DOI: https://doi.org/10.15276/hait.09.2026.25
UDC 519.87:004.942:517.977

A mathematical model for evaluating the controllability of information management systems in complex adaptive environments

Serhii V. Bazarnyi [1)]
ORCID: https://orcid.org/0000-0001-9545-1960; serhii.bazarnyi@edu.nuou.org.ua. Scopus Author ID: 58905874600
Pierre Murr[2)]
ORCID: https://orcid.org/0009-0007-4094-0223; murrpierre@gmail.com. Scopus Author ID: 26025143400
Oleksandr V. Voitko[1)]
ORCID: https://orcid.org/0000-0002-4610-4476, o.voitko@edu.nuou.org.ua. Scopus Author ID: 57210362201
Yurii, A. Husak[1)]
ORCID: https://orcid.org/0000-0002-3423-2112, y.husak1512@gmail.com; Scopus Author ID: 60033365500
Serhii, P. Yevseiev[3)]
ORCID: https://orcid.org/0000-0003-1647-6444; serhii.yevseiev@gmail.com. Scopus Author ID: 57190440690
[1)] National Defence University of Ukraine, 28, Air Force Ave. Kyiv, 03049, Ukraine
[2)] International University of Science and Technology in Kuwait, Ardiya Government Area Mohamad Bin Qasim Str. Ardiya, Kuwait
[3)] National Technical University "Kharkiv Polytechnic Institute", 2, Kyrpichova Str. Kharkiv, 61000, Ukraine

ABSTRACT

Modern information management systems operate in complex adaptive environments characterised by high dynamics, uncertainty and continuous hybrid disturbances, which significantly complicates the maintenance of coordinated control. Under such conditions, traditional approaches focused on reliability and performance of individual components are insufficient, as they do not account for systemic interactions between subsystems and the risk of loss of overall controllability. This creates a need for the development of mathematical approaches for quantitative assessment of system controllability as a key property of the resilience of critical information infrastructure. **The aim of this study** is to develop a mathematical model for assessing the controllability of information management systems operating in complex adaptive environments, taking into account the interaction of functional subsystems, external and internal disturbances, and control actions that influence system dynamics. **Methodology:** The study employs a vector–matrix approach to dynamic modelling, in which the information management system is represented as a set of interacting functional subsystems described in the state space by a system of differential equations. The model incorporates inter-subsystem interactions, degradation processes, external disturbances and control actions, as well as the influence of cognitive factors on system behaviour. Numerical verification of the proposed model is performed using the fourth-order Runge–Kutta method within a scenario-based analysis framework. The information management system is formalised as a set of five interacting functional subsystems, including infrastructural, network-communication, application, analytical-cognitive and user levels. An integral system controllability coefficient is introduced as a scalar functional of subsystem states, interaction parameters and control inputs. It is shown that this coefficient enables quantitative identification of transitions between stable, adaptive, crisis and pre-collapse operating regimes. An interpretation scale is developed that relates the values of the coefficient to subsystem coordination and the probability of management desynchronisation. The results of numerical modelling confirm the sensitivity of the proposed indicator to destabilising influences and its ability to reflect the effectiveness of compensatory control actions. The proposed approach extends existing methods of assessing system stability and reliability by introducing a dynamic integral indicator that captures the combined influence of structural interactions, control actions and cognitive factors on system behaviour. The scientific novelty lies in the formalisation of system controllability as a quantitative functional characteristic that reflects the ability of a complex system to maintain coordinated operation under destabilising conditions. **Practical value:** The developed model provides a practical tool for application in real-time monitoring systems and decision support platforms for critical information infrastructure, enabling early detection of loss of controllability and supporting the design of adaptive response strategies.

Keywords: Information systems; system controllability; adaptive systems; critical infrastructure; decision support; state security; mathematical modelling

***For citation*: Bazarnyi S. V., Murr P., Voitko O. V., Husak Yu. A., Yevseiev S. P. "A mathematical model for evaluating the controllability of information management systems in complex adaptive environments". *Herald of Advanced Information Technolog*. 2026; Vol.9 No.3: 380–399. DOI: https://doi.org/10.15276/hait.09.2026.25**

INTRODUCTION

The rapid digitalization of society, the growth in data volumes and the increasing complexity of management information system (hereinafter MIS) architectures are transforming these systems from traditional information-processing tools into complex adaptive structures, upon whose stability the quality of management decisions directly

depends. Modern MIS integrate distributed computing resources, network and communication subsystems, application services, analytical and cognitive modules, and human-machine interfaces, operating in an environment characterized by highly dynamic events, heterogeneous data sources, and constant external and internal disturbances. Under such conditions, it is not only the performance or reliability of individual components that becomes crucial, but also the system's ability to maintain controllability – that is, to ensure coordinated interaction between subsystems, the stability of information flows, and the predictability of responses to changes in the environment.

In this study, the term "complex adaptive environment" is used in an extended sense as a dynamic system that modifies its parameters and interaction structure in response to the state of the MIS. Unlike classical control theory, where adaptivity is considered an inherent property of the system itself, the environment is interpreted here as an active factor that shapes the evolving conditions of system operation.

Research in the field of information systems mainly focuses on individual aspects of fault tolerance, cybersecurity, service quality and compliance with SLA (service level agreement) metrics, and rarely provides a holistic view of the information system as a single managed entity [1], [2]. Typical metrics, such as availability, reliability or MTBF (mean time between failures), describe important but local properties and do not account for systemic interactions between subsystems, the effects of accumulated delays [3], long-term degradation processes, and the increase in entropy of the information environment. Consequently, there is a lack of formalized tools that would allow the detection of early signs of loss of controllability, the monitoring of the transition from a stable to a critical operating mode, and the quantitative assessment of the impact of control actions on the overall state of the system, particularly when it comes to MIS of critical information infrastructure objects.

Scientific research is developing approaches involving goal-oriented design, the use of agent-based models, game theory methods, and cognitive and scenario-based modelling to describe complex techno-social systems [4], [5]. At the same time, these approaches are predominantly applied to the analysis of individual subsystems of user behavior, network traffic and cyber incidents, and rarely result in the formation of a coordinated integrated indicator that would characterize the global controllability of the MIS in dynamics. This creates a research gap between conceptual models of complex adaptive systems and practical requirements for the monitoring and control of real-world information management system.

In this context, it is important to develop a mathematical framework that enables the description of an information system as a system of interacting functional subsystems, each with its own states, resources and channels of influence; formalizes the processes of degradation and compensatory control; and provides for the introduction of an integrated indicator that quantitatively reflects the level of system controllability. Such an approach should be sufficiently versatile for application in various classes of information systems, whilst also being suitable for implementation in real-time computing environments and integration with modern decision support systems, in particular those utilizing artificial intelligence methods.

The scientific novelty of this work lies in the formalization of the controllability of information management systems as a dynamic integral indicator that reflects the coherence of the functioning of interacting functional subsystems within a complex adaptive environment. Unlike classical indicators of reliability, stability or structural controllability, this work introduces, for the first time, the coefficient of system controllability (hereinafter referred to as the CSC), which is defined as a functional of the system state vector, subsystem interaction parameters and control influences, and allows for the quantitative identification of transitions between stable, crisis and collapse modes of operation.

To achieve the main objective of the study, a number of specific research tasks must be addressed. Firstly, to carry out a conceptual formalization of the MIS as an object comprising interdependent functional subsystems, the operation of which is described by a state vector of their capacity. Secondly, to develop a mathematical framework in the form of a system of vector-matrix differential equations that accounts for the dynamics of inter-subsystem interaction via the connection intensity matrix, cognitive penetration effects and degradation processes. Thirdly, to scientifically justify the introduction of the proposed integral coefficient of system controllability (CSC) as a scalar functional that aggregates deviations of the system's current states from optimal values. Furthermore, to numerically verify the model using the 4th-order Runge-Kutta method and to develop an algorithmic scheme by integrating it into a decision support system (DSS), in order to transition to proactive monitoring and the formulation of adaptive

strategies for the protection of critical information infrastructure assets.

RELATED WORKS

In the study [6], the issue of controllability of information systems in complex adaptive environments, or Cyber-Physical-Social Systems (CPSS), is being explored along several complementary lines of research; however, it has not yet resulted in a single integrated approach. Research on the controllability and observability of networked and non-linear systems demonstrates that the structural properties of networks, the ranks of controllability/observability matrices and the types of connections critically determine the possibility of achieving desired states of multi-system objects, which creates a theoretical basis for introducing an integral coefficient of system controllability in information management system. In parallel, models of reliability and survivability for critical information infrastructure are being developed, which focus on the fault tolerance of components, recovery times and the preservation of functions under cyber threats, however, these typically remain oriented towards post-event assessment rather than continuous real-time monitoring of controllability.

The study [7] focuses on decision support systems for the protection of critical infrastructure and agent-based scenario models of socio-technical systems, which provide tools for scenario analysis, simulation of actor behavior and the formulation of adaptive response strategies, yet do not combine these capabilities with a formalized dynamic controllability metric for the information management system as a single entity. Taken together, these approaches highlight a scientific challenge arising from the absence of an integrated mathematical model that would simultaneously account for the network controllability, reliability and resilience of critical infrastructure, cognitive and informational influences, and would be directly embedded in decision-support systems for the quantitative assessment of the controllability of information management system in complex adaptive environments.

The theoretical foundations of controllability and observability in networked dynamic systems are set out in [8], [9], which formalize the dependence of the controllability of network states on the topology of connections, the rank of controllability matrices, and the heterogeneity of nodes.

In particular, the research [10] highlights the role of node heterogeneity in multi-subsystem objects, which directly correlates with the need to introduce an influence intensity matrix into the model to describe the interaction between such functional subsystems, which are structural elements of the MIS and the spaces in which the subsystem performs its functions (*infrastructural-physical*, *network-communication-cybernetic*, *applied-informational*, *analytical-cognitive*, and *user-psychological*). These approaches provide the basis for introducing an integral coefficient of system controllability as a characteristic of multi-subsystem MIS.

