MCIT
Modeling, control & information technologies

# *Ensuring Information Security within the Military Environmental Safety System*

https://doi.org/10.31713/MCIT.2025.055

Ramil Akhundov
National Defence University
ORCID ID: 0009-0001-8798-8044
Baku, Azerbaijan
mr.axundov1@gmail.com

Bayram Ibrahimov
National Defence University
Azerbaijan Technical University
Baku, Azerbaijan
i.bayram@mail.ru

**Abstract** - The growing complexity of military operations in environmentally hazardous zones has led to the increased reliance on digital technologies for radiation and chemical monitoring. Modern military environmental safety systems depend on distributed sensor networks, unmanned aerial vehicles (UAVs), automated data processing modules, and real-time telemetry to detect, assess, and respond to ecological threats. However, the integration of these digital components introduces new vectors of vulnerability, particularly in the domains of cyber and information security.

This paper analyzes the crucial role of information security in maintaining the integrity, availability, and reliability of environmental monitoring data within military contexts. It outlines a comprehensive threat model that identifies common cyberattack scenarios such as data spoofing, signal interception, denial of service, and unauthorized access. To counter these risks, the article proposes a layered security architecture that incorporates encryption, authentication, anomaly detection, access control, and secure logging mechanisms. Each layer of the data lifecycle, from initial sensor acquisition to command-level decision support, is addressed in terms of its specific protection requirements and operational constraints.

In addition to architectural design, a risk-based response matrix is introduced to guide the prioritization of protective measures based on threat probability and mission-criticality. The proposed framework is evaluated through scenario analysis and performance metrics, highlighting its potential to improve resilience and reduce system vulnerability in the face of both cyber and environmental threats.

The study concludes that robust information security is not a peripheral function but a foundational element of effective environmental safety systems in modern armed forces. Its integration directly influences decision-making accuracy, troop protection, and mission continuity in complex operational theaters.

**Keywords** - military environmental safety, information security, radiological threats, cyber protection, UAV telemetry, secure architecture, risk matrix, command integration, anomaly detection, operational resilience.

## I.INTRODUCTION

The evolution of military environmental safety systems has brought a growing reliance on automated data collection, networked sensors, and unmanned platforms [1-7]. These systems provide crucial situational awareness in the context of radiological, chemical, and biological threats, enabling timely decisions and protective actions. However, as these platforms increasingly depend on real-time information exchange and remote control, they become vulnerable to a range of cyber and information security threats.

In this context, ensuring the confidentiality, integrity, and availability of environmental monitoring data is not only a technical necessity but also a strategic imperative [8, 9]. Compromised or falsified data from radiation sensors, UAVs, or field-deployed monitoring stations can lead to delays in warnings, flawed threat assessments, or misdirected protective responses. Such disruptions can have cascading consequences: exposing troops to contamination, misallocating decontamination resources, or even triggering unnecessary evacuations [10-15].

This article addresses the intersection of environmental and information security within military systems. It proposes a conceptual framework for securing data flows and decision-making processes in environmental safety infrastructures. The aim is to analyze the most relevant cyber threats, define architectural principles for resilient systems, and present practical measures for protecting critical data across the entire chain from sensor to command.

## II.BACKGROUND AND RELATED WORK

In military contexts, environmental safety systems are increasingly intertwined with digital communication and sensing technologies [15-18]. From mobile radiation reconnaissance units and chemical detection networks to unmanned aerial vehicles (UAVs) and automated meteorological stations, modern environmental monitoring depends on real-time telemetry, remote access, and cloud-based analytics. While these technologies greatly enhance situational awareness and decision-making, they also introduce vulnerabilities traditionally associated with information and communication systems.

The threat landscape includes data interception, spoofing, signal jamming, malware injection, and denial-of-service attacks targeting environmental monitoring platforms [19-23]. For example, a false radiation alert generated by a compromised sensor may provoke unnecessary evacuation or disrupt mission execution. Alternatively, a cyberattack on UAV telemetry systems could suppress the transmission of contamination data, delaying protective measures and exposing personnel to unseen hazards. These threats are particularly dangerous during joint operations or in high-tempo scenarios where decision cycles are compressed and situational clarity is paramount.

