessing the spoofing threat: development of a portable GPS civilian spoofer // Proceedings of the institute of navigation GNSS Conference. – 2008

6. Shuai, H., Lu, J., & Sun, W. GPS Spoofing detection for UAVs based on high-speed motion constraints // Sensors, – 19(8), – 2019.

7. Hamza, A., Arafat, M. Y., & Mirza, M. Defense against DDoS attacks on UAV networks // IEEE International Conference on Communications, – 2018, – pp.1-6.

8. Wang, P., Zhu, Z., & Xia, H. A Security Framework for drones against cyber attacks // Security and communication networks, Article ID 1565123, – 2019. – 9 p.

Elmi Əsərlər
Proceedings of Science

Heydər Əliyev adına Hərbi İnstitutun **Elmi Əsərlər** jurnalı, Cild 22, № 2, 2024 / 43-50
Proceedings of Science of the Military Institute named after Heydar Aliyev, Volume 22, № 2, 2024 / 43-50

Daxilolma tarixi / Received date: 15.07.2024
Qəbulolma tarixi / Accepted date: 16.09.2024

DOI: 10.30546/8967.2024.22.2.1017

İNFORMASİYA ŞƏBƏKƏLƏRİ ÜZƏRİNDƏ QURULMUŞ İDARƏETMƏ SİSTEMLƏRİNDƏ TƏTBİQ EDİLƏN MARŞRUTİZATORLARIN FUNKSİONAL MODELİNİN TƏKMİLLƏŞDİRİLMƏSİ VƏ TƏDQİQİ

Ənvər Həzərxanov
texnika elmləri doktoru, professor
Heydər Əliyev adına Hərbi İnstitut, Bakı
E-mail: enver-xan@mail.ru

Vasif Neymətov
Azərbaycan Dövlət Neft və Sənaye Universiteti, Bakı
E-mail: vasif.nematov.a@asoiu.edu.az

Xülasə

Məqalənin mövzusu müasir və aktual olub, informasiya şəbəkələri üzərində qurulmuş idarəetmə sistemlərində marşrutizatorun funksional modelinin təkmilləşdirilməsi və tədqiqinə həsr olunmuşdur. İnformasiya şəbəkələri ilə təchiz edilmiş idarəetmə sistemlərinin dayanıqlılığı, digər ehtiyat əmsalları ilə yanaşı, həmçinin rabitə kanalının imtinaları və bərpaları əmsallarına görə də müəyyən ehtiyata malik olmaqla qiymətləndirilir. Bu ehtiyat əmsalları marşrutizatorun işlək, imtinalar və bərpa vəziyyətləri arasında keçid ehtimallarına təsir etməklə, dayanıqlılığı müəyyən edirlər. Lakin təklif edilən təkmilləşdirilmiş modeldə şəbəkə taymerinin müəyyən etdiyi zaman intervalında xarici təsirlərin olmasına baxmayaraq, marşrutizatorun olduğu vəziyyətlərinin qərarlaşmış hallarını qoruyub saxladığı öz-özünə keçidləri də əks etdirir. Riyazi mənada belə öz-özünə keçidlər xətti bircins diferensial tənliklərlə təsvir edilmişlər. Məhz bu tənlikləri nəzərə almaqla əldə edilmiş həllərin əsasında asılılıq qrafikləri qurulmuş, alınmış qrafiki nəticələr təhlil edilmişdir. Əldə olunmuş əsas nəticə ondan ibarətdir ki, bu qərarlaşmış hallar imtina və bərpa intensivlikləri əmsallarının orta qiymətinə nəzərən 8-10%-i qədərində mümkündür.

Açar sözlər: marşrutizator, rabitə kanalı, imtinalar və bərpaolunma intensivliklərinin əmsalları, idarəetmə sistemi, dayanıqlıq, vəziyyətlərarası keçid ehtimalları.

IMPROVEMENT AND RESEARCH OF THE FUNCTIONAL MODEL OF THE ROUTER USED IN CONTROL SYSTEMS BASED ON INFORMATION NETWORKS

Enver Hazarkhanov
doctor of technical sciences, professor
Military Institute named after Heydar Aliyev, Baku

Vasif Neymatov
Azerbaijan State Oil and Industry University, Baku

Abstract

The topic of the article is devoted to the study of an improved router model of the branch system, built on the basis of an information network and thus is relevant and modern. Stability of a control system equipped with information networks, in addition to other coefficients for stability reserves, communication channels should also have coefficients for reserves of failures and recoveries. These coefficients, by their effects on the probabilities of transitions between the operational state, failure states and recoveries, affect the stable state of the overall system. But in the proposed improved model, transitions to oneself are shown, preserving the established states in the presence of external influences during time, the interval of which is determined by the network timer. The mathematical meaning of such transitions on oneself is expressed using homogeneous linear differential equations. The construction of dependency graphs and the analysis of the half-finished graphical results was carried out

precisely on the basis of those solutions. In which these differential equations were taken into account. The main result obtained is that the presented setable states are possible only when the values of the coefficients of failure and recovery rates are equal to 8-10% of their average values.

Keywords: router, communication channel, failure and recovery rates, control system, stability, probability of transitions between states.

УСОВЕРШЕНСТВОВАНИЕ И ИССЛЕДОВАНИЕ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ МАРШРУТИЗАТОРА, ПРИМЕНЯЕМОГО В СИСТЕМАХ УПРАВЛЕНИЯ, ПОСТРОЕННЫХ НА ОСНОВЕ ИНФОРМАЦИОННЫХ СЕТЕЙ

Энвер Хезерханов
доктор технических наук, профессор
Военный Институт имени Гейдара Алиева, Баку

Васиф Нейматов
Азербайджанский Государственный Университет
Нефти и Промышленности, Баку

Аннотация

Тема статьи посвящена исследованию усовешенстной модели маршрутзатора системы управления, построенной на основе информационной сети и тем самым является актуальной и современной. Устойчивость системы управления, оснащенной информационными сетями, помимо иных коэффициентов по запасам устойчивости, также должны иметь коэффициенты по запасам отказов и восстановлений канала связи. Эти коэффициенты своими воздействиями на вероятности переходов между работоспособным состоянием, состояниями отказов и восстановлений влияет на устойчивое состояние общей системы. Но в предложенной усовершенственной модели показаны переходы на самого себя, сохраняющие установившие состояния при наличии внешних воздействий в течении времени, интервал которого определяется со стороны сетевого таймера. Математический смысл подобных переходов на самого себя выражается с помощью однородных линейных дифференциальных уравнений. Построение графиков зависимостей и анализ полученных графических результатов осуществлялся именно на основе тех решений, в которых были учтены эти дифференциальные уравнения. Основной полученный результат заключается в том, что представленные устанавливаемые состояния возможны только при значениях коэффициентов интенсивностей отказов и восстановления, равными на 8-10% от их средних значений.

Ключевые слова: маршрутизатор, канал связи, коэффициенты интенсивностей отказов и восстановлений, система управления, устойчивость, вероятность переходов между состояниями

Giriş

Marşrutizatorların modelləşdirilməsinə həsr olunmuş elmi işləri əks etdirən internet ədəbiyyatının xülasəsini ümumiləşdirərək aşağıdakı üç tipik məqalə üzərindən belə formalaşdırmaq olar. Bir qisim elmi işlərdə marşrutizatorların modelləşdirilməsi, onların protokolları üzərindən aparılmışdır. Belə ki, [1] elmi işində NS-3 sistemində QoS metodlarının realizasiyasını təmin edən marşrutizatorların modelləşdirilməsi zamanı qarşıya çıxan problemlər təhlil edilmiş, bu təhlil əsasında müəlliflər tərəfindən təklif edilən həll üsulu budur ki, bu problemlər OSİ açıq tipli şəbəkənin tətbiqi səviyyəsində həll edilsin.

Məsələnin bu formada qoyuluşu və həlli istiqamətində aparılmış tədqiqatların nəticəsi olaraq, müəlliflərin son qənaətinə görə təklif edilmiş modelləşdirmə üsulu NS-3 sistemində intellektual marşrutizatorun realizasiyasını təmin edə bilər, həmçinin NS-3 sisteminin yeni modifikasiyaları ilə də tam uyğunlaşma bacarığına malikdir.

Lakin NS-3 sisteminin öz təsnifat sinfində malik olduğu bir sıra unikal üstünlüklərinə, yəni bütün komponentləri üçün açıq çıxış koduna, modelləşdirmənin baza proqramlaşdırma dili kimi “C++”-dan istifadə etmək imkanına, protokol proqramının CPL lisenziyası əsasında yayılması imkanına, Lunix əməliyyat sistemində işləmə qabiliyyətinə malik olmasına baxmayaraq, təklif edilən model QoS sisteminin yüksək səviyyəli digər şəbəkə sistemləri ilə qarşılıqlı qoşulmada və mübadilədə tətbiq edilə bilməz.

Növbəti tipik hal [2] elmi işi əsasında izah edilə bilər. Belə ki, bu tip məqalələr marşrutizatorların modelləşdirilməsinin zəruriliyini təsbit edən müasir və aktual bir probləmə - informasiya sistemlərində və şəbəkələrində marşrutizatorların növbələşmələrinin idarə edilməsi alqoritmlərinin yaradılmasına həsr

edilmişdir. Məqalədə şəbəkədə marşrutizasiya prosesinin idarə edilməsi prosesinin müasir təsviri verilmiş, marşrutizasiya prosesi qeyri-xətti proses kimi tədqiq edilmiş, onun üçün gecikməsi olan qeyri-xətti diferensial tənliklər sistemi tərtib edilmiş, sistemin məxsusi həlləri əsasında xarakteristik xüsusiyyətlər müəyyən edilmişdir.