The next critical area of research involves transforming classical approaches to reliability into a concept of the viability of complex systems. The fundamental principles of reliability modelling for complex systems, laid out in [11], allow for the formalization of probabilistic failure characteristics. However, for modern MIS real-time control systems, standard parameters are no longer sufficient.

An important contribution to the development of the mathematical framework for evaluating complex systems is the research [12] devoted to the development of models for reliable structures of information and control systems. This work emphasizes the need to account for the structural integrity and functional stability of systems under dynamic conditions and confirms that the reliability of an MIS depends on the configuration of interactions between subsystems, which logically supports the use of a matrix of local control influences. The authors' proposed approach to modelling structural components correlates with the concept of dividing MIS into infrastructure, network, application and cognitive subsystems, and the use of analytical models to describe the states of control systems serves as the basis for a vector-matrix differential equation that describes the dynamics of the performance of functional subsystems. This therefore allows the concept of a 'reliable structure' to be integrated into the broader context of 'controllability' and enables the proposed coefficient system controllability (CSC) to be interpreted as a measure of management effectiveness and an indicator of the preservation of the system's structural viability under conditions of high entropy.

Modern methods for assessing the survivability of complex systems operating in an uncertain and stochastic environment occupy a special place in this analysis. In [13], a mathematical framework for assessing reliability parameters is proposed, which is based on taking into account uncertainty factors, which is critical for systems facing unpredictable

external influences. The use of parameter assessment methods under conditions of uncertainty provides a basis for calculating the entropy of the cognitive field, which serves as an indicator of chaos and instability. Therefore, the application of such models extends the classical understanding of reliability to the level of strategic stability and enables the proposed model to detect failures and predict the threshold values beyond which resonant instability and complete loss of system coordination occur.

A contribution to the development of the theory of resilience in complex control systems is also demonstrated by the study [14], which proposes a framework for enhancing the cyber resilience of critical infrastructure based on a dynamic capabilities approach. The authors emphasize that, in the context of modern cyber threats, the resilience of facilities depends not only on static protection but also on the system's ability to adapt and rapidly transform its functions during the active phase of an attack. The study authors' conclusions regarding the need for continuous improvement of defense capabilities underscore the relevance of introducing the (CSC) as a tool for the early detection of transitions to collapse modes. The integration of the dynamic capabilities approach into the mathematical framework allows the controllability of the MIS to be viewed not as a steady state, but as a continuous process of maintaining the functional capacity of subsystems under conditions of high entropy. This makes it possible to interpret the proposed scale of values as a measure of the realization of the system's dynamic capabilities in countering destabilizing threats.

An important step in developing a methodology for assessing critical infrastructure systems is to take into account the findings of the study [15], which presents a unified conceptual framework for assessing the resilience of critical infrastructure. The authors use the *Delphi* method to verify stability parameters, which allows the most significant influencing factors to be identified in the context of complex systemic risks. The justification of the integrated approach in this work demonstrates the need for a unified assessment framework for interdependent systems, which directly correlates with the objective of developing an integrated coefficient of system controllability (CSC). The application of expert methods to determine the weighting of indicators forms the methodological basis for using the expert assessment method when determining the weighting of functional subsystem parameters. The authors' emphasis on creating measurable viability indicators underscores the idea of introducing a scale of CSC values to classify MIS operating modes into stable, transitional and critical. The integration of provisions on a unified stability assessment allows the mathematical model to be interpreted as an applied implementation of similar frameworks for digital environments [16]. This links dynamic changes in the state vector of subsystems with global standards for ensuring the resilience of critical information infrastructure objects, which is particularly important for enhancing the predicted resilience of public administration.

The current stage of development of decision support systems (DSS) in the field of critical information infrastructure protection is characterized by a shift from static knowledge bases to intelligent real-time monitoring platforms. Research conducted within the framework of international projects such as CIPRNet/ERNCIP [17] and RESIIST [18] demonstrates the effectiveness of integrating large datasets on systemic risks to develop scenario-based emergency response plans. In particular, the methodological approaches of this project focus on assessing the interdependencies between different types of infrastructure, which provides the basis for using the (CSC) proposed in this work as a key input parameter for DSS analytical modules.

The integration of mathematical models into DSS enables a shift from merely recording incidents to predicting the controllability of the entire system. According to the findings in [19] regarding the rethinking of management and control processes, modern control systems require tools to detect early signs of subsystem desynchronization before a critical collapse occurs. In this context, the use of artificial intelligence methods to analyse critical destabilization nodes, as mentioned in [20], [21], directly correlates with the model for finding equilibrium trajectories using the methods described in [22]. Thus, the developed model formalizes the level of controllability via an indicator and serves as the algorithmic core for automated situational analysis systems, ensuring the selection of the most robust response configurations in the face of modern cyber threats.

Ensuring the MIS in complex adaptive environments requires taking into account the non-linear dynamics of interaction between technical components and the human factor, which justifies the use of agent-based modelling methods for socio-technical systems. The methodological foundations developed in the study [23] allow the structure of

such systems to be formalized through a set of autonomous agents, each of which is endowed with its own behavioral rules and utility functions. This approach creates conditions for modelling emergent effects and cognitive turbulence, which in the model correlates with the analysis of cognitive field entropy and the probability of service desynchronization. In parallel, the concepts of agent-based modelling [24] provide a toolkit for scenario-based simulation of large-scale self-organization processes, enabling the investigation of the resilience of MIS to cascading failures and targeted destabilizing influences. The integration of agent-based models with scenario analysis enables the translation of theoretical principles regarding complex adaptive systems into applied algorithms for solving dynamic games with incomplete information.

The use of the approaches in [25] confirms the validity of the transition from deterministic calculations to stochastic modelling of equilibrium trajectories, which is necessary for real-time calculation of the integral (CSC). Thus, the agent-scenario approach serves as a link between the structural stability of the network and the dynamics of management collapse, ensuring the high predictive capability of the proposed mathematical model.

A study of the integration of blockchain technologies into comprehensive information security systems for state registers [26] presents a systematic approach to enhancing the resilience of critical state-level information systems through decentralized transaction verification and consensus protocols, emphasizing audit transparency, the impossibility of insider data manipulation, and the creation of immutable event logs in distributed ledgers. Despite the progressive nature of the approach, this work focuses on static resilience, and blockchain logging is reactive (post-event audit) rather than proactive (predictive controllability), which limits its integration into DSS for crisis response.

An analysis of research in this field indicates that most existing approaches focus either on the structural controllability of network systems or on the reliability and resilience metrics of individual critical infrastructure components. At the same time, these works lack a formalized indicator that integrates the dynamics of inter-subsystem interaction, degradation processes and control actions into a single quantitative measure of the global controllability of an information management system. The system controllability coefficient proposed in this paper fills this research gap by combining the apparatus of control theory, the modelling of complex adaptive systems, and the practical requirements of decision support systems.

RESEARCH AIM AND OBJECTIVES

The aim of this article is to develop a mathematical model for assessing the controllability of information management systems operating in complex adaptive environments.

To achieve this aim, the following objectives were identified:

– to analyze the features of the functioning of modern management information systems as complex adaptive systems in destabilized environments;

– to decompose the MIS structure into key subsystems (infrastructure, network, application, cognitive and user) to determine their impact on overall manageability;

– to define and formalize the indicator (CSC) as an integral metric of stability and manageability;

– to develop a system of differential equations that describe the dynamics of changes in the MIS state under the influence of destabilizing factors, resource degradation and cognitive penetration;

– to develop an interpretative scale of manageability levels for classifying system states (from stable to collapse) in order to support management decision-making;

– to test (verify) the model on examples of real crisis states of critical infrastructure (in particular, under martial law) to confirm its adequacy.

Despite the extensive use of classical controllability and stability metrics, a direct quantitative comparison with the proposed system controllability coefficient remains limited due to the absence of universal integral indicators of a similar type. However, qualitative comparison shows that the proposed coefficient is consistent with established approaches in control theory, including Lyapunov stability criteria and structural controllability concepts, while extending them by incorporating inter-subsystem interactions and cognitive influences.

RESEARCH METHODOLOGY

To achieve this objective, an integral coefficient of system controllability is introduced, which enables the classification of CSC operating modes into stable, transitional (adaptive and crisis) and critical (pre-collapse and limit) modes, as well as

supporting the decision-making process regarding adaptive control and the enhancement of the stability of such systems. The paper formalizes the dynamics of interaction between the functional subsystems of an information system, introduces the integral coefficient of system controllability and justifies its interpretation, and analyses the possibilities for the practical integration of the proposed model into decision-support systems and critical information infrastructure monitoring platforms.

Within the proposed approach, the management information system is represented as a vector of states of interacting functional subsystems, each of which is characterized by its own set of parameters: resource availability, query processing intensity, sensitivity to external disturbances, and recovery capability. This approach makes it possible to describe both normal and degraded modes of operation through a single dynamic model, as well as to account for both local and global control influences at the system-wide level. For formalization, a vector-matrix framework is employed, within which changes in the state of subsystems are defined by a system of differential equations describing the balance between intra-system interactions, natural degradation processes, and compensatory control actions.

Particular attention has been paid to modelling the interaction of subsystems under stochastic disturbances characteristic of modern digital environments. The intensity of interaction is described by a connection matrix, the elements of which reflect the strength and direction of influence of one subsystem on another, and which may also change over time under the influence of external factors (load variations, the occurrence of abnormal events, changes in network configuration). Numerical integration methods and scenario analysis are used to study the model's behavior, enabling the assessment of the system's sensitivity to parameter changes, the identification of critical combinations of loads and disturbances, and the determination of ranges of stable operation.

The integral CSC is introduced as a function of the current states of the subsystems and the parameters of their interaction, aggregating information about the level of coordination of the system's operation into a single scalar indicator. Based on an analysis of the coefficient's dynamics, an interpretation scale is formed, which allows for the identification of regions of stable operation, transient modes with increased sensitivity to disturbances, and critical states in which the system's controllability is significantly reduced. This provides the basis for developing monitoring algorithms that track the indicator's value in real time, generate warning signals when threshold levels are reached, and initiate adaptive control strategies aimed at restoring the information system to an acceptable operating mode.