Previous work on information security in military systems has focused on tactical communications, command and control infrastructures, and critical national cyber defense [24, 25]. NATO STANAG 5066, US DoD Directive 8500, and NIST SP 800-82 provide robust cybersecurity guidelines for military and industrial control systems [26,27,28]. However, these standards do not fully address the specific challenges associated with environmental data: mobile sensors, hybrid data types (e.g., chemical, radiological, meteorological), and dynamic field conditions.

Recent studies have explored secure sensor networks for smart cities and industrial safety systems, incorporating encryption, anomaly detection, and blockchain auditing. Some dual-use frameworks, such as those proposed for CBRN (Chemical, Biological, Radiological, and Nuclear) emergency networks, are applicable to military use [29-34]. However, in most cases, these frameworks are not directly adapted to the hybrid nature of military environmental security, where battlefield constraints, intermittent connectivity, and adversarial interference require a more tailored approach.

This paper builds upon these foundations by identifying the specific vulnerabilities of military environmental safety architectures and proposing countermeasures that align with both operational requirements and cybersecurity best practices. The goal is to bridge the current gap between environmental monitoring technologies and the principles of military-grade information assurance.

## III. THREAT MODEL AND REQUIREMENTS

The operational environment of military environmental safety systems is inherently exposed to a wide spectrum of information threats. These threats target the critical properties of military data systems: confidentiality (preventing unauthorized access), integrity (ensuring that data is not tampered with), and availability (guaranteeing timely access to information when needed). In the context of ecological safety operations such as radiation or chemical reconnaissance, UAV monitoring, or automated early warning, breaches in any of these dimensions can lead to operational failure or environmental catastrophe [35, 36].

The threat model in this domain includes both passive and active adversaries. Passive threats involve interception of unencrypted data streams, allowing hostile actors to observe troop movements, contamination zones, or mission-sensitive telemetry. Active threats include data manipulation (altering sensor readings), spoofing (injecting false alarms or suppressing real ones), denial-of-service attacks on communication nodes, and remote takeovers of unmanned systems [37]. These attacks may be technologically sophisticated or opportunistic and can be executed via kinetic means such as destruction of relay drones or cyber means such as protocol exploitation or wireless hijacking.

Additionally, insider threats must be considered. Unauthorized access by personnel or compromise of mobile devices used in the field can create entry points into otherwise hardened systems. The threat model must therefore account for human error, poor credential management, and undisciplined security zones, especially in post-conflict operations or peacekeeping deployments where joint forces or civilian contractors are present [38].

To mitigate these threats, a resilient system should incorporate multiple protective layers. These begin with encrypted data transmission from field sensors and UAVs, authenticated session management, and continuous integrity checks on all critical data streams. Sensor hardware should support secure boot and tamper detection, while communication channels must employ frequency hopping, dynamic routing, and redundancy [39]. Ground stations and command interfaces require strict role-based access control, network segmentation, and intrusion detection systems capable of recognizing anomalies in telemetry rather than just standard IT traffic.

At the same time, the system must meet real-time performance constraints dictated by the nature of environmental hazards. Delays in recognizing contamination spread or sensor failure may result in irreversible consequences for personnel or infrastructure. Therefore, information protection must not degrade responsiveness. It is essential to strike a balance between cryptographic security and operational speed, particularly in mobile, bandwidth-limited, or contested environments [40-44]. These requirements form the foundation for the architectural principles explored in the following section.

## IV. ARCHITECTURE OF PROTECTED ECO-SECURITY INFORMATION SYSTEMS

A secure environmental safety system in the military domain must function reliably in unpredictable, adversarial, and resource-constrained conditions. Its architecture must integrate environmental sensing, threat assessment, communication, and command response into a unified structure with embedded protection at every level. Unlike civilian monitoring systems, military eco-security infrastructure must not only collect data but also ensure its authenticity, confidentiality, and resilience throughout the data lifecycle.

The foundational layer of this architecture consists of field-deployed sensors and reconnaissance platforms, including radiological and chemical detectors,

meteorological stations, and UAV-based payloads. These sensors must support onboard encryption, tamper-proof firmware, and secure communication protocols. Each device should be uniquely authenticated to prevent spoofing or unauthorized data injection. Data packets generated by sensors are tagged with time, geolocation, and digital signatures to preserve provenance and integrity.