Marşrutizatorlarda buferləmə parametrlərinin rabitə kanalının cəldliyinə, kanalda ötürmə sürətinin stabilliyinə və digər istismar parametrlərinə əhəmiyyətli təsiri əsaslandırılmışdır. Bu məsələlərin tədqiqinin texniki sistemlər üçün real əhəmiyyəti ondan ibarətdir ki, informasiya şəbəkələri üzərində qurulan idarəetmə sistemlərində (çoxsəviyyəli, paylanmış idarəetmə sistemləri) sistemin dayanıqlığı korlana, yaxud tamamilə yox ola bilər, idarəetmənin və tənzimlənmənin keyfiyyət göstəriciləri tələb olunan səviyyədə təmin olunmaya bilər. Müəlliflər əsaslandırmışlar ki, marşrutizatorların buferləmə parametrlərinin düzgün təyin edilməməsi səbəbindən rabitə kanalında informasiyanın ötürmə sürətinin stabilliyinin pozulması daha çox, praktiki olaraq, rəqslərin yaranması ilə müşayiət olunan fəsadlar törədir. Bu fəsadların paylanmış idarəetmə sistemlərində nisbətən daha çox neqativ təsirlərə malik olduğunu bildirən müəlliflər bu amili onunla əsaslandırmışlar ki, belə idarəetmə sistemlərində informasiya ötürülməsinin yüksək cəldliyinin təmin olunması tələbi ilə yanaşı olaraq, idarəetmə sistemi boyunca paylanan informasiyanın sərt alqoritmli sinxronizasiyasının da təmin edilməsi tələb olunur. Üstəlik, onu da qeyd etmək lazımdır ki, paylanmış avtomatik idarəetmə sisteminin konfiqurasiyası mürəkkəbləşdikcə informasiyanın sinxronizasiyasının korlanması daha da ağırlaşır. Beləliklə, məqalədə tərtib edilmiş qeyri-xətti diferensial tənliyin tapılmış ayrı-ayrı həllərinin modelləşdirilməsi yerinə yetirilmiş və həllərin ümumi xarakterini nəzərə alaraq, təklif olunan modelləşdirmə üsulunun yalnız Ethernet şəbəkəsi üçün yararlılığı təsdiq edilmişdir.

[3] elmi işi və ona analoji digər əsərlərdə marşrutizatorun funksional fəaliyyəti modelləşdirilmişdir. Bu tip tədqiqat işlərinin fərqli xüsusiyyətləri, əsasən onunla müəyyən edilir ki, burada marşrutizator yalnız aparat vasitəsi kimi tədqiq edilmiş, onun protokol tərəfinə toxunulmamışdır. Belə yanaşmanın üstünlüyü odur ki, marşrutizatorun özü ümumiyyətlə, rabitə şəbəkələrinin texniki vasitəsi kimi tədqiq edilir. Yəni tədqiqatın istiqaməti nisbətən daha da konkretləşdirilərək, proqram təminatına toxunulmamış, əldə edilmiş nəticələr isə istismar edilən bir texniki vasitə kimi mümkün qədər ümumiləşdirilmişdir.

Təqdim olunan məqalədə marşrutizatorun funksional olaraq, nisbətən təkmilləşdirilmiş modeli yaradılmış və şəbəkədə baş verən imtinaların timsalında qəbul edilən xarici həyəcanlandırıcı təsirin altında istismar parametrlərinin dəyişməsi tədqiq edilmişdir.

1. Məsələnin qoyuluşu

[4] məqaləsinə istinad edərək, belə qənaətə gəlmək olar ki, informasiya şəbəkələri üzərində qurulan avtomatik idarəetmə sistemlərinin dayanıqlılığının təmin edilməsi problemi məlum səbəblərlə yanaşı, şəbəkədə yaranan imtinalara görə də korlana bilər. İnformasiya şəbəkələri tətbiq edilən idarəetmə sistemlərində bu neqativ təsir destruktiv təsir kimi də adlanır. Belə bir prizmadan yaxınlaşdıqda, marşrutizator idarəetmə sisteminin dayanıqlılığını destruktiv təsirlərdən şəbəkə səviyyəsində qoruyan texniki vasitə kimi qiymətləndirilir. Nəticə etibarilə, belə yanaşmanın marşrutizatorların modelləşdirilməsi zamanı formalaşdırdığı əsas tədqiqat vəzifəsi ondan ibarət olur ki, informasiyanın rabitə şəbəkəsində paketli ötürülməsinin təşkili (müvafiq protokol da nəzərə alınmaqla) imtinalara qarşı dayanıqlılığı qorumaq səviyyəsinə malik olmalıdır. Məhz bu vəzifəyə uyğun gələn modeldə marşrutizator işləmə prinsipinə uyğun olaraq, müxtəlif vəziyyətlər arasında keçid prosesi şəklində təqdim edilmişdir (şəkil 1).

Modeldə əsas tədqiq edilən parametrlər aşağıdakılar seçilmişdir:

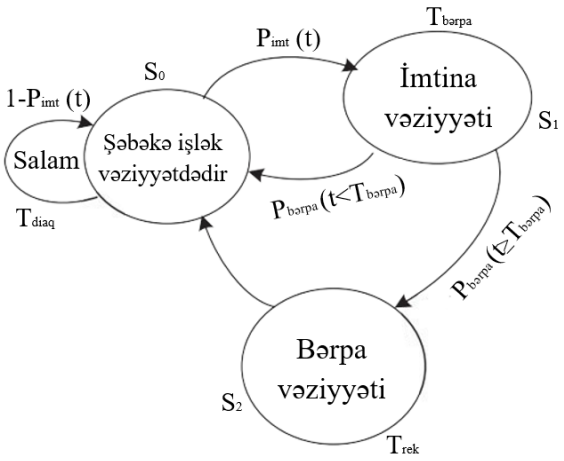
- $P_{imt}(t)$ - imtina ehtimalı;
- $P_{bərpa}(t)$ - bərpaolma ehtimalı;
- $T_{bərpa}$ - bərpaolunma müddəti.

Yəni şəkil 1-də təklif edilən model marşrutizatoru ya işlək, ya da işlək halından çıxmış (o da elə bərpa olunma prosesi deməkdir) vəziyyətdə təsvir edir. Əgər idarəetmə sisteminin tərkibindəki rabitə kanalı $P_{imt}(t)$ ehtimalı ilə imtina edibsə, marşrutizator öz işçi vəziyyətini S_0 vəziyyətindən S_1 vəziyyətinə dəyişir. Marşrutizatorun S_1 vəziyyətinin təsviri belədir: imtina bitdikdən sonra yeni rekonfiqurasiya

haqqında heç bir qərar yoxdur və bu şərt daxilində kanalın diaqnostikasını yerinə yetirən paket çatdırılmayıb, buna görə də T_{diaqc} müddəti təsadüfi nasazlığın yaranıb, davametmə periodunu təyin edir. Bu zaman çərçivəsində informasiya axınının marşrutlanması əvvəlki cədvəllər əsasında yerinə yetirilir.

Əgər uğursuzluq təsadüfi olmayıb, destruktiv təsirlərin marşrutizatorun işində yaratdığı fəsadlardan biri kimi yaranırsa, bu informasiyanın itirilməsinə səbəb olur. Nəticə etibarilə, bu və ya digər səbəbdən S_1 vəziyyətinə keçid heç də arzuolunan keçid olmadığı üçün marşrutizatorun bu vəziyyəti informasiya şəbəkəsinin və onun üzərində qurulan idarəetmə sisteminin dayanıqsızlığı zəifləmiş, yaxud tamam yox olmuş vəziyyətidir.

Rabitə kanalı $T_{bərpa}$ müddətində öz iş qabiliyyətini bərpa etdikdə (əgər bərpa mümkün olarsa) sistem $S_1 \rightarrow S_0$ keçidi ilə işlək vəziyyətinə qayıdır. Əksinə, əgər $T_{bərpa}$ dövründə rabitə kanalı bərpa edilmədiyi təqdirdə, sistem T_{rek} dövründə $S_1 \rightarrow S_2$ keçidini edir və əldə etdiyi yeni vəziyyətində matşrutizator marşrutlaşdırma cədvəllərinin yenilənməsini həyata keçirir. Yenilənmə müddəti bitdikdən sonra işlək vəziyyət $S_2 \rightarrow S_0$ keçidi ilə əldə edilir.



Şəkil 1. Marşrutizatorun funksionallaşdırılması prosesinin modeli

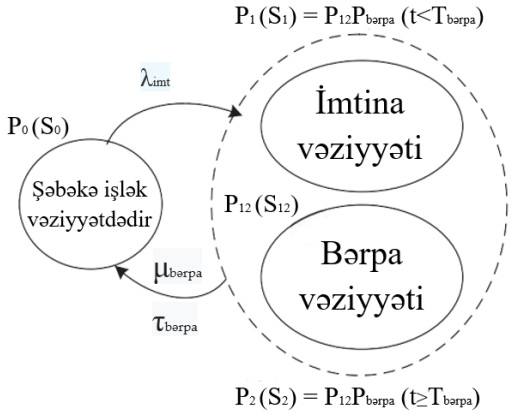
Beləliklə, tərtib edilmiş modelə əsasən:

✓ S_0 – "Şəbəkə işlək" vəziyyətdədir, marşrutizator və rabitə kanalı işləyir;

✓ S_1 – "İmtina" vəziyyətidir, marşrutizatora qoşulmuş hər hansı bir rabitə kanalından imtina baş versə də marşrutizator imtina qəbul edilmiş rabitə kanalına paketləri göndərməkdə davam edir;

✓ S_2 – "Bərpa" vəziyyətidir, şəbəkə topologiyasının dəyişdirilməsi haqqında qərarın qəbul edilməsi və marşrutlaşdırma cədvəlinin müvafiq formada yenilənməsi.

Bu model vəziyyət keçidləri modeli kimi də adlandırıla bilər. Rabitə kanalının informasiya sistemlərində baş verən imtina və bərpa prosesləri üçün Puasson axını şərtlərini nəzərə alsaq, gətirilmiş Markov dövrələrini (proseslərini) əks etdirən modelə keçid etmək olar (şəkil 2) [5].



Şəkil 2. Marşrutizatorun modelinin Markov dövrələrinə gətirilməsi sxemi

Bu şərtlərə görə, yəni:

- əgər hər hansı mürəkkəb sistemin elementlərinin imtinaları gözlənilmədən, birdən yaranarsa;
- istənilən elementin imtinası bütün sistemin imtinasına səbəb olarsa;
- elementlərin aşınması gözlənilməz deyilsə, onda belə imtinalar seli qeyri-stasionar Puasson imtinaları adlanırlar [6].

Sel yarada bilən təsadüfi imtinalar Puasson qanununa tabedirlər: $\{t_0,t_0+\Delta t\}$ intervalında m sayda imtinaların yaranması ehtimalı - P_m selin intervalda müşahidə olunma müddətindən və sel axınının zaman oxu boyunca səpələnməsindən asılıdır [7].