In the context of the digital transformation of information systems and the intellectualization of situational analysis, this research is based on the mathematical modelling of the controllability dynamics of management information system as complex adaptive systems comprising five interrelated functional subsystems: infrastructure, network and communications, application, analytical and cognitive, and user subsystems. The input variables of this work are presented in the form of resources and information flows, and the output effects take the form of strategic advantage or the neutralization of destabilizing influences.

The state of each subsystem i at time *t* is described by a scalar power variable: $P_i(t), i(i=\overline{1,5})$, which forms the system's state vector, with dynamics defined by a vector-matrix differential equation that accounts for inter-subsystem interactions via the connection intensity matrix, cognitive penetration, and degradation processes (in particular, with accumulated delays and the entropy of the information environment).

The scalar power variable x_i (t) is interpreted as an integral indicator of the functional capability of a subsystem, whose physical or informational meaning varies depending on its level. In particular, at the technical level it represents throughput and computational resources; at the information level, the intensity of data processing and transmission; at the cognitive level, the level of cognitive load and decision-making capability; and at the managerial level, the efficiency of coordination and response speed.

In this study, the concept of cognitive penetration is interpreted as a generalised external disturbing influence of a socio-technical nature that affects the state of a subsystem through informational, behavioural and managerial mechanisms, and is mathematically associated with the class of uncontrolled or partially controlled disturbances in control theory. Unlike the classical approach in control theory, where a disturbance is treated as an additive input signal that affects the system without altering its internal structure, in the proposed model the cognitive penetration vector $\vec{\varphi}(t)$ has a structural – dynamic character.

Its influence manifests not only in changes of subsystem states but also in modifications of the intensity of inter-subsystem interactions, the level of cognitive coherence, and the parameters of system operation. In the proposed model, the terms "cognitive" and "adaptive" are not introduced as independent mathematical categories but are treated as interpretative extensions of the classical framework of dynamical systems theory. At the same time, their distinguishing feature lies in the fact that the corresponding influences are formalised as input signals that affect the structure of inter-subsystem interactions, which differentiates the model from classical approaches.

The introduced variables x_i (t) are interpreted as a quantitative measure of the functional capability of the *i*-th subsystem, integrating resource availability, information processing intensity, disturbance resilience, and recoverability. The set of these variables forms the system state vector. In a generalised form, the model can be represented in the state-space form as a system:

$$\dot{x} = f(x,u,d),$$

where x(t) is the state vector of the subsystems, u(t) denotes the control inputs, and d(t) represents external disturbances.

To formulate scenario analysis rules, the dynamic model has been supplemented with a logical-algebraic framework utilizing methods of Boolean algebra and set theory, which allow the formalization of relationships between threat sources, system vulnerability and compensatory control actions [27], [33].

A quantitative assessment of system controllability is carried out using the integral coefficient CSC(t), which aggregates the deviations of the current states of the subsystems from their optimal values, taking into account the permissible stability intervals, where an increase in the coefficient above unity signals a risk of cascading loss of control.

Numerical verification was performed using the fourth-order Runge-Kutta method for three scenarios [22] (steady state, degradation under cyberattacks, adaptive correction) with normalised initial conditions and parameters (a 30 % increase in interaction intensity, cognitive penetration by 50 %), with results presented as dynamic coefficient curves and tables confirming the transition from stable values of 0.15 to critical values of 0.82, followed by a recovery to 0.22.

The research methodology is supplemented by the theory of dynamic games with incomplete information for stochastic agents with utility functions, expert assessment of the weighting of interaction matrix parameters, and cognitive scenario modelling for integration into decision support systems focused on crisis management, cybersecurity and critical infrastructure monitoring, with the potential for real-time implementation based on artificial intelligence platforms. The scientific objective of the research is to construct an integrated mathematical model that combines approaches from analytics, modelling, information security and applied mathematics to analyze interactions in the context of critical infrastructure protection, and involves assessing activity based on a matrix of aggregate reactivity.

Table 1 has been compiled to illustrate the proposed indicator (CSC), presenting a comparative analysis of the terminological framework, formalization mechanisms and specific applications of the relevant concepts within the context of mathematical modelling.

To verify the proposed CSC model, a comparative analysis was carried out of the key elements of the state system's functioning during two crisis phases – 2014 and 2022 (Table 2) – presenting relevant indicators, including the level of strategic controllability, cognitive resilience and information security [28].

Based on the generalised characteristics for the periods of 2014 and 2022, a hypothetical trajectory of the CSC can be constructed, which confirms the consistency of qualitative assessments with the model dynamics.

This trajectory is not derived from direct numerical reconstruction of historical data but represents a qualitative projection of CSC dynamics within the proposed model framework. It reflects the transition between system states through changes in subsystem coordination, cognitive resilience and control integrity, thereby providing indirect validation of the model's adequacy without requiring explicit empirical time-series data.

A comparative analysis of specific crisis phases in the operation of the control system is used in this paper as an illustrative example of the application of the proposed system controllability coefficient scale. The estimates provided are not the result of a direct numerical calculation of the model, but serve as a conceptual interpretation of possible values of the CSC based on known characteristics of management coordination, information stability and cognitive unity of the system in different periods [29], [30].

Table 1. **A comparison of concepts relating to the coefficient system controllability**

No. Item	Term	Description of the mechanism	Formalization	Use in modelling
1	State Collapse / Failure	Loss of management functions	The controllability coefficient, defined in terms of the loss-of-control function	Modelling the loss of control system functionality in a crisis situation
2	Loss of Command and Control	Breakdown of the chain of command	Determined by a decline in the effectiveness of management channels and a reduction in the responsiveness of management structures	Modelling disturbances in control loops and their impact on stability
3	Strategic Decapita-tion	Removal/suspension of management	The strategic loss of management structures is described by an indicator that reflects a decline in management functions	Modelling the consequences of a lack of strategic management in a conflict situation
4	Leadership Vacuum	A lack of guiding principles for society	It can be modelled mathematically due to the low level of strategic controllability	Modelling the decline in system stability in a context of political disorientation
5	Disruption Index	Loss of system functionality	The breach index is determined based on digitalization and data security parameters, which include stochastic factors	Use in technical models to identify the extent of disruption to critical systems
6	Instability Factor (IF)	Level of system instability	Evaluation using functions that describe entropy changes in a system, characterizing the degree of chaos and instability	Modelling systemic instability using deterministic or stochastic models
7	Collapse Trigger Threshold	System collapse	It is determined by the threshold values in the stability dynamics parameters corresponding to critical points	Modelling of system collapse points under conditions of significant external and internal disturbances
8	Coefficient System Controllabi-lity (CSC)	A formalized indicator of a loss of controllability	A mathematical model for calculating CSC (t), which assesses managerial competence based on the combined impact of all components	Proposed for a model of interactions and the prediction of managerial collapse

***Source*: prepared by the authors**

Table 2. **The dynamics of system controllability and strategic coherence**

Criterion	The crisis phase of 2014 (Administrative collapse)	The crisis phase of 2022 (Resilient governance)
The state of the country's leadership	A complete loss. No centralized control	Maintaining continuity of leadership. A clear chain of command
Coordination of Ukraine's defense forces	Absent. Some members of the leadership and other bodies are disoriented and disorganized	Coordination at the appropriate level. Rapid response to external factors, proactive resource development
Civilian control	Panic. No official statements from the system's leadership	A major information campaign
Information security	A complete failure. Agents of influence controlled the communication platforms	A coordinated information policy. Blocking channels, institutionalizing information security
Societal cognitive resilience	High level	A high level of unity
Reaction from international partners	Uncertainty, confusion. Doubts about the effectiveness of the management system	Strong international support, clear agency. Direct financial and humanitarian aid
level CSC	$CSC(t) \approx 0,9$ – the near-total collapse of the chain of command	$CSC(t) \approx 0,1-0,2$ operational control has been maintained, and effective strategic management has been implemented
Results within the first 30 days	The onset of loss of control	A strategic victory in the system defense phase

***Source:* compiled by the authors**

Analytical summary. In 2014, the controllability of the management system declined – this is a classic example of a management collapse. In 2022, by contrast, the absence of a collapse (low index) formed the basis for a successful response. The constructed model forms the basis for determining the CSC coefficient function, which mathematically describes the system's controllability at various points in time and allows for a quantitative assessment of the degree of preservation of informational subjectivity. The values of the CSC, as a function of time and the influence of functional subsystems, provide a basis for predictive modelling of the interaction of their scenarios in the context of developing adaptive strategies to counter destabilizing threats.

The proposed scale of values for the system controllability coefficient is based on an interpretation of the power dynamics of functional subsystems and the level of entropy in the system's cognitive field, as shown in Table 3. The identified intervals of the system controllability coefficient correspond to qualitatively different modes of operation – ranging from stable to collapsing – and can be used as threshold benchmarks in monitoring and decision-support systems for the timely detection of loss of controllability.

The proposed threshold values of the CSC are obtained based on scenario analysis and generalisation of numerical simulation results. They are interpretative in nature and may be refined through statistical processing of empirical data in future studies.

The development of the mathematical framework is based on an analysis of the key principles governing the interaction of functional subsystems [31] and the countering of external influences, which involve the simultaneous use of physical, informational, cognitive and cybernetic components to achieve strategic objectives.

The beginnings of mathematical modelling Equation (1) is introduced as a generalised model of the dynamic interaction of subsystems, based on the principle of influence balance (interaction–degradation-control) and analogous to state-space representations. All variables are normalised, which ensures model consistency without the explicit introduction of physical dimensions.

