Information systems modeling

UDC 519.876.5:519.83 **doi:** https://doi.org/10.20998/2522-9052.2025.3.03

Serhii Bazarnyi[1], Yurii Husak[1], Tetiana Voitko[1], Fuad Aliew[2], Serhii Yevseiev[3]

[1] National Defence University of Ukraine, Kyiv, Ukraine
[2] Vocational School, Yeditepe University, Istanbul, Turkey
[3] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

MATHEMATICAL MODEL OF MULTI-DOMAIN INTERACTION BASED ON GAME THEORY

Abstract. The article presents a formalised mathematical model of multidomain interaction in hybrid warfare, which covers the cognitive, information, cyber, psychological and physical domains. The object of the study is the nonlinear dynamics of cross-domain destabilisation, which can lead to managerial collapse due to information overload of the control system. The purpose of the study is to identify phase transitions in the management system by analysing domain synergy and coherence degradation. Within the framework of the model based on game theory, the author proposes a matrix of domain reactivity, which determines the strength of mutual influences between domains, and a system of stochastic differential equations with variable coefficients that depend on the emotional state of society, the intensity of information influence and changes in the cognitive background. Two new indicators are introduced for the first time: the coefficient of cognitive penetration and the coefficient of interdomain integration, which allow quantifying the level of cognitive coverage and the degree of synergistic interaction between domains. The introduced parameter of management capacity is used as an indicator of phase shift and system collapse. A mechanism for dynamic correction of the model based on the forecasting accuracy metric is proposed, which includes adaptation of the PID-controller and updating the weighting coefficients. An empirical analysis of the impact of information campaigns through social networks is carried out, which confirms the feasibility of using the proposed model to assess the risks of information influence and formulate scenarios for counteraction in the information space.

Keywords: multidomain interaction; information technology; social networks; cognitive space; mathematical model.

Introduction

In the modern world, socio-technical systems have acquired a fundamentally new character, turning into a multi-domain environment that combines the physical, cybernetic, information, cognitive and psychological domains. The coordinated functioning of these domains is crucial for decision-making, information process management, development of adaptive strategies and maintaining the stability of complex systems in changing conditions. At the same time, the existing cross-domain integrated models remain limited in theoretical approaches [1, 2]. That is why this study is driven by the need to create a mathematical description of the dynamics of a multi-domain system of different components to function in a single planning process. The use of differential games in a multidomain environment is one of the promising areas of mathematical modelling of interagent interaction in complex socio-technical systems. Traditional approaches to analysing scenarios in cyberspace, as presented in [3], can be generalised by using non-cooperative games with dynamics described by systems of coupled differential equations. In view of this, the mathematical model proposed by the authors follows the fundamental architecture of this approach, which ensures scenario prediction and system adaptation to changing conditions. Study [4] systematises the game model according to the types and strategies of protection with a focus on non-cooperative and dynamic games to detect and neutralise ART (Advanced Persistent Treats) threats. Unlike the existing ones, the approach proposed by the authors takes into account the systemic interdependence between domains through a matrix of coefficients, determines the quantitative dependencies of the ratio of the level of dominance in the respective domains and cross-domain synergy, which forms a complete analytical framework for evaluating decisions in complex multi-agent environments.

Theoretical foundations of multidomain interaction. In the scientific literature, multidomain interaction is a form of system dynamics that is implemented in several interrelated domains, in particular: physical, information, cyber, cognitive and psychological [5]. These domains form a multidimensional environment within which actors (parties A and B) implement their own strategies using available resources and channels of interaction. Conceptually, such interaction is described by means of mathematical modelling, which allows to describe competitive strategies and equilibrium states in a system with many domains of influence. Typical examples of domains are:

physical - includes spatial actions on land, in the air, at sea and in space;

cyber - covers the impact on information and digital infrastructures;

information - concerns the manipulation of information flows, disinformation and content strategies;

cognitive - describes the processes of forming beliefs, mental models and interpretive structures;

psychological - covers emotional reactions, stressful states and psycho-emotional background.

In the context of cross-domain interaction, it is relevant to create a unified mathematical model that allows tracking the influence between domains, assessing their mutual dependence and predicting the effects of combined influence strategies in conditions of limited resources and incomplete information.

Literature review

The study considers multidomain interaction as a complex system in accordance with the structural-functional approach, where the input variables are: resources, information and strategic plans; procedural mechanisms are the interaction of physical, information, cyber and cognitive domains; and output effects are the achievement of an advantage or neutralisation of influence. To formalise the processes of influence, the mathematical apparatus of discrete mathematics, in particular Boolean algebra and set theory, is used to build a system of logical rules that reflects the links between the type of influence, source, society's susceptibility and the availability of countermeasures [6]. A similar approach is used in Boolean regulation models of regulatory networks, where Boolean logic formalises transitions between system states depending on input signals.

Study [7] proposes an innovative use of the Tau technique to build Nash equilibrium models in games with many players, which reflects the possibility of formalising dynamic interactions between opposing parties, taking into account the complex dependence of strategies on time and system states. In this context, there is another scientific approach presented in [8], where the authors model economic strategies as a system of coupled differential equations, where each of the parties, in our case (A and B), has its own payoff function, control variables and constraints.

It should also be noted that this method allows us to effectively approximate equilibrium trajectories without the need to solve complex analytical expressions, which in our case makes it possible to interpret domains as independent agents, each of which interacts with others within a generalised game with multiple objectives. A systematic review of the application of game theory in conjunction with the analysis of reliability risks in complex infrastructure systems is presented in [9]. The authors prove how cooperative and non-cooperative games, including multi-step and stochastic models, formalise agent behaviour and minimise losses and maximise gains, taking into account the risks of complex systems. According to our study, such approaches are integrated to formalise the multi-domain interaction of two parties (A and B), where each domain is considered as a separate node in the network of influences, and the structure itself is considered as a non-cooperative game with dynamic risks. It is also necessary to take into account the approach presented in [10], where dynamic modelling of cyber-physical-social systems is considered with a focus on the interaction strategy. In this paper, the domains (cyber, physical, social) are presented as interacting subsystems with their own evolutionary trajectories and priorities, and the proposed model takes into account not only intra-domain dynamics but also inter-domain feedback and the impact of context on interaction outcomes. This methodology can be considered a relevant basis for building a system of confrontation between two parties, where synergistic effects are integrated dependencies that are modelled in the form of a matrix.

A combination of game theory, system analysis and intelligent computing methods to model the dynamics of interaction between components (domains) under conditions of uncertainty and limited rationality is presented in [11]. The application of the approach of simulating strategic scenarios in distributed information structures that have analogies with a multi-domain environment allows us to consider in more detail the multi-domain model, where each domain (e.g., cognitive, informational, psychological) is modelled as a strategically active agent with its own function.

