UDC 004.056.5: 004.738.5 **doi:** https://doi.org/10.20998/3083-6298.2025.02.07

Stanislav Milevskyi[1], Natalia Voropay[1], Alla Havrylova[1], Olha Korol[1], Iryna Aksonova[1], Vladyslav Khvostenko[1]

[1] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine

MESSAGE TRANSMISSION CONTROL MODELS FOR SPECIAL PURPOSE COMMUNICATION NETWORKS

Abstract. Relevance of the study. In modern conditions of managing specialized special-purpose communication networks, the problem of adaptive control of message transmission in conditions of dynamic changes in the network structure, which can be caused by equipment failures, cyber attacks and other factors, is relevant. Ensuring reliable and uninterrupted operation of such networks is critical for the effectiveness of control systems.**The subject of study**. Models of message transmission control in special-purpose communication networks, namely hierarchical models with a variable structure, their interaction and coordination at different levels. **The purpose of the study.** Formation of a control model that allows adaptive change in the structure of the operational communication network, taking into account new operating conditions and the current position of discrete objects (message packets) in the network. **The following results** were obtained. A model base is proposed that includes three classes of models: task models, perception models and interpretation models. Two types of mappings for task models are formulated and their interrelations are described. The problems of coordinating the joint use of models of different classes are identified. The presented models allow to formalize the process of functioning of the communication network and its redevelopment in real time. **Conclusions.** The developed models allow to automate the process of managing the transmission of messages and changing the configuration of a special-purpose network, which increases the efficiency of management and the resistance of the network to the influence of negative factors, such as cyberattacks or equipment failures.

Keywords: special purpose networks; models of control; message transmission; communication network; task coordination.

Introduction

Problem relevance. The problem of message transmission control in special-purpose communication networks remains highly relevant due to the increasing complexity and criticality of modern automated control systems. Unlike conventional communication infrastructures, special-purpose networks—such as those used in defense, emergency response, critical infrastructure management, and industrial control—operate under strict requirements of reliability, timeliness, and resilience against both technical failures and cyber threats. The growing scale of such systems, characterized by a large number of discrete objects (message packets) moving across dynamically changing network topologies, creates unique challenges that cannot be fully addressed by traditional routing and fault-tolerance mechanisms.

Moreover, the operational environment of these networks is often unpredictable: nodes and channels may fail due to physical damage, overload, or deliberate cyberattacks, while the spatio-temporal distribution of message flows directly affects the stability and efficiency of communication processes. Existing models typically focus on isolated aspects, such as packet-level routing or detection of network failures, without providing an integrated approach that captures both the structural dynamics of the network and the behavior of discrete information flows in real time. This fragmentation of solutions limits their applicability in mission-critical domains where uninterrupted information exchange is essential for decision-making and system control.

In this context, the development of comprehensive models for message transmission control in special-purpose communication networks is of particular importance. Such models must combine adaptability, resilience, and situational awareness, enabling the network not only to withstand disruptions but also to reorganize its operational structure dynamically, taking into account the current distribution and movement of message packets. Addressing this challenge will significantly enhance the efficiency, reliability, and security of automated control systems, ensuring their stable functioning in complex and adverse environments.

Literature review. Over the past few years, various aspects of ensuring the reliability and adaptability of communication networks have been actively studied. Researchers have proposed different methods for dynamic routing and fault tolerance, especially in the context of critical infrastructure and mission-critical communication systems [1]. Significant progress has been made in developing dynamic models for reconfigurable networks, including approaches based on software-defined networking (SDN) and network function virtualization (NFV), which increase the flexibility of communication structures [2]. Additionally, recent studies have explored artificial intelligence techniques for predictive failure detection and proactive reconfiguration of network topologies [3]. These developments have expanded the capabilities of communication networks in dynamic and adverse environments.

However, despite these advances, there is still a lack of comprehensive models that simultaneously account for both the dynamically changing operational conditions of special-purpose networks (e.g., caused by equipment breakdowns or targeted cyber-attacks) and the actual spatial-temporal positions of discrete objects (message packets) at the moment when the network structure is reconfigured. Most existing solutions focus separately either on fault detection or routing optimization, without integrating both aspects into a unified model of message transmission control.

