Comprehensive Security as an Interdisciplinary Problem: Integrating Technical, Social, and Managerial Approaches

Kirill P. Malyshkin[*]

Moscow State University of Sport and Tourism, Moscow, Russia

Abstract. *Background and relevance*. Contemporary security threats have evolved from conventional challenges into complex, hybrid, and asymmetric phenomena that transcend traditional disciplinary boundaries. Despite the interconnected nature of these threats, security research and practice remain fragmented across technical, socio-psychological, and managerial paradigms, creating dangerous blind spots. *Objective*. This article aims to develop an integrated interdisciplinary framework for comprehensive security that systematically bridges these disparate approaches and demonstrates its applicability. *Methods*. Drawing on socio-technical systems theory and supported by conceptual analysis of core concepts from each paradigm, a three-layer framework is developed encompassing physical-technical infrastructure ("hard" layer), human-social dimensions ("soft" layer), and organizational-managerial processes ("procedural" layer). The framework is illustrated through a case study of security in a modern sports complex. *Results*. The resulting model reveals that security is an emergent property of the entire socio-technical system, not reducible to any single component. The three layers interact dynamically: failures in one layer can undermine effectiveness in others, while alignment across layers produces synergistic effects. The sports facility case demonstrates how advanced technologies (hard layer) require supporting procedures (procedural layer) and security culture (soft layer) to achieve sustainable security. *Conclusion*. Sustainable security emerges from the systematic alignment of technical infrastructure, human capabilities, and organizational processes. The framework provides both a diagnostic tool for analyzing security failures and a design tool for developing comprehensive solutions, with implications for professional education, policy development, and future research.

Keywords: Comprehensive Security, Interdisciplinary Approach, Socio-Technical Systems, Risk Management, Security Culture, Organizational Resilience

1. Introduction

The global security landscape has undergone a fundamental transformation in recent decades. Traditional threats—characterized by predictability, linear causality, and clear boundaries between physical and digital domains—have given way to hybrid, asymmetric, and non-linear challenges that defy simple categorization (Koca & Çiftçi, 2025). Cyberattacks now target not only information systems but also critical infrastructure, healthcare networks, and professional sports venues (Ayub et al., 2025). The convergence of physical and digital vulnerabilities creates cascading effects whereby a breach in one domain rapidly propagates to others.

Contemporary data illustrate the magnitude of this challenge. Over one billion cyberattacks occur globally every day, with breaches increasing by 75% year over year (Koca & Çiftçi, 2025). Projections suggest that cybercrime will cost $23 trillion annually by 2027, affecting corporations, families, small businesses, and critical systems such as hospitals, emergency communications, and power grids. Simultaneously, insider threats—whether malicious, negligent, or resulting from compromise—now account for approximately 60% of data breaches, with internal actors involved in 47% of all security incidents (Thai &

[*] Corresponding author: e-mail address: ppt012@yandex.ru
DOI: 10.38098/nsom_2025_05_04_08

Tanaka, 2026).

Despite the interconnected nature of contemporary threats, security research and practice remain highly fragmented. Technical paradigms focus on IT security, cybersecurity, and engineering resilience, often treating the "human factor" as an exogenous variable to be controlled rather than understood (Hashmi et al., 2024). Social and psychological approaches contribute valuable insights into risk perception, human error, and organizational culture but frequently lack integration with technical implementation (Tao & Yu, 2025). Managerial frameworks such as ISO 31000 provide structured risk governance yet may overlook the micro-level dynamics of human-technology interaction (Xu & Shi, 2025).

This disciplinary fragmentation creates dangerous blind spots. Organizations implement sophisticated technological defenses while neglecting the cultural and procedural conditions necessary for their effectiveness. Security teams and human resources departments—both essential for insider threat prevention—often operate in isolation, speaking "different languages" and missing early warning signs that manifest at the intersection of their domains (Mahmoudian et al., 2025).

The fragmentation of security research into technical, socio-psychological, and managerial paradigms has resulted in the absence of a unifying theoretical framework that systematically bridges these perspectives. This gap leaves organizations vulnerable to threats that exploit the interstices between disciplinary domains. Consequently, security interventions often address symptoms rather than root causes, and investments in one dimension may be undermined by neglect of others.

This article addresses this problem by advancing a central thesis: comprehensive security must be understood and managed as an interdisciplinary problem, requiring the systematic integration of technical, social, and organizational knowledge. We argue that security is not a property of any single component—whether firewall, policy, or training program—but an emergent property of the entire socio-technical system. The purpose of this study is to develop and present an integrated three-layer framework that bridges existing disciplinary approaches and to demonstrate its applicability through a case study of sports facility security.