The proposed methodological approach in the study [12] to modelling interdependencies in critical infrastructure is based on the identification of interconnections and scenario analysis of their impact on system resilience, which makes it relevant to our study by interpreting domains as critical subsystems with functional links in the form of an integration matrix.

Risk modelling in power substations is presented in [13] in the form of a non-cooperative game conflict with limited resources, in which each party chooses a strategy based on an assessment of potential gains and losses. This approach adapts the concept of strategic confrontation in a multi-domain environment, in which each domain acts as an autonomous agent with its own goals.

A differentiated game model of conflict interaction in the context of cybernetic systems of ‘smart manufacturing’ is presented in [14], which is based on the Stackelberg game with limited resources. This model considers both direct and delayed effects of attacks, taking into account the synchronisation of impact and time delays, which allows modelling asymmetric reactions in conditions of incomplete information. This approach justifies the methodological feasibility of moving from single-domain models to an integrated approach to describe the interaction between domains in a changing information environment.

The replicator dynamics of describing the evolution of security investment strategies in the system is presented in [15], where agents make decisions based on benefits and taking into account the risks generated by interdependence with other players. This model relates to two parties in a conflict environment, similar to the relationship between cybersecurity strategies in interdependent organisations and the behaviour of agents in domains, which allows us to interpret each domain as a separate player in an evolutionary game. The use of such dynamics will allow modelling the adaptation of strategies over time, taking into account current conditions and mutual influence, which corresponds to the task of modelling cross-domain risks in systems with a high level of interaction between components.

A thorough review of existing approaches to game-theory-based modelling in new environments such as the Internet of Things (IoT) is provided in [16, 17], which describes key models of cooperative and non-cooperative games that allow for the behaviour of agents in an uncertain and resource-limited environment. This paper focuses on multilevel trust models that take into account individual assessments, contextual information formalised through game win functions, which can be used in modelling cross-domain interaction, where trust and risk assessment in domains are considered as strategic variables.

In [18], the authors systematised the use of evolutionary and repetitive games in the context of multi-agent systems operating in a complex decision-making environment with high entropy and interdependencies. This paper substantiates the use of matrix game structures with dynamic or stochastic functions, emphasises the relevance of hybrid approaches (combining game models with methods of artificial intelligence, machine learning and control theory), which allows for the implementation of real-time models.

The methodological basis of the study is a mathematical model that allows to describe the cause-and-effect relationships between information impact, cognitive reaction of society and decision-making. To substantiate the model, the method of expert evaluation of the importance of parameters was used, and the effectiveness of the impact was assessed through scenario and cognitive modelling. The results are presented in the form of a graph of functional dependencies for use in applied systems of situational analysis in the field of information technology.

The development of the model is driven by significant changes in the nature of competitive confrontation, which is increasingly going beyond traditional logic and becoming non-linear and systemic. The absence of a single regulatory document that systematically formalises all domains according to a certain logic is compensated by the presence of key concepts in the strategic legal field that determine the direction of evolution. This model is based on the formation of an analytical framework for planning and evaluating cross-domain interaction in the context of multifactorial confrontation, which justifies its scientific and practical significance. The introduction of this method of comparative analysis will allow structuring the model and expanding its capabilities for predicting synergistic effects between domains.

The purpose of this study is to develop a mathematical model for describing and predicting cross-domain interaction based on a comprehensive theoretical analysis of the phenomenon of multi-domain confrontation as a systemic modern phenomenon that goes beyond the classical understanding. The study analyses the peculiarities of cross-domain interaction on the example of Russian-Ukrainian relations, which allows identifying key patterns and mechanisms of influence in the context of synergistic use of physical, information, cognitive and cybernetic, etc. means.

Main results

Particular attention is paid to the formalisation of these influences using mathematical modelling [19], which provides an opportunity to objectively assess the strength, direction and effectiveness of domain activity. The scientific objective of the study is to integrate knowledge from information technology, psychology, cognitive science, social engineering and applied mathematics within a single system of formalised analysis of interagent interaction in a multi-domain environment [20, 21]. Particular emphasis is placed on the need to build a mathematical model for evaluating domain activity, identifying synergistic effects of interaction between domains, taking into account the dependencies that are formalised in the form of a cross-domain integration matrix [22, 23]. In the context of multidomain interaction in Ukraine, the interaction between domains is characterised by a consistent evolution. During the period (February-May 2022), the physical component was dominated by Russia, while large-scale information campaigns were conducted to demoralise Ukrainian society. Subsequently, cyber influences, information actions, and campaigns to expand channels of influence on the mental constructs of society were given priority [24], as shown in Table 1.

2022-2023, there was a high concentration of information campaigns, particularly in messengers and TikTok [25]. The main narratives are shown in Table 2.

Table 1 – **Functional characteristics of the key domains**

Domain	**Means of influence**	**Main objective**
Physical	Defence forces units	Control over territory
Cyber	DDoS, viruses, hacking	Paralysis of critical infrastructure
Information	Social media, propaganda	propaganda Manipulation of public opinion
Cognitive	Narratives, culture, language	Formation loyalty, identity
Psycho-logical	Spreading fear, PTSD	Undermining trust in the current government

Table 2 – **Fake news reports by individual months**

Month	**Number of fakes**	**Key narrative**	**Level of impact**
March 2022	183	‘Kyiv is captured’	High
August 2022	126	‘Ukraine's Armed Forces are losing’	Medium
May 2023	201	‘Mobilisation chaos’	High

Symmetry and asymmetry in the confrontation between parties A and B (Table 3). The confrontation in Ukraine can be called asymmetric: party B has an advantage in traditional means of influence, while party A has shifted to using current innovative tools - digital mobilisation, confrontation in the media space, mass media, information campaigns, and actions. Party B uses a symmetrical model based on dominance in physical deterrence. Party A uses an asymmetric model, which includes such components as adaptive information mobilisation, international support, volunteer networks, and cyber respondents [26].

Table 3 – **Comparison of confrontation models**

Parameter	**russia (symmetrical)**	**Ukraine (asymmetrical)**
Main resource	Force, technology	Information, speed
Strategy	Large-scale movement	Resistance movement, digital
Main domains	Physical, cyber information	Cognitive

Table 4 shows the modelled values of the main model parameters, which allow us to trace the change in influence between domains during a conditional calendar year. The key variables include: the emotional tone of the information influence (E), the intensity of information dissemination (I), the public reaction (R), and the values of the the intensities (w), which determine the strength of interdomain interaction. The conditional data allow us to illustrate the functionality of the mathematical apparatus and the model's ability to describe cognitive dynamics.