Therefore, there remains an urgent need for improved models that can jointly manage both the packets of information as discrete objects and the structure of the operational network itself, while accounting for dynamically emerging operational conditions. Addressing this challenge requires developing a relevant model basis capable of representing and coordinating different levels of tasks, perceptions, and interpretations of the network state.

The purpose of the research is to develop a comprehensive model framework for message transmission control in special-purpose communication networks, which ensures adaptive management of both network topology and message flows, taking into account dynamically changing operational conditions and the real-time distribution of discrete objects on the network.

1. Message control models for a network with a variable structure

In the context of the stated goal – we propose an approach to the construction of message control models for networks with variable structures.

To address the problem of forming a feasible structure for the operational network, a three-level hierarchy of models is introduced. This hierarchy decomposes the original problem into three interrelated and coordinated subproblems:

z_1 – formation of the structure of the operational network;

z_2 – construction of the schedule for the movement of discrete objects (message packets) across the network structure formed as a result of solving subproblem z_1;

z_3 – real-time adjustment and correction of the movement schedule derived from subproblem z_2 in response to new operational conditions.

Each of these subproblems corresponds to a specific type of model:

1. Subproblem z_1 is solved using a mathematical programming model M_1, which defines the optimal configuration of the operational network topology based on current constraints and performance criteria.

2. Subproblems z_2 and z_3 are addressed using simulation models M_2 and M_3, respectively. These models reflect the dynamic movement of discrete objects through the network and enable the evaluation of scheduling and routing strategies under evolving network conditions.

3. To improve computational feasibility and adaptability, heuristic optimization procedures are incorporated, particularly for the correction model M_3, allowing for rapid responses to disruptions such as node failures or cyber-attacks.

This hierarchical modeling approach ensures not only adaptability and fault tolerance but also real-time alignment of network configuration and message routing, which is critical for the effective operation of special-purpose automated control systems.

Table 1 shows a comparison of models M_1, M_2 and M_3.

Table 1 – **Comparative Characteristics of Models M_1, M_2, M_3**

Purpose	*Input Parameters*	*Output*	*Methods Used*	*Features*
M_1				
Formation of the operational network topology	Network graph (nodes, channels), constraints (bandwidth, reliability), current failures	Optimal/feasible network structure	Mathematical programming (e.g., integer programming, MILP)	Static optimization at the planning stage
M_2				
Scheduling the movement of discrete objects (packets)	Network topology from M_1, initial object positions, message priorities	Movement schedule	Discrete-event simulation, heuristic scheduling	Dynamic modeling with evaluation of message delivery metrics
M_3				
Correction of the movement schedule due to changes	Updated object positions, new constraints (failures, congestion)	Updated schedule	Real-time simulation, local search heuristics	Adaptive response to runtime events

The comparative analysis of models M_1, M_2, and M_3 demonstrates that each model plays a distinct yet complementary role in achieving adaptive message transmission control within special-purpose communication networks. Model M_1 focuses on the static optimization of network topology at the planning stage, ensuring that the operational structure is both feasible and efficient under given constraints. Model M_2 builds upon the output of M_1 by generating a movement schedule for discrete objects through dynamic simulation, enabling evaluation of delivery metrics under varying traffic loads and message priorities. Model M_3 serves as a real-time corrective mechanism, adapting the schedule to unforeseen events such as failures or congestion, thus ensuring operational resilience.

Together, these models form a hierarchical framework where strategic, tactical, and operational decision-making processes are closely integrated, enabling continuous adaptation to dynamic operational conditions. This layered approach ensures that both the topology and the flow of messages can be effectively managed in real time.

With this foundation in place, we now turn to a more detailed examination of the types of models in the hierarchy, exploring their structure, interrelations, and the principles guiding their coordinated application.

2. Types of models in the hierarchy

Management in the conditions of using an automated control system for special purposes is carried out using a fairly wide range of control actions, which allows you to set a certain order in their use, depending on the depth of their influence on the controlled process.

This circumstance is a decisive condition for constructing hierarchies of control models for a complex system. The issues of identifying control actions, their distribution by control levels, and determining the control levels themselves are among the insufficiently developed in control theory. When developing specific systems, all these issues have to be solved, relying on common sense, intuition and analogies. Significant help on this path can be obtained by identifying any one, fairly common class of systems for which it is possible to form control problems and construct models that do not differ too much when moving from system to system within the selected class. Special-purpose control systems are considered as such a class.

