

S. V. Onyshchenko,
orcid.org/0000-0002-6173-4361,
Ye. O. Zhyvylo,
orcid.org/0000-0003-4077-7853,
A. D. Hlushko*,
orcid.org/0000-0002-4086-1513,
O. S. Gaydash,
orcid.org/0009-0009-0030-1528

National University “Yuri Kondratyuk Poltava Polytechnic”
Poltava, Ukraine

* Corresponding author e-mail: glushk.alina@gmail.com

SUBSTANTIATION OF SELF-ORGANIZATION APPROACHES IN INFORMATION NETWORKS TO STRENGTHEN CYBER RESILIENCE

Purpose. To formalize mathematical approaches and models that can be effectively applied to key self-organization methods of information networks within economic entities, considering the estimated dependencies between operational parameters and controllable variables across various levels of the OSI model.

Methodology. This research proposes an approach to modeling information infrastructure resilience based on the application of route optimization algorithms (Dijkstra, Bellman-Ford), Markov process theory, machine learning tools (SVM, neural networks), as well as entropic analysis and asymmetric encryption methods (RSA, ECC). The systematic approach is implemented through the analysis of interdependencies between the layers of the OSI network model to identify vulnerable segments and risk control points.

Findings. Methods of self-organization of information networks have been developed that ensure early detection of anomalies, effective management of routing and data encryption, as well as adaptability to changes in the external environment and reduction of the risk of cyber-attacks. An information infrastructure protection architecture has been developed that covers seven levels of the OSI model, ensuring the integrity, availability, and confidentiality of data in the information networks of economic entities.

Originality. This research proposes an approach to ensuring the resilience of information networks, distinguishing itself from existing methods by the coordinated application of mathematical, cryptographic, and cognitive methods within the context of the OSI network layer hierarchy. The expediency of incorporating entropic control as an indicator of system randomness and potential vulnerability has been substantiated.

Practical value. The practical significance of this research lies in the applicability of its results in developing information and cybersecurity policies for economic entities. The proposed solutions contribute to strengthening not only information security but also financial and personnel security amidst digital transformation, as well as minimizing the consequences of cyber incidents.

Keywords: *information security, information infrastructure, OSI model, entropy, economic entity*

Introduction. In the contemporary context of the digital transformation of economic systems at both national and global levels, the cyber resilience of information networks serves as a foundation for ensuring the uninterrupted operation of critical infrastructure, the integrity of information, and the continuity of operational processes [1]. It represents a key component of the information security system, since any breach of the integrity, availability, or confidentiality of information resources directly affects the effectiveness of managerial decisions and the financial stability of economic entities. In this regard, cyber resilience should be viewed not merely as a technical characteristic of information infrastructure but as a strategic factor that underpins financial security, guarantees the protection of personal data, and thereby acts as a cornerstone for preserving human capital and maintaining the functional stability of economic entities within the digital environment. The increasing complexity of cyber threats – which are becoming increasingly multi-vector, targeted, and autonomous in nature – along with the emergence of dynamic and decentralized attack models and the growing interconnectivity of digital systems, generates new challenges for conventional approaches to protecting information

networks [2, 3]. These developments call into question the effectiveness of traditional, static security paradigms. Furthermore, the active use by attackers of legitimate services and tools (the so-called Living-off-the-Land techniques), which significantly complicates the processes of timely detection and effective neutralization of attacks at both the network and endpoint levels [4], necessitates a comprehensive revision of information security architecture based on the principles of resilience and self-organization.

The ability of systems to autonomously detect threats, restructure their internal architecture, adapt data transmission routes, and restore functionality without centralized intervention constitutes a critical factor in ensuring their cyber resilience [5]. Considering the complex interdependencies within modern information systems, the mathematical modeling of such adaptive processes requires further refinement from both theoretical and applied perspectives. In this regard, the development and mathematical substantiation of self-organization methods for information networks, capable of enhancing their cyber resilience in the context of emerging threats, represents an undeniably relevant and significant scientific problem.

Literature review. Considering the crucial role of cyber resilience in information networks for ensuring not only information security, but also the financial, per-

sonnel, and technological security of economic entities [6], contemporary scientific research is increasingly focused on the development of conceptual foundations, structural models, and practical mechanisms aimed at enhancing the resilience of IT infrastructures against cyber threats.

Thus, the systemic approach presented in [7] conceptualizes cyber resilience as a comprehensive construct, the mechanisms of which should be based on game theory, control theory, and machine learning. The study demonstrates that modern information and communication systems operate within highly dynamic environments, where traditional reactive protection mechanisms lose their effectiveness. The author proposes a proactive threat analysis-driven approach to ensuring cyber resilience. Meanwhile, the authors of [8], through a bibliographic and conceptual review, identified key approaches to defining cyber resilience and outlined the main stages of its development. Their research substantiates the necessity of transitioning toward adaptive, real-time risk management to strengthen cyber resilience. However, since these studies [7, 8] primarily address the conceptual foundations of cyber resilience in information networks, the applied aspect – specifically, the integration of proactive threat detection mechanisms with adaptive self-organization algorithms in networks operating under conditions of high uncertainty and transformational cyber threat dynamics – remains an open and insufficiently explored research issue.