The transmission layer includes wireless relays, mobile ad hoc networks, and satellite uplinks. Here, data is routed through protected channels using encrypted tunnels, frequency-hopping techniques, and error-correcting protocols. To reduce the risk of interception or delay, redundant communication paths and dynamic routing policies should be implemented. In case of electronic warfare or signal degradation, the system must degrade gracefully and preserve data for later synchronization.

At the core of the architecture lies the fusion and analysis module. It aggregates data from multiple sources and applies integrity checks, anomaly detection algorithms, and correlation filters. Any discrepancy between expected and received values, such as a sudden drop in radiation without an atmospheric change, is flagged for human review or automatic quarantine. This layer also feeds into AI-based predictive systems, enabling early warnings about contamination spread or equipment malfunction.

The decision support and command layer connects with military information systems and uses role-based access control, multifactor authentication, and session audit logging. Access to critical dashboards is segmented according to security clearance, operational role, and physical location. The system must also support autonomous decision logic when disconnected from higher command due to jamming or sabotage.

Overall, the architecture must be modular, scalable, and adaptable. It should allow secure integration of new platforms and remain auditable according to national defense cybersecurity standards. Most importantly, the architecture must ensure that environmental data, which directly influences the health and safety of personnel, cannot be falsified, delayed, or leaked by internal or external actors. This integration of cyber hygiene with environmental awareness defines the next generation of military environmental safety systems.

The layered architecture of military environmental information systems integrates security mechanisms across all stages of data flow. This structure is visualized in Figure 1.

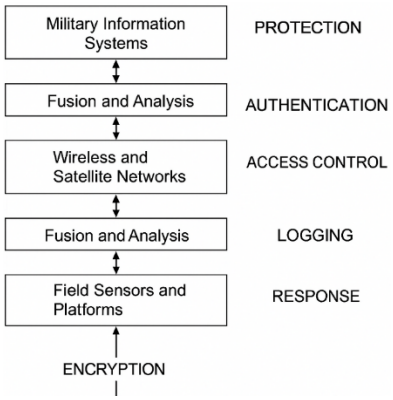


Figure 1. Information flow and protection layers in the military eco-security system

## V. RISK-BASED SECURITY MECHANISMS

The implementation of information security in military environmental safety systems requires more than static protections. It must rely on dynamic, risk-oriented mechanisms that prioritize response based on the likelihood and potential impact of threats. This approach ensures that system resources are directed where they matter most, particularly under constrained conditions such as limited bandwidth, contested environments, or partial system degradation.

In this context, a threat matrix is used to map typical cyber and data-related risks across the eco-security architecture. These include data falsification, signal jamming, denial of service, sensor spoofing, and unauthorized access. Each threat is evaluated according to two primary criteria: probability of occurrence and impact severity if exploited. Based on these factors, system designers and commanders can define appropriate security responses and prioritize mitigation strategies accordingly.

The table below outlines a simplified risk matrix for core information security threats in military environmental monitoring operations:

Table 1. Risk Matrix for Information Security Threats in Military Eco-Safety Systems

| Threat Type | Probability | Impact Severity | Risk Level | Recommended Security Measures |
|---|---|---|---|---|
| Data spoofing (sensor) | High | High | Critical | Sensor authentication, signature validation, anomaly filters |
| Signal jamming (UAV link) | Medium | High | High | Frequency hopping, redundant comms, directional antennas |
| Data interception | High | Medium | High | End-to-end encryption, rotating keys, VPN tunneling |
| Denial-of-service (DoS) | Medium | Medium | Moderate | Rate limiting, IDS/IPS, edge-based filtering |
| Unauthorized dashboard access | Low | High | Moderate | Role-based access, MFA, session logs |
| Tampering with stored data | Low | High | Moderate | Integrity hashes, audit trails, secure storage |

## VI. DISCUSSION

The integration of risk-based security mechanisms into military environmental safety systems represents a necessary evolution in the face of increasingly hybrid threats. Traditional cyber defense strategies designed for fixed networks and office infrastructures are insufficient for the demands of battlefield scenarios, where connectivity is intermittent, sensor platforms are mobile, and adversaries actively attempt to corrupt situational awareness. In this environment, information security functions as an operational enabler rather than just a protective layer.