The network structure is understood as the structure of flows of discrete objects. The unit of movement is the fact of the passage of a discrete object through a given point of the operational network. Certain vertices or points on the arcs of the network are chosen as such control points. The choice of control points is determined by the nature of the particular system.

At the substantive level, the global goal of controlling the movement of objects on the network can be formulated as follows: in time T, carry out a given number of message transfers on the network.

Based on the analysis of a number of real systems belonging to the class under consideration [4-6], it is possible to single out three subgoals into which the global goal of controlling the movement of discrete objects on networks can be decomposed:

1) C_1 –from optimal considerations determined by the conditions of a particular problem, form a network for message transmission (task z_1).

2) C_2 –for a given network, construct a schedule for the transmission of messages on it objects (task z_2).

3) C_3 –synchronize the transmission of messages on the network with a given schedule in case of process deviations (task z_3).

The complex problem Z = {z1, z2, z3} formulated in this way will be called the problem of controlling the transmission of messages on networks.

In accordance with the above list of subgoals, the hierarchy structure looks like fig. 1, where M_1 – model of forming the structure of the operational network; M_2 – simulation model for scheduling message transmission; M_3 – a simulation model for adjusting the message transmission schedule on the network; V_1, V_2, V_3 – models of perception of initial information (information about the state of the network at the time of the start of the main models: M_1, M_2, M_3); I_1, I_2, I_3 – models for interpreting the results of the work of models M_1, M_2, M_3 in a form convenient for human perception; $M_1 \rightarrow M_2$ – displaying the interpretation of the results of the model's work in a form that allows the use of these results as tasks in the M_2 model; $M_2 \rightarrow M_3$ –displaying the interpretation of the results of the M_2 model in terms of the M_3 model. By analogy with $M_1 \rightarrow M_2$ mapping $M_2 \rightarrow M_3$ generates a task for the M_3 model based on the results of the M_2 model.

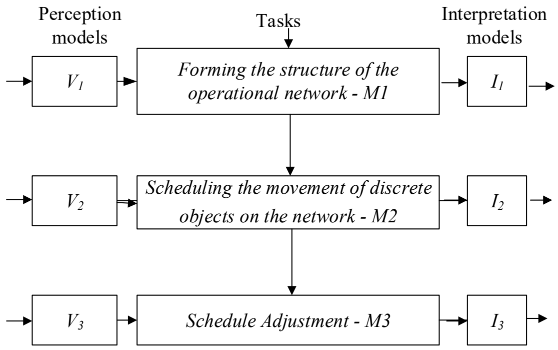

Fig.1. Model Hierarchy Structure

The hierarchical system of models (Fig. 1) in terms of information is immersed in a certain language environment formed by the language spoken about the process by people involved in managing this process [7]. It should be noted that in all systems where the role of operational management tasks is high, their own command languages of communication are formed. Abbreviations and symbols of various objects and technological concepts serve as the basis for command communication languages. Using them, they build, as a rule, a limited set of meaningful structures that describe events on the network. Such meaningful command language constructs are called messages. The message is an indivisible piece of information transmitted through communication channels from the command center to the executors and vice versa. Perception models V_1, V_2, V_3 perform the task of deciphering message arrays and filling with initial information the main models M_1, M_2, M_3.

The solution of control problems z_1, z_2, z_3 requires a different degree of detail in the description of the considered process of message transmission on the network. In particular, the model M_1 of the hierarchy operates with types of discrete objects. In models M_2, M_3 all discrete objects are personified. The results of solving problems z_1, z_2, z_3, obtained using models M_1, M_2, M_3, serve as a means of controlling (scheduling) the transmission of messages on networks at planning intervals T_1, T_2, T_3. Planning intervals are multiples of duration, i.e. $T_1=\alpha T_2$ and $T_2=\beta T_2$, Where α, β are multiplicity factors.

In the hierarchy of models under consideration, each control level has access to the controlled system. Models I_1, I_2, I_3 are designed to bring the results of models M_1, M_2, M_3 into a form that is convenient for human perception.