Aşağıdakı tənliklər sistemi bu prosesin vəziyyətlərinin son ehtimallarına uyğundur:

$$\begin{cases} \frac{dP_0}{dt} = \mu_{bərpa} P_{12}(t) - \lambda_{imt} P_0(t) \\ \frac{dP_{12}}{dt} = \lambda_{imt} P_0(t) - \mu_{bərpa} P_{12}(t) \end{cases} \quad (1)$$

və

$$\begin{cases} P_1(t) = P_{12}(t) * P_{bərpa}(t < T_{bərpa}) \\ P_2(t) = P_{12}(t) - P_1(t) \\ P_0(t) + P_1(t) + P_2(t) = 1 \end{cases} \quad (2)$$

Bu zaman sistemin S_1 və S_2 vəziyyətində olma ehtimalı $T_{bərpa}$ dövründə rabitə kanalının bərpası ehtimalı ilə müəyyən ediləcək:

$$\begin{cases} P_1(t) = P_{12} * P_{bərpa}(t < T_{bərpa}) = P_{12}(1 - e^{-\mu_{bərpa} T_{bərpa}}) \\ P_2(t) = P_{12} * (t \geq T_{bərpa}) = P_{12} * e^{-\mu_{bərpa} T_{bərpa}} \end{cases} \quad 3)$$

Beləliklə, tədqiqatın əsas məsələsini aşağıdakı kimi formalaşdırmaq olar:

Şəkil 1-də və şəkil 2-də göstərilmiş modelləri təkmilləşdirməklə, (2) tənliklər sistemini stasionar hala gətirmək, əldə edilmiş həllər əsasında marşrutizatorun əsas parametrlərini qiymətləndirmək.

2. Məsələnin həlli

Marşrutizatorun funksional modelini təkmilləşdirmək məsələsinin həllinə yanaşmada nəzərə almaq lazımdır ki:

- trafiklərin strukturlarının təsirləri, kütləvi xidmət sistemi kimi, funksiyaları tədqiq edilməlidir;
- bufer parametrlərinin təsirinin qiymətləndirilməsi aparılmalıdır;
- informasiya sellərinin paylanılması alqoritmlərinin təsirləri müqayisəli təhlil edilməlidir.

Tərəfimizdən aparılan nəzəri tədqiqatlarda marşrutizatorların elə modeli qurulmuşdur ki, bu model etibarlılığın məhdud ödənilməsi şəraitində informasiya selinin təkanlı dəyişməsi və imtinaların yaranması zamanı dayanıqsızlığın aradan qaldırılması problemini təhlil etmişdir.

Marşrutizator üçün təklif edilən yeni funksional model şəkil 3-də göstərilmişdir.

.

Şəkil 3. Marşrutizatorun vəziyyət-keçid-vəziyyət modeli

Modelin əsasında aşağıdakı vəziyyət keçidlərini təsvir etmək mümkündür:

- dayanıqlı vəziyyətdən çıxma halı - imtinaların yaranması ehtimalı ilə müəyyən edilir;
- dayanıqlı vəziyyətə qayıtma halı - bərpaların baş verməsi ehtimalı ilə təyin edilir;
- yaranmış imtinaların saxlanılması - bərpaların baş vermə ehtimalının olmaması;
- bərpaların saxlanılması - imtinaların baş vermə ehtimalının olmaması.

Sonuncu iki vəziyyətin tədqiqi məhz təkmilləşdirilmiş modelin hesabına mümkün olmuşdur. Nəzərə almaq lazımdır ki, bu hallar marşrutizatorun malik olduğu vəziyyəti kənar təsirlərə məruz qalmadığı qapalı, stasionar sistemlərə çevirir. Belə qapalı sistemlər üçün yazılan diferensial tənliklər təbii ki, bircins, xətti diferensial tənliklərdir.

Şəkil 3-də göstərilən funksional model əsasında marşrutizatorun tədqiqinin əsas məsələləri ondan ibarət olmalıdır ki, bütün vəziyyətlərdə qalma, vəziyyətlərarası keçidlərin başvermə ehtimallarının imtinaların intensivliyindən asılılıqları təsvir edilsin.

Stasionar proses qərarlaşarsa, onda buna uyğun gələn həllərdən ibarət olan tənliklər sistemi aşağıdakı kimi olacaq:

$$:\begin{cases} 0 = -\lambda_{imt} P_0 + \mu_{bərpa} P_{12} \\ 0 = \lambda_{imt} P_0 - \mu_{bərpa} P_{12} \\ P_1(t) = P_{12} * P_{bərpa}\left(t < T_{bərpa}\right) \\ P_2(t) = P_{12} * P_1(t) \end{cases} \quad (4)$$

Sadə riyazi çevrilmələrdən sonra asanlıqla:

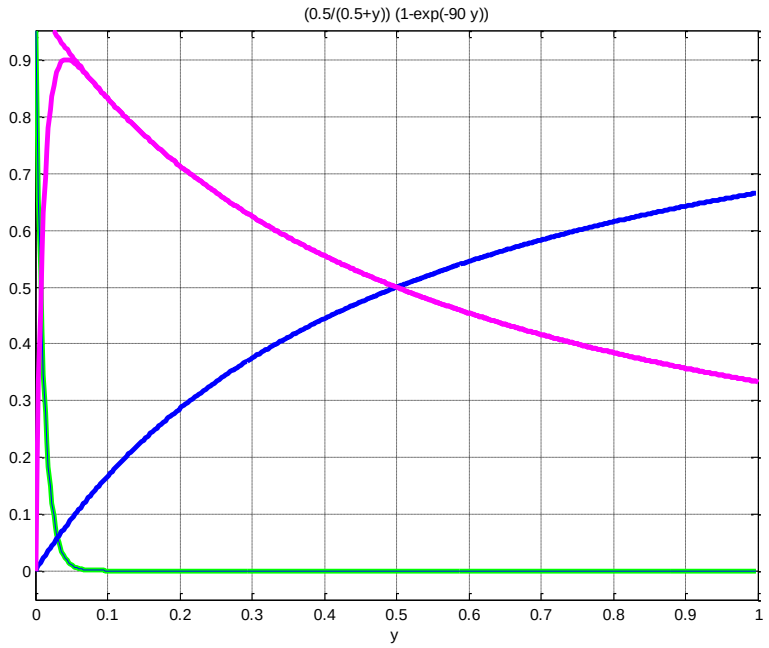
$$\begin{cases} P_{12} = \frac{\lambda_{imt}}{\lambda_{imt} + \mu_{bərpa}} \\ P_0 = 1 - P_{12} \\ P_1(t) = P_{12} * P_{bərpa}\left(t < T_{bərpa}\right) \\ P_2(t) = P_{12} - P_1(t) \end{cases} \quad (5)$$

tənliklər sistemini, nəhayət, imtinalar və bərpaolunma intensivliklərini nəzərə almaqla isə:

$$\begin{cases} P_0 = 1 - \frac{\lambda_{imt}}{\lambda_{imt} + \mu_{bərpa}} \\ P_1 = \frac{\lambda_{imt}}{\lambda_{imt} + \mu_{bərpa}} (1 - e^{-\mu_{bərpa} T_{bərpa}}) \\ P_2 = \frac{\lambda_{imt}}{\lambda_{imt} + \mu_{bərpa}} * e^{-\mu_{bərpa} T_{bərpa}} \end{cases} \quad (6)$$

tənliklər sistemini yazmaq olar.

Şəkil 4-də (6) həlləri əsasında Matlab proqram mühitində imtinasız, imtinalı və bərpalı vəziyyətlərarası keçidlərin başvermə ehtimallarının imtina və bərpa intensivliklərindən asılılıqları göstərilmişdir. Qrafiklərin qurulması üçün istifadə olunmuş ədədi qiymətlər: imtina intensivliyi - 0.5; marşrutizatorun taymerinin perioda qayıtdığı zaman müddəti - T=90 san olmuşdur.



Şəkil 4. Funksional modellə müəyyən edilən vəziyyətlərarası ehtimalların intensivliklərdən asılılıq qrafikləri:
çəhrayı qrafik - $P_1=f(\mu_{bərpa})$; mavi qrafik - $P_0=f(\mu_{bərpa})$; yaşıl qrafik - $P_2=f(\mu_{bərpa})$

Qrafiklərin təhlili nəticəsində aşağıdakıları bildirmək olar:

1. İmtina və bərpa intensivliklərinin bərabərqiymətli halında marşrutizatorun dayanıqlılığı təmin edilir;
2. Bərpa intensivliyinin 0.2 qiymətinə qədər marşrutizatorun dayanıqsızlığı hələ ki davam edə bilər;
3. İmtinaların təsadüfi halında marşrutizatorun dayanıqlılığı bərpa intensivliyinin təqribən 3.05 qiymətinə qədər təmin edilə bilər;
4. İmtinalar təsadüfi yarandığı halda, marşrutizatorun əvvəlki cədvəllərlə dayanıqlı işlək vəziyyətinin ən yaxşı halı ($P_1=f(\mu_{bərpa})=0.9$) seçilmiş imtina intensivliyinin təqribən 8-10%-ə qədər hissəsində təmin edilə bilər.

Nəticə

1. Tədqiq edilən marşrutizatorun formalizasiyasını müəyyən edən riyazi tənliklər əsasında onun diferensial tənliklərinin həllərinin qrafikləri stasionarlıq şərtlərinin həqiqiliyini təsdiq edir.

2. Qurulmuş asılılıqlar, əsasən iki parametrə görə tədqiq edilmişdir - rabitə kanalında imtinaların və bərpaların intensivlik əmsalları. Tədqiqatlar zamanı müəyyən edilmişdir ki, imtinaların intensivlik əmsalı sistemin bərpası ehtimalının 30%-i qədər olduqda marşrutizatorun işlək qabiliyyəti 80% saxlanılır. Lakin bundan sonra intensivliklərin artması rabitə kanalının tamamilə işlək vəziyyətdən kənarlaşmasına səbəb olur.

3. Marşrutizatorun işlək qabiliyyəti üçün ən dayanıqsız şərait o zaman yaranır ki, imtinaların intensivlik əmsalı nisbi qiymətlə götürüldükdə şəbəkənin konfiqurasiyasının cari stasionar vəziyyətinin saxlanılması müddətindən çox olsun. Bu zaman intensivliklərin özləri marşrutizatorun daxili dayanıqlılığını təmin etməyə imkan verməyənə qədər yüksək olur.

Ədəbiyyat

1. Соснин, В.В., Шинкарук, Д.Н. Моделирование маршрутизатора с поддержкой методов QoS в среде NS-3

2. Туманов, М.П., Абдуллин, С.Р. Моделирование нелинейной системы маршрутизации (AQM) в Ethernet. Лесной вестник математичекое моделирование. – 2/2015. – с.115-120.