Interaction *i*-th functional subsystem $P_i(t)$ with other subsystems can be expressed in terms of a differential equation describing the interaction between the systems, based on research [5]:

$$\frac{dP_i(t)}{dt} = \sum_{j=1}^{n} \omega_{ji}(t) \cdot Pi(t) \bullet \varphi_{ji}(t) - \delta_i \cdot Pi(t) + u_i(t), \quad (1)$$

where $w_{ji}(t)$ is intensity of the effect *j*-th functional subsystem on *i*-th subsystem, $i, j = \overline{1,n}$; δ_i is degradation factor *i*-th subsystems (power loss *i*-th subsystem); u_i (t) is a decisive influence on *i*-th subsystem; *n* is number of functional subsystems

In general, the power control model for functional subsystems can be represented by a vector-matrix differential equation:

$$\frac{d\vec{P}(t)}{dt} = W(t)\vec{P}(t)\vec{\varphi}(t) - \vec{\delta}(t)\vec{P}(t) + B(t)\vec{u}(t), \quad (2)$$

where $\vec{P}(t) = (P_1(t), P_2(t), ..., P_n(t))$ is power vector of subsystems; $\vec{\varphi}(t) = (\varphi_1(t), \varphi_2(t), ..., \varphi_n(t))$ is the cognitive penetration vector into the subsystems at

Table 3. **A scale of a system's management capability in an information environment**

Value CSC	System status	Cognitive field entropy H (U)	Power *Pi* (t) relative to *P*opt (t)	Probability of desynchronization (%)	Interpretation
0.00-0.20	Stable	Low	Maximum	≤ 5 %	Optimal system performance
0.21-0.45	Adaptive	Moderate	75-90 %	10-25 %	The risk of cognitive conflict
0.46-0.65	Crisis	High	45-74 %	40-70 %	Intervention required
0.66-0.80	Pre-collapse	Very high	15-44 %	> 80 %	Resonance instability
> 0.81	Extreme conditions	Maximum	< 15 %	≈100 %	Complete loss of coordination

Source: **compiled by the authors**

a given point in time *t*;. $\vec{\delta}(t)=\left(\delta_1(t),\delta_2(t),...,\delta_n(t)\right)$ is vector of subsystem degradation intensity; $\vec{u}(t)=(u_1(t),u_2(t),...,u_n(t))$ is power control vector for subsystems;

$W(t)=\begin{bmatrix}\omega_{11}(t) & \cdots & \omega_{1n}(t)\\ \vdots & \ddots & \vdots \\ \omega_{n1}(t) & \cdots & \omega_{nn}(t)\end{bmatrix}$ is impact intensity matrix.

Thus, unlike classical models: $\dot{x}=Ax+Bu+Dw$, of the form in which the disturbance enters W(t) additively, in the proposed model $\varphi(t)$ the disturbance influences both the state vector and, indirectly, the interaction matrix A(t), reflecting structural changes in the interconnections between subsystems under the influence of information and cognitive factors;

B(t) – matrix of local management influences (local management matrix) on functional subsystems. The matrix of local control actions defines the intensity and direction of control inputs applied to the subsystems; its elements are determined based on expert assessments or statistical characteristics of system operation.

Equation (2) can then be written as follows:

$$\frac{d\vec{P}(t)}{dt}=\left[W(t)\vec{\varphi}(t)-\vec{\delta}(t)\right]\vec{P}(t)+\vec{u}(t)B(t), \quad (3)$$

or:

$$\frac{d\vec{P}(t)}{dt}=A(t)\vec{P}(t)+B(t)\vec{u}(t), \quad (4)$$

where $A(t)=W(t)\vec{\varphi}-\vec{\delta}(t)$ is impact matrix.

To derive an expression for the CSC, we shall formulate a system of vector differential-algebraic equations for the optimal power control of the functional subsystems:

$$\begin{cases}\dfrac{d\vec{P}(t)}{dt}=A(t)\vec{P}(t)+B(t)\vec{u}(t)\\ \vec{P}_{opt}(t)=C(t)\vec{P}(t)+D(t)\vec{u}(t)\end{cases}, \quad (5)$$

where $\vec{P}_{opt}(t)=(P_{1opt}(t),P_{2opt}(t),...,P_{nopt}(t))$ is vector of optimal power values *i*-th subsystems $\vec{P}_{i\,opt}(t)$ at a given moment $i,\ j=\overline{1,n};$ $C(t)$ is matrix of the performance and interaction of subsystems; $D(t)$ is matrix of crisis management subsystems (crisis management interventions). The optimal values are defined as those that minimise deviations of subsystem states from the target level under stability and resource constraints and can be obtained as a solution to an optimal control problem. The crisis management matrix represents compensatory control actions applied under critical deviations; its elements are specified either through scenario-based design or expert assessment depending on the type of threats.

Let us consider a steady-state condition in which: $\dfrac{d\vec{P}(t)}{dt}\to 0$ provided that $t\to\infty$.

We can then express the system of equations (5) as follows:

$$\begin{cases}0=A(t)\vec{P}(t)+B(t)\vec{u}(t)\\ \vec{P}_{opt}(t)=C(t)\vec{P}(t)+D(t)\vec{u}(t)\end{cases}, \quad (6)$$

Accordingly, the system of vector algebraic equations can be written as follows:

$$\begin{cases}\vec{P}(t)=-\dfrac{B(t)}{A(t)}\vec{u}(t)\\ \vec{P}_{opt}(t)=C(t)\vec{P}(t)+D(t)\vec{u}(t)\end{cases} \quad (7)$$

Substituting the first equation from system (7) into the second, we obtain the following mathematical expression:

$$\vec{P}_{opt}(t)=-C(t)\frac{B(t)}{A(t)}\vec{u}(t)+D(t)\vec{u}(t), \quad (8)$$

or:

$$\vec{P}_{opt}(t)=\left[D(t)-C(t)\frac{B(t)}{A(t)}\right]\vec{u}(t). \quad (9)$$

We shall assume that the power control of the subsystems is stable if the power values of the subsystems lie within:

$$\overrightarrow{P}_{i\,opt}(t)-\varepsilon_i\le\vec{P}_{i\,opt}(t)\le\overrightarrow{P}_{i\,opt}(t)+\varepsilon_i. \quad (10)$$

The error ε_i term defines the permissible deviation of subsystem states from their optimal values and accounts for model uncertainty as well as the influence of uncontrolled disturbances. Let us illustrate this in Fig. 1.

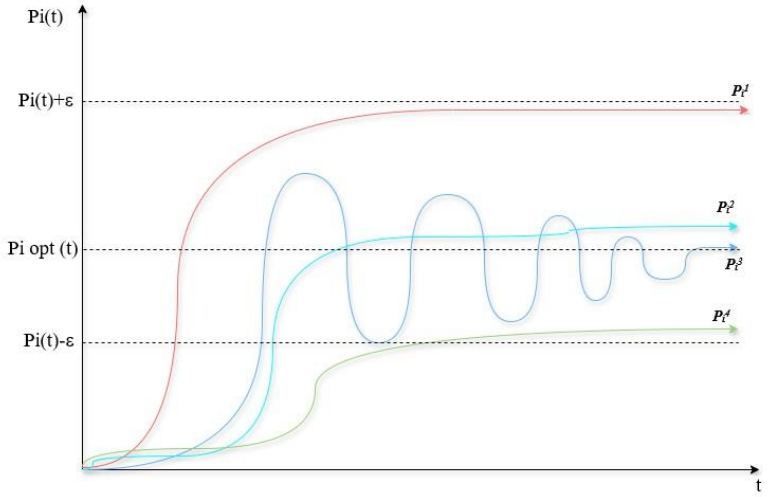

Fig. 1. **An example of stable power control *i*– th subsystems $P_i(t)$; P_i^1 – control at the upper limit; P_i^4– control at the lower limit; P_i^2, P_i^3 – optimal management (Time axis is given in normalised time units)**

Source: **compiled by the authors**

From the inequality given in (10), the following can be written:

$$\vec{P}_{opt}{}^{+} - \vec{P}_{opt} = \vec{E}\ , \qquad (11)$$

$$\vec{P}_{opt} - \vec{P}^{-}{}_{opt} = \vec{E}\ . \qquad (12)$$

Then, subtracting expression (12) from expression (11), we obtain:

$$\vec{P}^{+}{}_{opt} - \vec{P}^{-}{}_{opt} = 2\vec{E}\ , \qquad (13)$$

where $\overrightarrow{P^{+}{}_{opt}} = (P_{1opt} + \varepsilon_1, P_{2opt} + \varepsilon_2, ..., P_{nopt} + \varepsilon_n)$ is the vector of the upper power limit of the subsystems; $\vec{P}_{iopt}(t)$ is optimal power *i*-th subsystems; $\vec{E}$ – subsystem power deviation vector; $\vec{E} = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_n),\ i = \overline{1,n};$ $\overrightarrow{P^{-}{}_{opt}} = \left(P_{1opt} - \varepsilon_1, P_{2opt} - \varepsilon_2, ..., P_{nopt} - \varepsilon_n\right)$ is lower power limit vector *i*-th subsystems; ε_i is power deviation vector *i*-th subsystems, $i = \overline{1,n};$. The two optimal control values correspond to the upper and lower stability bounds and are defined as those that minimise deviations within the corresponding range. The parameter *t* is considered as a fixed time instant of analysis; time optimality is not introduced, but rather corresponds to the selected system operation scenario. From expression (9) for a fixed value of $t_{opt} = \tau$ we have:

$$\vec{P}opt^{+}(\tau) = \left[D^{+}(\tau) - C^{+}(\tau)\frac{B^{+}(\tau)}{A^{+}(\tau)}\right]\vec{u}(\tau), \quad (14)$$

and

$$\vec{P}opt^{-}(\tau) = \left[D^{-}(\tau) - C^{-}(\tau)\frac{B^{-}(\tau)}{A^{-}(\tau)}\right]\vec{u}(\tau). \quad (15)$$

Substituting mathematical expression (14) into (13), we obtain:

$$\left[D^{+}(\tau) - C^{+}(\tau)\frac{B^{+}(\tau)}{A^{+}(\tau)}\right]\vec{u}(\tau) - \left[D^{-}(\tau) - C^{-}(\tau)\frac{B^{-}(\tau)}{A^{-}(\tau)}\right] \cdot$$

$$\cdot\vec{u}(\tau) = 2\vec{E}$$

After the transformations, we have:

$$\left[D(\tau) - \Delta F(\tau)\right]\vec{u}(\tau) = 2\vec{E}\ , \qquad (16)$$

where $\Delta D(\tau) = D^{+}(\tau) - D^{-}(\tau)$ is matrix of permissible ranges of variation in the values of crisis management interventions; $D^{+}(\tau)$ is matrix of values for crisis management decisions at the upper limit of power control stability for subsystems; $D^{-}(\tau)$ is matrix of values for global control decisions at the lower limit of subsystem power control stability; $\vec{E}$ is power deviation vector of subsystems;

$$\Delta F(\tau) = C^{+}(\tau)\frac{B^{+}(\tau)}{A^{+}(\tau)}\vec{u}(\tau) - C^{-}(\tau)\frac{B^{-}(\tau)}{A^{-}(\tau)}\vec{u}(\tau)$$

is matrix of necessary changes affecting the performance of subsystems; $C^{+}(\tau)$ and $C^{-}(\tau)$ are matrices of performance and interaction metrics for subsystems at the upper and lower limits of control stability, respectively; $B^{+}(\tau)$ and $B^{-}(\tau)$ are local control matrices at the upper and lower control stability limits, respectively; $A^{+}(\tau)$ and $A^{-}(\tau)$ are impact matrices for the upper and lower limits of stability in interaction management, respectively.