Accounting for the dynamic nature of cyber threats is one of the core elements of contemporary scientific research, shifting the focus toward the formation of proactive and adaptive systems capable of functioning effectively in unstable environments. In particular, the importance of the preparation, adaptation, and recovery phases is emphasized, as they are critical both in responding to known types of attacks and in countering new, previously unidentified threats. In study [9], the learning and adaptation capabilities of information networks are considered a fundamental component of cyber resilience, determining a system's ability not only to recover after incidents, but also to use accumulated experience to improve the efficiency of countering future threats. The authors highlight that effective cyber risk management should be based on the creation of a closed feedback loop, within which the system continuously analyzes its vulnerabilities, evaluates the consequences of realized attacks, and adapts its security policies accordingly. The authors of [10] argue that the development of cyber resilience should rely on the concept of dynamic capabilities, which integrates both reactive and proactive mechanisms of adaptive management under conditions of heightened uncertainty. Despite the focus on the self-organization of information networks in studies [9, 10], the methodological toolkit for ensuring a sufficient level of adaptability of information systems to changes in the nature of cyber threats remains underdeveloped.

The authors of study [11] argue that cyber resilience represents a new security paradigm. The researchers explore the potential of applying reinforcement learning (RL) methods to develop adaptive cyber defense mechanisms. In particular, attention is devoted to implementing concepts such as moving target defense, cyber deception technologies, and tools supporting human fac-

tor operations. The advantage of using RL lies in the system's capacity for autonomous learning and rapid adaptation within a dynamic and unpredictable cyber threat environment, including the ability to adjust defensive behavior in real time during ongoing attacks. Article [12] presents a comprehensive review of contemporary approaches to intrusion detection in communication networks based on reinforcement learning methods, emphasizing their effectiveness, implementation challenges, and the potential for adaptive protection in dynamic environments. Study [13] proposes an innovative approach to detecting cyberattacks in IIoT systems, founded on a hybrid LSTM-CNN-Attention model that enhances accuracy and adaptability. At the same time, the authors of [11–13] have not sufficiently addressed promising approaches to ensuring cyber resilience, particularly those based on the self-organization of information networks.

Unsolved aspects of the problem. While acknowledging the theoretical and practical value of existing studies [7–13] and the growing attention of the scientific community to the issues of cyber resilience of information networks, several areas remain underexplored. In particular, the mathematical foundations for applying self-organization methods under conditions of dynamic and adaptive counteraction to cyber threats are insufficiently developed. This highlights the need for further research.

Purpose. The purpose of this article is to substantiate mathematical approaches and models that can be applied to the key methods of self-organization of information networks of economic entities under conditions of an approximate interrelation between parameters and control variables across the levels of the OSI model. Particular attention is devoted to their implementation at specific OSI layers, which enables a detailed assessment of their impact on the stability and security of these networks in the context of cyber threats.

The objective of the article is to use mathematical models to determine the effectiveness of the proposed methods and to define their role in enhancing the resilience and adaptability of information systems to active digital transformation processes and emerging cyber threats.

Description of the research methodology: justification of self-organization methods in information networks. In the context of the rapid development of digital technologies and the increasing complexity of cyber threats, the implementation of effective self-organization methods capable of ensuring the resilience and stability of information network functioning has become particularly relevant. The reliability of the information infrastructure directly determines the financial, personnel, and technological security of economic entities, as well as their ability to operate effectively and continuously under turbulent conditions [14]. A critically important factor is the ability of networks to adapt to changes in the external environment, to detect and neutralize threats in a timely manner while maintaining a high level of system performance, information resource availability, and cybersecurity [15].

To reveal and further substantiate the mechanisms of self-organization in information networks, it is appropriate to identify the key parameters that determine the characteristics of this process at various levels of the Open Systems Interconnection (OSI) reference model (Table).

Interrelationship between optimization parameters and control implementation mechanisms across the levels of the OSI reference model

OSI Level	Controlled Objects	Optimization Parameters	Control Implementation Mechanisms
Physical	Communication links between directly connected nodes	Bandwidth, signal delay, transmitter power, energy consumption, modulation parameters	Power and signal direction adjustment, selection of modulation type, application of error-correcting codes, configuration of physical transmission parameters
Data Link	Frame-level connections between neighboring nodes	Transmission rate, latency, energy consumption, overhead	Selection of medium access algorithm (deterministic, random, hybrid), frame size configuration, delivery acknowledgment parameters
Network	Routing paths between network nodes	Delay, route stability, control data volume, number of routes, bandwidth, energy consumption	Application of routing algorithms (table-based, probe-based, hybrid, hierarchical), topology management, load balancing
Transport	Logical connections between sender and receiver	Bandwidth, delay, delay variation, delivery reliability	Congestion control, transmission window adjustment, timeout configuration, queue management
Session	Interaction sessions between application processes	Connection stability, number of sessions, session duration, recovery after failures	Management of session establishment, maintenance, synchronization, and termination; context recovery
Presentation	Data exchanged between application processes	Data formatting, compression, encryption, data representation compatibility, processing optimization	Use of data format conversion algorithms (JSON/XML/ASN.1, etc.), encoding/decoding methods, compression/decompression techniques
Application	Interaction of applications or end-users within the network	Performance (latency, bandwidth), energy consumption, security level	Use of application protocols (HTTP, FTP, MQTT, etc.), protection of transmitted information, service and session management, adaptive exchange via intelligent mechanisms

Thus, the research will be structured according to the presented OSI model levels, which will allow for a comprehensive coverage of all aspects of ensuring cyber-resilience – from the physical layer of network component operation to the application layer, where security management and self-organization algorithms are implemented. This approach enables a holistic understanding of the cyber-security system, as each layer of the model can function both as an independent subsystem and as a component of an integrated threat mitigation system.