2. Materials and Methods

This study employs a multi-method approach to develop an integrated framework for comprehensive security. The methodology comprises three interconnected components: conceptual analysis, systems thinking, and framework development.

2.1. Conceptual Analysis

The first phase involved systematic conceptual analysis—the examination and integration of core concepts from disparate security disciplines. This process entailed identifying key constructs within technical, socio-psychological, and managerial paradigms and exploring their interconnections (Xu & Shi, 2025). For each paradigm, we analyzed foundational concepts, assumptions, and explanatory mechanisms, mapping points of convergence and divergence.

For example, the engineering concept of "vulnerability" refers to weaknesses in technical systems that can be exploited by threats. The sociological concept of "fear of crime" addresses perceived rather than actual risk, influencing behavior independently of objective vulnerability. Integrating these concepts reveals that technical vulnerabilities and perceived vulnerabilities interact: visible security measures may reduce fear while actual vulnerabilities persist, or conversely, may create unwarranted confidence that undermines precautionary behavior (Pott et al., 2025).

Similarly, the psychological concept of "human error" connects to managerial concepts of "process failure" and technical concepts of "usability." Errors are not simply individual failures but result from mismatches between human cognitive capabilities and system demands (Tao & Yu, 2025). Understanding this interconnection shifts intervention focus from blaming individuals to redesigning systems.

2.2. Systems Thinking Approach

The second phase applied systems thinking as the theoretical foundation for integrating disparate concepts and paradigms. Drawing on socio-technical systems (STS) theory, organizations and facilities are conceptualized as complex systems composed of interacting technical and human components (Drew et al., 2023).

STS theory emphasizes that optimal system performance requires joint optimization of social and technical subsystems. Applied to security,

this means that technical controls cannot be effective if they conflict with social dynamics, and social interventions cannot succeed if technical infrastructure does not support them. Security emerges from the alignment—or misalignment—of these subsystems.

The MIT Partnership for Systems Approaches to Safety and Security exemplifies this thinking, explicitly rejecting separation of engineering design from human factors and organizational context, arguing that "effective solutions to safety problems usually require changes at all these levels, not just in the physical system itself" (Drew et al., 2023).

Key principles of systems thinking applied to security include:

Emergence: Security properties arise from interactions among components, not from components in isolation

Interconnectedness: Changes in one part of the system propagate to others

Feedback loops: Security behaviors create reinforcing or balancing dynamics

Adaptive capacity: Resilient systems adapt to changing conditions rather than relying on static defenses

2.3 Framework Development

Based on conceptual analysis and systems thinking, we developed a three-layer conceptual framework for comprehensive security. The framework organizes security dimensions into:

Physical and Technical Infrastructure (the "hard" layer): encompassing engineering resilience, cybersecurity, and security technologies

Human and Social Dimensions (the "soft" layer): including security culture, human error, and communication

Organizational and Managerial Processes (the "procedural" layer): covering risk governance, collaboration, and ethical frameworks

These layers are not independent but interact dynamically. Failures in one layer can undermine effectiveness in others, while alignment across layers produces synergistic effects. The framework thus provides both an analytical tool for understanding security problems and a design tool for developing comprehensive solutions.

3. Results

3.1. The Three-Layer Interdisciplinary Security Model

The primary result of this study is the development of an integrated three-layer model that systematically bridges technical, socio-psychological, and managerial paradigms. Each layer comprises distinct but interconnected components that together constitute comprehensive security.

3.1.1. Layer 1: Physical and Technical Infrastructure (The "Hard" Layer)

The hard layer encompasses foundational engineering decisions and technological systems that shape security possibilities. Engineering resilience refers to the ability of physical infrastructure to withstand, absorb, and recover from disruptive events, including structural integrity, redundant systems, and fail-safe mechanisms. Architectural design significantly influences security outcomes through Crime Prevention Through Environmental Design (CPTED) principles—natural surveillance, territorial reinforcement, access control (Pott et al., 2024).

Cybersecurity constitutes the digital dimension of the hard layer, including Identity and Access Management (IAM), network security, endpoint protection, data protection, and Security Information and Event Management (SIEM) systems (Hashmi et al., 2024). The evolution of cyber threats demands equally evolved defenses against adversarial machine learning attacks, false data injection, and privacy breaches (Ayub et al., 2025; Ajiboye et al., 2024).