3. Математическая модель анализа многоадресной маршрутизации в мультисервисной сети связи [Электронный ресурс] / URL:https://cyberleninka.ru/article/n/matematicheskaya-model-analiza-mnogoadresnoy-marshrutizatsii-v-multiservisnoy-seti-svyazi

4. Макаренко, С.И., Михайлов, Р.Л. Модель функционирования маршрутизатора в сети в условиях ограниченной надежности каналов связи. “Инфокоммуникационные технологии” Том 12, № 2, – 2014. с. 44-49.

5. Калыгин, Г.О., Ефимов, В.А. Модель надежности восстанавливаемой системы при изменяющейся интенсивности отказов. “Молодой учёный”. Технические науки № 25 (263). – Июнь 2019 г., – с.111-113.

6. Нестационарный пуассоновский поток отказов, его модель [Электронный ресурс] / URL: https://studfile.net/preview/7003577/page:5/

7. Немарковские случайные процессы, сводящиеся к марковским [Электронный ресурс] / URL: https://studfile.net/preview/725120/page:11/

Elmi Əsərlər
Proceedings of Science

Heydər Əliyev adına Hərbi İnstitutun **Elmi Əsərlər** jurnalı, Cild 22, № 2, 2024 / 51-56
Proceedings of Science of the Military Institute named after Heydar Aliyev, Volume 22, № 2, 2024 / 51-56

Daxilolma tarixi / Received date: 30.05.2024
Qəbulolma tarixi / Accepted date: 02.09.2024

DOI: 10.30546/8967.2024.22.2.1019

PİLOTSUZ UÇUŞ APARATLARININ İŞÇİ TEZLİKLƏRİ TƏSADÜFİ DƏYİŞƏN RABİTƏ KANALLARINDA SİQNALLARIN AŞKAR EDİLMƏSİ

Mehman Binnətov
texnika elmləri namizədi, dosent
Azərbaycan Texniki Universiteti, Bakı
E-mail:binnatov60@mail.ru

Mehman Hüseynov
Heydər Əliyev adına Hərbi İnstitut, Bakı
E-mail:mexman1967@rambler.ru

Zaur Hüseynov
"UNİNET" MMC, Bakı
E-mail:huseynovzaur182@gmail.com

Xülasə

Məqalə məlumat xarakterli olub, işçi tezlikləri təsadüfi ardıcıllıqlarla dəyişən radiosiqnallar tətbiq olunan pilotsuz uçuş aparatlarının radiorabitə kanallarının tezliklərinin aşkar edilməsindən bəhs edir. PUA-ların rabitə kanallarında spektri genişləndirilmiş mürəkkəb siqnallardan geniş istifadə olunur. Belə siqnallardan biri işçi tezliyi müəyyən qanunla, təsadüfi atlamalarla dəyişən (İTTD) siqnallardır. Müəyyən olunmuşdur ki, İTTD üsulu ilə spektrin genişləndirilməsində radiosiqnalın daşıyıcı tezliyi müəyyən qanunla dəyişir. Müəyyən zaman intervalında siqnal təsbit olunmuş tezlikdə ötürülür, növbəti zaman intervalında siqnal əvvəlki zaman intervalına bərabər başqa tezlikdə və daha sonra bu ardıcıllıqla ötürülür. İTTD siqnalların əsas üstünlüyü onların yüksək malik olmalarındadır. Müasir dövrdə rabitə sistemlərinin İTTD rejimli ötürmələrə keçməsi nəticəsində belə siqnalların aşkar edilməsi xüsusi aktuallığını saxlayır.

Müəyyən edilmişdir ki, hazırda işçi tezlikləri təsadüfi ardıcıllıqlarla dəyişən radiosiqnalların radiotezliklərinin aşkar edilməsi üçün adətən siqnalların enerji göstəricilərinə əsaslanan müxtəlif xətti üsullardan istifadə olunur. Bu üsulların tətbiqi zamanı aşağı enerji göstəricili radiosiqnalların aşkarlanması müəyyən çətinliklərlə müşayiət olunur. Həmçinin nəzərə alınmalıdır ki, işçi tezlikləri təsadüfi ardıcıllıqlarla dəyişən radiosiqnallara qeyri-xətti dinamikaya əsaslanan Hörst göstəricisi tətbiq olunduqda onlar əhəmiyyətli dərəcədə gizliliyə malik olurlar. Belə radiosiqnalların BDS statistikanın (Business Dynamics Statistics - xaotik təsvirlərin və küy şəraitində müntəzəm siqnalların parametrlərinin qiymətləndirilməsi üsulu) köməyi ilə aşkarlanması ehtimalı daha çoxdur. Perspektivdə işçi tezlikləri təsadüfi ardıcıllıqlarla dəyişən pilotsuz uçuş aparatlarının radiosiqnallarının aşkar edilməsi üçün BDS statistikaya əsaslanan radiotutma vasitələri bu siqnalları aşkar edə bilərlər. İşçi tezlikləri təsadüfi ardıcıllıqlarla dəyişən pilotsuz uçuş aparatlarının radiosiqnallarının daha effektiv aşkaretmə potensiallı BDS statistika üsulu ilə aşkarlanması mühüm praktiki əhəmiyyətə malik olmaqla yanaşı, daha mürəkkəb siqnalların digər tiplərinin də aşkarlanmasına imkan verir.

Açar sözlər: Hörst göstəricisi, pilotsuz uçuş aparatları, rabitə kanalları, qeyri-xətti dinamika.

DETECTION OF SIGNALS IN COMMUNICATION CHANNELS FREQUENCY-HOPPING SPREAD SPECTRUM (FHSS) OF UNMANNED AERIAL VEHICLES

Mehman Binnatov
candidate of technical sciences, associate professor
Azerbaijan Technical University, Baku

Mehman Huseynov
Military Institute named after Heydar Aliyev, Baku

Zaur Huseynov
"UNİNET" LLC, Baku

Abstract

The article is of an informative nature and tells about detection of frequencies of radio communication channels of unmanned aerial vehicles using radio signals, the operating frequencies of which change in a random sequence. Complex signals with an extended spectrum are widely used in UAV communication channels. One of such signals is signals of the operating frequency changing according to a certain law, with random jumps (FH). The FH method has established that the carrier frequency of the radio signal changes according to a certain law when the spectrum is expanded. In a certain time interval, the signal is transmitted at a fixed frequency, in the next time interval the signal is transmitted at another frequency equal to the previous time interval, and so on. The main advantage of FH signals is their high impedance. In modern times, detection of such signals remains especially relevant as a result of the transition of communication systems to transmission in the FH mode. It has been established that at present, various linear methods based on the energy indicators of signals are used to detect radio frequencies of radio signals, the operating frequencies of which change in a random sequence. When using these methods, detecting low-energy radio signals is accompanied by certain difficulties. It should also be taken into account that radio signals whose operating frequencies change in a random sequence have a significant degree of secrecy when using the Horst indicator based on nonlinear dynamics. Such radio signals are more likely to be detected using BDS statistics (Business Dynamics Statistics - a method for estimating the parameters of chaotic images and regular signals in noisy conditions). In the future, radio interceptors based on BDS statistics will be able to detect radio signals from unmanned aerial vehicles whose operating frequencies change in a random sequence. Detecting radio signals from unmanned aerial vehicles whose operating frequencies change in a random sequence using the statistical BDS method with a more effective detection potential is of great practical importance and allows detecting other types of more complex signals.

Keywords: Hurst exponent, unmanned aerial vehicles, communication channels, nonlinear dynamics.

ОБНАРУЖЕНИЕ СИГНАЛОВ В КАНАЛАХ СВЯЗИ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧИХ ЧАСТОТ (ППРЧ) БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Мехман Биннетов
кандидат технических наук, доцент
Азербайджанский Технический Университет, Баку

Мехман Гусейнов
Военный институт имени Гейдара Алиева, Баку

Заур Гусейнов
ООО "UNINET", Баку

Аннотация

Статья носит информативный характер и рассказывает об обнаружении частот каналов радиосвязи беспилотных летательных аппаратов с помощью радиосигналов, рабочие частоты которых изменяются в случайной последовательности. Сложные сигналы с расширенным спектром широко используются в каналах связи БПЛА. Одним из таких сигналов являются сигналы рабочей частоты, изменяющиеся по определенному закону, со случайными скачками (ППРЧ). Методом ППРЧ установлено, что несущая частота радиосигнала изменяется по определенному закону при расширении спектра. В определенном интервале времени сигнал передается на фиксированной частоте, в следующем интервале времени сигнал передается на другой частоте, равной предыдущему интервалу времени, и так далее. Основным преимуществом сигналов ППРЧ является их высокий импеданс. В современное время обнаружение таких сигналов остается особенно актуальным в результате перехода систем связи на передачу в режиме ППРЧ.

Установлено, что в настоящее время для обнаружения радиочастот радиосигналов, рабочие частоты которых изменяются случайной последовательностью, используются различные линейные методы, основанные на энергетических показателях сигналов. При применении этих методов обнаружение радиосигналов низкой энергии сопровождается определенными трудностями. Следует также учитывать, что радиосигналы, рабочие частоты которых изменяются в случайной последовательности, обладают значительной степенью скрытности при применении индикатора Хёрста, основанного на нелинейной динамике. Такие радиосигналы с большей вероятностью будут обнаружены с помощью статистики BDS (Business Dynamics Statistic – метод оценки параметров хаотических изображений и регулярных сигналов в шумных условиях). В будущем радиоперехватчики на основе статистики BDS смогут обнаруживать радиосигналы от беспилотных летательных аппаратов, рабочие частоты которых изменяются в случайной последовательности. Обнаружение радиосигналов беспилотных летательных аппаратов, рабочие частоты которых изменяются случайной последовательностью, с использованием статистического метода BDS обладающего более эффективным потенциалом обнаружения, имеет большое практическое значение и позволяет обнаруживать другие виды более сложных сигналов.

Ключевые слова: показатель Хёрста, беспилотные летательные аппараты, каналы связи, нелинейная динамика.