Particular attention should be paid to current aspects of modern cybersecurity, specifically the use of mathematical models that allow for a detailed examination of processes occurring under cyber-threat conditions [16, 17]. The application of formalized models enables the assessment of the effectiveness of protection mechanisms, identification of critical points within the network infrastructure, and simulation of system behavior under various cyberattack scenarios. These models facilitate not only a theoretical evaluation of the effectiveness of proposed methods but also their adaptation to specific network conditions. Moreover, they provide a foundation for the development of adaptive management algorithms that ensure a balance between productivity, resilience, and security of information networks.

In this context, the article presents key methods of self-organization in information networks, which form the foundation for building cyber-resilient network structures. For each of these methods, corresponding mathematical models can be formulated to enhance the understanding of their operation and their impact on the overall system resilience.

Specifically, the application of methods such as distributed architecture and virtualization, anomaly detection and incident response systems, cryptographic mechanisms for data protection, self-organizing adaptive networks, recovery mechanisms after attacks, as well as cybersecurity through behavioral models, is proposed. For each of these methods, mathematical models can be developed to evaluate their influence on network stability and security under complex cyber-threat conditions.

To gain a deeper understanding of the processes unfolding under cyber-threat conditions and to formalize mathematical models and approaches for each of the substantiated methods, it is appropriate to highlight the following points.

Firstly, the implementation of distributed and virtualized systems allows for reducing the risk of simultaneous impact of cyber threats on the entire information and communication network of an economic entity. Such architectures provide modularity, process isolation, and spatial diversification of data, which significantly mitigates the risk of the entire network being compromised due to a cyberattack or technical failure. From a mathematical perspective, the operation of a distributed system can be described as a set of interrelated subsystems in a state of stochastic interaction, with their resilience determined by the probability of successful functioning of each module under external influence. The use of resource virtualization enables dynamic load balancing, isolation of critical components, and flexible management of digital assets, ensuring the system's adaptive response to changing cyber threats in real time.

Secondly, the use of intelligent anomaly detection systems based on machine learning and artificial intelli-

gence [18] constitutes a key element in forming a proactive approach to cybersecurity. These systems are capable of analyzing large volumes of streaming data, identifying inconsistencies or behavioral deviations that may indicate attempts of unauthorized access or malicious activity. The mathematical modeling of such systems is based on classification algorithms (SVM, Random Forest, k-NN), deep neural networks, and clustering models, which enable the recognition of patterns even in high-dimensional and noisy data. Consequently, an adaptive learning mechanism is established, which continuously improves based on newly detected threats and minimizes the human factor in the monitoring process.

Thirdly, modern cryptographic methods [19] should be employed not only for securing communications but also for the storage of financial and personnel data, transaction processing, and user verification. The use of multi-factor authentication mechanisms and cryptographic protocols based on blockchain technologies [20] becomes particularly relevant, as they ensure data immutability, transaction transparency, and distributed trust among system participants. These systems are described through cryptographic hash functions, elliptic curves, and RSA- and ECC-based encryption algorithms, which enable the construction of a robust data protection model even under high computational load or attempted breaches. The integration of cryptography with blockchain technologies creates a distributed security ledger, within which information verification is performed collectively, effectively eliminating the possibility of manipulation.

Fourthly, self-organization within the information networks of economic entities involves the use of adaptive routing and data transmission methods [21], which reduce reliance on centralized points and provide higher resilience against attacks. The application of heuristic algorithms (e.g., ant colony optimization, particle swarm optimization, and genetic algorithms) enables autonomous identification of optimal data transmission paths, enhancing network survivability in the event of node failures. The mathematical modeling of such processes is based on graph theory and Markov processes, where nodes act as agents interacting within the network space, aiming to minimize delays and maximize throughput even under aggressive cyber influences.

Fifthly, a critical parameter is the regular execution of data backup procedures, including critical financial transactions and personnel data of employees and contractors. This approach reduces potential losses in the event of destructive attacks or internal system failures. The use of cloud infrastructures plays a particularly important role, providing geographic distribution of backup copies and minimizing the risk of simultaneous data loss. In the context of mathematical modeling, these processes can be described through an optimal resource planning model, which determines the frequency, volume, and prioritization of backups based on data criticality and available computational resources.

An essential component is the use of behavioral models to detect violations in user activity and anomalous transactions. This approach enables the timely identification of threats at the user interface level and in financial operations [22]. Behavioral models are based on the analysis of behavioral patterns that reflect typical

actions of legitimate users, allowing the detection of anomalies in the form of atypical operations, suspicious system logins, or unusual financial transfers. This makes it possible to promptly block potentially fraudulent transactions, thereby reducing risks for the economic entity. From the perspective of mathematical modeling, such systems are implemented through Bayesian networks, hidden Markov models (HMM), neural networks, and logistic regression classifiers, which predict the probability of malicious behavior.

In parallel, it is crucial to monitor and adapt the access policy to information resources and personal data by applying the principle of least privilege and ensuring real-time privilege control, automatically modifying access or revoking privileges upon detection of suspicious activities. In this context, collaboration with governmental authorities and international organizations is essential, as it enables timely information exchange regarding emerging threats and the ability to respond rapidly, including participation in national and international cybersecurity networks/systems and conducting regular audits and inspections to maintain high security standards [23].