Integration of security technologies—biometric authentication, video surveillance analytics, and access control systems—creates coherent security ecosystems. However, technological integration generates challenges including interoperability inconsistencies, legacy system incompatibilities, and privacy concerns (Hashmi et al., 2024), underscoring that technology must be embedded in appropriate social and organizational contexts.

3.1.2. Layer 2: Human and Social Dimensions (The "Soft" Layer)

The soft layer addresses the human factors that technical approaches often neglect. Security culture encompasses shared values, beliefs, and practices that shape security behavior throughout an organization (Mahmoudian et al., 2025). Research identifies cognitive, affective,

behavioral, and normative dimensions of security culture. Training programs must move beyond compliance checklists to engage employees in understanding why security matters (Tao & Yu, 2025).

The "knowing-doing gap" poses particular challenges—employees may understand security requirements yet fail to implement them due to competing pressures, usability barriers, or habituation (Tao & Yu, 2025). Insider threats represent the most complex challenge in this dimension, arising from individuals with legitimate access who misuse that access maliciously, negligently, or through compromise (Thai & Tanaka, 2026). Internal actors now account for 47% of security incidents, with risk factors including financial strain, mental health challenges, and feelings of isolation (Heller et al., 2025).

The human dimension also encompasses crisis communication with external stakeholders. Effective communication requires preparation addressing who speaks for the organization, through what channels, with what messages, and at what speed (Pott et al., 2025), balancing transparency with operational security considerations (Hashmi et al., 2024).

3.1.3. Layer 3: Organizational and Managerial Processes (The "Procedural" Layer)

The procedural layer provides governance structures that coordinate security activities. Integrated risk assessment methodologies move beyond siloed assessments to recognize that risk categories are analytical conveniences, not natural kinds (Xu & Shi, 2025). Integration requires common risk taxonomy, unified risk registers, and consistent evaluation criteria.

Xu and Shi (2025) propose a comprehensive national security risk assessment model structured around four interconnected elements: significant national interests (assets), national security threats, national security vulnerabilities, and national security measures. This framework demonstrates how complex multidimensional risks can be systematically evaluated.

Cross-departmental collaboration is essential yet often lacking. The relationship between security and Human Resources exemplifies both need and challenge—different professional languages create communication barriers, yet insider threats manifest precisely at this intersection (Mahmoudian et al., 2025). External collaboration extends beyond organizational boundaries through information sharing, public-private partnerships, and academic partnerships (Ajiboye et al., 2024).

Legal and ethical frameworks constrain what may legitimately be done in security, addressing data protection, surveillance limitations, employee monitoring, and discrimination. Beyond legal compliance, ethical questions arise regarding appropriate surveillance levels, privacy balance, and obligations to employees exhibiting potential insider threat indicators (Drew et al., 2023; Hashmi et al., 2024).

3.2. Synthesis: Layer Interactions

The model's analytical power derives from understanding interactions across layers. Security emerges from alignment across layers; failures propagate across layers. Consider a sophisticated access control system (hard layer). If organizational culture tolerates "tailgating"—employees holding doors for strangers—technical controls are bypassed (Pott et al., 2024). If procedures for revoking access when employees leave are not followed, former employees retain entry capability (Mahmoudian et al., 2025). If privacy concerns lead to insufficient monitoring, unauthorized access may go undetected (Ajiboye et al., 2024).

Conversely, positive interactions create reinforcing cycles. Strong security culture reduces errors and increases reporting of anomalies (soft layer), generating intelligence that improves risk assessment (procedural layer), which informs technology investment priorities (hard layer). Usable, well-designed technology reduces frustration and security fatigue, supporting rather than undermining culture (Thai & Tanaka, 2026).

3.3. Case Illustration: Security in a Modern Sports Complex

Modern sports facilities concentrate virtually all dimensions of comprehensive security in a bounded environment, featuring large crowds, mixed-use spaces, critical infrastructure, high media profile, diverse threats, and multiple stakeholders (Pott et al., 2024). Contemporary threats include physical threats (terrorism, hooliganism), cyber threats (ticketing systems, building management systems), and insider threats (employees, contractors) (Pott et al., 2025).

Application of the three-layer model reveals how each layer's effectiveness depends on others. Advanced biometric access control (hard

layer) requires procedures for enrolling and deactivating users (procedural layer) and staff who understand how to respond when authentication fails (soft layer). Security culture (soft layer) shapes whether staff report anomalies, providing intelligence for risk assessment (procedural layer) that may trigger technology adjustments (hard layer). Sustainable security emerges from alignment of all three layers.