One of the key trade-offs in implementing secure eco-monitoring systems lies in balancing protection and performance. For example, encrypting all telemetry data from UAVs improves confidentiality but may introduce latency or increase bandwidth requirements. Similarly, anomaly detection algorithms can successfully identify spoofed data but may consume significant computational resources in field-deployed edge devices. The system must therefore apply flexible and context-sensitive security policies that adjust protections based on mission phase, threat level, or terrain.

Another critical factor is human interaction. Even when systems are largely automated, final decisions often rest with operators or commanders. If the system generates too many false alarms or fails to detect threats in time, trust in the technology erodes. To avoid this, security mechanisms must be designed to support operational clarity, using understandable risk metrics and user-friendly interfaces.

A further consideration is the integration of these protected data streams into broader command and control systems. Environmental safety data must feed into decision-making platforms without introducing new points of vulnerability. Achieving this requires careful attention to system interoperability, secure interface design, and alignment with military cybersecurity doctrine.

By treating information protection as a dynamic and mission-critical component of environmental safety, the armed forces can reduce the risks posed by both technological compromise and environmental contamination. The result is not just a network of sensors but a resilient ecosystem that supports reliable decision-making in even the most uncertain conditions.

## VII.CONCLUSION

Information security is an essential component of military environmental safety systems, particularly as these systems evolve into networked and data-dependent infrastructures. In the context of radiological and chemical threats, the availability of timely and accurate environmental data is critical for effective protective measures. However, if this information is left vulnerable to cyber threats such as spoofing, interception, or disruption, it may cause more harm than good.

This article has outlined the primary threat vectors affecting eco-security information systems and introduced an architectural framework that incorporates protective measures throughout the data lifecycle. A risk-based approach was used to prioritize security mechanisms based on operational impact and likelihood of occurrence. By matching technical protections to mission conditions, military units can preserve both environmental awareness and operational readiness even in hostile or degraded environments.

Looking ahead, the focus should shift toward adaptive defense mechanisms, AI-supported risk evaluation, and deeper integration with existing command platforms. Enhancing information security within environmental safety operations is not just a technical improvement. It is a strategic necessity for maintaining resilience and trust in critical military systems.

## REFERENCES

[1] B. G. Ibrahimov, S. R. Ismaylova, A. H. Hasanov, and Y. S. Isayev, “Research and analysis criterion quality of service and experience multifractal traffic using fuzzy logic,” in Recent Developments and the New Directions of Research, Foundations, and Applications: Selected Papers of the 8th World Conference on Soft Computing, February 03–05, 2022, Baku, Azerbaijan, Vol. I, Cham: Springer Nature Switzerland, pp. 387–397, June 2023.

[2] A. H. Hasanov, K. I. Iskandarov, and S. S. Sadiyev, “The evolution of NATO's cyber security policy and future prospects,” Journal of Defense Resources Management, vol. 10, no. 1, pp. 94–106, 2019.

[3] A. H. Hasanov et al., “Scientific and technological progress or environmental safety,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 22–23, 2024.

[4] B. Zulfugarov, A. Hasanov, and E. Hashimov, “Comparative analysis of the efficiency of various energy storages,” in Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference, no. 6, pp. 42–45, Nov. 2023.

[5] A. H. Hasanov, A. H. Azizov, A. M. Mammadova, I. H. Ayyubov, and S. R. Khalilova, “Synthesis of perspective hydrocarbons for synthetic lubricants with a high viscosity characteristic,” International Journal, vol. 1, 2015.

[6] R. Akhundov, “Advancements in monitoring radiation and chemical hazards for military environmental safety,” Матеріали конференцій МЦНД, (04.07.2025; Ужгород, Україна), pp. 89–97, 2025. doi: 10.62731/mcnd-04.07.2025.002.

[7] A. M. Talibov et al., “The use of unmanned aerial vehicles for monitoring chemical and radiation contamination,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 4, pp. 88–89, 2025.