Furthermore, organizational cultural changes can significantly enhance resilience to cyber threats by engaging every employee in responsibility for security. The human factor often represents the most vulnerable link within the security structure. Fostering collective responsibility for maintaining information security and involving each employee in monitoring processes and adherence to internal security policies contributes to the establishment of an integrated system of digital trust within the organization. In particular, systematic training sessions, phishing attack simulations, and educational programs on countering social engineering methods improve personnel's ability to recognize manipulation attempts, unauthorized access, or confidential information theft. Integrating cybersecurity hygiene principles into daily work processes, including email communication, cloud service usage, and corporate mobile device management, ensures consistent compliance with security requirements at all management levels. Thus, organizational culture becomes not only a means of formal policy compliance but also a tool for self-regulation of employee behavior in the digital environment.

It is important to emphasize the potential of artificial intelligence for analyzing large volumes of data and predicting emerging types of attacks. The application of predictive analytics based on machine learning algorithms enables the development of proactive security models that not only respond to incidents but also prevent them at their inception. Such approaches contribute to increasing the autonomy of cybersecurity systems and reducing the burden on human resources, as decisions are made based on statistical patterns, time series, and contextual information about user behavior [24]. The integration of artificial intelligence technologies with other components of the security architecture [25] ensures comprehensive and multi-layered protection. This approach allows for the creation of adaptive, self-learning cybersecurity environments capable of monitoring, correlating, and neutralizing complex multi-vector attacks in real time.

Therefore, in light of the above, it can be assumed that the implementation of these methods will enable eco-

conomic entities not only to enhance their resilience to cyber threats but also to adapt to the dynamically changing cyberattack landscape, ensuring the security and stability of their electronic communication networks and systems.

Summary of the main material and scientific results.

In accordance with the above provisions, the following mathematical models and approaches are presented, which can be applied to the core methods of self-organization in information networks. These models enable a detailed description of adaptation and interaction processes under constantly evolving cyber threats, thereby ensuring the stability and security of the network.

1. Distributed Architecture and Virtualization (Levels 1–3: Physical, Data Link, Network). Distributed architecture constitutes a key element in the design of resilient information systems, as it reduces dependence on centralized nodes and enhances network fault tolerance and adaptability. Within the Physical and Data Link layers of the OSI model, such an architecture implies spatial and functional distribution of resources, thereby eliminating single points of failure. This, in turn, creates conditions for self-recovery of the network in the event of cyber incidents caused by attacks or technical failures. At the Physical layer, distributed networks can be represented using graph models and routing algorithms, where each node possesses specific reliability characteristics, and network connections can be dynamically adjusted depending on load or attack. These algorithms allow optimal data paths to be determined, minimizing the probability of network failure.

Graph Model (Level 3: Network). The network is represented as a graph $G = (V, E)$, where each node (e.g., a server or router) has a failure probability p_i . For each route through the network, reliability can be calculated as

$$P_{network} = \prod_{i=1}^n p_i,$$

where p_i is the probability that a channel/communication line or a node/element has not failed; n is the total number of channels/communication lines or nodes/elements through which the route passes in the distributed network (i.e., the path length in the graph model).

Adaptive Routing (Level 3: Network). Using dynamic routing algorithms such as OSPF or BGP, the network can adapt to new conditions. If the network adjusts routes based on the current topology and the state of nodes, a mathematical model of route changes can be employed, in particular using the Bellman–Ford or Dijkstra algorithms [26], to minimize delays or perform routing based on reliability

$$\min \left(\sum_{i=1}^n delay(i) + \sum_{i=1}^n reliability(i) \right), \quad (1)$$

where i is the index of an individual segment or node of the route (e.g., a communication link, router, or server node); n is the number of elements (nodes or links) in the route considered in the dynamic calculation of the routing metric; $delay(i)$ is the data delay time on the i^{th} element of the path, which may include processing time, queuing time, or transmission time.; $reliability(i)$ is the reliability factor or, conversely, the probability of failure of the node or channel.

Result. The use of these models allows for efficient traffic distribution among nodes and ensures network resilience, even under attacks or partial system failures. Networks based on distributed architectures are less vulnerable to centralized attacks and can adapt more quickly to changes in network topology. Virtualization, in turn, enables flexible reconfiguration of resources to maintain network reliability.

Advantages. High reliability, reduced probability of simultaneous failures, flexibility in routing.

Disadvantages. Increased management and monitoring complexity, the necessity for constant updates of strategies when adapting to new threats.

Justification. Overall, mathematical routing models help minimize the probability of failures due to local disruptions, which is critical for ensuring the resilience of an economic entity’s network under cyber threats. Routing algorithms adapt to network changes while maintaining high efficiency and data transfer speed even in the presence of attacks. Accordingly, the use of distributed structures and flexible routing algorithms forms the foundation of a cyber-resilient infrastructure capable of supporting the continuity of business processes of economic entities, even in the event of large-scale cyberattacks.

2. Anomaly-Based Incident Response Systems (Level 4–7: Transport, Session, Presentation, Application). Anomaly detection most often occurs at the application level (for example, through traffic or transaction analysis tools). Since cyber threats can manifest through abnormal requests or transactions, mathematical models for anomaly detection can be constructed using probabilistic methods or machine learning techniques. Unlike traditional signature-based approaches, which rely on identifying known attack patterns, anomaly analysis methods enable the identification of unknown or novel threats that deviate from the system’s normal behavior. This capability is particularly important in the context of the growing frequency of zero-day attacks and multi-stage hybrid intrusions.