4. Discussion

4.1. The Central Argument: Security as an Emergent Systemic Property

The primary contribution of this study is the demonstration that comprehensive security must be understood as an emergent property of socio-technical systems rather than as a collection of independent components. This finding challenges the dominant paradigm in which organizations invest disproportionately in technological solutions while treating human and organizational factors as secondary considerations. The evidence synthesized from multiple research streams—technical (Hashmi et al., 2024; Ayub et al., 2025), socio-psychological (Tao & Yu, 2025; Heller et al., 2025), and managerial (Xu & Shi, 2025; Mahmoudian et al., 2025)—converges on a single conclusion: sustainable security cannot be achieved through any single dimension alone.

The three-layer model provides a framework for understanding why discipline-specific approaches inevitably fail. Technical solutions alone cannot address security because they operate within human and organizational contexts that determine their effectiveness. The Equifax breach exemplifies this principle—sophisticated encryption and access controls existed, yet a failure in organizational processes (certificate updating) created vulnerability that technical controls could not prevent. Similarly, well-designed security policies remain ineffective when organizational culture tolerates non-compliance, and security-aware employees cannot compensate for fundamentally insecure technical architectures.

Table 1. Integration of Security Paradigms in the Three-Layer Model

Paradigm	Core Contribution	Characteristic Blind Spot	Addressed By
Technical	Tools for protection, detection, response	Treats human behavior as exogenous	Soft layer (culture, training)
Socio-psychological	Understanding human dimensions of security	Lacks technical specificity	Hard layer (usable design)
Managerial	Governance structures and processes	May become disconnected from operations	Soft + Hard layers (feedback)

4.2. Theoretical Implications: Advancing Socio-Technical Systems Theory

This study extends socio-technical systems theory by applying it specifically to the security domain and elaborating the mechanisms through which technical, human, and organizational dimensions interact. Previous STS applications in security have tended to focus on either technical or social dimensions without systematically articulating their interconnections. The three-layer model operationalizes STS principles for security contexts by specifying the content of each layer and, crucially, the nature of interactions between layers.

The concept of "joint optimization"—central to STS theory—acquires specific meaning in security contexts. Joint optimization requires that technical controls be designed with human cognitive capabilities and limitations in mind (addressing the "knowing-doing gap"), that organizational processes support rather than impede secure behavior, and that feedback loops enable continuous adaptation. The sports facility case illustrates how failures cascade when joint optimization is absent and how positive synergies emerge when layers are aligned.

4.3. Practical Contributions: A Diagnostic and Design Tool

The three-layer model offers practical value as both diagnostic and design tool. As a diagnostic tool, it enables organizations to identify the source of security failures. When incidents occur, the model directs attention beyond immediate technical causes to examine whether failures originated in the hard layer (technical vulnerability), soft layer (human error or cultural factors), procedural layer (process failure), or—most commonly—interactions among layers. This diagnostic capability addresses the limitation of traditional root cause analysis, which typically remains within disciplinary boundaries.

As a design tool, the model provides a checklist for comprehensive security planning. Organizations developing security strategies can use the three layers to ensure balanced investment across dimensions. The framework suggests specific questions: Have we addressed not only technical controls but also the cultural conditions for their effectiveness? Do our procedures account for human cognitive limitations? Does our technology create usability barriers that encourage circumvention? Are our governance structures integrated across traditionally siloed functions?

4.4. Comparison with Existing Frameworks

The three-layer model compares favorably with existing security frameworks. ISO 31000 provides robust principles for risk management but lacks specific guidance on technical-human integration. The NIST Cybersecurity Framework excels in technical and procedural dimensions but gives limited attention to organizational culture and human factors. Zero Trust Architecture appropriately emphasizes continuous verification but may underestimate the cultural changes required for implementation.

The proposed model complements rather than replaces these frameworks, providing an overarching structure within which they can be situated. Organizations can map ISO 31000 processes to the procedural layer, NIST controls to the hard layer, and cultural interventions to the soft layer, using the three-layer model to ensure that investments in each framework are coordinated and mutually reinforcing.

4.5. Limitations and Boundary Conditions

This study has several limitations that suggest directions for refinement. First, the framework's validity has been established primarily through conceptual analysis and illustrative case study rather than empirical testing. Future research should operationalize the model and test its predictive power across diverse organizational contexts. Second, the relative importance of each layer may vary across sectors—critical infrastructure may require greater emphasis on the hard layer, while service industries may find the soft layer particularly salient. Third, the model's applicability beyond organizational settings to national and international security domains requires further investigation.