A control collapse occurs when the stability condition defined in equation (10) is violated, i.e. when the subsystem power values leave the admissible interval.

Then, taking into account equation (16) for the CSC, we can write the following expression:

$$\left|CSC(\tau)\right| = \frac{\left|\Delta D(\tau) - \Delta F(\tau)\right|}{2\left|E\right|}, \qquad (17)$$

if $\left|CSC(\tau)\right| \le 1$, then the process is stable; if $\left|CSC(\tau)\right| > 1$, then the process is unstable.

Let the upper and lower stability limits of the control system be influenced by changes in the intensity of the input to the subsystems ω_{ji}. In that case, given that: $A(\tau) = W(\tau)\vec{\varphi}(t) - \vec{\delta}(t)$, for $\Delta F(\tau)$ we can write the following expression:

$$\Delta F(\tau) = C(\tau)\frac{B(\tau)}{A^{+}(\tau)} - C(\tau)\frac{B(\tau)}{A^{-}(\tau)} =$$

$$C(\tau)\frac{B(\tau)}{W^{+}(\tau)\vec{\varphi}(t) - \vec{\delta}(t)} - C(\tau)\frac{B(\tau)}{W^{-}(\tau)\vec{\varphi}(t) - \vec{\delta}(t)} =$$

$$C(\tau)B(\tau)\left[\frac{W^{-}(\tau)\vec{\varphi}(t) - \vec{\delta}(t) - W^{+}(\tau)\vec{\varphi}(t) + \vec{\delta}(t)}{\left[W^{+}(\tau)\vec{\varphi}(t) - \vec{\delta}(t)\right]\cdot\left[W^{-}(\tau)\vec{\varphi}(t) - \vec{\delta}(t)\right]}\right] = \qquad (18)$$

$$C(\tau)B(\tau)\left[\frac{W^{-}(\tau)\vec{\varphi}(t) - W^{|+}(\tau)\vec{\varphi}(t)}{A^{+}(\tau)A^{-}(\tau)}\right] =$$

$$C(\tau)B(\tau)\frac{\Delta W(\tau)}{A^{+}(\tau)A^{-}(\tau)}\vec{\varphi}(t)$$

So we have the following expression:

$$\Delta F(\tau) = C(\tau)B(\tau)\vec{\varphi}(t)\frac{\Delta W(\tau)}{A^{+}(\tau)A^{-}(\tau)}, \qquad (19)$$

In this paper, controllability is interpreted in an applied systemic sense as the ability of the MIS to maintain coordinated functioning under disturbances, rather than in the narrow classical Kalman sense. From the perspective of control theory, a system is considered controllable if there exist control inputs that ensure the subsystem states remain within an admissible region. In the proposed model, this is formalised through the CSC (t): when its value remains within the admissible threshold $CSC(t) \le CSC(t)_{crit}$, the system operates in a controllable state, whereas exceeding this threshold corresponds to a loss of controllability.

Accordingly, for the CSC, which depends on the intensity of the impact on the subsystems, we have the following expression:

$$CSC(t) = \frac{1}{2E}\left[\Delta D - \Delta F\right] = \frac{1}{2E}\left[\Delta D - CB\vec{\varphi}(t)\frac{\Delta W}{A^{+}A^{-}}\right], \qquad (20)$$

$$CSC(t) = \frac{\left|\Delta P(t)\right|W}{\left|\Delta P(t)\right|W_{w}^{max}}, \qquad (21)$$

where $\Delta P(t) = P(t) - P_{opt}(t)$ is the vector of deviations of the subsystem's power levels from their optimal values; $\left|\cdot\right|W$ is weighted average with a weight matrix W; $\left|\Delta P\right|_{W}^{max}$ is the maximum permissible value of this standard. It should be noted that the integral nature of the CSC may lead to smoothing of local critical failures of individual subsystems. Therefore, for practical applications, it is advisable to complement the coefficient with a local control mechanism, in which reaching a critical threshold by at least one subsystem triggers an emergency mode, regardless of the integral value of the coefficient.

Within the proposed model, the CSC (t): is defined as an integral function of the current state vector of the functional subsystems, the parameters of their inter-system interaction, and the control inputs. The physical meaning of the system controllability coefficient lies in the quantitative representation of the system's ability to maintain the permissible power values of the functional subsystems over time in the presence of external and internal disturbances.

Fig. 2 shows a flowchart of the proposed model, illustrating the sequence of steps from the initial data of the information environment to the formulation of adaptive management decisions based on the integral coefficient of system controllability.

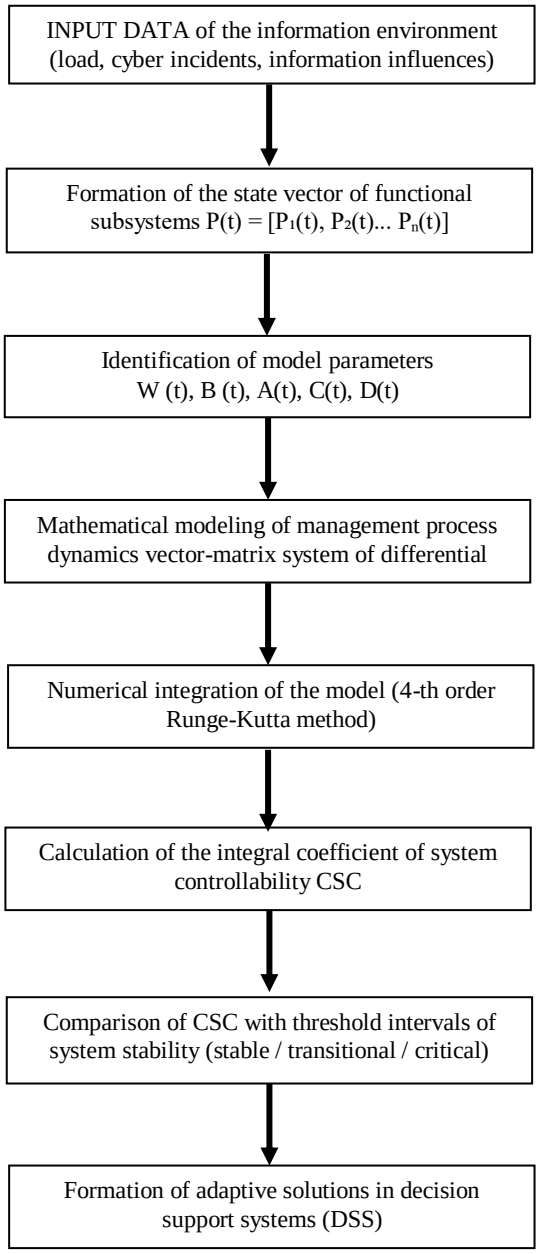

Fig. 2. **Algorithmic flowchart for implementing a mathematical model for assessing the controllability of information management system**
Source: **compiled by the authors**

This value CSC (t): aggregates information on the degree of coordination between subsystems and can be used as a generalized indicator of the overall controllability of the management information system. In terms of dynamical systems theory, the value of the (CSC) can be interpreted as an indicator of the stability of the system's steady-state operation.

Remaining CSC (t): within the permissible range corresponds to the existence of a quasi-stable regime with limited deviations in states, whereas the indicator exceeding the set limits indicates a loss of stability and a transition to a crisis or collapse regime. Thus, the CSC serves as a generalised controllability criterion, similar in meaning to Lyapunov-type stability functionals [32], as confirmed by modern approaches to the stabilization of multi-domain systems. Unlike classical abstract models, this criterion is geared towards applied problems of managing complex information systems and critical infrastructure objects, where stability is determined not only by technical parameters but also by the integrity of cognitive and information subsystems. Unlike classical stability margin indicators, which characterise the distance of a system from the stability boundary in the phase or frequency domain, the proposed CSC reflects the integral ability of the system to maintain admissible subsystem states under multifactor disturbances, including cognitive and informational influences.

Thus, the coefficient does not represent a static stability margin but acts as a dynamic functional that accounts for inter-subsystem interactions, degradation processes and control actions. The model parameters are determined based on a combination of expert assessments and normalised characteristics of subsystem operation. Such an approach is typical for complex socio-technical systems, where direct measurement of parameters is limited.

To verify the proposed mathematical model and assess the sensitivity of the integral coefficient of system controllability to dynamic disturbances, simulation modelling was carried out for a system comprising: n=5 subsystems (infrastructure, network – communications, application, analytical – cognitive, and user).

The modelling was carried out by numerically integrating the system of differential equations (1)–(5) using the 4th-order Runge–Kutta (RK4) method. The choice of the fourth-order Runge–Kutta method is justified by its computational simplicity and sufficient accuracy for analysing the overall system dynamics. However, for stiff systems, the use of adaptive numerical methods is more appropriate, which is planned for future research. The time variable t is represented in normalised (dimensionless) units corresponding to the numerical integration step, which ensures generality of the model and independence from specific physical time scales.