Fig. 1 shows the dynamics of changes in the model parameters in the time dimension. In particular, it shows the impact of changes in the emotional and informational background on the weighting coefficients of interaction between domains, as well as the correlation between the intensity of information influence and the reaction of society. Visualisation allows us to identify the periods of the greatest vulnerability or, conversely, the society's resistance to influence, which is necessary to predict the effectiveness of measures in the cross-domain paradigm.

Table 4 – **Input data for modelling cross-domain interaction within the model**

Month	E	I	R	w
1. January	0.1	150	300	135.04
2. February	0.3	180	350	159.12
3. March	-0.2	120	200	95.92
4. April	-0.1	130	220	104.96
5. May	0.2	160	330	147.08
6. June	0.4	170	340	153.16
7. July	0.5	190	360	165.2
8. August	0.2	155	310	139.58
9. September	-0.3	100	180	83.88
10. October	-0.4	90	160	74.84
11. November	0.1	140	250	117.04
12. December	0.3	160	270	129.12

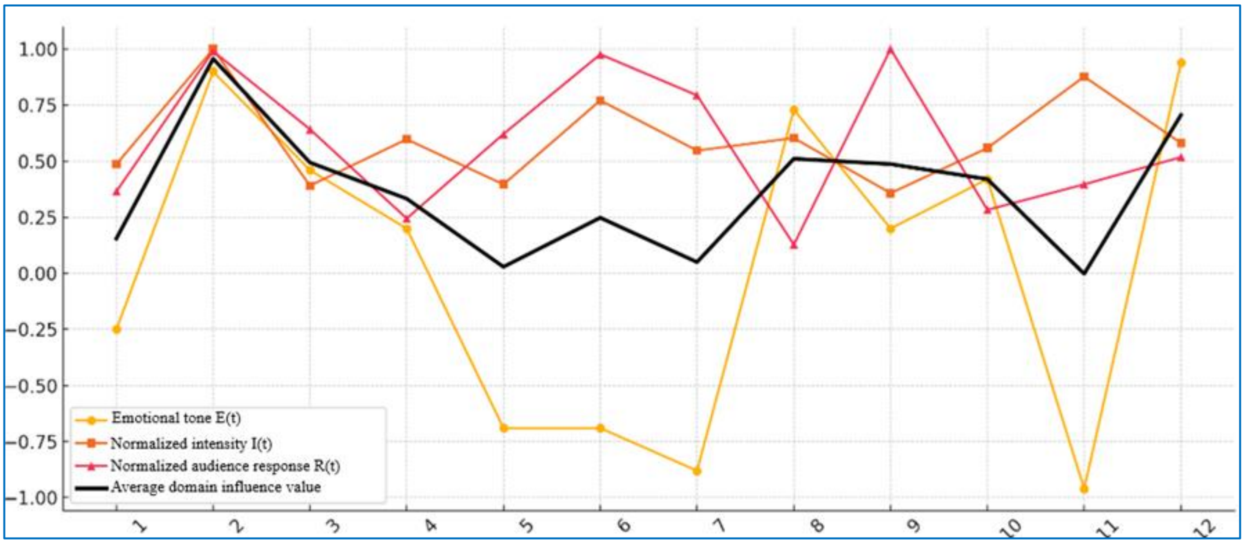

Fig. 1. Dynamics of domains' impact on society

Updating the model's mathematical apparatus. The mathematical framework of the model is an additional component for formalising the interaction of domains and assessing synergies between domains. However, such a model requires significant expansion and adaptation to the realities of multi-domain interaction [27].

Dynamic weighting coefficients are introduced: the cognitive penetration coefficient as a measure of the efficiency of the transition of an information signal to the cognitive state of the system and the cross-domain integration coefficient as a characteristic of the degree of interdependence between information flows in different domains. We consider the weighting coefficients within the model as dynamic values that change depending on the emotional state of society, the intensity of influence and fluctuations in the cognitive background. By cognitive background, we mean a set of dominant beliefs, attitudes, perceptions, emotional states and cognitive schemes that at a given time determine the way society perceives, processes and interprets information. A similar structured model of beliefs and its dynamics is described in [28], where an approach to modelling changes in public beliefs (convictions) under the influence of interpersonal and information interactions is updated on the basis of formal methods of statistical physics.

The developed mathematical apparatus is based on the results of the analysis of existing scientific approaches to the study of multidomain interaction, which define the simultaneous use of physical, information, cognitive and cybernetic components to achieve strategic goals [7-23]. In view of this, for further formalised analysis, we introduce the concept of domain power as a key variable that reflects the level of domain efficiency.

The power of the i-th domain at time t is denoted by $P_i(t)$. This is a scalar value that reflects the level of activity and efficiency of the domain. The change in domain power within the graph can be expressed through the dynamic equation as follows:

$$P_i(t+1) = P_i(t) + \sum_{j=1}^{n} w_{ij}(t) \cdot P_i(t) \cdot \varphi_{ji}(t), \qquad (1)$$

where $P_i(t+1)$ is the capacity of the i-th domain at a given time $(t+1), i=\overline{1n}$; $w_{ji}(t)$ is the intensity of the impact of domain j on domain i, which is updated on the basis of current data on the activities carried out (determined analytically through historical data, by expert evaluation), or adaptively (using machine learning technology or PID-controller) $i, j = \overline{1, n}$.

In such a model, the intensity: $w_{ji}(t)$ can be dynamic, i.e., that is, to change depending on external factors; n – number of domains; $\varphi_{ji}(t)$ – is the coefficient of cognitive penetration (CPC) into the i-th domain of the enemy from the j-th domain.

The interaction of the domain $P_i(t)$ with other domains is expressed through the differential equation of interdomain dynamics:

$$\frac{dP_i(t)}{dt} = \sum_{j=1}^{n} w_{ij}(t) \cdot P_i(t) \cdot \varphi_{ji}(t) - \delta_i \cdot P_i(t) + u_i(t), \quad (2)$$

where δ_i is the degradation coefficient of the *i*-th domain, which determines the power loss of the domain; $u_i(t)$ is the controlling influence on the i-th domain.

The intensity of the influence of the j-th domain on the *i*-th is determined as follows:

$$w_{ji}(t) = f(E(t), I(t), \Delta C_i(t)), \quad (3)$$

where $E(t)$ is the current emotional state of society, which is determined by analysing the tone of messages in the information space; $I(t)$ is intensity of cognitive influence, which is determined by the number of information contacts per unit of time; $\Delta C_i(t)$ is an indicator of change in cognitive impact, which is determined based on changes in the frequency of key messages.

To visualise the process of managing domain capacities, we will form a model as shown in Fig. 2.