3. Interlevel coordination of tasks

One of the features of the hierarchical management of special-purpose units is the requirement for the coordination of management tasks that are solved at different levels [8]. Coordination of management tasks is achieved by:

a) enabling the interpretation of concepts used in one model in terms of another model;

b) consistency of control criteria used in coordinated tasks.

Consider the issue of matching the control criteria used in problems z_1 and z_2. The variables of the model M_1 have the meaning of the intensities of the elementary contours. Implementation of the *l*-th elementary contour with intensity x_l, $l = \overline{1, L}$, (L– the set of elementary circuits, on the basis of which the model M_1 is built) in terms of the model M_1, means that during the time interval T_1 in the network will be spent:

time resource of messages in the amount of $x_l t_l$, where t_l is the cost of the time resource on the *l*-th elementary circuit at x_l=1;

an economic resource in the amount $x_l c_l$, where c_l is the cost of the economic resource on the *l*-th elementary circuit at x_l=1, and the effect is obtained in the amount $x_l e_l$, where el is the effect obtained with one movement of a discrete object along the *l*-th elementary circuit.

The control criteria for task z_1 are, as a rule, in two forms:

$$F_1(z_1) = \min_l \sum_l c_l x_l, \text{If } \sum_r n_r T_1 > R, \quad (1)$$

$$F_2(z_1) = \max_l \sum_l e_l x_l, \text{If } \sum_r n_r T_1 < R, \quad (2)$$

where n_r is the number of messages (discrete objects) of the r_{th} type in the network ($r = \overline{1, \omega}$); ω is the number of types of discrete objects; *R* is the amount of time resource of discrete objects required to perform elementary circuits in order to achieve a given value of the total effect $E = \sum_{l \in L^*} e_l x_l$; L* is a subset of elementary contours included in the solution of problem z_1.

Let us consider the technique for constructing a task for problem z_2 based on the results of solving problem z_1. Suppose, as a result of the operation of the model M_1, a subset of elementary contours *L** became known. Using the operation of set-theoretic union of graphs, we build the structure of the operational network. Having specified a system of control points in which the displacements of discrete objects on the network are calculated, we can formulate the task for problem z_2 as a vector:

$$G = \langle G_1, G_2, ..., G_i, ..., G_s \rangle, \quad (3)$$

where s is the number of control points in the network; G_i is the number of movements that must be made by discrete objects through the *i*-th control point in time $T_i, i = \overline{1, s}$. Wherein:

$$G_i = \sum_{l \in L_i} x_l, \quad (4)$$

$$E_i = \sum_{l \in L_i} e_l x_l, \quad (5)$$

where Li is a subset of contours passing through the i-th control point of the network; E_i is the total effect achieved by discrete objects when moving through the *i*-th control point.

Now we can formulate a control criterion for problem z_2, consistent with criteria (1), (2) of problem z_1, namely:

$$F(z_2) = \min_i \max_k T_i^k,$$
$$F(z_2) = \min_i \max_k T_i^k, \quad (6)$$

where T_i^k is the moment of the *k*-th passage of any of the discrete objects through the *i*-th control point of the network, after which the relation is satisfied:

$$\sum_{l \in L_i} e_l x_l \geq E_i. \quad (7)$$

With such a criterion in the M_2 model, schedules will be constructed that minimize the total time during which discrete objects will make so many transmissions on the network that relation (7) will be satisfied for all control points.

If T_2=T_1 and $F(z_2) \leq T_1$, that the solution of problem z_2 with criterion (6) is simultaneously the solution of problem z_1, since relation (7) is essentially one of the limitations of the M_1 model, and other model constraints (by the size of the time resource of discrete objects) are automatically fulfilled in the M_2 model.

The technique of transition in the described sense from the solution of problem z_1 to the task for problem z_2 is implemented in the hierarchy using the mapping $M_1 \rightarrow M_2$. A factor that complicates the technique of task formation for problem z_2 based on the solution of problem z_1 is the multiplicity of control intervals T_1 and T_2.

Information transition from model M_2 to M_3 is much easier than from M_1 to M_2. The fact is that both M_2 and M_3 belong to the same type of (simulation) models and are built on the basis of the same conceptual scheme - the scheme of state diagrams of discrete objects.