The results of the modelling of three baseline scenarios – stable operation, destabilizing influence

(cyberattacks) and adaptive compensation – are presented in Fig. 3 and detailed in Table 4 and Table 5. To clarify the role of cognitive influence, an additional hypothetical scenario is considered in which the cognitive parameter $\varphi(t)$ – increases while the level of technical disturbances remains fixed. In this case, the evolution of the CSC exhibits a smoother but persistent trend, reflecting the degradation of inter-subsystem coordination, in contrast to the rapid increase of the coefficient under purely technical attacks. Thus, while a technical attack manifests as an additive disturbance affecting subsystem states, the cognitive influence $\varphi(t)$ has a systemic character and leads to a reduction in coordination efficiency, which is reflected in a gradual increase of the CSC even in the absence of critical technical damage.

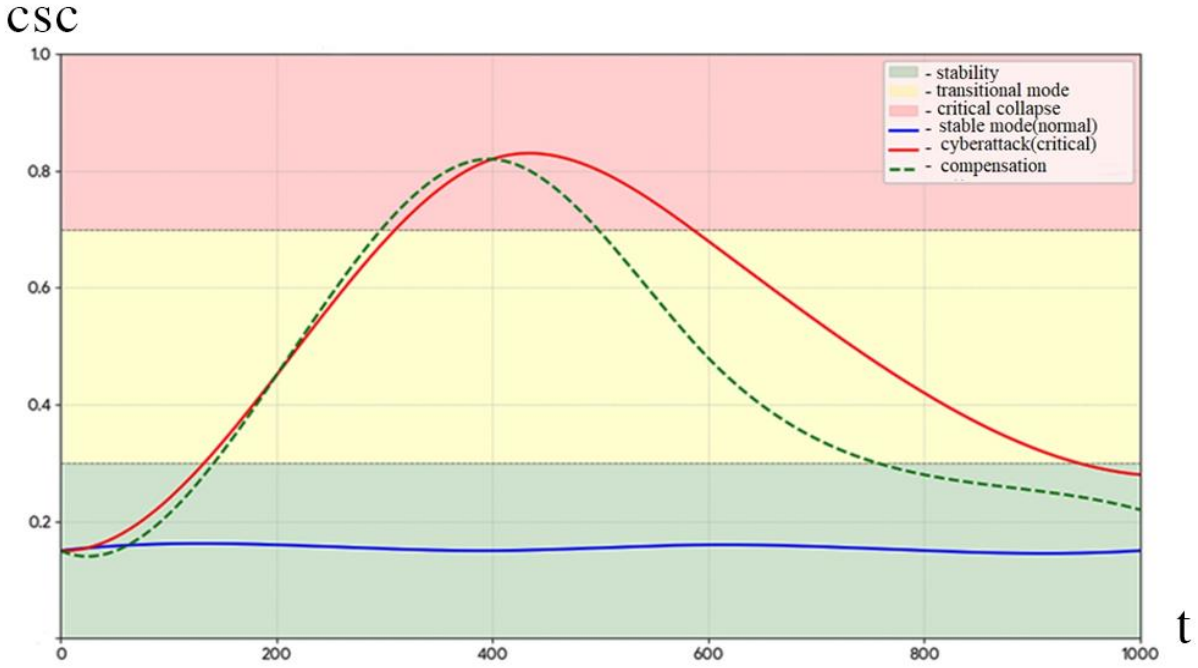

Fig. 3. **Dynamics of the integral coefficient of system controllability (CSC) under scenario-based loading. (Time axis is given in normalised time units)**

Source: **compiled by the authors**

Table 4. **Comparative impact of technical and cognitive factors on the system controllability coefficient**

Type of influence	CSC variation pattern	Underlying cause
Technical attack	Rapid increase	Subsystem degradation
Cognitive influence	Gradual increase	Disruption of coordination
Combined impact	Accelerated increase	Synergistic effect

Source: **compiled by the authors**

Table 5. **Verification data on the dynamics of the CSC based on the results of RK4 integration**

Time (t), (units)	CSC (Stable)	CSC (Attack)	CSC (Restoration)	System status
0	0.15	0.15	0.15	Stable
200	0.16	0.45	0.45	Onset of destabilization
400	0.15	0.82	0.82	Extreme / collapse regime
600	0.16	0.68	0.48	Adaptive response u(t)
1000	0.15	0.28	0.22	Restoring control

Source: **compiled by the authors**

An analysis of the curves shown in Fig. 3 confirms the model's performance, namely:

– in steady-state operation, the CSC index remains within the range [0.15, 0.16], which corresponds to optimal performance;

– when simulating an attack, a non-linear increase in the CSC to a value of 0.82 is observed, indicating a transition into the critical collapse zone;

– the implementation of compensatory control u(t) enables the CSC to be reduced to 0.22, demonstrating the effectiveness of the proposed decision support system (DSS) algorithms for restoring the system's viability.The updated mathematical model provides a comprehensive coverage of inter-system interactions through the integration of differential equations, a matrix structure of weighting coefficients, and a cognitive component of the propagation of informational influences. The proposed model describes a complex network of inter-system interaction and formalizes its impact through matrices of subsystem interaction, which identify positive synergy effects and the opponent's vulnerabilities. Such a model has the potential to serve as a basis for forecasting the results of subsystem activity, modelling informational and psychological pressure, and formulating strategic decisions in real time. In applied terms, this includes modelling directed psychological influence on target audiences in digital environments using modern information technologies [34]. A key feature of implementing the strategy for functional subsystems in the current environment is the deep integration of information resources with the civilian information infrastructure, and the influence exerted on public opinion. Through the systematic conduct of information operations (attacks), chaos and instability within the information subsystem create an information environment in which the state's traditional defense mechanisms lose their effectiveness. In such conditions, Ukraine and its international partners must develop joint and new, adaptive strategies based on a systematic analysis of dynamics and the construction of counter-scenarios to respond to contemporary challenges and threats.

The results of the study have made it possible to address key scientific challenges and develop a comprehensive methodology for assessing the stability of information and control systems in complex adaptive environments, for which a mathematical framework in the form of a system of vector-matrix differential equations has been devised. Mathematical modelling of the cognitive factor through the introduction of a cognitive penetration vector enabled the synthesis of an integral (CSC) as a scalar functional for the quantitative assessment of the system's control capability.

A scale for interpreting the CSC and its threshold values has been developed, which enables the classification of operating modes from stable to critical, whilst the model's performance and predictive properties have been confirmed through numerical verification of destabilization and adaptive recovery scenarios. The results obtained have been algorithmized into analytical modules of (DSS), creating an applied basis for the predictive monitoring of critical infrastructure objects in real time. It should be noted that the presented results are based on numerical simulation and do not rely on direct measurements of parameters from real technical systems under attack conditions. The historical cases of 2014 and 2022 are used for scenario validation rather than as sources of precise numerical model parameters.

LIMITATIONS OF THE STUDY

Despite the robustness of the proposed mathematical model, several limitations should be acknowledged.

Firstly, the model relies on normalized and partially expert-defined parameters, which may limit the direct transferability of results to specific real-world systems without additional calibration.

Secondly, the numerical verification is based on scenario simulation rather than empirical datasets from operational information systems, which constrains the statistical validation of the model.

Thirdly, the integral nature of the CSC may lead to smoothing of localized subsystem failures, requiring complementary local monitoring mechanisms for high-resolution diagnostics.

Finally, the representation of cognitive penetration as a generalized disturbance vector, while analytically justified, remains an abstraction that requires further empirical grounding and refinement. These limitations define directions for future research and do not reduce the conceptual validity of the proposed approach.

CONCLUSIONS

This study addresses the scientific challenge of developing an integrated mathematical model for assessing the controllability of information management systems in complex adaptive environments. A formalisation of such systems as five interacting functional subsystems (infrastructural, network-communication,

application, analytical-cognitive and user) is proposed, described by a vector of their capacity and a system of vector-matrix differential equations, taking into account inter-system reactivity, cognitive penetration, managerial influences and degradation processes.

The main result is the introduction and scientific justification of the (CSC) as an integral indicator of the controllability of information management systems, reflecting, in particular, the digital component of state controllability. For the CSC, the operating conditions of the MIS in stable, adaptive, crisis, pre-collapse and boundary modes have been substantiated, allowing the dynamics of transitions between them to be quantitatively identified. The proposed interpretative scale is supplemented by links to the entropy of the cognitive field, the probability of desynchronization of subsystems, and the relative power of their functioning.

The proposed system controllability coefficient occupies an intermediate position between classical control theory criteria (such as Lyapunov stability criteria, stability margins, and Kalman controllability) and system reliability and survivability indicators. Unlike these approaches, the system controllability coefficient integrates dynamic, structural and cognitive aspects of the functioning of complex socio-technical systems, which allows it to be used as a generalised indicator of controllability in real time. Similarly, in the proposed model, cognitive penetration is not reduced to a classical disturbance but acts as a factor that modifies both the system state and the structure of interactions between subsystems.

The operational capability and sensitivity of the CSC to destabilizing influences have been confirmed through numerical verification of the proposed model using the 4th-order Runge–Kutta method in scenarios involving stable operation, cyberattacks and adaptive recovery. The results demonstrate that the CSC is an informative indicator that integrates organizational, informational, cognitive and technical aspects of the MIS operation and allows for the quantitative tracking of phase transitions between stable and collapse states.

The practical significance of this work lies in the possibility of integrating the CSC into the analytical modules of decision support systems and systems for monitoring critical information infrastructure, thereby laying the groundwork for predictive analysis, condition diagnostics and the timely application of adaptive management interventions. The proposed approach can be extended to interdisciplinary tasks, particularly in the context of assessing state governability under complex hybrid influences, where critical infrastructure management systems serve as the digital foundation for the relevant processes.

Further development of the research is focused on the parameterization of the inter-system reactivity matrix, refining cognitive penetration models, identifying weighting coefficients through expert assessment, and extending the model using agent-oriented methods and dynamic games to simulate the adaptive behavior of destabilizing factors in real time.

REFERENCES

1. Nicolazzo, S., Nocera, A. & Pedrycz, W. “Service Level Agreement (SLA) and Security SLA (SecSLA): A comprehensive survey”. *Journal of Network and Systems Management*. 2026; 34 (3): 10041, https://www.scopus.com/results/results.uri?src=s&st1=10.1007%2Fs10922-026-10041-w.
DOI: https://doi.org/10.1007/s10922-026-10041-w.