Probabilistic Models for Anomalies (Level 4: Transport). At the transport level of the network architecture, the primary objective is to monitor data flows and detect statistically significant deviations in connection parameters – such as packet frequency, transmitted data volume, average response time, or the number of repeated requests. To identify anomalous behavioral patterns in network connections, statistical methods such as Markov models [27] are applied

$$P(X_t | X_{t-1}, \theta) = f(X_{t-1}, \theta),$$

where X_t is the current state of the session (for example, the volume of data transmitted); X_{t-1} is the previous state of the session; θ is the model parameters describing behavior under steady-state conditions.

If the observed values X_t fall outside the established confidence interval, the system interprets this as an anomaly and initiates a response procedure (blocking, isolation, or event logging). The application of Markov models makes it possible to predict future system states and determine the probability of anomalous patterns emerging in real time, which is critically important for proactive cybersecurity.

Machine Learning Models (Level 7: Application). For the analysis of transactions or network traffic, ma-

chine learning methods such as Support Vector Machines (SVM) or neural networks [28] can be applied. For instance, to detect anomalies in transactions, a mathematical classification model can be formulated as

$$f(x) = \arg \max_p \left(\sum_{i=1}^m \omega_i \cdot x_i + \beta \right),$$

where x_i is the vector describing user behavior; ω_i is the weights assigned to each feature; β is the classification threshold parameter; m is the number of features (observation parameters); p is the class or type of event that the model selects based on the maximum probability or score.

The function $f(x)$ makes it possible to determine whether specific behavior belongs to the normal or anomalous group. Such models can be self-learning, meaning they continuously update their parameters as data accumulates, enabling the system to adapt to the evolving cybersecurity environment.

Result. The use of Markov models and machine learning algorithms makes it possible to detect latent anomalies that lack explicit signatures but are characterized by changes in the correlations between traffic parameters or user behavioral patterns. Machine learning models can identify even the most complex anomalies, such as deviations from a user's typical behavioral profile or abnormal transactions indicative of fraud or cyberattacks. Anomaly detection systems enable rapid response to suspicious actions, significantly reducing the risk of major attacks.

Advantages. Rapid response to anomalous events; reduced number of false positives; automation of the detection process.

Disadvantages. Continuous dependence on large volumes of training data required to build effective models increases the risk of missing zero-day attacks until the system adapts to them.

Justification. The use of Markov models and machine learning methods enables the prediction of the probability of detecting specific types of attacks and anomalies based on previous cybersecurity incidents. These approaches provide not only retrospective analysis of known attacks but also the formation of proactive response scenarios, whereby the system, using accumulated behavioral patterns, predicts potential deviations in user or network component behavior. This allows organizations to take timely countermeasures and adapt their systems to new types of threats without manual configuration.

3. Cryptographic Mechanisms for Data Protection (Level 6: Presentation). Cryptographic methods represent a fundamental tool for ensuring information security at the presentation level, as it is at this stage that data are transformed into forms suitable for storage, transmission, or processing. Cryptographic mechanisms guarantee the confidentiality, integrity, and authenticity of information, which are critically important for the stable functioning of the information systems of economic entities under the conditions of growing cyber threats.

Cryptosystem Robustness Assessment (Level 6: Presentation). One of the ways to assess the robustness of a cryptosystem is by using entropy to determine the degree of randomness in encryption systems, as well as

asymmetric encryption (RSA, ECC) [29] to ensure data confidentiality and integrity. Entropy $H(X)$ defines the level of unpredictability of encrypted messages

$$H(X) = -\sum_{i=1}^n p_i \log_2 p_i,$$

where p_i is the probability of occurrence of the i^{th} symbol in the message. The higher the entropy, the more difficult it is to recover the key or to mount a successful attack against the cryptosystem.

Evaluation of Cryptographic Resilience (Level 6: Presentation). If a cryptographic system uses keys of length n bits, the number of possible keys for brute-force search is

$$C = 2^n.$$

The larger the key size, the higher the resistance to attacks.

Result. Cryptography forms the foundation for the protection of confidential information. The use of cryptographic methods in multi-level information systems enables reliable data protection at all stages of processing: from generation and storage to transmission and user authentication. Employing high entropy in encryption algorithms (e.g., during key generation) ensures resilience against brute-force attacks. Asymmetric encryption methods, such as RSA or ECC (Elliptic Curve Cryptography), are used to safeguard data exchange between users and systems.

Advantages. High resilience to attacks, protection against data interception and manipulation.

Disadvantages. Computational resource costs for encrypting/decrypting large volumes of data; risk of vulnerability of digital assets due to "compromised" cryptographic protocols.

Justification. The security level of encryption can be mathematically assessed using an entropy-based model, which allows measuring the complexity of breaking the system. The higher the entropy, the more difficult it is to successfully attack the encrypted channel. Moreover, resistance to cryptanalysis attacks directly depends on the length and complexity of cryptographic keys.

4. Self-Organized Adaptive Networks (Level 2–3: Data Link and Network). Network self-organization involves adaptive routing and structural changes in the network based on current conditions. This includes dynamic traffic rerouting in the event of an attack or component failure. Such an architecture ensures continuous operation even if individual nodes or communication links fail, which is a key property for building cyber-resilient infrastructures.

Adaptive Routing and Resource Management (Level 3: Network). Routing can be adapted in real time using algorithms such as Dijkstra's algorithm (formula (1)), where the shortest path or minimal delay is calculated for each route, or using the Bellman-Ford algorithm for more complex scenarios with dynamic changes in the network

$$D(u) = \min_{v \in N(u)} (D(v) + w(v, u)),$$

where $D(u)$ is the best distance to node u ; $N(u)$ is neighbors of node u ; $w(v, u)$ is weight of the edge between v and u .