An increase in the degree of detail of the description of the process of moving discrete objects on a network in the M_3 model compared to the M_2 model is achieved by adding some new parameters to the description of discrete objects. The trajectories of discrete objects formed in the M_2 model in the course of solving problem z_2 are transferred to the M_3 model using the mapping $M_2 \rightarrow M_3$without any changes. After that, in the M_3 model, the moments of messages (discrete objects) hitting the network control points are fixed. The choice of the composition of control points for the M_3 model is determined by the nature of the real process and the capabilities of the information system. The set of breakpoints used in M_3 includes the set of breakpoints used in M_2.

The task z_3, solved with the help of model M_3, is to use information about the actual position of discrete objects on the network and compare it with the "model" position planned using M_2, to act on those discrete objects that by the time of such comparison have accumulated temporary or spatial lag from its planned position on the network. In this case, the control action is to give higher priorities to lagging discrete objects in queuing places on the network.

The control criterion used in problem z_3 has the form

$$F_1\left(z_3\right) = \min_{l} \max_{s} \Delta\varepsilon_j^s, \tag{8}$$

where $\Delta\varepsilon_j^s$ is the value of the time lag of the j-th discrete object, measured at the s-th control point.

Another form of the criterion for problem z_3, which estimates the spatial lag of discrete objects from the planned positions on the network, has the form^

$$F_2\left(z_3\right) = \min_{j} \max_{s} \Delta\rho_j^s, \tag{9}$$

where $\Delta\rho_j^s$ is the value of the spatial lag of the j-th discrete object from the s-th control point, measured at time t.

Measurement moment $\Delta\varepsilon_j^s$ is determined by the moment when the j-th message passes the s-th checkpoint on the network. Measurement moment $\Delta\rho_j^s$ is determined by the moment of retrieval of information about the position of the j-th discrete object on the network, which is the scheduled moment of the passage of the j-th discrete object of the s-th control point.

It is clear from the form of the criteria $F_1(z_3)$ and $F2(z_3)$ that if task z_3 is solved, then task z_2 will be solved, since in this case all control points in the model M_2 will be passed by discrete objects or with zero lag, or ahead of time. This ensures the coordination of tasks z_2 and z_3.

The analysis of interlevel coordination of tasks highlights its critical role in ensuring the effectiveness and coherence of hierarchical management within special-purpose units. The requirement to align management activities across different levels stems from the necessity to maintain both conceptual and procedural unity within the decision-making process. Achieving this involves two fundamental mechanisms: firstly, enabling the interpretation of concepts used in one model in terms of another, which ensures semantic compatibility and facilitates mutual understanding between levels; and secondly, guaranteeing the consistency of control criteria applied in coordinated tasks, which prevents conflicts in objectives and ensures uniform evaluation standards. Together, these measures establish a robust framework for integrated management, enhancing operational synergy, reducing the risk of misaligned decisions, and ultimately increasing the efficiency of the unit's activities in fulfilling its objectives.

4. Discussion of results

The proposed approach to message transmission control in special-purpose communication networks demonstrates both theoretical and practical significance. From a scientific perspective, the study expands the existing body of knowledge by addressing the dual problem of dynamic reconfiguration of network topology and simultaneous control of discrete message flows. Unlike conventional models that typically focus on either routing optimization or fault tolerance in isolation, the presented framework integrates these aspects into a unified structure. This enables a more realistic representation of operational conditions, where the spatial-temporal distribution of packets and dynamically emerging disruptions must be considered simultaneously.

From a practical standpoint, the obtained results can enhance the robustness and efficiency of communication processes in mission-critical environments. In particular, the implementation of such models can improve the reliability of military and defense communication systems, increase the fault tolerance of industrial control networks, and strengthen the resilience of critical infrastructure against both accidental failures and deliberate cyberattacks. The developed methodological basis may also serve as a foundation for designing adaptive algorithms capable of real-time adjustment to adverse operational scenarios, thereby ensuring the continuity of decision-making processes in automated control systems.

The scientific novelty of this work lies in the conceptual integration of discrete object management and structural network adaptability into a single modeling framework. This provides opportunities for developing intelligent communication control strategies that go beyond traditional static or semi-static approaches. Furthermore, the study highlights the relevance of incorporating predictive mechanisms, such as artificial intelligence and machine learning, for early detection of failures and proactive reconfiguration.