2. Yang, Z., Barroca, B., Laffréchine, K., Weppe, A., Bony-Dandrieux, A. & Daclin, N. “A multi-criteria framework for critical infrastructure systems resilience”. *International Journal of Critical Infrastructure Protection*. 2023; 42: 100616, https://www.scopus.com/results/results.uri?src=s&st1=10.1016%2Fj.ijcip.2023.100616. DOI: https://doi.org/10.1016/j.ijcip.2023.100616.

3. Khadidos, A. O., Khadidos, A. O., Selvarajan, S., Al-Shehari, T., Alsadhan, N. A. & Singh, S. “CyberSentry: Enhancing SCADA security through advanced deep learning and optimization strategies”. *International Journal of Critical Infrastructure Protection*. 2025; 50: 100782, https://www.scopus.com/results/results.uri?src=s&st1=10.1016%2Fj.ijcip.2025.100782.
DOI: https://doi.org/10.1016/j.ijcip.2025.100782.

4. Bellini, E., D'Aniello, G., Flammini, F. & Gaeta, R. “Situation awareness for cyber resilience: A review”. *International Journal of Critical Infrastructure Protection*, 2025; 49: 100755, https://www.scopus.com/results/results.uri?src=s&st1=10.1016%2Fj.ijcip.2025.100755.
DOI: https://doi.org/10.1016/j.ijcip.2025.100755.

5. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F. & Yevseiev, S. “Mathematical model of multi-domain interaction based on game theory”. *Advanced Information Systems,* 2025; 9 (3): 22–31, https://www.scopus.com/sourceid/21101186339. DOI: https://doi.org/10.20998/2522-9052.2025.3.03.

6. Pasandideh, S., Pereira, P., & Gomes, L. “Cyber-physical-social systems: Taxonomy, challenges, and opportunities”. *IEEE Access.* 2022; 10: 38552–38573, https://www.scopus.com/results/results.uri?src=s&st1=10.1109%2FACCESS.2022.3167441. DOI: https://doi.org/10.1109/ACCESS.2022.3167441.

7. Yilma, B. A., Panetto, H. & Naudet, Y. “Systemic formalisation of cyber-physical-social system (CPSS): A systematic literature review”. *Computers in Industry,* 2021; 129: 103458, https://www.scopus.com/results/results.uri?src=s&st1=10.1016%2Fj.compind.2021.103458. DOI: https://doi.org/10.1016/j.compind.2021.103458.

8. Zhou, T. “On the controllability and observability of networked dynamic systems”. *Automatica.* 2015; 52: 63–75, https://www.scopus.com/results/results.uri?src=s&st1=10.1016%2Fj.automatica.2014.10.121. DOI: https://doi.org/10.1016/j.automatica.2014.10.121.

9. Leitold, D., Vathy-Fogarassy, Á. & Abonyi, J. “Controllability and observability in complex networks: The effect of connection types”. *Scientific Reports,* 2017; 7: 151, https://www.scopus.com/results/results.uri?src=s&st1=10.1038%2Fs41598-017-00160-5. DOI: https://doi.org/10.1038/s41598-017-00160-5.

10. Coccia, M. “Theory of subsystems driving technological coevolution in modular architecture of complex innovations”. *Technologies.* 2026; 14 (3): 156, https://www.scopus.com/results/ results.uri?src=s&st1=10.3390%2Ftechnologies14030156. DOI: https://doi.org/10.3390/technologies14030156.

11. Kapur, K. C. “Mathematical models for system reliability”. *Journal of Quality Technology*. 2009; 41 (2): 214, https://www.scopus.com/results/results.uri?src=s&st1=10.1080%2F00224065.2009.11917775. DOI: https://doi.org/10.1080/00224065.2009.11917775.

12. Al-Ammouri, A., Lebid, I., Dekhtiar, M., Lebid, I. & Al-Ammori, H. “Development of a mathematical model of reliable structures of information-control systems”. *Eastern-European Journal of Enterprise Technologies.* 2022; 5 (9 (119)): 68–78, https://www.scopus.com/sourceid/21100450083. DOI: https://doi.org/10.15587/1729-4061.2022.265953.

13. Alburaikan, A., Khalifa, H. A. E. W., Kumar, P., Mirjalili, S. & Mekawy, I. “Mathematical modeling and evaluation of reliability parameters based on survival possibilities under uncertain environment”. *Computer Modeling in Engineering and Sciences*. 2022; 134 (3): 1943–1956, https://www.scopus.com/results/results.uri?src=s&st1=10.32604%2Fcmes.2022.021815. DOI: https://doi.org/10.32604/cmes.2022.021815.

14. Järveläinen, J., Dang, D., Mekkanen, M. & Vartiainen, T. “Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: A dynamic capabilities approach”. *Journal of Decision Systems,* 2025; 34 (1): 2479546, https://www.scopus.com/results/results.uri?src=s&st1=10.1080%2F12460125.2025.2479546. DOI: https://doi.org/10.1080/12460125.2025.2479546.

15. Rathnayaka, B., Adikariwattage, V., Siriwardana, Ch. “A unified framework for evaluating the resilience of critical infrastructure: Delphi survey approach”. *International Journal of Disaster Risk Reduction.* 2024; 110: 104598, https://www.scopus.com/results/results.uri? src=s&st1=10.1016%2Fj.ijdrr.2024.104598. DOI: https://doi.org/10.1016/j.ijdrr.2024.104598.

16. Rathnayaka, B., Robert, D., Adikariwattage, V., Siriwardana, C., Kuligowski, E., Setunge, S., & Amaratunga, D. “Novel methodology for resilience assessment of critical infrastructure considering the interdependencies: A case study in water, transportation and electricity sector”. *International Journal of Disaster Risk Reduction,* 2025; 119: 105271, https://www.scopus.com/ results/ results.uri?src=s&st1=10.1016%2Fj.ijdrr.2024.105271. DOI: https://doi.org/10.1016/j.ijdrr.2025.105271.

17. Dodonov, O. H., Kuznietsova, M. H., & Horbachyk, O. S. “Information systems of critical infrastructure under modern threats: supporting functional resilience”. *Reiestratsiia, zberihannia i obrobka danykh.* 2026; 28 (1). DOI: https://doi.org/10.35681/1560-9189.2026.28.1.358608.

18. Liu, W., Shan, M., Zhang, S. & Zhai, Z. “Resilience in infrastructure systems: A comprehensive review”. *Buildings.* 2022; 12 (6): 759, https://www.scopus.com/results/ results.uri?src=s&st1=10.3390%2Fbuildings12060759, DOI: https://doi.org/10.3390/buildings12060759.

19. Uzun, I. & Lobachev, M. “Decision Passport for Streaming Decision Support with Multimodal Time Series”. *Collection of Scientific Papers with the Proceedings of the 3rd International Scientific and Practical Conference “Scientific Progress: Theories, Applications and Global Impact”.* Braga, Portugal. 2026. p. 132–134. DOI: https://doi.org/10.70286/EOSS-02.03.2026.002.132-134.

20. Chotia, V., Khoualdi, K., Broccardo, L. & Yaqub, M. Z. “The role of cyber security and digital transformation in gaining competitive advantage through strategic management accounting”. *Technology in Society.* 2025; 81: 102851, https://www.scopus.com/results/results.uri?src=s&st1=10.1016%2Fj.techsoc.2025.102851. DOI: https://doi.org/10.1016/j.techsoc.2025.102851.

21. Oesch, S., Hutchins, J., Austria, P. & Chaulagain, A. “Agentic AI and the cyber arms race”. *Computer.* 2025; 58 (5): 82–85, https://www.scopus.com/results/results.uri? src=s&st1=10.1109%2FMC.2025.3544116. DOI: https://doi.org/10.48550/arXiv.2503.04760.

22. Megaheed, A. A. E., Kamel, N. M., Hanafy, I. M. & Omar, N. A. “A numerical solution for nash differential games based on the Runge Kutta 4th-order method”. *European Journal of Pure and Applied Mathematics.* 2025; 18 (4): 6007. DOI: https://doi.org/10.29020/nybg.ejpam.v18i4.6007.

23. Adenuga, O. T., Mpofu, K. & Adeyeri, M. K. “Agent-based control system: A review and platform for reconfigurable bending press machine”. *Procedia Manufacturing,* 2019; 35: 50–55, https://www.scopus.com/results/results.uri?src=s&st1=10.1016%2Fj.promfg.2019.05.007
DOI: https://doi.org/10.1016/j.promfg.2019.05.007.

24. Tundis, A. & Ramírez-Agudelo, O. H. “Safeguarding critical infrastructures with digital twins and AI”. *23rd International Conference on Modeling & Applied Simulation.* 2024. DOI: https://doi.org/10.46354/i3m.2024.mas.010.

25. Fonseca, L. L., Böttcher, L., Mehrad, B. & Laubenbacher, R. C. “Optimal control of agent-based models via surrogate modeling”. *PLoS Computational Biology,* 2025; 21 (1), e1012138. https://www.scopus.com/results/results.uri?src=s&st1=10.1371%2Fjournal.pcbi.1012138,
DOI: https://doi.org/10.1371/journal.pcbi.1012138.

26. Balatska, V., Tkachuk, R., Ivanusa, A., Yashchuk, V. & Maslova, N. “Integration of blockchain technologies into complex information protection systems to improve the security of state registers”. *Visnyk Lvivskoho Derzhavnoho Universytetu Bezpeky Zhyttiediialnosti.* 2025; 32: 90–99. DOI: https://doi.org/10.32447/20784643.32.2025.07.

27. Saridas, G. “Effective use of Boolean operators in academic research: A practical guide to database search strategies”. *International Society that Learn Journal.* 2025; 2 (2): 329–345. DOI: https://doi.org/10.64782/istlj.2253329-345.

28. Kyzym, M. O., Yudenko, Y. V. & Yaholnytskyi, O. “The resilience of the economies of Ukraine and the world and the assessment of their vulnerability and ability to recover after crises and shocks”, *Business Inform.* 2025; 6 (568): 77–89. DOI: https://doi.org/10.32983/2222-4459-2025-6-77-89.