Giriş

Müasir dövrdə hərbi rabitə sistemlərində İTTD siqnalların tətbiqi geniş vüsət almışdır. Daşıyıcı tezliklərin dəyişmə alqoritmi, ancaq ötürücü və qəbulediciyə məlum olan ötürücüdə təsadüfi ardıcıllıqlarla dəyişdiyindən, belə siqnalların müxtəlif tezliklərdə aşkar edilməsi çox mürəkkəbdir. İTTD-li siqnallar bir daşıyıcı tezlikdə çox qısa müddətdə şüalandığından, həmçinin siqnalların və maneələrin parametrləri barədə heç bir informasiya daşımadığından, belə siqnalların enerji göstəricilərinə görə aşkar edilməsi çox çətindir və yaxud praktiki olaraq mümkün deyildir.

Bu istiqamətdə müxtəlif vaxtlarda aparıcı dövlətlərin elmi-araşdırma və tədqiqat institutlarının mütəxəssisləri tərəfindən tədqiqatlar aparılaraq müəyyən nəticələrin alınmasına baxmayaraq, İTTD-li siqnalların aşkar edilməsi məsələsi çox mürəkkəb problem olmaqla, hələ də öz aktuallığını saxlayır. Müəyyən olunmuşdur ki, İTTD-li siqnalların digər siqnallardan fərqləndirən əsas müsbət cəhəti onların yüksək maneədayanıqlığına malik olmalarıdır ki, bunun nəticəsində radiorabitə düşmənin radioelektron mübarizə vasitələrinin təsirindən tamamilə qorunur.

Eyni zamanda nəzərə alınmalıdır ki, İTTD siqnallı radiorabitədə əlaqə məsafəsi digər siqnallara nisbətən 15 - 25 % azalır. Bu da, İTTD-li siqnalların formalaşmasına sərf olunan zamanla əlaqədardır.

Həmçinin müəyyən olunmuşdur ki, aparılan araşdırmalarda İTTD-li radiosiqnalların aşkar edilməsi və tutulması üçün aşağıdakı yanaşmalar mövcuddur:

– İTTD siqnalların enerji göstəricilərinə görə aşkar edilməsi;
– İTTD siqnalların xətti və qeyri - xətti dinamiki üsullarla aşkar edilməsi;
– İTTD siqnallarının qeyri – parametrik səviyyəyə görə aşkaretmə alqoritminin tətbiqi ilə aşkar edilməsi;
– İTTD siqnalların Hörst göstəricisinə görə aşkar edilməsi;
– İTTD siqnalların BDS statistikaya görə aşkar edilməsi.

İTTD siqnallarının aşkar edilməsində qeyri – parametrik səviyyəyə görə aşkaretmə alqoritmi təqdim olunmaqla, İTTD siqnallarının aşkar edilməsi üçün n kanallı qəbuledici təklif olunmuşdur. Bu radioqəbuledicidə İTTD siqnalı maneələrlə birgə, çıxışında tezlik mövqeləri ayrılan darzolaqlı paralel kanallara daxil olaraq, ayrılan tezlik mövqeli analoq – rəqəm çeviricilərinə daxil olur və kvantlanmış tezlikli tezlik parçalarını formalaşdırır. Səviyyə formalaşdırıcısında müəyyən zaman momentində hesabat modulları azalmalarla səviyyələrə bölünürlər. Bu modulların birincisini (maksimumuna) 0, ikincisini 1 və ardıcıllıqla sonuncunu n-1 kimi təqdim etməklə səviyyələrə bölürlər. Nəticədə səviyyə formalaşdırıcısının çıxışında səviyyələr vektoru alınır. Səviyyələr vektorunun kiçik qiymətləri tezlik kanalında zaman momentində İTTD-li siqnalın olması əlamətini göstərir [1].

Radioelektron boğma vasitələrinin təsiri şəraitində İTTD-li radiorabitə sistemlərinin ümumiləşdirilmiş təcrübə və tədqiqat işləri araşdırılaraq İTTD-li radiorabitə sistemlərinin son texnologiya ilə istehsal olunan radiorabitə və radioelektron boğucu vasitələrin tətbiqi zamanı yaranan müxtəlif problemlərin aspektləri və radiosistemin maneədayanıqlığının qiymətləndirilməsi və həmçinin radioelektron mübarizə vasitələrinin konfiqurasiyasının modelləşdirilməsi istiqamətində təcrübə və

tədqiqat işləri aparılmışdır. Bu işin nəticəsində müəyyən edilmişdir ki, rabitə sistemlərinin göstəricilərini, buraxılış qabiliyyəti və vaxtında rabitəni qurmaq imkanlarını artırmadan hərbi idarəetmə sistemlərini mükəmməlləşdirmək mümkün deyil. Həmçinin müasir silahlı toqquşmalarda radioelektron mübarizə (REM) vasitələrinin rabitə və idarəetmə sistemi ilə birlikdə əsas mübarizə vasitəsi kimi tətbiqi qeyd olunmuşdur.

REM təsiri şəraitində rabitə sisteminin fəaliyyəti və verilənləri ötürmə prosesi yenə də öz aktuallığını saxlayır. Hərbi və xüsusi təyinatlı müasir rabitə sistemlərinin maneədayanıqlığını artırmaq üçün əsas üsul kimi hazırda İTTD rejiminin geniş tətbiqi hesab olunur [2].

Qrup şəklində fəaliyyət göstərən PUA-ların idarəetmə siqnallarının tutulmasına imkan verən üsulun hazırlanması, idarəetmə siqnallarının tezliklərinin dəyişmə ardıcıllığının təyin edilməsi, boğma zonasında PUA-nın idarəetmə siqnallarının boğulması məsələləri və siqnalın parametrlərinə əsasən onların aşkarlanması müəyyən edilir [3].

İTTD-li siqnalların aşkar edilməsi, bir mənbədən şüalandırılan qəbul olunan çoxsaylı İTTD siqnallarının tanınması və mənsubluğunu ayırd etmək üçün radiomonitorinq sisteminin yaradılması vacibdir. Radioqəbuledici qurğuların SCAN rejimində İTTD siqnallarının aşkarlanması, İTTD siqnal tutucusunun ümumi fəaliyyət sxemi və aşkar edilmiş siqnalların mənsubluğunu təyin etmək üçün siqnalın bir tezlikdən digər tezliyə keçməsi və radioqəbuledicinin qərar qəbul etməsi qaydalarından istifadə olunur [4].

1. PUA-dan ötürülən radiosiqnalların aşkarlanması

PUA-larla yerüstü idarəetmə kompleksi (YİK) arasında uçuşların idarə olunması və real zamanda radiosiqnalların ötürülməsi üçün daimi fəaliyyətdə olan dayanıqlı rabitə kanalının olması əsas şərtdir. Nəzərə alınmalıdır ki, video təsvirləri translyasiya edən kanaldan uçuş aparatının idarə olunması və onun vəziyyətinə nəzarət etməkdən əlavə, digər xidməti (telemetrik) məlumatların ötürülməsində də istifadə olunur. Xüsusi təyinatlı PUA-larda telemetrik məlumatlar İTTD rejimli maneədayanıqlı kanalla həyata keçirilir. PUA siqnallarının aşkarlanması bəzi xüsusiyyətlər istisna olmaqla demək olar ki, YİK siqnallarının tutulması ilə eynidir.

Nəzərə alınmalıdır ki, istehsal olunan müasir dronların çoxunda idarəetmə və videosiqnalları ötürmə kanallarının işçi tezlik diapazonları eynidir və üst-üstə düşürlər.

Hazırda istehsal olunan müxtəlif tipli PUA-larda İTTD texnologiyasından istifadə olunur. Bu texnologiyalı radiotezlik vasitələri onları aşkarlama sürəti və imkanları nöqteyi-nəzərindən digər texnologiyalarla müqayisədə bir çox üstünlüklərə malikdir. İTTD texnologiyalı PUA-nı aşkar etmək üçün tətbiq olunan radiotezlik vasitələrinin işi İTTD radiosiqnalların aşkar edilməsi ilə məşğul olan radiokəşfiyyatla birbaşa əlaqəlidir. Həmçinin nəzərə alınmalıdır ki, bu işlər ötürülən siqnalın aşkar edilməsi, onun strukturunun təyin edilməsi və ötürülən informasiyanın açılması məsələləri ilə eyni vaxtda baş verməlidir. Məhz bu addımlardan sonra PUA-nın verilənləri ötürmə radioxətlərini boğmaq və ona müdaxilə etməklə yalan iş rejimlərini tətbiq etmək (yeritmək, spufinq) olar.

PUA-nın idarə olunması üçün tətbiq olunan rabitə standartları, həmçinin bu standartlara əlavə edilmiş kriptoqrafik mühafizə protokollarının zəifliyi faydalı siqnalın tezliyini və strukturunu hədəfləyən maneələr formalaşdırmaqla, PUA-nı endirən komandalar imitasiya edərək idarəetmə kanallarını avtomatik "sındıran" rejimin reallaşdırılmasına imkan verir. Belə yanaşma digər tezliklər və idarəetmə kanallarından geniş istifadə edən PUA-lara aid edilmir.

Digər yanaşma İTTD radiosiqnallarının aşkar edilməsi üçün enerji şüalarını aşkarlayan vasitələrdən istifadə olunmasıdır. Belə vasitələrin iş prinsipi məsafədən idarə olunan İTTD-li PUA-ların radiosiqnallarının aşkar edilməsi üçün təklif olunan aşkarlama alqoritminə əsaslanır.

Aşkarlama alqoritminin əsasını cəld Furye çevirməsini ardıcıl realizə edən spektral sıxlığın maksimumuna uyğun tezliklərin toplanması və sonradan statistikanın formalaşması təşkil edir. Statistika hansısa elementin vektorunun meyletmə qiymətinin kvadratının həmin vektorun orta və maksimal qiymətləri ilə müqayisəsi nəticəsində formalaşır.

Radiosiqnalların aşkar edilməsi istiqamətində aparılan məsələlərdə alternativ həll kimi daha müasir istiqamət qeyri-xətti dinamika üsulları [5] müəyyən edilmişdir. Bu üsullara Hörst göstəricisini

(H), BDS statistikanı ($\overline{W}(\varepsilon)$) və digər göstəriciləri misal çəkmək olar. Hörst göstəricisi (H) – periodik və təsadüfi proseslərin bir-birindən ayrılmasına imkan verir və aşağıdakı ifadə ilə təyin olunur:

$$R/S = (\tau/2)H\,, \tag{1}$$

burada, R – normalaşdırılmış variasiya diapazonu (ölçülən parametrin maksimal və minimal qiymətlərinin fərqi); S – standart meyletmə (dispersiyanın kvadrat kökü); τ – müşahidə periodudur.