5. Conclusion

This article has addressed the problem of disciplinary fragmentation in security research by arguing that comprehensive security must be understood as an inherently interdisciplinary problem requiring integration across technical, social, and organizational dimensions. The three-layer model presented here provides a framework for analyzing security challenges and developing integrated solutions.

Several key findings emerge from this analysis. First, each disciplinary paradigm—technical, socio-psychological, and managerial—addresses essential aspects of security while exhibiting characteristic blind spots that can only be addressed through integration. Second, the three layers of the proposed framework are not independent but interact dynamically; failures in one layer can undermine effectiveness in others, while alignment across layers produces synergistic effects. Third, sustainable security emerges not from technological sophistication alone, but from the systematic alignment of technical infrastructure, human capabilities, and organizational processes.

The implications extend beyond academic understanding to professional practice, organizational governance, and public policy. Developing T-shaped professionals capable of interdisciplinary collaboration, moving from fragmented to integrated governance structures, and investing in research that bridges disciplinary boundaries are essential steps toward more effective security.

The evolution of threats—from conventional to hybrid, from linear to non-linear, from predictable to emergent—demands evolution in thinking about security. The recognition that security is a systemic property, not a collection of components, provides the foundation for that evolution. Future research should focus on

developing metrics for security culture, modeling technical-social interactions, evaluating intervention effectiveness, addressing ethical dimensions of comprehensive surveillance, and exploring human-as-sensor frameworks. Only through such interdisciplinary efforts can organizations and societies develop the comprehensive security posture required for the challenges of the twenty-first century.

CRediT author statement: The author contributed to all aspects of this work, including conceptualization, methodology, formal analysis, investigation, and writing. The final manuscript has been read and approved by the author, who assumes full responsibility for its content.

Funding: No funding was obtained for this study.

Conflict of interest: The author declares no competing interests.

Highlights:

- Security threats have evolved into hybrid, asymmetric phenomena requiring integrated responses
- Traditional discipline-specific approaches create dangerous blind spots in security management
- A three-layer framework integrates technical, human-social, and organizational-managerial dimensions
- Sports facilities serve as microcosms demonstrating the necessity of interdisciplinary security
- Sustainable security requires synergistic alignment across all three layers, not technological sophistication alone

References

1. Ajiboye, P. O., Agyekum, K. O.-B. O., & Frimpong, E. A. (2024). Privacy and security of advanced metering infrastructure (AMI) data and network: a comprehensive review. *Journal of Engineering and Applied Science*, 71(1), 91. https://doi.org/10.1186/s44147-024-00422-w

2. Ayub, A., Abidin, Z. Z., Alhammadi, A., Khan, M. A., Soliman, N. F., Ghazali, N. B., & Algarni, A. D. (2025). Comprehensive analysis of security threats and privacy issues in indoor localization systems. *Scientific Reports*, 15(1), 44625. https://doi.org/10.1038/s41598-025-22204-x

3. Drew, M. K., Toohey, L. A., Smith, M., Baugh, C. M., Carter, H., McPhail, S. M., Jacobsson, J., Timpka, T., & Appaneal, R. (2023). Health Systems in High-Performance Sport: Key Functions to Protect Health and Optimize Performance in Elite Athletes. *Sports Medicine*, 53(8), 1479–1489. https://doi.org/10.1007/s40279-023-01855-8

4. Hashmi, E., Yamin, M. M., & Yayilgan, S. Y. (2024). Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security. *AI and Ethics*, 5(1), 1–19. https://doi.org/10.1007/s43681-024-00529-z

5. Heller, I., Michel, G., Seiler, R., Raguindin, P. F., & Schumacher Dimech, A. (2025). Long-term effects of childhood sport participation and social support on social anxiety: Findings from a 15-year longitudinal study in Switzerland. *Journal of Public Health*. Advance online publication. https://doi.org/10.1007/s10389-025-02568-0

6. Koca, M., & Çiftçi, S. (2025). A comprehensive bibliometric analysis of Big Data and Cyber Security: intellectual structure, trends, and global collaborations. *Knowledge and Information Systems*, 67(1), 10245–10270. https://doi.org/10.1007/s10115-025-02531-1

7. Mahmoudian, A., Izadi, B., & Pyun, D. Y. (2025). Challenges of social media workers in football clubs using technology-organization-environment (TOE) framework. *Future Business Journal*, 11(1), 188. https://doi.org/10.1186/s43093-025-00619-2

