**Міністерство освіти і науки України**
**Харківський національний економічний університет**
**імені Семена Кузнеця**

***ІІІ ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ***

# *«ФІЗИЧНЕ ВИХОВАННЯ, БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ І СУЧАСНІ ТЕХНОЛОГІЇ ВИРОБНИЦТВА»*

***12 березня 2026 року***

## *Збірник наукових праць*

УДК [796+614+338](063.034)
**Ф50**
**Фізичне виховання, безпека життєдіяльності і сучасні технології виробництва** : збірник тез доповідей ІІІ Всеукраїнської науково-практичної конференції (електронне видання), 12 березня 2026 року / за заг. ред. А. А. Івашури. Харків : ХНЕУ ім. С. Кузнеця, 2026. 284 с.

*Рекомендовано до видання рішенням вченої ради*
*Харківського національного економічного університету імені Семена Кузнеця.*
*(протокол № 4 від 26.03.2026 р.)*



Збірник містить матеріали ІІІ Всеукраїнської науково-практичної конференції «Фізичне виховання, безпека життєдіяльності і сучасні технології виробництва». У наукових працях висвітлено актуальні проблеми та розвиток фізичного виховання молоді, представлена методологія, конструктивні міждисциплінарні підходи, сучасні технології й можливі моделі підвищення ефективності концепції здорового способу життя, спортивних заходів, безпеки людини і довкілля в сучасних умовах, розглянуті актуальні питання сучасних технологій виробництва та надання послуг.

Матеріали конференції можуть бути використані в науково-дослідній роботі та освітньому процесі закладів вищої освіти.

# *IV. ПИТАННЯ БЕЗПЕКИ ЛЮДИНИ І ДОВКІЛЛЯ В СУЧАСНИХ УМОВАХ*

# *IV. ПИТАННЯ БЕЗПЕКИ ЛЮДИНИ І ДОВКІЛЛЯ В СУЧАСНИХ УМОВАХ*

UDC 504.05 : 327

**Ivashura A. A.**
Ph.D. in Agriculture, Associate Professor,
Simon Kuznets Kharkiv National University of Economics

## ENVIRONMENTAL SECURITY IN THE ERA OF HYBRID THREATS: SYSTEMIC DEGRADATION AND ADAPTATION STRATEGIES

Contemporary geopolitical instability has thrust the environmental factor to the forefront of hybrid confrontation [1]. The environment is no longer viewed merely as a victim of conflict; it has evolved into a complex theater of operations in which natural processes are deliberately distorted to achieve strategic superiority. Unlike traditional conflicts, hybrid warfare involves exploiting ecological catastrophes to engineer zones of strategic chaos. This is executed through cyber-physical attacks on Industrial Control Systems (ICS) of potentially hazardous facilities, allowing aggression to be masked as industrial accidents.

At the intersection of ecology, political science, and defense technologies, a new multidisciplinary vector is actively emerging, defining the priorities for future scholarly inquiry within the changing nature of global conflicts. One of the most perilous strategies of hybrid warfare in this context is the artificial construction of an «architecture of scarcity». Unlike a direct economic blockade, this approach involves covert and purposeful interference with the reproduction of natural resources. This method is closely linked to manifestations of resource nationalism, characterized by the imposition of rigid control over critical minerals essential to the global «green transition» and the use of this dominance as an effective tool for political blackmail.

Sabotaging supply chains for lithium, cobalt, or rare earth elements can critically paralyze an adversary’s defense industry. Such actions are deliberately disguised as spontaneous environmental protests or sudden tightening of environmental legislation in exporting countries, thereby complicating their unambiguous identification as acts of aggression.

To counter these challenges, environmental forensics and attack attribution have become critically important fields. These disciplines focus on developing methodologies that distinguish natural environmental anomalies with high precision from the effects of covert technical interference. This necessitates the creation of an extensive database of anthropogenic signatures that represent interventions in natural processes.

In parallel, a priority area is the development of «digital twins» of ecosystems – dynamic, AI-based biosphere models capable of predicting the consequences of precision attacks on ecological infrastructure and proposing optimal scenarios for the rapid containment of damage.

From a legal perspective, there is an urgent need for the scientific substantiation of new international norms to regulate the «gray zone». Such frameworks should classify cyberattacks on environmentally hazardous facilities and the intentional disruption of critical raw material supplies under the guise of regulatory measures as war crimes, even in the absence of an officially declared state of war.

Simultaneously, research in the field of bioengineered resilience opens the door to using synthetic biology to create biocenoses resistant to the specific pollutants typical of hybrid attacks. This, in effect, becomes a component of the passive ecological defense of territories.

Finally, the social dimension of the problem necessitates a profound analysis of psycho-ecological resilience to understand the impact of environmental terrorism and resource scarcity on public stability. It further requires the development of methods to protect the collective consciousness from panic induced by artificially engineered life-support crises [2].

Modern environmental geospatial intelligence (ECOINT) transforms the natural environment from a passive backdrop into an active source of strategic information. In an era where traditional camouflage techniques have reached near-perfection, the ability of artificial intelligence to interpret minute biochemical and geophysical alterations becomes decisive.

By leveraging hyperspectral analysis, algorithms can transcend the limitations of human vision, capturing unique spectral signatures of vegetation stress. For instance, specific emissions from internal combustion engines or the metabolic waste products of personnel alter foliar metabolism, creating a «digital footprint». AI unerringly identifies these as anomalies in the chlorophyll index, even beneath the dense canopies of forested areas.

In parallel, Synthetic Aperture Radar (SAR) interferometry technologies enable continuous, all-weather, day-and-night monitoring of the Earth’s surface. Neural networks analyze microscopic ground subsidence, detecting voids and underground utilities that remain invisible to optical sensors. This effectively renders the landscape a transparent medium, where any large-scale engineering intervention becomes accessible to intelligence.