Antipersistent proseslər (erqodik sıralar) üçün Hörst göstəricisi 0÷0,5 qəbul olunur, 0,5÷1 isə bu və ya digər nizamlı formaya malik sistemlər üçün xarakterikdir, H ≈ 0,5 qiyməti ağ küyə uyğundur. Hörst göstəricisi 0÷0,5 olduqda antipersistent proses baş verir, yəni sistem təsadüfi dəyişmələrdən də daha tez dəyişir. Nəticədə H göstəricisinin nə qədər yüksək olması ilə zaman sırasında nizamsız dəyişikliklərin də bir o qədər az olacağı alınır. Erqodiklik - bəzi dinamiki sistemlərin fəaliyyəti prosesində hər bir vəziyyətinin sistemin digər vəziyyətlərinin yaxınlığından müəyyən ehtimalla keçdikdə yaranan xüsusi xassəsidir.

Ağ küy – spektral mürəkkəbələri tətbiq olunan tezlik diapazonunda bərabər paylanmış stasionar küydür.

BDS statistika – tədqiq olunan prosesin fazaya görə fəzada korrelyasiya inteqralı ilə təyin olunan korrelyasiya ölçüsünün statik xassələri əsasında yaranır. Bu xassələr enerji göstəricilərinə nəzərən təsadüfi, xaotik və müntəzəm proseslər haqqında daha çox informasiya verir. BDS statistika - *w(x)* statistik kəmiyyətinə əsaslanır və aşağıdakı ifadə ilə təyin olunur;

$$W_{m,N(\varepsilon)} = \sqrt{N-m+1}\,\frac{C_{m,N(\varepsilon)} - C_{1,N-m(\varepsilon)}{}^{m}}{\sigma_{m,N(\varepsilon)}}, \tag{2}$$

burada, $C_{m,N(\varepsilon)}$ - korrelyasiya inteqralları, $\sigma_{m,N(\varepsilon)}$ - orta kvadratik meyletmədir.

Qeyd olunmuş qeyri-xətti dinamiki üsullarla İTTD-li siqnalların aşkar edilməsi nadir hallarda rast gəlinir. Bu nöqteyi-nəzərdən İTTD-li siqnalların aşkar edilməsi üçün qeyri-xətti dinamiki üsulların öyrənilməsi praktiki və elmi maraq kəsb edir.

2. İTTD-li rabitə sistemlərinin tətbiqi məsələləri

İTTD əsaslı rabitə sistemləri də digər rabitə sistemləri kimi ötürücü və qəbuledici hissələrdən, verilənlər koderindən, modullaşdırıcıdan, təsadüfi ardıcıllıqlar hasil edən generatordan, tezlik sintezatorundan və s. hissələrdən ibarətdirlər.

Ötürücü və qəbuledici hissələrdə təsadüfi ardıcıllıqlar hasil edən generatorlar ötürmədə ötürülən məlumatların spektrinin genişlənməsinə, qəbulda isə onun sıxlaşdırılmasına imkan yaradır.

Praktiki tətbiq üçün İTTD siqnalların küy və maneələr şəraitində yenilənməyə ehtiyac olmadan və xassələrinə görə iki mərhələli alqoritmdən çox da geri qalmayan bir mərhələli alqoritmdən istifadə olunur [6]. Aparılan hesablamalar nəticəsində İTTD-li radiosiqnallar üçün Hörst göstəricisi H≈0,55 alınmışdır ki, bu da İTTD-li radiosiqnalların H≈0,55 olan ağ küyə çox yaxın olduğunu göstərir. Hörst göstəricisi tətbiq olunan aşkaretmə üsulunda İTTD-li radiosiqnallar gizliliyə malikdirlər və İTTD-li PUA-ların idarəetmə kanallarının aşkar edilməsi üçün nəzərdə tutulan radiotezlik vasitələri onları tuta və yaxud aşkar edə bilməzlər. Beləliklə, radiosiqnallar BDS statistikanın köməyi ilə daha yaxşı aşkar olunduğundan, perspektivdə İTTD-li PUA-ların idarəetmə kanallarının aşkar edilməsi üçün tətbiq olunan radiotutma vasitələrində tətbiqi daha məqsədəuyğun sayılır.

Yuxarıda göstərilən üstünlükləri nəzərə alaraq qeyd etmək olar ki, İTTD-li PUA-ların radiosiqnallarının daha effektiv aşkaretmə potensiallı BDS statistika üsulu ilə aşkarlanmasının mühüm praktiki əhəmiyyətə malik olması mürəkkəb siqnalların digər müxtəlif tiplərinin də müəyən edilməsinə imkan yaradır.

Nəticə

Məqalədə BDS statistikadan və ona adaptasiya ola bilən digər radiotezlik üsullarının müştərək tətbiqi nəticəsində PUA-ların aşkar edilməsi məsələlərinin müxtəlif metodları təhlil edilmiş və onların fəaliyyətinə əks-təsir göstəriciləri üçün daha effektiv sistemlərin yaradılması imkanlarına baxılmışdır.

Radiosiqnalların İTTD-li PUA-ların idarəetmə kanallarının aşkar edilməsi üçün tətbiq olunan radiotutma vasitələrində tətbiqi digər radiotezlik üsullarının köməyi ilə onların aşkar edilməsi və əks-təsirlər üçün effektiv sistemlərin qurulması istiqaməti müəyyənləşdirilmişdir. Aşkaretmə üsulu kimi tətbiq olunan Hörst göstəricili radiotutma vasitələri İTTD-li PUA-ların radiosiqnallarını aşkar edə bilmədiyindən, BDS statistikadan və ona adaptasiya ola bilən digər radiotezlik üsullarının müştərək tətbiqi daha məqsədəuyğundur. Həmçinin İTTD-li PUA-ların radiosiqnallarının daha effektiv aşkaretmə potensiallı BDS statistika üsulu ilə aşkarlanmasının mühüm praktiki əhəmiyyətə malik olması müəyyən edilmiş mürəkkəb siqnalların digər tiplərinin də aşkarlanmasında istifadə edilə bilər.

BDS statistikadan və ona adaptasiya ola bilən digər radiotezlik üsullarının müştərək tətbiqindən PUA-ların aşkar edilməsi və onların fəaliyyətinə əks-təsirlər göstərmək üçün daha effektiv sistemlərin yaradılmasında istifadə oluna bilər.

Ədəbiyyat

1. Бизюков, П.Е., Литвиненко, В.П., Литвиненко, Ю.В. Исследование рангового алгоритма обнаружения сигнала с ППРЧ. [Электронный ресурсы], URL: https://cyberleninka.ru/article/n/issledovanie-rangovogo-algoritma-obnaruzheniya-signala-s-pprch

2. Макаренко, С.И. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография / С.И.Макаренко, М.С.Иванов, С.А.Попов, – СПб.: Свое издательство, – 2013. – 166 с.

3. Альтман, Е.А., Малютин, А.Г., Чижма, С.Н. Повышение скрытности шумоподобных сигналов в системах радиосвязи // Сборник докладов (“РЭИС-2013”), – Омск: ОАО “ОНИИП”. – 2013. – с. 329–337.

4. Алексеев, Д.А. Чураков, П.П. Токарев, А.Б. Обнаружение сигналов с псевдослучайной перестройкой рабочей частоты на основе буферизированной обработки данных // Воронежский государственный технический университет. Журнал “Радиотехника” №6 – 2016. – с.40-43.

5. Гавришев, А.А., Осипов, Д.Л. Применение методов нелинейной динамики для обнаружения радиосигналов с псевдослучайной перестройкой рабочей частоты, используемых в каналах связи беспилотных летательных аппаратов // ФГАОУ ВО Северо-Кавказский федеральный университет, Научно-аналитический журнал: “Сибирский пожарно-спасательный вестник” – № 1 (20) – 2021. – с. 68-74.

6. Бородич, Ё.Ю. Разработка и исследование алгоритма обнаружения сигналов с ППРЧ // Научный вестник НГТУ. – 2008. – № 1 (30), – с. 57-67.

ELMİ MƏQALƏLƏRİN YAZILMASINA VƏ TƏRTİB EDİLMƏSİNƏ DAİR TƏLƏBLƏR

Təqdim edilən məqalələr jurnalın elmi istiqamətinə (hərbi elmlər, humanitar elmlər və milli təhlükəsizlik, fundamental və təbiət elmləri, texniki elmlər, iqtisadiyyat və informasiya texnologiyaları) uyğun, aktual elmi problemlərə aid tədqiqatların ilk dəfə dərc olunması üçün nəzərdə tutulmuş, orijinal, heç bir jurnalda çap olunmamış materiallara malik olmalıdır.

Kağız ölçüsü	- A4
Yazı mətni, şrift	- MS WORD, Times New Roman
Şriftin ölçüsü	- 12 pt
Sətirlərarası interval	- 1
Abzas	- 1 sm
Boş sahə	- hər tərəfdən 20 mm
Həcmi	- 5-10 səhifə (2000-5000 söz)
Məqalənin adı	- üç dildə, ortada, böyük hərflərlə, qalın şriftlə
Müəllifin(lərin) adı və soyadı	- üç dildə, ortada, qalın şriftlə
Elmi dərəcəsi və elmi adı (hərbi rütbəsi)	- üç dildə, ortada
İş yeri, şəhər	- üç dildə, ortada
E-mail	- ortada
Xülasə (150-250 söz)	- azərbaycan, ingilis və rus dillərində
Açar sözlər (3-5)	- azərbaycan, ingilis və rus dillərində
İstinadlar	- kvadrat mötərizədə: [5, s.156]; [10]
Ədəbiyyat	- Mətndəki ardıcıllıqla sıralanmalı (AAK-nın tələblərinə uyğun)

Xülasədə tədqiqat işinin məzmunu, aktuallığı, elmi cəhətdən yeniliyi, tətbiqi əhəmiyyəti, istifadə olunan metodlar və s. yığcam şəkildə öz əksini tapmalıdır. Giriş hissəsində elmi məqalənin mahiyyəti, mövzunun aktuallığı, məqsəd və vəzifələri, tələb olunan məlumatlar, əvvəllər aparılan işlərin qiymətləndirilməsi, nəzəri və praktiki əhəmiyyəti, istifadə olunan metodlar əks olunmalıdır.

Nəticə hissəsində müəllifin araşdırma zamanı gəldiyi elmi nəticələr, tövsiyə və təkliflər əks olunmalıdır.

Cədvəllər, qrafiklər, diaqramlar, şəkillər və fotolar mətnin daxilində yerləşdirilməklə məqaləyə daxil edilə bilər.

