Alina Kulbachna
Kyiv National University of Technologies and Design
(Kyiv, Ukraine)
Maryna Vyshnevska
Kyiv National University of Technologies and Design
(Kyiv, Ukraine)

INFORMATION SECURITY IN NETWORKS

The rapid evolution of information and communication systems, global networks, and converged technologies introduces increasingly complex challenges for the field of information security. As digital ecosystems expand, the volume of Internet traffic grows exponentially, and network architectures become more heterogeneous-incorporating cloud services, edge computing, and space-based segments-traditional perimeter-based security models demonstrate diminishing effectiveness. The emergence of multi-level network infrastructures, often characterized by dynamic topologies and diverse protocols, demands a holistic view of data protection. In this context, information security in networks is no longer solely a technical discipline but also a socio-technical and systemic endeavor. A comprehensive approach must integrate technical countermeasures, organizational policies, human factors, and structural vulnerabilities. This article argues that only through such multidimensional analysis can modern network environments be adequately secured against evolving threats.

One of the fundamental methodologies proposed for protecting network resources is multi-level analysis encompassing technical, social, and structural dimensions. Unlike conventional models that focus exclusively on encryption or access control, this approach recognizes that security failures often originate at the intersection of different layers-for example, when protocol design (syntactic level) fails to account for user behavior (pragmatic level) or when data semantics are misinterpreted by intrusion detection systems. As the author states, "The use of a semiotic model makes it possible to streamline approaches to protecting various types of traffic and protocols in infocommunication networks" (Tolkachov, 2024, 85). Therefore, network security must

be conceived as an integrated system where technical encryption mechanisms and protocol specifications cannot operate in isolation from the operational context. The semiotic model proposed by Tolkachov offers a structured way to decompose security into three analytical planes: the semantic level (content of transmitted data, including hidden metadata), the syntactic level (structure of packets, headers, and state machine logic), and the pragmatic level (social impact, user intentions, and real-world usage patterns of network traffic). Analyzing all three levels is essential to design protection that is not only cryptographically sound but also practically effective under actual network conditions, including insider threats, misconfigurations, and social engineering attacks.

Another critical area of focus involves the standardization and quantification of risk assessment processes. Current risk assessment methods in many organizations remain largely qualitative and subjective, relying on expert judgments that vary significantly between individuals and across contexts. Such subjectivity leads to inconsistent decision-making, misallocation of security resources, and ultimately residual risk that is poorly understood. To address this gap, researchers have developed frameworks such as the Information Security Continuous Protection (ISCP) model, which introduces scientific and quantitative techniques into risk evaluation. As the authors assert: "ISCP's scientific and quantitative methods make risk assessments more objective... assisting organizations in reliably and effectively prioritizing essential controls" (Alsafwani, Fazea & Alnajjar, 2024, 2). To achieve robust information security in networks, quantitative models are needed to reduce the influence of human bias and subjective rankings. The ISCP framework enables organizations to prioritize security measures based on objective criteria-specifically, vulnerability severity level, threat impact magnitude, and estimated remediation cost. This data-driven prioritization ensures that security investments are allocated efficiently, especially in large-scale or complex networks where hundreds of potential vulnerabilities compete for limited attention. By adopting such quantitative approaches, network administrators can reduce risks to an

acceptable level while maintaining operational continuity, even in dynamic environments such as software-defined networking or multi-tenant data centers.

In highly complex network architectures, such as space information networks (SINs), threat analysis becomes particularly challenging due to long propagation delays, intermittent connectivity, and exposure to physical adversarial actions. For a systematic approach, protection efforts are often organized around three core security attributes: confidentiality, integrity, and availability (the classic CIA triad). However, in space and multi-layer networks, each attribute acquires specialized sub-functions. According to Wu et al., "the confidentiality includes confidential information-exchange and Authentication and Key Agreement (AKA), the integrity includes information identification and information restoration, and the availability includes link establishment, routing mechanism, and mobility management" (Wu, Du, Fan, Guo, Ren, Wu & Zheng, 2023, 3429). This decomposition illustrates that, despite technological heterogeneity, the foundational principles of security remain constant: protection against data leakage and unauthorized access (confidentiality), assurance that data is not altered undetectably (integrity), and guaranteed access to resources when needed (availability). Moreover, in space networks, integrity mechanisms must include both proactive identification of corrupted packets and reactive restoration using erasure coding or retransmission protocols. Availability, in turn, depends on resilient link establishment under high latency, adaptive routing mechanisms that tolerate node failures, and mobility management for low-earth-orbit satellite constellations. Thus, a thorough threat analysis maps each network function to the relevant security attribute, enabling layered defenses that are both technically rigorous and operationally feasible.

The overarching idea behind modern information security in networks is that protection must be thorough, multi-layered, and context-aware. Isolated solutions-such as firewalls or antivirus software alone-are no longer sufficient. Instead, security architects must consider how information traverses networks, accounting for technical constraints (bandwidth, topology), structural features (protocol stacks, routing policies),

and social factors (user behavior, administrative procedures). Standardized quantitative risk management models, such as ISCP, play an essential role in transforming security from an art into a measurable science, helping stakeholders objectively determine security priorities across large-scale infrastructures. Additionally, the attribute-based approach linking threats to confidentiality, integrity, and availability provides a step-by-step methodology for analyzing even the most complex networks, including space-based systems. By integrating semiotic analysis, quantitative risk assessment, and the CIA triad, organizations can design defense strategies that are not only reactive but also predictive and adaptive to emerging threats. Future research should focus on automated risk quantification using machine learning, real-time semantic anomaly detection, and cross-layer security optimization for terrestrial and extra-terrestrial networks.

REFERENCES:

1. Alsafwani, N., Fazea, Y., & Alnajjar, F. (2024). Strategic approaches in network communication and information security risk assessment. Information, 15(6), 353.
2. Tolkachov, M.Yu. (2024). Mekhanizmy zakhystu trafiku v kiberprostori. [Mechanisms of traffic protection in cyberspace]. Suchasnyi zakhyst informatsii, No. 4, pp. 85–99. [in Ukrainian].
3. Wu, X., Du, Y., Fan, T., Guo, J., Ren, J., Wu, R., & Zheng, T. (2023). Threat analysis for space information network based on network security attributes: a review. Complex & Intelligent Systems, 9(3), 3429-3468.

Maksym Marshuba
Kyiv National University of Technologies and Design (Kyiv, Ukraine)
Liudmyla Roienko
Kyiv National University of Technologies and Design (Kyiv, Ukraine)

POLITICAL SCIENCE AS ONE OF THE MOST IMPORTANT PROFESSIONS IN MODERN UKRAINE

In the 21st century — the era of the digital revolution, everyone has the right to choose their profession and start being interested in it from childhood. Studies have shown that due to the full-scale war and access to Internet resources the profession of political scientist has become important for the future of Ukraine. It should also be noted