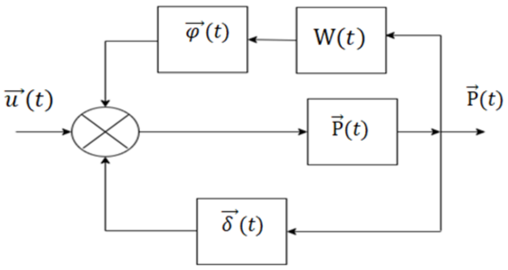

Fig. 2. Domain power management model

In general, the domain power management model can be represented by a vector-matrix differential equation:

$$\frac{d\vec{P}(t)}{dt} = W(t)\vec{P}(t)\vec{\varphi}(t) - \vec{\delta}\vec{P}(t) + \vec{u}(t), \quad (4)$$

where $\vec{P}(t) = (P_1(t), P_2(t), ..., P_n(t))$ is domain power vector; $\vec{\varphi}(t) = (\varphi_1(t), \varphi_2(t), ..., \varphi_n(t))$ is the vector of cognitive penetration into domains at time t; $\vec{\delta}(t) = (\delta_1(t), \delta_2(t), ..., \delta_n(t))$ – vector of domain degradation intensity; $\vec{u}(t) = (u_1(t), u_2(t), ..., u_n(t))$ – vector of domain power management;

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

Consider two sides A and B, consisting of *n* and *m* domains, respectively:

$$A = \{A_j\}, B = \{B_i\}, i = \overline{1, n}, \; j = \overline{1, m} .$$

The interaction of domains can be represented as an oriented graph, as shown in Fig. 3.

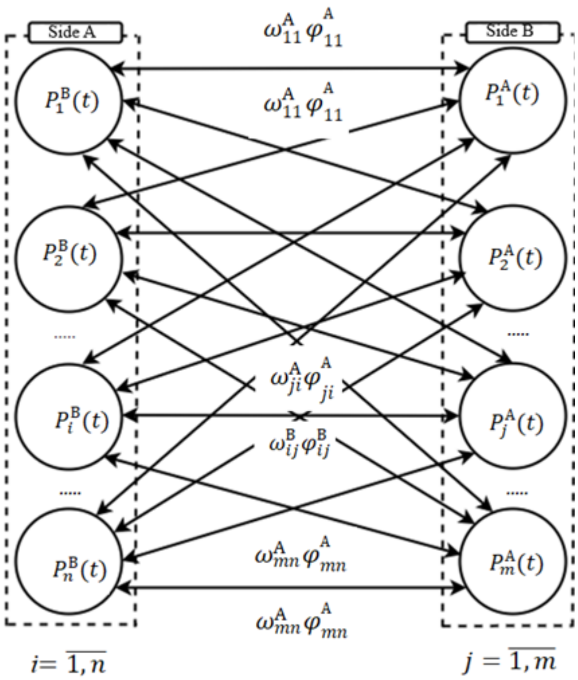

Fig. 3. Interaction graph between the domains of parties A and B

The interaction of the domains of parties A and B is described by the recurrent equations:

$$P_i^B(t+1) = P_i^B(t) + \sum_{j=1}^{n} w_{ji}^{A} \cdot P_i^B(t) \cdot \varphi_{ji}^{A}(t); \quad (5)$$

$$P_j^A(t+1) = P_j^A(t) + \sum_{i=1}^{n} w_{ij}^{B} \cdot P_j^A(t) \cdot \varphi_{ij}^{B}(t). \quad (6)$$

The process of cross-domain interaction according to the graph in Fig. 3 and equation (4) is described by the following system of differential equations for side A:

$$\begin{cases} \frac{dP_1^A(t)}{dt} = \sum_{j=1}^{m} w_{j1}^{B}(t) P_1^A(t) \varphi_{j1}^{B}(t) - \delta_1^A P_1^A(t) + u_1^A(t); \\ \frac{dP_2^A(t)}{dt} = \sum_{j=1}^{m} w_{j2}^{B}(t) P_2^A(t) \varphi_{j2}^{B}(t) - \delta_2^A P_2^A(t) + u_2^A(t); \\ \dots \\ \frac{dP_j^A(t)}{dt} = \sum_{j=1}^{m} w_{ji}^{B}(t) P_i^A(t) \varphi_{ji}^{B}(t) - \delta_i^A P_i^A(t) + u_i^A(t); \\ \dots \\ \frac{dP_n^A(t)}{dt} = \sum_{j=1}^{m} w_{jn}^{B}(t) P_n^A(t) \varphi_{jn}^{B}(t) - \delta_n^A P_n^A(t) + u_n^A(t), \end{cases} \quad (7)$$

where $P_1^A(t)$ – capacity of the i-th domain of the party A, $i=\overline{1,n}$; $w_{ji}^B(t)$ – is the intensity of influence of the j-th domain of party B on the i-th domain of party A, $i=\overline{1,n}$, $j=\overline{1,m}$; $\varphi_{ji}^B(t)$ – is the coefficient of cognitive penetration of the j-th domain of party B into the i-th domain of party A; $\delta_i^A(t)$ – is the intensity of degradation of the i-th domain of the party A, $i=\overline{1,n}$; $u_i^A(t)$ – controlling influence on the i-th domain of the party A.

For party B:

$$\begin{cases} \dfrac{dP_1^B(t)}{dt} = \sum_{i=1}^n w_{i1}^A(t)P_1^B(t)\varphi_{i1}^A(t) - \delta_1^B P_1^B(t) + u_1^B(t); \\ \dfrac{dP_2^B(t)}{dt} = \sum_{j=1}^n w_{i2}^B(t)P_2^B(t)\varphi_{i2}^B(t) - \delta_2^B P_2^B(t) + u_2^B(t); \\ \dots \\ \dfrac{dP_i^B(t)}{dt} = \sum_{i=1}^n w_{ij}^A(t)P_j^B(t)\varphi_{ij}^A(t) - \delta_j^B P_j^B(t) + u_j^B(t); \\ \dots \\ \dfrac{dP_m^B(t)}{dt} = \sum_{i=1}^n w_{im}^B(t)P_m^B(t)\varphi_{im}^B(t) - \delta_m^B P_m^B(t) + u_m^B(t), \end{cases} \quad (8)$$

where $P_j^B(t)$ is the capacity of the j-th domain of party B, $i=\overline{1,n}$; $w_{ij}^B(t)$ is the intensity of the influence of the *i*-th domain of party A on the j-th domain of the party B, $i=\overline{1,n}$, $j=\overline{1,m}$; $\varphi_{ij}^A(t)$ is the coefficient of cognitive penetration of the *i*-th domain of party A into the *j*-th domain of party B; $\delta_i^B(t)$ is is the degradation rate of the i-th domain of party B, $i=\overline{1,n}$; $u_j^B(t)$ is the controlling influence on the j-th domain of party B, $i=\overline{1,n}$. In general, let's represent the system of differential equations for side A and side B in the form of matrix forms.