Elmi mənbələrə edilən istinadlar mətndə kvadrat mötərizədə verilməlidir (məsələn, [1] və ya [1, s.119]). Məqalənin sonunda verilən ədəbiyyat siyahısı mətndəki ardıcıllıqla göstərilməli, son 10 ildə nəşr edilmiş elmi məqalələrə, monoqrafiyalara və digər etibarlı mənbələrə üstünlük verilməlidir. İstinad olunan mənbənin biblioqrafik təsviri verilərkən Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyasının tələbləri əsas götürülməlidir.

Müəllif(lər) məqalənin A4 formatında çap olunmuş nüsxəsini, elektron variantını, eləcə də əlaqə saxlamaq üçün telefon nömrəni redaksiyaya təqdim etməli və ya harbiinstitut@gmail.com ünvanına göndərməlidir.

Redaksiyaya daxil olmuş məqalələr anonim rəyçilərin rəyindən (2 müsbət rəydən) sonra sahə redaktoru və ya redaksiya heyətinin mütəxəssis üzvlərindən biri tərəfindən çapa tövsiyə olunacaq. Təqdim olunan məqalənin dərc olunmasından imtina edildiyi halda jurnalın redaksiyası yazılı şəkildə müəllifə imtina cavabı göndərəcəkdir.

MƏQALƏ NÜMUNƏSİ:

QALIN VƏ BÖYÜK HƏRFLƏ

Ad və Soyad
elmi dərəcə, elmi adı, (hərbi rütbə)
İş yeri, Şəhər
Elektron ünvan, ORCİD (olduğu təqdirdə), telefon nömrə

Xülasə.
Açar sözlər:

GİRİŞ

1. Başlıq

1.1. Yarım başlıq

Nəticə

Ədəbiyyat

Ədəbiyyatın tərtibat qaydası / The arrangement of literature / Расположение литературы

Kitab / Book / Книга

– Qasımov, V. İnfomasiya təhlükəsizliyi. Dərslik / V.Qasımov. – Bakı: MTN-nin Nəşriyyat-Poliqrafiya Mərkəzi, – 2009. – 340 s.

– Maslow, A. Motivation and personality / A.Maslow. – New York: NY Harper & Row, – 1954. – 394 p.

– Paşayev, A.M. Atmosfer proseslərinin fiziki əsasları. Dərslik. / A.M.Paşayev, H.İ.Quliyev, S.H.Səfərov – Bakı: Nafta-Press, –2007. – 416 s.

– Azərbaycan folkloru: (məktəblilər üçün seçmələr) / tərt. ed. B.Abdulla – Bakı: Şərq-Qərb, – 2005. – 360 s.

Məqalə / Article / Статья

– Həşimov, E. Q., Hüseynov, B. S. Müasir PUA-ların döyüş imkanları və tətbiqinin bəzi aspektləri / - Bakı: Milli təhlükəsizlik və hərbi elmlər, – 2021. №3 (7), – s.14-24

– Емельянов, Г.В., Стрельцов А.А. Гуманитарные проблемы обеспечения информационной безопасности Российской Федерации // - Москва: Качество: теория и практика, – 2000. – № 4, – с. 34

Konfrans materialı / Conference proceedings / Материал конференции

– Hüseynov, Ə.Q. Portativ optik rabitə sistemi // "Telekommunikasiyada innovativ texnologiyalar" mövzusunda Beynəlxalq elmi-texniki konfransın materialları, – Bakı: – 4 – 6 dekabr, – 2019, – s.165-167

– Абдуллаев, С.К., Карамалиев, Н.Р. Весовые оценки сингулярных, слабо сингулярных интегралов, максимальных и дробно максимальных функций, ассоциированных обобщенным сдвигом // Труды IV Международного симпозиума «Ряды Фурье и их приложения», – Ростов-на-Дону: – 28 мая – 3 июня, – 2006, – с. 44-52.

– Gatys, L.A., Ecker, A.S., Bethge, M. Image style transfer using convolutional neural networks // IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas, Nevada, USA, – 2016, – p. 2414-2423.

Dissertasiyalar / Dissertations / Диссертации

Səfərov, E.S. Xəzər dənizinin səviyyə tərəddüdlərinin məsafədən zondlama üsulları ilə tədqiqi: / coğrafiya üzrə fəlsəfə doktoru dissertasiyası) / – Bakı, 2018. – 151 s.

Dissertasiyanın avtoreferatı / Dissertation abstract / Автореферат диссертации

– Səfərov, E.S. Xəzər dənizinin səviyyə tərəddüdlərinin məsafədən zondlama üsulları ilə tədqiqi: / coğrafiya üzrə fəlsəfə doktoru dissertasiyanın avtoreferatı) / – Bakı, 2018. – 26 s.

Elektron resurs / Electronic resource / Электронный ресурс

– Hüseynov, R. İnsan hüquq və azadlıqlarının təmin olunması istiqamətində vətəndaş cəmiyyəti və siyasi partiyaların rolu: başlıca amillər nələrdir? [Elektron resurs] / URL: https://editor.az/insan-huquq-ve-azadliqlarinin-temin-olunmasi-istiqametinde-vetendas-cemiyyeti-ve-siyasi-partiyalarin-rolu-baslica-amiller-nelerdir

Gleason, E. A. Viewpoint: Soft Metal Gains Hulk-Like Strength: [Electronic resource] / Physics 12, 125. – November 11, 2019. URL: https://physics.aps.org/articles/v12/125

Patentlər / Patents / Патенты

– Səfərov, A.R., 1,4 – Butandiolun alınma üsulu, İxtira i2017 0005, Azərbaycan Respublikası / Əliyev A.M., Əliyev F.V., Mətiyev K.İ. [və b.].

Normativ-hüquqi sənədlər / Normative-legal documents / Нормативно-правовые документы

– Azərbaycan Respublikasının Konstitusiyası // 12 noyabr 1995-ci ildə qəbul edilmişdir (24 avqust 2002-ci il tarixdə olan dəyişiklik və əlavələr). – Bakı: Qanun, – 2002, – 48 s.

Qəzet məqalələri / Newspaper articles / Газетные статьи

– Abdullayev, F. Azərbaycanı Respublikası Konstitusiyasının qəbul edilməsindən 24 il keçir // Respublika. – 2019, 9 noyabr. – s. 2.

Arxiv materialları / Archival materials / Архивные материалы

– Xarici İşlər naziri Məhəmməd Həsən Hacınskinin məruzəsi (Gəncə: 15 iyul 1918-ci il) // Azərbaycan Respublikası Dövlət Arxivi, Fond № 1061, siyahı №1, iş № 95, vərəq – 1.

REQUIREMENTS FOR WRITING AND COMPILATION OF SCIENTIFIC ARTICLES

The submitted articles have to be compliant with the magazine's scientific direction (military sciences, humanitarian sciences and national security, fundamental and natural sciences, technical sciences, economics and information technologies) original, unpublished materials intended for the first publication of research related to current scientific problems.

Papersize:	- A4
Text, font -	- MS WORD, Times New Roman
Font size:	- 12 points
Line spacing	- 1
Paragraph	- 1 cm
Free space	- 20 mm from each side
Volume-	- 5-10 pages (2000-5000 words)
Title of the article	- in 3 language, in the middle, in capital letters, in bold font
Name and surname of the author(s)	- in 3 language, in the middle, in bold font
Scientific degree and scientific name (military rank)	– in 3 language, in the middle
Workplace, city	- in 3 language, in the middle
E-mail	- in the middle
Abstract (150-250 words)	- in Azerbaijani, English and Russian languages
Keywords (3-5)	- in Azerbaijani, English and Russian languages
References	- square meters: [5, p.156]; [10]
Reference	- in the order in the text (according to the requirements of the High Attestation Commission)

In the abstract, the content, relevance of the research work, the scientific novelty of the work, the importance of application, research methods etc. should be concisely reflected. The introductory part should reflect the essence of the scientific article, the relevance of the topic, goals and objectives, required information, evaluation of previous work, theoretical and practical importance, and used methods.

In the conclusion part, the author's scientific conclusions, recommendations and suggestion from the research should be reflected.

Tables, graphs, diagrams, pictures and photos can be included in the article by placing them inside the text.

References to scientific sources should be given in square brackets in the text (eg [1] or [1, p.119]). The list of literature given at the end of the article should be listed in the order in the text, preference should be given to scientific articles, monographs and other reliable sources published in the last 10 years. The requirements of the High Attestation Commission under the President of the Republic of Azerbaijan should be taken into account when giving a bibliographic description of the cited source.

The author(s) should submit a printed copy of the article in A4 format, an electronic version, as well as a contact phone number to the editorial office or send it to harbiinstitut@gmail.com.

The articles included in the editorial board will be recommended for publication by the field editor or one of the specialist members of the editorial board after the opinion of anonymous reviewers (2 positive opinions). In case of refusal to publish the submitted article, the editorial office of the journal will send a written refusal response to the author.

SAMPLE OF ARTICLE:

BOLD AND CAPITAL LETTERS

Name and Surname
scientific degree, scientific name (military rank)
Workplace, City
E-mail address, ORCİD (if it is) telephone number

Abstract.
Keywords:

Introduction

1.Title

1.1. Half title

Conclusion

Reference

ТРЕБОВАНИЯ К НАПИСАНИЮ И ОФОРМЛЕНИЮ НАУЧНЫХ СТАТЕЙ

Предъявленные статьи, соответствующие научному направлению журнала должны обладать, теми материалами, которые не напечатаны ни в одном журнале. Имеется ввидуте исследования с актуальными проблемами, которые печатается впервые: (военные науки, гуманитарные науки и национальная безопасность, фундаментальные и естественные науки, технические науки, экономические и информационные технологии).

Формат бумаги	- A4
Содержаниетекста	- MS Word Times New Roman
Размер шрифта	- 12 pt
Межстрочный интервал	- 1
Абзац	- 1 cm
Пробелы	- с каждой стороны 20 мм
Объём	- 5-10 страниц (2000-5000 слов)
Название статьи	- в 3 языках, с середины, с большой буквой, с жирным шрифтом
Имя, фамилия автора	- в 3 языках,с середины, с жирным шрифтом
Научная степень, ученное звание (военное звание)	- в 3 языках,с середины
Место работы, город	- в 3 языках,с середины
E-mail	- с середины
Аннотация (150-250 слов)	- на азербайджанском, английском, русском языках
Ключевые слова (3-5)	- на азербайджанском, английском, русском языках
Ссылки	- в квадратных скобках [5, с.156]; [10]
Список	- по порядку в тексте (по требованию Высшей Аттестационной Комиссии)

В аннотация должны быть лаконично отражены содержание, актуальность исследовательской работы, научная новизна работы, важность применения, использованные методы и т.д. В вводной части научных статей отражены актуальность темы, цели и задачи, требующие сведения; оценивание предыдущих работ и их теоретические и практические значения и ещё использованные методы.