[8] A. R. Jabrayilov et al., “Development of a comprehensive environmental protection system for military facilities,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 4, pp. 82–83, 2025.

[9] I. Islamov et al, “Integrating environmental security into defense strategy with a focus on radiological and chemical risks,” Strategic directions of science development: Factors of influence and interaction: Collection of scientific papers with materials of the VII International Scientific Conference, Cherkasy, Ukraine, Sept. 26, 2025, pp. 115–125. doi: 10.62731/mcnd-26.09.2025.

[10] S. M. Babayev et al., “The impact of new technologies on the progress of military art,” in Proc. Int. Sci. and Practical Conf., vol. 6, pp. 54–56, 2024.

[11] R. G. Akhundov and E. A. Eldarov, “Special operations forces in modern conflicts,” Вестник науки и образования, no. 6(149), pp. 16–20, 2024.

[12] A. R. Jabrayilov et al., “Experience of international cooperation in the field of military environmental safety,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 1, pp. 116–117, 2025.

[13] R. Akhundov and I. Islamov, “Operational modes of environmental security systems in the armed forces facing radiation and chemical threats,” Collection of Scientific Papers

«SCIENTIA», (Aug. 22, 2025; Bern, Switzerland), pp. 103–111, 2025.

[14] Р. Г. Ахундов, А. Г. Ахмедова, Ш. Д. Даньялов, и И. И. Мустафаев, “Радиационно-стимулированные процессы получения активного угля,” Санкт-Петербург, vol. 25, no. 1, p. 47, 2020.

[15] A. Talibov et al., “The main anthropogenic sources of atmospheric pollution,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 53–54, Baku–Kharkiv–Bielsko-Biala, 2024.

[16] R. Akhundov and I. Islamov, “Innovative technologies for radiation and chemical protection in the armed forces,” Collection of Scientific Papers «ΛΌГОΣ», (June 6, 2025; Bologna, Italy), pp. 247–255, 2025.

[17] R. Akhundov, “Modern developments in the field of weapons of mass destruction and defence against them,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 132–133, 2024.

[18] R. Akhundov and I. Islam, “Ensuring environmental safety in military activities considering radiological and chemical protection,” Collection of Scientific Papers «SCIENTIA», (May 23, 2025; New York, USA), pp. 175–182, 2025.

[19] R. Mammadov et al., “Enhancing special forces management efficiency in modern operations,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 31–32, 2024.

[20] R. Akhundov and I. Islamov, “Comprehensive approach to establishing operational modes of environmental security systems in military forces under radiation and chemical hazards,” Collection of Scientific Papers «SCIENTIA», (Aug. 8, 2025; Liverpool, UK), pp. 108–116, 2025.

[21] R. Akhundov and E. Hashimov, “The impact of new technologies on enhancing the efficiency of armed,” Матеріалы конференцій МЦНД (13.06.2025; Lutsk, Ukraine), pp. 186–195, 2025.

[22] R. G. Akhundov and A. M. Talibov, “Environmental safety as a component of national security,” in The Latest Technologies – for the Protection of Airspace: Abstracts of the 20th Int. Sci. Conf. of Kharkiv National University of the Air Force Named After Ivan Kozhedub, Kharkiv, Ukraine, May 2–3, 2024, pp. 25–27.

[23] A. R. Jabrayilov et al., “The role of environmental monitoring in ensuring the safety of military units,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 1, pp. 128–129, 2025.

[24] R. Akhundov and D. Sh., “The use of modified activated coal in sorption of carbon-monoxide,” in Materials of the Int. Sci.-Practical Conf. “Radiation and Chemical Safety Problems”, Baku, Nov. 2019, pp. 161–162.

[25] A. M. Talibov et al., “Training military personnel in radiation and chemical threat protection methods,” in Proc. 15th Int. Sci. and Tech. Conf., vol. 4, pp. 94–95, 2025.

[26] R. Q. Axundov, “Azərbaycan Ordusunda radiasiya, kimyəvi və bioloji kəşfiyyatın xüsusiyətləri,” in 4-cü Sənaye İnqilabı və İqtisadiyyatın Rəqəmsallaşdırılması: Beynəlxalq Elmi Konfransın Materialları, pp. 104–108, 2023.