29. Hrechaninov, V. “ Models and technologies of intelligent protection of information systems of critical infrastructure for enhancing resilience”. *Cybersecurity: Education, Science, Technique.* 2025; 1 (29): 877–896. DOI: https://doi.org/10.28925/2663-4023.2025.29.948.

30. Dzhalladova, I. A.-K. & Kaminskyi, O. Ye. “Socio-psychological stability of cyber security systems”. *Modern Information Technologies in the Sphere of Security and Defence*. 2025; 53 (2): 43–50. DOI: https://doi.org/10.33099/2311-7249/2025-53-2-43-50.

31. Volchenkov, D. “Mathematical frameworks for network dynamics: A six-pillar survey for analysis, control, and inference”. *Mathematics.* 2025; 13 (13): 2116. DOI: https://doi.org/10.3390/math13132116.

32. Karas Kutlucan, N., Ucun, L. & Dasdemir, J. “Event-triggered secure control design against false data injection attacks via Lyapunov-based neural networks”. *Sensors,* 2025; 25 (12): 3634. DOI: https://doi.org/10.3390/s25123634.

33. Herasymov, S., Tkachov, A. & Bazarnyi, S. “Complex method of determining the location of social network agents in the interests of information operations”. *Advanced Information Systems.* 2024; 8 (1): 31–36, https://www.scopus.com/sourceid/21101186339. DOI: https://doi.org/10.20998/2522-9052.2024.1.04.

34. Yevseiev, S., Milevskyi, S., Pribyliev, Y., Melenti, Y., Nalivayko, A., Bazarnyi, S., Morozov, O., Kazak, I., Hrebeniuk, A. & Ivashchenko, O. “Development of a method of psychological impact on target audiences of gamers using modern information technologies”. *Eastern-European Journal of Enterprise*

Technologies. 2025; 3 (9 (135)): 55–64, https://www.scopus.com/sourceid/21100450083. DOI: https://doi.org/10.15587/1729-4061.2025.332271.

Conflicts of Interest: The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship, or other, which could influence the research and its results presented in this article

Received 08.04.2026
Received after revision 11.06.2026
Accepted 17.06.2026

DOI: https://doi.org/10.15276/hait.09.2026.25
УДК 519.87:004.942:517.977

Математична модель оцінювання керованості інформаційних систем управління у складних адаптивних середовищах

Базарний Сергій Васильович[1)]
ORCID: https://orcid.org/0000-0001-9545-1960; serhii.bazarnyi@edu.nuou.org.ua. Scopus Author ID: 58905874600
Мурр П'єр [2)]
ORCID: https://orcid.org/0009-0007-4094-0223; pierre.murr@iuk.edu.kw. Scopus Author ID: 26025143400
Войтко Олександр Володимирович[1)]
ORCID: https://orcid.org/0000-0002-4610-4476; o.voitko@edu.nuou.org.ua. Scopus Author ID: 57210362201
Гусак Юрій Аркадійович[1)]
ORCID: https://orcid.org/0000-0002-3423-2112; y.husak1512@gmail.com. Scopus Author ID: 60033365500
Євсеєв Сергій Петрович[3)]
ORCID: https://orcid.org/0000-0003-1647-6444; serhii.yevseiev@khpi.edu.ua. Scopus Author ID: 57190440690
[1)] Національний університет оборони України, проспект Повітряних Сил, 28. Київ, 03049, Україна
[2)] Міжнародний університет науки і технологій у Кувейті, Урядовий район Ардія, вул. Мохамада бін Касіма. Ардія, Кувейт
[3)] Національний технічний університет "Харківський політехнічний інститут", вул. Кирпичова, 2. Харків, 61000, Україна

АНОТАЦІЯ

Сучасні інформаційні системи управління функціонують у складних адаптивних середовищах, що характеризуються високою динамічністю, невизначеністю та безперервними гібридними збуреннями, які суттєво ускладнюють забезпечення узгодженого управління. За таких умов традиційні підходи, орієнтовані на надійність і продуктивність окремих компонентів, є недостатніми, оскільки не враховують системну взаємодію підсистем і ризик втрати загальної керованості. Це зумовлює необхідність розроблення математичних підходів до кількісного оцінювання керованості систем як ключової властивості стійкості об'єктів критичної інформаційної інфраструктури. **Метою дослідження є** розроблення математичної моделі оцінювання керованості інформаційних систем управління, що функціонують у складних адаптивних середовищах, з урахуванням взаємодії функціональних підсистем, зовнішніх і внутрішніх збурень, а також керувальних впливів, які визначають динаміку системи. **Методологія:** У дослідженні використано векторно-матричний підхід до динамічного моделювання, у межах якого інформаційна система управління представлена як сукупність взаємодіючих функціональних підсистем, описаних у просторі станів системою диференціальних рівнянь. Модель враховує міжпідсистемну взаємодію, процеси деградації, зовнішні збурення та керувальні впливи, а також вплив когнітивних факторів на поведінку системи. Чисельну верифікацію запропонованої моделі здійснено із застосуванням методу Рунге–Кутти четвертого порядку в межах сценарного аналізу. Інформаційну систему управління формалізовано як сукупність п'яти взаємодіючих функціональних підсистем: інфраструктурної, мережево-комунікаційної, прикладної, аналітико-когнітивної та користувацької. Введено інтегральний коефіцієнт системної керованості як скалярний функціонал від станів підсистем, параметрів їх взаємодії та керувальних впливів. Показано, що значення цього коефіцієнта дає змогу кількісно ідентифікувати переходи між стабільним, адаптивним, кризовим і передколапсним режимами функціонування. Розроблено шкалу інтерпретації, яка пов'язує значення коефіцієнта з рівнем узгодженості підсистем та ймовірністю десинхронізації управління. Результати чисельного моделювання підтверджують чутливість запропонованого індикатора до дестабілізуючих впливів і його здатність відображати ефективність компенсувальних керувальних дій. Запропонований підхід розширює існуючі методи оцінювання стійкості та надійності систем шляхом введення динамічного інтегрального показника, що враховує сукупний вплив структурних взаємодій, керувальних впливів і когнітивних факторів на поведінку системи. Наукова новизна полягає у формалізації керованості системи як кількісної функціональної характеристики, що відображає здатність складної системи підтримувати узгоджене функціонування в умовах дестабілізуючих впливів. **Практичне значення:** Розроблена модель є практичним інструментом для застосування в системах моніторингу реального часу та платформах підтримки прийняття

рішень у сфері критичної інформаційної інфраструктури, забезпечуючи раннє виявлення втрати керованості та підтримку формування адаптивних стратегій реагування.

Ключові слова: інформаційні системи; керованість системою; адаптивні системи; критична інфраструктура; підтримка рішень; державна безпека; математичне моделювання

ABOUT THE AUTHORS

Serhii V. Bazarnyi - PhD, deputy head of Research department for the study of issues related to the development and implementation of strategic communications of Institute of Strategic Communications. National Defence University of Ukraine, Air Force Ave. 28. Kyiv, 03049, Ukraine
ORCID: https://orcid.org/ 0000-0001-9545-1960; serhii.bazarnyi@edu.nuou.org.ua. Scopus Author ID: 58905874600
***Researchfield*:** dynamical systems, information technology, strategic communications, information warfare

Базарний Сергій Васильович - доктор філософії, заступник начальника Науково-дослідного відділу дослідження проблем розвитку та впровадження стратегічних комунікацій Інституту стратегічних комунікацій. Національний університет оборони України, пр. Повітряних Сил, 28. Київ, 03049, Україна

Pierre Murr - PhD, Assistant professor, Computer Engineering Department, International University of Science and Technology in Kuwait, Ardiya Government Area Mohamad Bin Qasim Street. Ardiya, Kuwait
ORCID: https://orcid.org/0009-0007-4094-0223; murrpierre@gmail.com. Scopus Author ID: 26025143400
Research field: information technology, cyber security

Мурр П'єр - доктор філософії, доцент кафедри Комп'ютерної інженерії. Міжнародний університет науки і технологій у Кувейті. Урядовий район Ардія, вулиця Мохамада бін Касіма. Ардія, Кувейт

Oleksandr V. Voitko - Doctor of military sciences, docent, head of Institute of Strategic Communications. National Defence University of Ukraine, 28, Air Force Ave. Kyiv, 03049, Ukraine
ORCID: https://orcid.org/0000-0002-4610-4476; o.voitko@edu.nuou.org.ua. Scopus Author ID: 57210362201
Research field: strategic communications, information warfare, information systems

Войтко Олександр Володимирович - доктор військових наук, доцент, начальник Інституту стратегічних комунікацій. Національний університет оборони України, пр. Повітряних Сил, 28. Київ, 03049, Україна

Yurii A. Husak - Doctor of military sciences, professor, Department of information and analytical support at Institute of information and communication technologies and cyber defence. National Defence University of Ukraine, 28, Air Force Ave. Kyiv, 03049, Ukraine
ORCID: https://orcid.org/0000-0002-3423-2112, y.husak1512@gmail.com; Scopus Author ID: 60033365500
Research field: dynamical systems, information technology, strategic communications, information warfare

Гусак Юрій Аркадійович - доктор військових наук, професор кафедри Інформаційно-аналітичного забезпечення Інституту інформаційно-комунікаційних технологій та кібероборони. Національний університет оборони України, пр. Повітряних Сил, 28. Київ, 03049, Україна

Serhii P. Yevseiev - Doctor of Engineering sciences, professor, Head of Cybersecurity Department. National Technical University "Kharkiv Polytechnic Institute", 2, Kyrpichova Str. Kharkiv, 61000, Ukraine
ORCID: https://orcid.org/0000-0003-1647-6444; serhii.yevseiev@gmail.com. Scopus Author ID: 57190440690
Research field: cyber security, post-quantum cryptography, crypto-code constructions

Євсеєв Сергій Петрович - доктор технічних наук, професор, завідувач кафедри Кібербезпеки. Національний технічний університет "Харківський політехнічний інститут", вулиця Кирпичова, 2. Харків, 61000, Україна