For party A:

$$\frac{dP^A(t)}{dt} = W^B(t)P^A\Phi^B(t) - D^A P^A(t) + U^A(t), \quad (9)$$

where $P^A(t) = \left\{P_i^A(t)\right\}$ is matrix-power column of domains of party A; $P_i^A(t)$ is the capacity of the i-th domain of party A, $i=\overline{1,n}$; $W^B(t) = \left[w_{ji}^B(t)\right]$ is matrix of intensity of influence of domains of party B on domains of party A; $w_{ji}^B(t)$ is the intensity of influence of the j-th domain of party B on the *i*-th domain of party A, $i=\overline{1,n}$, $j=\overline{1,n}$; $\Phi^B(t) = \varphi_{ji}^B(t)$ is matrix of cognitive penetration coefficients; $\varphi_{ji}^B(t)$ is the coefficient of cognitive penetration into the j-th domain of party B from the *i*-th domain of party A; $D^A = \left[\delta_i^A(t)\right]$ is a matrix-string of the intensity of degradation of domains of party A, $i=\overline{1,n}$; $\left[\delta_i^A(t)\right]$ is the intensity of degradation of the i-th domain of party A, $i=\overline{1,n}$; $U^A(t) = \left\{u_j^A(t)\right\}$ is matrix-string of controlling influence on the domains of party A; $u_j^A(t)$ is controlling influence on the *i*-th domain of party A, $i=\overline{1,n}$.

For party B:

$$\frac{dP^B(t)}{dt} = W^A(t)P^B\Phi^A(t) - D^B P^B(t) + U^B(t), \quad (10)$$

where $P^B(t) = \left\{P_i^B(t)\right\}$ is matrix-power column of domains of party B; $P_i^B(t)$ is the capacity of the *i*-th domain of party B, $i=\overline{1,n}$; $W^A(t) = \left[w_{ij}^A(t)\right]$ is matrix of intensity of influence of domains of party A on domains of party B; $w_{ij}^A(t)$ is the intensity of influence of the j-th domain of party A on the *i*-th domain of party B, $i=\overline{1,n}$, $j=\overline{1,n}$; $\Phi^A(t) = \varphi_{ji}^A(t)$ is matrix of cognitive penetration coefficients; $\varphi_{ji}^A(t)$ is the coefficient of cognitive penetration into the j-th domain of party A from the i-th domain of party B; $D^B = \left[\delta_i^B(t)\right]$ is a matrix-string of the intensity of degradation of domains of party A, $i=\overline{1,n}$; $\left[\delta_i^B(t)\right]$ is the intensity of degradation of the i-th domain of party B, $i=\overline{1,n}$; $U^B(t) = \left\{u_i^B(t)\right\}$ is matrix-string of controlling influence on the domains of party B; $u_i^B(t)$ is controlling influence on the i-th domain of party B, $i=\overline{1,n}$.

The system can be adaptively trained using historical data, adjusting the W matrix for each period of confrontation at the appropriate level (tactical, operational, strategic). The diagonal elements may be important: $w_{ij}^A(t) > 0$, if the domain is capable of self-reinforcement. To ensure the mathematical stability of the model, the intensity normalisation by the expression is used:

$$\sum_{j=1}^n \left|w_{ij}^A(t)\right| \le 1. \quad (11)$$

This expression reflects the fact that a domain cannot be more influential than the system as a whole. A change in one value of intensity: $w_{ij}^A(t)$ in time t affects the outcome of the confrontation by activating the process of strengthening or weakening the influence of domains. The introduced cognitive penetration rate (CPR) is determined by the ratio of the power of cognitive messages that reached the target audience to the total power of the activities:

$$\varphi_{ij}^B(t) = \sum_{j=1}^n \left(w_{ij}^A \cdot C_j^B(t)\right) \Big/ \sum_{i=1}^n \sum_{j=1}^n \left(w_{ij}^A \cdot C_j^B(t)\right), \quad (12)$$

where $C_j^B(t)$ is the power of the cognitive component of domain j, which is determined by the total intensity of information messages over a period of time t.

The introduced cross-domain integration coefficient (CDI) determines the level of synergy between domains in the context of multidomain interaction and is calculated as:

$$k_j^A(t) = \frac{\sum_{j=1}^{n} w_{ij}^A P_j^B \cdot \varphi^B(t)}{\sum_{j=1}^{n} P_j^B(t) w_{ij}^A}, \qquad (13)$$

where k_j^A – CDI at a point in time t.

Given the above, equation (2) can be written as follows:

$$\frac{dP^B(t)_i}{dt} = \sum_{j=1}^{n} \begin{pmatrix} a_{ij}^A \cdot P_i^B(t) \cdot \varphi_{ij}^A(t) \cdot k_j^A(t) - \\ -\delta_i^B \cdot P_i^B(t) + u_i^B(t) \end{pmatrix}, \qquad (14)$$

where $a_{ij}^A(t) = \dfrac{w_{ij}^A(t)}{k_j^A(t)}$ is the weighting factor of the interdomain interaction between the j-th domain of party B and the i-th domain of party A, $i = \overline{1,n}$, $j = \overline{1,n}$;

To ensure dynamic adaptation (correction) of content in response to changes in the emotional state of society, it is advisable to use a PID-controller calculated using the formula:

$$\Delta C(t) = K_p^A \cdot e^A(t) \cdot \varphi^A(t) \cdot K^A(t) + $$
$$+ K_i^A \cdot \int_0^t e^A(t) \cdot \varphi(t) \cdot k(t) dt + K_d \cdot \frac{d_e(t)}{dt} \cdot \varphi(t), \qquad (15)$$

where K_p^A – coefficient of proportional scaling of the current error, K_i^A – integral coefficient, which takes into account the accumulated history of errors, K_d – coefficient of differential forecasting of a possible deviation based on the rate of change of the error. These coefficients are adapted in real time based on the forecasting accuracy metric $e(t)$, which ensures the model's resilience to changes in the information environment [29];

$$e(t) = E_{t\arg t} - E(t), \qquad (16)$$

where $e(t)$ –is an indicator of the deviation of current efficiency from the desired value.

Target emotional tone: $E_{t\arg t}$ defines the value of the emotional state of the target audience during the transaction. In the context of this model, it is a controlled parameter used for comparison with the current emotional state $E(t)$.

$$E_{t\arg t} = \sum_{k=1}^{n} E_k(t) \Big/ n, \qquad (17)$$

where $E_k(t)$ is emotional tone of the k-th information message at a given time *t*; *n* – number of messages in the analysed period of time; $E_{t\arg t}$ is a parameter for correcting cognitive influences through the PID-controller and for assessing the efficiency of operations in real time. If $E_{t\arg t} > 0$, the operation has a positive emotional impact (e.g., strengthening the morale of the personnel; if $E_{t\arg t} = 0$, the emotional impact is neutral; if $E_{t\arg t} < 0$, the information campaign (operation) has a negative emotional impact (e.g. demoralisation or intimidation). To visualise the operation of the PID-controller, we form Fig. 4, taking into account the domain power control model shown in Fig. 2, where $\overrightarrow{P_i^*}(t)$ –the set value of the domain power.