Within the framework of adaptive resource management, the weights $w(v, u)$ can be modified using feedback functions that take into account the channel status, bandwidth, and failure frequency. This allows optimization of routing according to the current operating conditions of the system.

Result. Adaptive networks have the ability to independently adjust their topology and routing in response to changes in the network environment or emerging threats. This reduces network load during peak periods or attacks on specific nodes. Additionally, such networks can employ heuristic or hybrid algorithms that combine classical routing methods with intelligent predictive mechanisms, including elements of machine learning or neuro-evolutionary computations. This enables forecasting of potential failures or attacks and proactive rerouting of data to ensure minimal delays and maximum reliability.

Advantages. Flexibility in response to network changes, high adaptability to new conditions and threats.

Disadvantages. Increased configuration complexity, need for continuous monitoring to ensure effectiveness.

Justification. Self-organized adaptive networks implement the principle of autonomous optimization, minimizing the impact of external disturbances on overall system performance. Routing algorithms in adaptive networks enhance resilience against attacks such as DoS (Denial of Service), reducing the likelihood of data blocking or delay due to unavailable or attacked routes. Thus, the use of mathematical models for adaptive routing forms the foundation for building next-generation intelligent networks capable not only of reacting to incidents but also of anticipating potential risks in real time, which is critical for maintaining the cyber-resilience of economic entities.

5. Post-Attack Recovery Mechanisms (Level 5: Session). Post-attack recovery mechanisms are an integral component of ensuring information resilience and the continuity of digital system operations. Recovery after an attack includes restoration from backups and recovery mechanisms, with possible automatic switching to reserve resources. These mechanisms aim to minimize system downtime and prevent the loss of critical data due to attacks such as ransomware, DDoS, or internal technical failures.

Mathematical Model of Data Recovery (Level 5: Session). The probability of successful data recovery from a backup can be described using the probability of access to backup data

$$\Pi_{\text{recovery}} = \frac{\text{number of restored data}}{\text{total amount of data}}.$$

This indicator allows evaluating the effectiveness of the recovery system. The greater the number of backups or recovery options, the higher the probability of achieving a successful outcome.

Result. The mathematical model enables the determination of the probability of successful recovery after an attack based on available backups and the speed of their restoration. The higher this metric, the faster the system can return to normal operation following an attack or other incident.

Advantages. Ensures continuity of system operations, reduces data loss.

Disadvantages. This model may require significant resources for implementation and maintenance, and there are potential challenges in achieving full recovery in the case of large-scale cyberattacks.

Justification. The data recovery time and accuracy of restored files directly depend on the available backups and the presence of adaptive strategies for system restoration. Mathematical models allow assessing the efficiency of backups and selecting optimal strategies to ensure continuity of the operational cycle. Combined with intelligent monitoring methods, these approaches form the foundation of a cyber-resilient infrastructure capable of rapid adaptation and autonomous recovery after destructive impacts.

Thus, in summary, it should be noted that each of the presented methods of self-organization and security can be represented through mathematical models corresponding to the appropriate OSI levels. It is important to emphasize that this approach not only preserves the capabilities for technical control of the network but also ensures resilience against cyber threats through the application of adaptive algorithms, cryptography, and anomaly detection by intelligent systems. The discussed mathematical models fully enable the assessment of reliability, efficiency, and resistance to attacks at each OSI level, as well as the development of methods for adaptive response.

Considering the evaluation of the effectiveness of these mathematical models, which are applied to key methods of self-organization in information networks of economic entities, it is appropriate to note that, overall, each approach contributes to enhancing their cyber-resilience. In turn, the cyber-resilience of information systems plays a crucial role in ensuring the financial and personnel security of economic entities [30]. A reliable infrastructure minimizes the risks of data leakage, failures in settlements and financial operations, and enables timely detection of internal threats associated with personnel behavior. Thus, the self-organization of information networks forms the foundation of comprehensive security in the digital environment.

Evaluating the overall effectiveness of the models discussed, it should be noted that high efficiency is observed in distributed architectures, adaptive networks, anomaly detection systems, and cryptographic mechanisms. These approaches ensure a high level of network resilience against attacks, allow for rapid response to emerging threats, and reduce the likelihood of serious incidents. At the same time, moderate effectiveness is characteristic of recovery mechanisms after attacks. These mechanisms provide an adequate level of protection; however, their effectiveness depends on the proper configuration of recovery strategies and the speed of their implementation.

Conclusions. The study substantiates that the self-organization of information networks serves as the foundation for strengthening their cyber-resilience amid increasing risks and threats in the digital environment. It also constitutes an integral component in ensuring the financial, personnel, and technological security of economic entities, as well as the stability of their operations. The application of mathematical models and intelligent algorithms has been analyzed in the context of enhancing the resilience of information networks of economic

entities, taking into account the hierarchical structure of OSI levels. It was determined that the implementation of routing algorithms (specifically, Bellman–Ford and Dijkstra) at the Network Level contributes to the optimization of data transmission paths and the reduction of delays. At the Transport and Data Link Levels, adaptive modulation and error correction protocols play a crucial role, directly influencing the reliability and efficiency of data transfer.

The application of behavioral analytics models, neural networks, and support vector machines (SVM) at the application, presentation, and session levels enables early detection of anomalies in user actions and transactions, thereby enhancing information security. The use of cryptographic protection, including entropy analysis, asymmetric encryption (RSA, ECC), and key management, strengthens security at the Presentation and Session Levels.