However, such profound technological integration in monitoring creates specific vulnerabilities inherent in the architecture of the neural networks themselves. An adversary may employ adversarial machine learning techniques to conduct «data poisoning» attacks. By introducing nearly imperceptible distortions into data streams or training datasets, an aggressor can force the system to ignore genuine ecological threats or, conversely, generate false signals of industrial disasters. Such disinformation triggers chaos in decision-making systems and compels the state to exhaust colossal resources on localizing non-existent accidents, undermining economic stability from within.

Of particular danger is the synergy between AI and hydrological modeling. The application of Graph Neural Networks (GNNs) enables an aggressor to calculate, with near-perfect precision, the cascading effects of destroying civilian infrastructure. Instead of direct military engagement, the focus shifts to managing natural processes: selecting the optimal moment to breach dams or discharge pollutants triggers a chain reaction. In this scenario, flooding simultaneously incapacitates energy hubs, blocks transport arteries, and destroys food resources. Consequently, ecology becomes not merely an object of protection but a high-precision instrument of hybrid warfare, where the boundary between a natural disaster and a planned act of sabotage virtually disappears.

Modern hybrid warfare reimagines the environmental landscape, transforming it from a theater of operations into a tool for profound psychological destabilization. Within this paradigm, nature is used as a «resonator» to amplify collective fears, with the ultimate objective not the physical destruction of the adversary but the erosion of the social contract between society and the state. Socio-ecological erosion begins the moment basic human needs – access to clean water, food, and housing security – are threatened by forces that cannot be seen, felt, or independently measured.

The phenomenon of the «invisible threat», such as radioactive contamination or the dissemination of synthetic pathogens, possesses a unique psychopathological potential. Unlike an artillery barrage, which is localized in space and time, toxic contamination engenders a state of permanent anxiety. The anticipation of delayed health consequences, fear for future generations, and the uncertainty regarding the boundaries of contamination paralyze the population’s will to resist. At this juncture, ecological sabotage is supplemented by massive information campaigns. Social networks become conduits for broadcasting catastrophic scenarios, where empirical facts are intermingled with hyperbolized rumors. The artificially constructed vacuum of reliable information is filled with «expert» opinions that discredit the official reports of monitoring services, portraying them as either incompetent or criminally deceptive.

This systemic crisis of trust constitutes a critical node of hybrid aggression. When citizens cease to trust state institutions regarding biological or environmental protection, the stage of delegitimizing authority begins. Provoked panic leads to spontaneous migration, economic collapse in affected regions, and mass protests that appear to an external observer as an internal social explosion. Thus, the aggressor achieves their objectives «by proxy», utilizing the natural human instinct for self-preservation as a battering ram against state structures. Here, ecological destruction serves merely as a trigger, initiating long-term processes of social capital degradation and transforming the territory into an unmanageable zone of chaos, where restoring order requires disproportionate resources.

The challenge of environmental restoration following hybrid attacks is exacerbated by the deliberate mining of territories and the placement of «chemical traps». Traditional soil remediation methods often prove ineffective against complex mixtures of synthetic pollutants. In this context, environmental diplomacy must transform into a tool of preventive deterrence. The establishment of international registries for «gray zone environmental crimes» would provide a legal basis for holding

actors accountable for transboundary damage, even when inflicted by non-state actors or through cyberattacks.

The future of security lies in transitioning from reactive crisis management to the creation of «environmental armor» – a system of decentralized and autonomous infrastructure nodes. Local water filtration systems, distributed energy resources based on renewables, and digital ecosystem passports can minimize the damage from centralized attacks, rendering the state less vulnerable to environmental blackmail.

The question of whether nature can possess legal personhood under conditions of war has become a subject of intense debate. Recognizing ecosystems as entities with a right to protection could fundamentally alter the rules of engagement. However, in the context of hybrid conflicts, where the boundaries between peace and war are blurred, implementing such norms requires the creation of a fundamentally new international inspection system. Such a system must be capable of conducting independent expertise under the auspices of the UN, even amidst active hostilities.

A technological response remains the only viable way to mitigate the risks posed by a high-tech aggressor. The future of environmental security is inextricably linked to the development of autonomous, intelligent monitoring systems and rapid-response technologies for detecting and responding to ecological anomalies. Only by integrating environmental parameters into the broader national security framework can a state ensure its resilience in the face of the covert challenges of the 21st century.

At the intersection of ecology, political science, and defense technologies, a new multidisciplinary vector is actively emerging, defining the priorities for future scientific inquiry. A key area in this field is environmental forensics and attack attribution, aimed at developing methodologies that enable high-precision differentiation between natural environmental anomalies and the results of covert technical interference. This necessitates the creation of a comprehensive database of anthropogenic signatures that reflect interventions in natural processes.

In parallel, a critically important direction is the development of «digital twins» of ecosystems – dynamic, AI-based biosphere models capable of predicting the consequences of precision attacks on ecological infrastructure and proposing optimal scenarios for the rapid containment of damage.

Simultaneously, research in bioengineered resilience opens the possibility of using synthetic biology to create biocenoses resistant to specific pollutants typical of hybrid attacks, effectively becoming a component of the passive ecological defense of territories.

## References

1. Ivashura A., Protasenko O., Mykhailova E., Severinov O. Study of strategies for sustainable production and consumption in the economic conditions of Ukraine. *Economics of Development.* 2022. 1, 8–16.

2. Ivashura A. A., Borysenko O. M. Analysis of eco-conscious food behavior as a factor of ecological sustainability formation. *Visnyk of V. N. Karazin Kharkiv National University. Series «Ecology».* 2021. 25, 101–110.