[27] R. Akhundov and I. Islamov, “Implementation of new technologies for cleaning and neutralizing radiological and chemical contaminants in military environments,” Матеріали конференцій МЦНД, (30.05.2025; Київ, Україна), pp. 321–329, 2025.

[28] R. Akhundov, “Establishing a global system for radiation and chemical security monitoring: importance and opportunities for international cooperation,” Collection of Scientific Papers «ΛΌГОΣ», (July 4, 2025; Zurich, Switzerland), pp. 121–127, 2025.

[29] R. Akhundov and I. Islamov, “Exploring the potential, challenges, and future of robots and autonomous systems in warfare,” Матеріали конференцій МЦНД, (18.07.2025; Тернопіль, Україна), pp. 117–126, 2025.

[30] Р. Г. Ахундов, “Построение экспериментальных изотерм адсорбции образцами угленаполненного химзащитного субстрата,” Наука, техника и образование, no. 10(63), pp. 16–20, 2019.

[31] A. M. Talibov et al., “Application of biotechnology to mitigate the consequences of radiological and chemical contamination,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 1, pp. 86–87, 2025.

[32] R. Akhundov and E. Hashimov, “The environmental impact of war: Effects, challenges, and solutions,” Матеріали конференцій МЦНД (27.06.2025; Dnipro, Ukraine), pp. 103–112, 2025.

[33] A. M. Talibov et al., “Modeling and forecasting radiological and chemical threats in the military sphere,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 1, pp. 120–121, 2025.

[34] A. Jabrayilov et al., “Digital technologies and artificial intelligence in the management of environmental safety in the army,” in Current Directions of Development of Information and Communication Technologies and Control Tools: Proc. 15th Int. Sci. and Tech. Conf., vol. 1, pp. 110–111, 2025.

[35] E. V. Mammadov et al., “Development of multilayered protection systems against chemical, radiological, and biological hazards for military personnel,” in Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 1, pp. 112–113, 2025.

[36] A. Talibov et al., “Environmental safety of nanomaterials application,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 55–56, Baku–Kharkiv–Bielsko-Biala, 2024.

[37] S. Babayev et al., “Prospects for the application of nanotechnology in the military sector,” in Problems of Informatization: Proc. 12th Int. Sci. and Tech. Conf., vol. 3, pp. 14–15, 2024.

[38] R. Akhundov, “Application of innovative technologies for the decontamination and neutralization of radiological and chemical hazards in military environments,” Collection of Scientific Papers «ΛΌГОΣ», (Aug. 1, 2025; Seoul, South Korea), pp. 107–115, 2025. doi: 10.36074/logos-01.08.2025.017.

[39] A. R. Jabrayilov et al., “Prospects for creating closed ecological life support systems,” Current Directions of Development of Information and Communication Technologies and Control Tools, vol. 4, pp. 92–93, 2025.

[40] R. Akhundov and I. Islamov, “Implementation of new technologies for cleaning and neutralizing radiological and chemical contaminants in military environments,” Матеріали конференцій МЦНД, (30.05.2025; Київ, Україна), pp. 321–329, 2025.

[41] R. Akhundov, “Ecocide in the Nagorno-Karabakh conflict: an analysis of Armenia’s environmental impact on Azerbaijan,” in Current Directions of Development of Information and Communication Technologies and Control Tools. Abstracts of the 14th Int. Sci. and Tech. Conf., Kharkiv, Ukraine, vol. 2, pp. 95–96, Apr. 2024.

[42] R. Q. Axundov, “Azərbaycan Ordusunda ekoloji təhlükəsizliyin təşkili və təkmilləşdirilməsi,” Hərbi Bilik, no. 4, pp. 7–15, 2024.

[43] R. Akhundov and I. Islamov, “Innovative technologies for enhancing environmental security in armed forces under radiation and chemical threats,” Матеріали конференцій МЦНД, (15.08.2025; Харків, Україна), pp. 141–150, 2025.

[44] R. Akhundov, “The environmental impact of military activities,” ResearchGet, 2024. [Online]. Available: ResearchGet. [Accessed: Oct. 4, 2025].