It has been demonstrated that the implementation of these models contributes to increased adaptability to emerging threats while ensuring a high level of data protection through cryptographic mechanisms, allowing for effective system recovery after incidents. A structured security management architecture aligned with OSI levels establishes the foundation for comprehensive protection of information, and, consequently, the financial and personnel security of economic entities. In particular, the resilience and adaptability of the information infrastructure directly affect the reliability of management decisions, the protection of personal data, and the preservation of human resources.

Additionally, it has been established that the synergy of mathematical modeling, intelligent data analysis technologies, and cryptographic tools forms an integrated concept of cyber resilience, in which each OSI level performs a specialized function to support the overall information security of the system. The implementation of a multi-level adaptive approach ensures not only the real-time detection and neutralization of cyberattacks but also the creation of self-learning mechanisms that enhance the effectiveness of countering new types of threats. This establishes conditions for the development of intelligently managed networks capable of self-recovery, risk prediction, and optimization of cybersecurity across all levels of the information infrastructure.

References.

1. Onyshchenko, S., Hlushko, A., Maslii, O., & Chumak, O. (2024). Digital transformation of the national economy in the context of information environment development in Ukraine. *Transformations of national economies under conditions of instability*, (6), 169–197. Scientific Route OÜ. <https://doi.org/10.21303/978-9916-9850-6-9.ch6>
2. World Economic Forum (2025). *The global risks report 2025 (20th ed.)*. Retrieved from <https://www.weforum.org/publications/global-risks-report-2025/>
3. Onyshchenko, S., Yanko, A., Hlushko, A., & Maslii, O. (2023). Economic cyber security of business in Ukraine: Strategic directions and implementation mechanism. In *Economic and cyber security*, (pp. 30–58). <https://doi.org/10.15587/978-617-7319-98-5.CH2>
4. Operativnyi tsentr reahuvannia na kyberintsydeny Derzhavnoho tsentru kyberzakhystu Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy (2024). Systems for vulnerability detection and response to cyber incidents and cyberattacks: Annual report 2024. Retrieved from <https://spsc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927e88006>
5. Onyshchenko, S., Yanko, A., & Hlushko, A. (2023). Improving the efficiency of diagnosing errors in computer devices for processing economic data functioning in the class of residuals. *Eastern-European*

- Journal of Enterprise Technologies*, 5(4(125)), 63–73. <https://doi.org/10.15587/1729-4061.2023.289185>
6. Shefer, O., Laktionov, O., Pents, V., Hlushko, A., & Kuchuk, N. (2024). Practical principles of integrating artificial intelligence into the technology of regional security predicting. *Advanced Information Systems*, 8(1), 86–93. <https://doi.org/10.20998/2522-9052.2024.1.11>
 7. Zhu, Q. (2024). Foundations of cyber resilience: The confluence of game, control, and learning theories. *Electrical Engineering and Systems Science*. <https://doi.org/10.48550/arXiv.2404.01205>
 8. Araujo, M. S. d., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences*, 14(5), 2116. <https://doi.org/10.3390/app14052116>
 9. Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity standards: Managing risk and creating resilience. *Computer*, 47(9), 70–76. <https://doi.org/10.1109/MC.2013.448>
 10. Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of business continuity & emergency planning*, 9(2), 185–195. <https://doi.org/10.69554/PRJY4917>
 11. Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement learning for feedback-enabled cyber resilience. *Annual Reviews in Control*, 53, 273–295. <https://doi.org/10.1016/j.arcontrol.2022.01.001>
 12. Kheddar, H., Dawoud, D. W., Awad, A. I., Himeur, Y., & Khan, M. K. (2024). Reinforcement-learning-based intrusion detection in communication networks: A review. *IEEE Communications Surveys & Tutorials*. <https://doi.org/10.1109/COMST.2024.3484491>
 13. Gueriani, A., Kheddar, H., & Mazari, A. C. (2024). Adaptive cyber-attack detection in IIoT using attention-based LSTM-CNN models. *2024 International Conference on Telecommunications and Intelligent Systems (ICTIS)*, (pp. 1–6). IEEE. <https://doi.org/10.1109/ICTIS62692.2024.10894509>
 14. Gaydash, O. (2025). Comparative Analysis of External and Internal Factors Affecting the Formation of Personnel Security in Ukrainian Enterprises. *Bulletin of the Academy of Labor, Social Relations and Tourism. Series: Economics, Psychology and Management*, 6. <https://doi.org/10.54929/3041-2390-2025-06-04-02>
 15. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., & Bilko, S. (2023). Determination of the peculiarities of using information security systems in financial institutions in order to increase the financial security level. *Eastern-European Journal of Enterprise Technologies*, 5(13(125)), 65–76. <https://doi.org/10.15587/1729-4061.2023.288175>
 16. Trenchev, I., Dimitrov, W., Dimitrov, G., Ostrovska, T., & Trencheva, M. (2023). Mathematical Approaches Transform Cybersecurity from Protoscience to Science. *Applied Sciences*, 13(11), 6508. <https://doi.org/10.3390/app13116508>
 17. Alyami, H., Nadeem, M., Alharbi, A., Alosaimi, W., Ansari, M. T. J., Pandey, D., Kumar, R., & Khan, R. A. (2021). The Evaluation of Software Security through Quantum Computing Techniques: A Durability Perspective. *Applied Sciences*, 11(24), 11784. <https://doi.org/10.3390/app112411784>
 18. Miller, T., Durlík, I., Kostecka, E., Sokołowska, S., Kozłowska, P., & Zwolak, R. (2025). Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies. *Electronics*, 14(9), 1844. <https://doi.org/10.3390/electronics14091844>
 19. Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies*, 12(12), 241. <https://doi.org/10.3390/technologies12120241>
 20. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, 8, 21091–21116. <https://doi.org/10.1109/ACCESS.2020.2968985>
 21. Hamarshah, A. (2024). An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning. *Applied Sciences*, 14(11), 4530. <https://doi.org/10.3390/app14114530>
 22. Tang, T., Yao, J., Wang, Y., Sha, Q., Feng, H., & Xu, Z. (2025). Application of deep generative models for anomaly detection in complex financial transactions. *Proceedings of the 2025 4th International Conference on Artificial Intelligence, Internet and Digital Economy (IC-AID)*, (pp. 133–137). IEEE. <https://doi.org/10.1109/ic-aid65275.2025.11034573>
 23. Maslii, O., Buriak, A., Chaikina, A., & Cherviak, A. (2025). Improving conceptual approaches to ensuring state economic security under conditions of digitalization. *Eastern European Journal of Enter-*