The introduction of a PID- controller allows content to be adjusted in real time based on feedback from the cognitive reactions of society, ensuring dynamic adaptation of the influence strategy.

Synergistic analysis and forecasting. An integration indicator is used to assess the integration effect:

$$\sum(t) = \sum_{i=1}^{n} P_i(t) \cdot k(t). \qquad (18)$$

This allows you to predict the synergistic effect between domains and evaluate the effectiveness of the measures taken in real time.

Total synergistic effect. Assessment of the model's integral efficiency:

$$X(t) = \sum_{i,j} P_i(t) \cdot P_j(t) \cdot w_{ij}(t), \qquad (19)$$

where $X(t)$ – is an indicator that reflects the overall effectiveness of multi-domain influence.

The metric of forecasting accuracy $(\varepsilon(t))$ is an indicator for assessing the effectiveness of the proposed model in the context of cognitive influence, which quantifies the discrepancy between the predicted and actual values of the power of influence on society. This metric is defined as the relative error between the predicted power of influence $(P_{pred}(t))$ and the actual power of influence $(P_{real}(t))$ at time t:

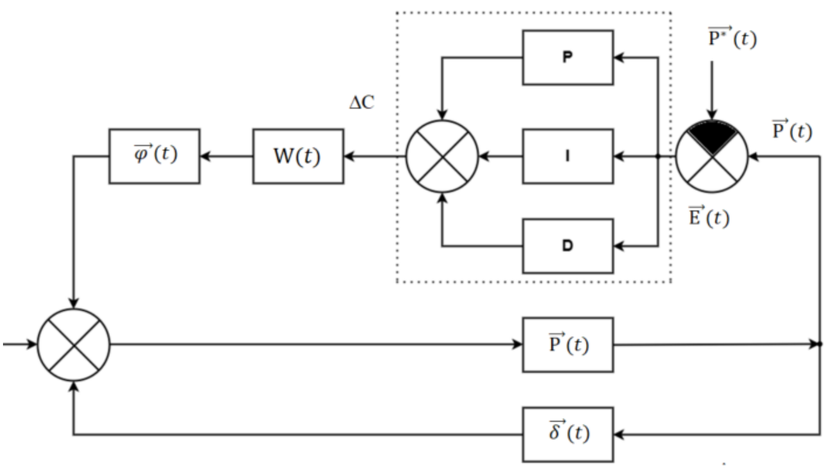

Fig. 4. PID-controller in the domain power management model

$$\varepsilon(t) = \frac{\left|P_{pred}(t) - P_{real}(t)\right|}{P_{real}(t)} \times 100\%, \qquad (20)$$

where $P_{pred}(t)$ – the predicted power of cognitive influence, which is determined on the basis of the system of equations of differential dynamics and PID-controller; $P_{real}(t)$ – the actual power of cognitive influence, which is assessed by the results of the reverse analysis of cognitive indicators; $\varepsilon(t) \in [0,100]\%$ –relative forecasting error.

Thus, the forecasting accuracy metric presented in Table 5 enables a quantitative assessment of predictive performance and serves as a trigger for adaptive model correction in real-time mode [30].

This ensures dynamic updating of weighting coefficients, PID parameters, and the structure of the graph-based model.

Table 5 – **Interpretation of forecast accuracy metric values and correction procedures**

The value of is ≈ (t)	Interpretation of forecasting accuracy	Correction procedure
ϵ(t)0%	High level of forecasting accuracy, the model effectively monitors the dynamics of cognitive influences	No correction is required. The current PID-controller structure is retained
$0\% < \varepsilon(t) \le 10\%$	Acceptable level of forecasting accuracy, the model requires minor adjustments	Adaptation of intensities $w_{ij}(t)$ based on cognitive background analysis
$10\% < \varepsilon(t) \le 30\%$	Medium level of forecasting accuracy, correction of weighting coefficients and PID-controller parameters is required	Changing the parameters K_p, K_i, K_d taking into account the dynamics of cognitive influence
$\varepsilon(t) > 30\%$	Low level of forecasting accuracy, the model requires significant adaptation	Updating the structure of the graph model, integrating new feedback

This model allows us to track changes in the emotional state of society in response to influences from the domain. In particular, if the intensity of the impact $P_2(t)$ increases, the cognitive impact C(t) increases accordingly, which leads to an increase in the synergistic effect between the domains.

The updated mathematical model provides coverage of cross-domain interaction through the integration of differential equations, the matrix structure of weighting coefficients, and the cognitive component of information influence propagation.

The introduction of a PID-controller allows to dynamically adjust the impact on individual domains based on feedback, which formalises an adaptive approach to managing information and cognitive influences.

The proposed model describes a complex network of cross-domain interaction and formalises its impact through domain interaction matrices that identify positive synergy effects and vulnerabilities of one of the parties. Such a model is a potential basis for predicting the results of domain activity, modelling impacts and formulating future strategies in real time.

The peculiarity of the implementation of the multi-domain strategy of the russian federation at this stage is the deep integration of civilian information infrastructure, cyberspace and the influence on the public consciousness to the plane of confrontation.

The massive spread of fake news and narratives, chaotic instability in the media space, and undermining of public trust are creating an environment in which classical mechanisms of state protection are losing their relevance. In such circumstances, Ukraine and its international partners must develop new, adaptive strategies based on a systematic analysis [31] of cross-domain dynamics and the construction of counter-domain response scenarios.

Conclusion

This study determines that multi-domain interaction is a systemic form of modern confrontation that integrates physical, cyber, information, cognitive and psychological components to achieve a synergistic effect. The mathematical model developed in the study formalises cross-domain interactions and assesses their impact on society.

The conceptual apparatus is developed and introduced: the coefficient of cognitive penetration and the coefficient of cross-domain integration, which additionally reflects the quantitative assessment of the intensity of cognitive influence and the level of synergy between domains, which helps to improve the process of determining indicators for predicting the effects of one of the parties (A or B). An empirical analysis of information and cognitive influences on society has demonstrated the low efficiency of traditional technologies in countering challenges and threats. This highlights the need to introduce integrated cyber defence systems capable of neutralising DDoS attacks and countering them in the information space. In this context, a promising area of research is the use of artificial intelligence (AI) for the timely identification of disinformation campaigns in real time. Further development of research in the field of multidomain interaction is associated with the development of dynamic models of the evolution of the total interdomain interaction, taking into account temporal and spatial changes in the information environment. It is also advisable to introduce adaptive indicators of cognitive resilience to assess the psychological readiness of the population to information influences. The definition of such indicators is based on an analysis of the level of critical thinking, the speed of detecting disinformation and the emotional stability of society. The successful implementation of the developed model also involves the creation of a multi-domain early warning system that can predict cyber threats, socio-technical manipulations and information influences at different levels. This task requires the integration of new concepts of information technology aimed at ensuring a strategic advantage in the confrontation between the two systems.