В заключительной части научной работы должны найти своё отражение научные выводы, доказанные автором; рекомендации и предложения при исследовании.

Ссылки, сделанные на научные источники должны быть указаны в квадратных скобках (например, [1] или [1, s.119]). Список литературы, приведенный в конце статьи, следует располагать по порядку в тексте, предпочтение следует отдавать научным статьям, монографиям и другим достоверным источникам, опубликованным за последние 10 лет. Требования Высшей аттестационной комиссии при Президенте Азербайджанской Республики следует учитывать при даче библиографического описания цитируемого источника.

Автору(ы) необходимо предоставить печатную копию статьи в формате A4, электронную версию, а также контактный телефон в редакцию или отправить на адрес harbiinstitut@gmail.com.

Статьи, поступившие в редакцию после рецензий анонимных рецензентов (2 положительные рецензии) будут рекомендованы на издание ответственным редактором или же одним членом редакционной коллегии. В случаях отказа напечатать статью редакция журнала в письменной форме уведомляет автора.

ОБРАЗЕЦ СТАТЬИ:

ПОЛУЖИРНЫЕ И ПРОПИСНЫЕ БУКВЫ

Имя и Фамилия
научная степень, ученное звание (военное звание)
Место работы, Город
Электронной почты, ORCİD (если это) номер телефона

Аннотация
Ключевые слова:

Вступление

1. Название

1.1. Половинаназвания

Заключение

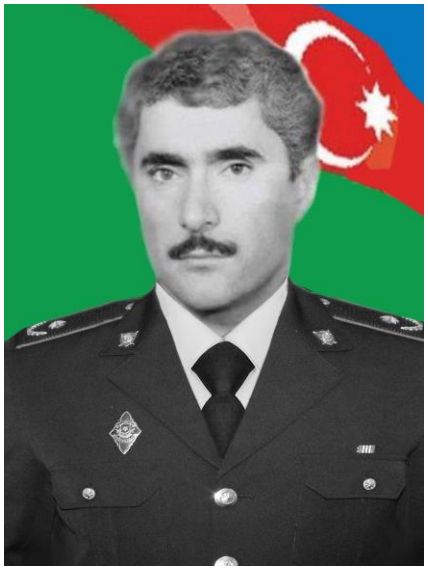
Литература

Qəhrəmanlarımız unudulmur

Azərbaycanın azadlığı, müstəqilliyi uğrunda mübarizə aparan, igidlik göstərən qəhrəmanlarımızla xalqımız hər zaman fəxr edir...

İlham Əliyev

ƏLİF HACIYEV



Əlif Lətif oğlu Hacıyev, 1953-cü ilin iyun ayının 24-də Xocalı şəhərində anadan olmuşdur.

1970-ci ildə məktəbi bitirərək, Xankəndi şəhərində sürücülük peşəsinə yiyələnmişdir. 1971-ci ildə Əlif Hacıyev ordu sıralarına çağırılmışdır. Hərbi xidməti Minsk şəhərində keçmişdir. 1973-cü ildə ordudan tərxis olunaraq, Xankəndi Avtonəqliyyat Müəssisəsində sürücü işləmişdir. 1974-84-cü illərdə Əlif Hacıyev Belarusiya DİN-nin və Azərbaycan SSR DQMY-nin daxili işlər orqanlarında müxtəlif vəzifələrdə işləmişdir.

1976-cı ildə Əlif Hacıyev SSRİ DİN-nin Frunze adına Xüsusi Orta Milis Məktəbinə daxil olmuşdur. O, 1979-cu ildə həmin məktəbi bitirmiş, 1981-ci ildən təhsilini SSRİ DİN-nin Akademiyasında davam etdirmişdir.

DQMV-də işləyərkən uzun müddət fəaliyyət göstərən gizli erməni millətçi mərkəzini ifşa etməyə çalışmışdır. Buna görə də erməni millətçiləri onu saxta ittihamlarla günahlandıraraq, 10 il həbs cəzasına məhkum etdirmişdilər. 1987-ci ildə Əlif Hacıyevin işinə yenidən baxılmış, 10 il həbs cəzası 6 ilə endirilmişdir. Sonra o, bəraət almış, azadlığa buraxılmışdır.

1990-cı ildə Əlif Hacıyev Xocalıya qayıdır və Dağlıq Qarabağ üzrə Təşkilat Komitəsində, Qarabağa Xalq Yardımı Komitəsində fəaliyyət göstərərək erməni millətçilərinə qarşı mübarizəsini yenidən davam etdirmişdir. O, 1990-cı ilin dekabr ayında daxili işlər orqanlarına yenidən bərpa olunmuş və Xocalı Təyyarə Limanı Xətt Daxili İşlər bölməsinə rəis təyin edilmişdir. Eyni zamanda o, Xocalı aeroportunun komendantı olmuşdur. Yaxşı işinə görə 1991-ci ilin dekabr ayında ona mayor rütbəsi verilmişdir.

Qarabağ cəngavəri Əlif Hacıyevin əzmkarlığı nəticəsində Xocalı aeroportu erməni millətçilərinin nəzarətindən tamamilə çıxmışdı. Bunun əvəzini çıxmaq üçün düşmən – "Xocalının alınması əməliyyatı"na başlamışdı. Qədim Xocalının başı üzərində real təhlükə yaranmışdı. Bunu çoxları kimi Əlif Hacıyev də görmüşdü. Faciə 1992-ci ilin fevral ayının 25-dən başladı. Düşmən nə qədər güclü olsa da Qarabağ cəngavəri dinc əhalini təhlükəsiz yerə çıxarmaqdan ötrü misilsiz qəhrəmanlıqlar göstərdi. Vətənini, torpağını canından əziz bilən Əlif Hacıyev avtomatın darağını dəyişərkən düşmən gülləsindən Qarabağ torpağında - Xocalı faciəsi zamanı şəhid oldu.

Azərbaycan Respublikası Prezidentinin 6 iyun 1992-ci il tarixli 831 saylı Fərmanı ilə mayor Hacıyev Əlif Lətif oğluna (ölümündən sonra) **"Azərbaycanın Milli Qəhrəmanı"** adı verilmişdir.

Ailəli idi. İki qız övladı var.

Əlif Hacıyev Bakı şəhərində, Şəhidlər Xiyabanında dəfn edilmişdir. Bakı şəhərinin Nizami rayonundakı küçələrdən biri Qəhrəmanın adını daşıyır.

CEYHUN HƏSƏNOV

Ceyhun Aydın oğlu Həsənov, 1985-ci il oktyabr ayının 29-da Tovuz rayonunun Çeşməli kəndində anadan olub. 1992-2001-ci illərdə Xətai rayonunda Ə.Abbasov adına 257 nömrəli tam orta məktəbdə, 2001-2003-cü illərdə isə Cəmşid Naxçıvanski adına Hərbi Liseydə təhsil alıb. 2004-2008-ci illərdə Heydər Əliyev adına Azərbaycan Ali Hərbi Məktəbində (indiki Heydər Əliyev adına Hərbi İnstitut) "Motoatıcı" ixtisası üzrə ali hərbi təhsil alıb. Ailəli idi. 2 əkiz oğlu var.

Həsənov Ceyhun Aydın oğlu, 2009-2019-cu illərdə Azərbaycan Silahlı Qüvvələrinin Naxçıvan şəhərində yerləşən "N" saylı hərbi hissəsində, 2019-cu ildən isə Beyləqan rayonunda yerləşən "N" saylı hərbi hissəsində xidmət edib.

Azərbaycan Ordusunun kapitanı olan Ceyhun Həsənov 2020-ci il sentyabrın 27-də Azərbaycan Silahlı Qüvvələri tərəfindən Ermənistanın işğalı altında olan ərazilərin azad edilməsi üçün başlanan Vətən Müharibəsi zamanı Füzulinin azadlığı uğrunda gedən döyüşlərdə savaşıb. Ceyhun Həsənov sentyabrın 27-də Füzuli döyüşləri zamanı şəhid olub. İkinci Fəxri Xiyabanda dəfn olunub.

Azərbaycanın ərazi bütövlüyünün bərpa edilməsində xüsusi xidmətlərinə və işğal olunmuş ərazilərin azad olunması zamanı düşmənin məhv edilməsi üzrə qarşıya qoyulmuş döyüş tapşırığını yerinə yetirən zaman göstərdiyi qəhrəmanlıq nümunəsinə görə, həmçinin hərbi qulluq vəzifəsini yerinə yetirən zaman igidlik və mərdlik nümayiş etdirdiyinə görə Azərbaycan Respublikasının Prezidenti İlham Əliyevin 09.12.2020-ci il tarixli Sərəncamına əsasən Ceyhun Həsənova ölümündən sonra **"Vətən Müharibəsi Qəhrəmanı"** adı verilib.

Azərbaycanın ərazi bütövlüyünün təmin edilməsi uğrunda döyüş əməliyyatlarına qatılan və hərbi hissə qarşısında qoyulmuş tapşırıqların icrası zamanı vəzifə borcunu şərəflə yerinə yetirdiyi üçün Azərbaycan Respublikasının Prezidenti İlham Əliyevin 15.12.2020-ci il tarixli Sərəncamına əsasən Ceyhun Həsənov ölümündən sonra "Vətən uğrunda" medalı ilə təltif edilib.

Azərbaycanın Füzuli, Qubadlı, Şuşa rayonlarının işğaldan azad edilməsi uğrunda aparılan döyüş əməliyyatlarına qatılaraq, şəxsi igidlik və şücaət nümayiş etdirdiyinə görə Azərbaycan Respublikasının Prezidenti İlham Əliyevin 25.12.2020-ci il tarixli Sərəncamına əsasən Ceyhun Həsənov ölümündən sonra "Füzulinin azad olunmasına görə", 29.12.2020-ci il tarixli Sərəncamına əsasən "Qubadlının azad olunmasına görə", 24.06.2021-ci il tarixli Sərəncamına əsasən "Şuşanın azad olunmasına görə" medalları ilə təltif edilib.

Heydər Əliyev adına

HƏRBİ İNSTİTUT