prise Technologies, 1(13(133)), 35-45. <https://doi.org/10.15587/1729-4061.2024.319256>

24. Moon, P. S., Deshmukh, A. B., Sarode, H. J., Sharma, S., Birare, K. M., & Anandpwar, W. N. (2025). Implementation of machine learning techniques for predictive security analytics. V. Bhateja, M. Dey, & R. Senkerik (Eds.), *Proceedings of FICTA 2024 – Innovations in information and decision sciences*, 422. Springer. https://doi.org/10.1007/978-981-96-0147-9_41

25. Yanko, A., Krasnobayev, V., & Martynenko, A. (2023). Influence of the number system in residual classes on the fault tolerance of the computer system. *Radioelectronic and Computer Systems*, 3(107), 159-172. <https://doi.org/10.32620/reks.2023.3.13>

26. Bannister, M. J., & Eppstein, D. (2012). Randomized speedup of the Bellman–Ford algorithm. *Proceedings of the 2012 Meeting on Analytic Algorithmics and Combinatorics (ANALCO12)*, (pp. 41-47). Society for Industrial and Applied Mathematics. <https://doi.org/10.1137/1.9781611973020.6>

27. Ren, H., Ye, Z., & Li, Z. (2017). Anomaly detection based on a dynamic Markov model. *Information sciences*, 411, 52-65. <https://doi.org/10.1016/j.ins.2017.05.021>

28. Abuali, K. M., Nissirat, L., & Al-Samawi, A. (2023). Advancing Network Security with AI: SVM-Based Deep Learning for Intrusion Detection. *Sensors*, 23(21), 8959. <https://doi.org/10.3390/s23218959>

29. Monteiro, V. (2024). The importance of entropy sources in cryptography: Randomness to secure communications. *Journal of Information Technology & Software Engineering*, 14, 393. <https://doi.org/10.35248/2165-7866.24.14.393>

30. Maslii, O., & Maksymenko, A. (2025). Digital transformation and economic deindustrialisation: Impact on state financial security. *Financial and Credit Activity: Problems of Theory and Practice*, 1(60), 401-414. <https://doi.org/10.55643/fcaptop.1.60.2025.4599>

Обґрунтування методів самоорганізації інформаційних мереж для зміцнення їхньої кіберстійкості

С. В. Онищенко, Є. О. Живило, А. Д. Глушко*,
О. С. Гайдаш

Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна

* Автор-кореспондент e-mail: glushk.alina@gmail.com

Мета. Формалізація математичних підходів і моделей, що можуть бути ефективно застосовані до ключових методів самоорганізації інформаційних мереж економічних суб'єктів в умовах орієнтовної залежності між параметрами функціонування й керуваннями змінними на різних рівнях моделі OSI.

Методика. На основі застосування алгоритмів оптимізації маршрутів (Дейкстра, Беллман–Форд), теорії марковських процесів, апарату машинного навчання (SVM, нейронні мережі), а також ентропійного аналізу й методів асиметричного шифрування (RSA, ECC) запропоновано підхід до моделювання стійкості інформаційної інфраструктури. Системний підхід реалізовано через аналіз взаємозв'язків між рівнями мережевої моделі OSI для визначення вразливих сегментів і точок контролю ризиків.

Результати. Обґрунтовані методи самоорганізації інформаційних мереж, що забезпечують раннє виявлення аномалій, ефективне управління маршрутизацією та шифруванням даних, а також адаптивність до змін зовнішнього середовища й зниження ризику реалізації кібератак. Розроблена архітектура захисту інформаційної інфраструктури, яка охоплює сім рівнів моделі OSI, що забезпечує цілісність, доступність і конфіденційність даних в інформаційних мережах економічних суб'єктів.

Наукова новизна. Запропоновано підхід до забезпечення стійкості інформаційних мереж, що відрізняється від існуючих узгодженим застосуванням математичних, криптографічних і когнітивних методів у контексті ієрархії мережевих рівнів OSI. Обґрунтована доцільність включення ентропійного контролю як індикатора рівня випадковості системи й потенційної вразливості.

Практична значимість. Полягає в тому, що результати можуть бути використані при розробленні політики інформаційної й кібербезпеки економічних суб'єктів. Запропоновані рішення сприяють зміцненню не лише інформаційної, але й фінансової та кадрової безпеки в умовах цифрової трансформації, а також мінімізації наслідків кіберінцидентів.

Ключові слова: інформаційна безпека, інформаційна інфраструктура, модель OSI, ентропія, економічний суб'єкт

The manuscript was submitted 23.07.25.