Thus, the proposed model reflects the coverage of cross-domain interaction through the dynamic integration of differential equations, graph models and PID-controller. It makes it possible to quantify the synergistic effects between domains and provides adaptive correction of information influences in real time. In the current conditions of confrontation in the information environment, the developed model is the basis for creating scenarios that can increase the indicator of cognitive resilience of society to external influences.

References

1. Faigle, U. (2020), "Mathematical Game Theory", *arXiv preprint*, 2020, available at: https://arxiv.org/pdf/2001.08873
2. Anbarasu S., Hinkelman K., Wang J.and Zuo W. (2024), "Exploring the effects of interdependencies on energy systems in smart communities: A multi-domain modeling and quasi-Monte Carlo sensitivity analysis", *Energy and Buildings*, vol. 319, 114510, doi: https://doi.org/10.1016/j.enbuild.2024.114510
3. Kour, R., Karim, R. and Dersin, P. 92025), "Modelling cybersecurity strategies with game theory and cyber kill chain", *Int J Syst Assur Eng Manag*, doi: https://doi.org/10.1007/s13198-025-02733-4
4. Khalid, M.N.A., Al-Kadhimi, A.A. and Singh, M.M. (2023), "Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): A Systematic Review", *Mathematics*, vol. 11(6), 1353, doi: https://doi.org/10.3390/math11061353
5. Sobb, T., Turnbull, B. and Moustafa, N. (2023), "A Holistic Review of Cyber–Physical–Social Systems: New Directions and Opportunities", *Sensors*, vol. 23(17), 7391, doi: https://doi.org/10.3390/s23177391
6. Saadatpour, A. and Albert, R. (2013), "Boolean modeling of biological regulatory networks: a methodology tutorial", *Methods*, vol. 62(1), pp. 3–12, doi: https://doi.org/10.1016/j.ymeth.2012.10.012
7. Alabdala, A. T., EL-Seidy, E. and Adel, W. (2024), "Applying the Tau technique in multi-player differential games: A novel approach in economic strategy analysis", *Partial Differential Equations in Applied Mathematics*, vol. 10, 100724, doi: https://doi.org/10.1016/j.padiff.2024.100724
8. Alabdala, A. T., Alhassan, A., Alabdullah, M. T. and Adel, W. (2025), "Dynamic analysis of competitive marketing strategies using differential game models and Runge–Kutta solutions", *Partial Differential Equations in Applied Mathematics*, vol. 14, 101156, doi: https://doi.org/10.1016/j.padiff.2025.101156
9. Hausken, K., Welburn, J. W. and Zhuang, J. (2025), "A Review of Game Theory and Risk and Reliability Analysis in Infrastructures and Networks", *Reliability Engineering & System Safety*, vol. 261, 111123, doi: https://doi.org/10.1016/j.ress.2025.111123
10. Cheng, L., Wei, X., Li, M., Tan, C., Yin, M., Shen, T. and Zou, T. (2024), "Integrating Evolutionary Game-Theoretical Methods and Deep Reinforcement Learning for Adaptive Strategy Optimization in User-Side Electricity Markets: A Comprehensive Review", *Mathematics*, vol. 12(20), 3241. doi: https://doi.org/10.3390/math12203241
11. Grigoryan, G. and Collins, A.J. (2021), "Game Theory in Systems Engineering: A Review", *International Journal of System of Systems Engineering*, vol. 11(2), pp. 121–158, doi: https://doi.org/10.1504/IJSSE.2021.116044
12. Leoneti, A.B. and Gomes, L.F.A.M. (2021), "Modeling multicriteria group decision making as games from enhanced pairwise comparisons", *Operations Research Perspectives*, vol. 8, 100194, doi: https://doi.org/10.1016/j.orp.2021.100194
13. Boujnoui, A., Zaaloul, A. and Haqiq A. (2018), "Mathematical Model based on Game Theory and Markov Chains for Analysing the Transmission Cost in SA-ZD Mechanism", *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 10, pp. 197–207, available at: http://www.mirlabs.net/ijcisim/index.html
14. Ho, E., Rajagopalan, A., Skvortsov, A., Arulampalam, S. and Piraveenan, M. (2022), "Game Theory in Defence Applications: A Review", *Sensors*, vol. 22(3), 1032, doi: https://doi.org/10.3390/s22031032
15. Li, T., Sun, J. and Fei, L. (2025), "Application of Multiple-Criteria Decision-Making Technology in Emergency Decision-Making: Uncertainty, Heterogeneity, Dynamicity, and Interaction" *Mathematics*, vol. 13(5), 731, doi: https://doi.org/10.3390/math13050731
16. Wang, Y., Lu, X., Liu, Z. nd Lin, Y. (2024), "A Review of Game Theory-Based Trust Modeling Approaches in IoT", *Computer Communications*, vol. 218, 111023, doi: https://doi.org/10.1016/j.comcom.2024.111023
17. Kuchuk, H., Mozhaiev, O., Kuchuk, N., Tiulieniev, S., Mozhaiev, M., Gnusov, Y., Tsuranov, M., Bykova, T., Klivets, S. and Kuleshov, A. (2024), "Devising a method for the virtual clustering of the Internet of Things edge environment", *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 9 (127), pp. 60–71, doi: https://doi.org/10.15587/1729-4061.2024.298431
18. Renna, P. (2024), "A Review of Game Theory Models to Support Production Planning, Scheduling, Cloud Manufacturing and Sustainable Production Systems", *Designs*, vol. 8(2), 26, doi: https://doi.org/10.3390/designs8020026
19. Oesch, S., Hutchins, J., Austria, P. and Chaulagain, A.(2025), "Agentic AI and the Cyber Arms Race", *arXiv preprint*, arXiv:2503.04760, available at: https://arxiv.org/abs/2503.04760
20. Klein, G., Woods, D. D., Bradshaw, J. M., Hoffman, R. R. and Feltovich, P. J. (2004), "Multiscale decision-making: Bridging organizational scales in systems with distributed decision-makers", *Cognitive Systems Research*, vol. 5(2), pp. 193–213, doi: https://doi.org/10.1016/j.cogsys.2003.07.002
21. Yao, L., Zhang, Q. and Deng, S. (2025), "A combined approach of evolutionary game and system dynamics for user privacy protection in human–AI interaction", *Scientific Reports*, vol. 15, 13730, doi: https://doi.org/10.1038/s41598-025-98805-3
22. Rich, M. S. and Aiken M. P. (2024), "An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics", *Forensic Science*, vol. 4(1), pp. 110–151, doi: https://doi.org/10.3390/forensicsci4010008
23. Herasymov, S., Tkachov, A. .and Bazarnyi, S. (2024), "Complex method of determining the location of social network agents in the interests of information operations", *Advanced Information Systems*, vol. 8, no. 1, pp. 31–36, doi https://doi.org/10.20998/2522-9052.2024.1.04 .