8. Pott, C., Spiekermann, C., Breuer, C., & ten Hompel, M. (2024). Managing logistics in sport: a comprehensive systematic literature review. *Management Review Quarterly*, 74(4), 2341–2400. https://doi.org/10.1007/s11301-023-00361-5

9. Pott, C., Zubrod, P., Reining, C., Breuer, C., & ten Hompel, M. (2025). How does the ball get onto the pitch? Equipment logistics management in sport organizations. *Review of Managerial Science*. Advance online publication. https://doi.org/10.1007/s11846-025-00874-1

10. Shao, Y., Wang, L., Jin, H. T., & Ye, H. X. (2025). The motivational factor of working to involve outdoor sport as mediated by health awareness and social influence: a case study for China and Malaysia. *BMC Public Health*, 25(1), 1389. https://doi.org/10.1186/s12889-025-22661-z

11. Tao, H., & Yu, F. (2025). The impact of psychological needs, social support, and sport

motivation on college students' sport commitment and sports participation. *BMC Psychology*, 13(1), 821. https://doi.org/10.1186/s40359-025-03173-2

12. Thai, B. L. T., & Tanaka, H. (2026). Security and characteristics of Japanese user-created passwords: a comprehensive analysis. *International Journal of Information Security*, 25(1), 1–16. https://doi.org/10.1007/s10207-025-00412-2

13. Xu, Z., & Shi, J. (2025). Research on the national security risk assessment model: a case study of political security in China. *Humanities and Social Sciences Communications*, 12(1), 906. https://doi.org/10.1057/s41599-025-05278-w

Комплексная безопасность как междисциплинарная проблема: интеграция технических, социальных и управленческих подходов

К. П. Малышкин

Московский государственный университет спорта и туризма, Москва, Россия

Резюме. *Актуальность.* Современные угрозы безопасности эволюционировали от традиционных вызовов к сложным, гибридным и асимметричным феноменам, выходящим за рамки традиционных дисциплинарных границ. Несмотря на взаимосвязанный характер этих угроз, исследования и практика в области безопасности остаются фрагментированными между технической, социально-психологической и управленческой парадигмами, что создает опасные «слепые зоны». *Цель* данной статьи — разработать интегрированную междисциплинарную модель комплексной безопасности, которая системно объединяет эти разрозненные подходы, и продемонстрировать ее применимость. *Методы.* Опираясь на теорию социотехнических систем и концептуальный анализ ключевых понятий из каждой парадигмы, разработана трехуровневая модель, включающая физико-техническую инфраструктуру («жесткий» уровень), человеко-социальные аспекты («мягкий» уровень) и организационно-управленческие процессы («процедурный» уровень). Модель иллюстрируется на примере обеспечения безопасности в современном спортивном комплексе. *Результаты.* Полученная модель демонстрирует, что безопасность является эмерджентным свойством всей социотехнической системы, а не сводится к какому-либо отдельному компоненту. Три уровня взаимодействуют динамически: сбои на одном уровне могут подрывать эффективность других, в то время как согласованность между уровнями создает синергетические эффекты. Пример спортивного объекта наглядно показывает, как передовые технологии («жесткий» уровень) требуют поддерживающих процедур («процедурный» уровень) и культуры безопасности («мягкий» уровень) для достижения устойчивой безопасности. *Заключение.* Устойчивая безопасность достигается путем системного согласования технической инфраструктуры, человеческого потенциала и организационных процессов. Предложенная модель служит как диагностическим инструментом для анализа провалов в безопасности, так и инструментом проектирования комплексных решений, что имеет значение для профессионального образования, разработки политики и будущих исследований.

Ключевые слова: комплексная безопасность, междисциплинарный подход, социотехнические системы, управление рисками, культура безопасности, организационная устойчивость

Information about the author

Kirill P. Malyshkin, PhD student, Moscow State University of Sport and Tourism, Moscow, Russia, e-mail: ppt012@yandex.ru

Информация об авторе

Малышкин Кирилл Павлович, соискатель, Московский Государственный Университет спорта и туризма (МГУСиТ), e-mail: ppt012@yandex.ru

Citation: Malyshkin, K. P. (2025). Comprehensive Security as an Interdisciplinary Problem: Integrating Technical, Social, and Managerial Approaches. *Natural Systems of Mind, 5(4),* 122-129. doi: 10.38098/nsom_2025_05_04_08