Future research directions include several promising areas. First, the integration of machine learning methods into the proposed models can support predictive routing and adaptive anomaly detection. Second, further experimental validation under simulated and real-world scenarios will be crucial to assess the practical applicability and scalability of the models. Finally, extending the framework to next-generation communication technologies, such as 6G and beyond, will allow addressing the requirements of ultra-reliable low-latency communication (URLLC) and distributed intelligent systems.

Overall, the results of this study form a solid foundation for advancing both the theoretical understanding and practical implementation of message transmission control models, thereby contributing to the development of resilient, adaptive, and secure communication infrastructures for special-purpose applications.

5. Conclusions

The conducted study is highly relevant in the context of modern challenges in cyber defense, where the operational stability of special-purpose communication networks is increasingly threatened by equipment failures, targeted cyber-attacks, and other dynamically emerging adverse conditions. Given the growing dependence of critical infrastructure and mission-oriented systems on uninterrupted and secure data transmission, the ability to adaptively manage both network topology and the movement of discrete message objects has become a priority task. The proposed approach addresses this need by integrating conceptual, methodological, and computational tools that enhance the resilience and adaptability of such networks under real-time constraints.

The core achievement of the research lies in the formulation of the problem of determining an operational network structure variant that simultaneously accounts for dynamically emerging operational conditions and the actual spatial-temporal distribution of discrete objects at the moment of reconfiguration. This dual consideration ensures that network management decisions are both context-aware and immediately applicable to the current operational state.

To address this problem, a comprehensive model basis was developed, encompassing three main classes of models:

1. Task models, which define the operational and optimization problems to be solved;
2. Perception models, which capture and formalize the state of the network and its environment;
3. Interpretation models, which translate the perceived state into actionable decision-making parameters.

Furthermore, two types of mappings for task models were introduced, enabling transformations between problem formulations at different levels of abstraction. The interrelation and mutual display between these classes of models were systematically presented, providing a coherent framework for their coordinated application.

Special attention was given to the coordination of joint use of different model classes, ensuring semantic compatibility between them and consistency of control criteria. This guarantees that decisions taken at one level of management remain compatible with and supportive of those made at other levels, thereby avoiding conflicts in objectives and evaluation metrics.

The proposed models of functioning for special-purpose communication networks enable the formalization of both the network's operational processes and its reconfiguration mechanisms. This formalization is a prerequisite for the automation of these processes, which is particularly critical in time-sensitive and security-critical applications. Implementing the described model basis is expected to significantly enhance the efficiency, reliability, and cyber-resilience of control processes in special-purpose networks, directly contributing to the strengthening of national and organizational cybersecurity capabilities.

Further research will focus on applying AI for predictive routing, real-time anomaly detection, and system adaptation to next-generation communication technologies, including 6G and distributed intelligent networks.

In summary, the results of this study contribute to the development of robust and adaptive communication models that support the continuity and reliability of information exchange in complex cyber environments.

REFERENCES

1. Lan, Z. (2023), "A Comprehensive Review of Fault-Tolerant Routing Mechanisms for the Internet of Things", *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 14, No. 7, pp. 1083–1093, PDF (open access): https://thesai.org/Downloads/Volume14No7/Paper_116-A_Comprehensive_Review_of_Fault_Tolerant_Routing_Mechanisms.pdf
2. Ayodele, B. and Buttigieg, V. (2024), "SDN as a defence mechanism: a comprehensive survey", *International Journal of Information Security*, Vol. 23, pp. 141–185, https://doi.org/10.1007/s10207-023-00764-1
3. Bourgerie, R. and Zanouda, T. (2023), "Fault Detection in Telecom Networks using Bi-level Federated Graph Neural Networks", *arXiv:2311.14469*, https://doi.org/10.48550/arXiv.2311.14469
4. Mukhin, V. (2005), "Metody i sredstva effektivnogo upravleniya peredachi dannyh v zashchichennykh kompyuternykh networks", *System Research and Information Technologies*, No. 2, pp. 61-75.
5. Roth, M., Simmons, R. and Veloso, M. (2004), "Decentralized Communication Strategies for Coordinated Multi-Agent Policies", 10.1007/1-4020-3389-3_8
6. Pankayaraj, P., and Maithripala, D. H. S. (2020), "A Decentralized Communication Policy for Multi Agent Multi Armed Bandit Problems", *European Control Conference (ECC). IEEE*, pp. 356-361. DOI:10.23919/ECC51009.2020.9143811
7. Morgan, G., Frankenstein, W. and Carley, K. (2015), "Introduction to Dynamic Network Analysis", *Conference Behavior Representation in Modeling and Simulation (BRiMS)*, At: University of California, DC Campus, Washington, DC, Volume: 24, https://www.researchgate.net/publication/275033958_Introduction_to_Dynamic_Network_Analysis
8. Novoseltsev, V., Orlova, D., Dubrovin, A. and Irkhin, V. (2018), "Mathematical model and coordination algorithms for ensuring complex security of an organization", *Journal of Physics*: Conference Series. DOI 10.1088/1742-6596/973/1/012042