24. Pierri, F., Luceri, L., Jindal, N. and Ferrara E. (2023), “Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine”, *Proceedings of the 15th ACM Web Science Conference*, pp. 65–74, doi: https://doi.org/10.1145/3578503.3583597
25. (2023), “Mass Media”, *VoxUkraine*, available at: https://voxukraine.org/en/propaganda-diary-2022-2023-voxcheck-presents-the-database-of-russian-propaganda-in-the-european-mass-media
26. Monzon, Baeza V., Parada, R., Concha, Salor L. and Monzo, C. (2025), “AI-Driven Tactical Communications and Networking for Defense: A Survey and Emerging Trends”, *arXiv preprint*, arXiv:2504.05071, doi: https://doi.org/10.48550/arXiv.2504.05071
27. Petrovska, I., Kuchuk, H., Kuchuk, N., Mozhaiev, O., Pochebut, M. and Onishchenko, Yu. (2023), “Sequential Series-Based Prediction Model in Adaptive Cloud Resource Allocation for Data Processing and Security”, *2023 13th International Conference on Dependable Systems, Services and Technologies*, DESSERT 2023, 13–15 October, Athens, Greece, code 197136, doi: https://doi.org/10.1109/DESSERT61349.2023.10416496
28. (2024), *Analogies for modeling belief dynamics*, Santa Fe Institute ScienceDaily, 29 July 2024, available at: https://www.sciencedaily.com/releases/2024/07/240729173319.htm
29. Petrovska, I., Kuchuk, H. and Mozhaiev, M. (2022), “Features of the distribution of computing resources in cloud systems”, *2022 IEEE 4th KhPI Week on Advanced Technology*, KhPI Week 2022 – Conference Proceedings, 03-07 October 2022, Code 183771, doi: https://doi.org/10.1109/KhPIWeek57572.2022.9916459
30. Qin, S. J. and Badgwell, T. A. (2003), “A survey of industrial model predictive control technology”, *Control Engineering Practice*, vol. 11(7), pp. 733–764, doi: https://doi.org/10.1016/S0967-0661(02)00186-7
31. Yuwono, S., Arend, D. and Schwung, A. (2024), “MLPro-GT – Game Theory and Dynamic Games Modeling in Python”, *SoftwareX*, vol. 28, 101956, doi: https://doi.org/10.1016/j.softx.2024.101956

Received (Надійшла) 05.03.2025
Accepted for publication (Прийнята до друку) 11.06.2025

ABOUT THE AUTHORS / ВІДОМОСТІ ПРО АВТОРІВ

Базарний Сергій Васильович – доктор філософії, Національний університет оборони України, Київ, Україна;
Serhii Bazarnyi – PhD, National Defence University of Ukraine, Kyiv, Ukraine;
e-mail: serhii.bazarnyi@edu.nuou.org.ua; ORCID Author ID: https://orcid.org/0000-0001-9545-1960;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=58905874600.

Гусак Юрій Аркадійович – доктор військових наук, професор,, Національний університет оборони України, Київ, Україна;
Yurii Husak – Doctor of Military Sciences, Professor, National Defence University of Ukraine, Kyiv, Ukraine;
e-mail: y.husak1512@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-3423-2112.

Войтко Тетяна Миколаївна – наукова співробітниця НДВ, Національний університет оборони України, Київ, Україна;
Tetiana Voitko – Researcher of Research Department, National Defence University of Ukraine, Kyiv, Ukraine;
e-mail: t.voytko@ukr.net; ORCID Author ID: https://orcid.org/0000-0002-4326-0633;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=58741186300.

Алієв Фуад – професор, професійно-технічне училище, університет Єдитепе, Стамбул, Туреччина;
Fuad Aliew – Professor, Vocational School, Yeditepe University, Istanbul, Turkey;
e-mail: fuad.aliew@yeditepe.edu.tr; ORCID Author ID: https://orcid.org/0000-0002-0153-7868;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=44060941600.

Євсеєв Сергій Петрович – доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Serhii Yevseiev – Doctor of Technical Sciences, Professor, Head of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: serhii.yevseiev@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0003-1647-6444;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190440690.

Математична модель багатодоменної взаємодії на основі теорії ігор

С. В. Базарний, Ю. А. Гусак, Т. М. Войтко, Ф. Алієв, С. П. Євсеєв

Анотація. У статті розроблено математичну модель багатодоменної взаємодії, як елементу концепції сучасного протистояння у таких просторах, як: кібернетичний, інформаційний, когнітивний та психологічних. В дослідженні акцентовано увагу на аналізі багатодоменної взаємодії, та висвітлює особливості використання різних доменів для вирішення поставлених задач. Розроблена модель формалізує міждоменні взаємодії та кількісно обчислює синергетичний ефект між доменами. Вперше у межах моделі впроваджено новий понятійний апарат: Коефіцієнт когнітивного проникнення та коефіцієнт міждоменної інтеграції. Врахування цих показників впливає на підвищення точності оцінювання проникнення розроблених та поширених інформаційних матеріалів у когнітивний простір суспільства та визначити рівень інтеграції впливів між доменами. Запропонований математичний апарат ґрунтується на основі системи диференціальних рівнянь, з урахуванням динамічних вагових коефіцієнтів, які залежать від емоційного стану суспільства, інтенсивності інформаційного впливу та зміни когнітивного фону. Окрім того, застосовано PID-регулятор для адаптивного управління когнітивними впливами. У рамках емпіричного дослідження проаналізовано вплив на прикладах інформаційних кампаній у соціальних мережах та засобах масової інформації. Запропоновано новий підхід до корегування прогнозів когнітивного впливу на основі метрики точності прогнозування та динамічної адаптації параметрів PID-регулятора. Отримані результати дозволяють обґрунтувати доцільність використання даної моделі, як інструменту аналізу багатодоменної взаємодії в конкурентних умовах та розробки сценаріїв для забезпечення ефективного протистояння в сучасному інформаційному просторі.

Ключові слова: багатодоменна взаємодія; інформаційні технології; соціальні мережі; когнітивний простір; математична модель.