Received (Надійшла) 11.08.2024
Accepted for publication (Прийнята до друку) 25.08.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Мілевський Станіслав Валерійович – доктор технічних наук, доцент, професор кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Stanislav Milevskyi – Doctor of Technical Sciences, Associate Professor, Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: milevskiysv@gmail.com; ORCID Author ID: https://orcid.org/0000-0001-5087-7036;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57211218421.

Воропай Наталя Ігорівна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Natalia Voropay – PhD, Associate Professor, Associate Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: voropay.n@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-1321-7324;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=58505137500.

Гаврилова Алла Андріївна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Alla Havrylova – PhD, Associate Professor, Associate Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: alla.havrylova@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-2015-8927;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57208029999.

Король Ольга Григорівна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Olha Korol – Candidate of Technical Sciences, Associate Professor, Associate Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Olha.Korol@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-8733-9984;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190437459.

Аксьонова Ірина Вікторівна – кандидат економічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Iryna Aksonova – Candidate of Economic Science, Associate Professor, Associate Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: ivaksyonova@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-2605-0455;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57206727489.

Хвостенко Владислав Сергійович – кандидат економічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Vladyslav Khvostenko – PhD in Economics, Associate Professor, Associate Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: vladyslav.khvostenko@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-6436-4159;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57218950543.

МОДЕЛІ УПРАВЛІННЯ ПЕРЕДАЧЕЮ ПОВІДОМЛЕНЬ ДЛЯ СПЕЦІАЛЬНИХ ЗВ'ЯЗКОВИХ МЕРЕЖ

С.В. Мілевський, Н.І. Воропай, А.А. Гаврилова, О.Г. Король, І.В. Аксьонова, В.С. Хвостенко

Анотація. Актуальність дослідження. У сучасних умовах управління спеціалізованими мережами зв'язку спеціального призначення актуальною є проблема адаптивного управління передачею повідомлень в умовах динамічних змін структури мережі, які можуть бути спричинені відмовами обладнання, кібератаками та іншими факторами. Забезпечення надійної та безперебійної роботи таких мереж має критичне значення для ефективності систем управління. **Предмет дослідження**. Моделі управління передачею повідомлень у мережах зв'язку спеціального призначення, а саме ієрархічні моделі зі змінною структурою, їх взаємодія та координація на різних рівнях. **Мета дослідження**. Формування моделі управління, яка дозволяє адаптивно змінювати структуру операційної мережі зв'язку з урахуванням нових умов експлуатації та поточного положення дискретних об'єктів (пакетів повідомлень) у мережі. **Отримано наступні результати**. Запропоновано модельну базу, що включає три класи моделей: моделі задач, моделі сприйняття та моделі інтерпретації. Сформульовано два типи відображень для моделей задач та описано їх взаємозв'язки. Визначено проблеми координації спільного використання моделей різних класів. Представлені моделі дозволяють формалізувати процес функціонування мережі зв'язку та її перебудови в режимі реального часу. **Висновки.** Розроблені моделі дозволяють автоматизувати процес управління передачею повідомлень та зміною конфігурації мережі спеціального призначення, що підвищує ефективність управління та стійкість мережі до впливу негативних факторів, таких як кібератаки або збої обладнання.

Ключові слова: мережі спеціального призначення; моделі управління; передача повідомлень; комунікаційна мережа; координація завдань.