System-Information and Cognitive Technologies of Man-Made Infrastructure Cyber Security

Liubomyr S. Sikora[1], Nataliia K. Lysa[1], Yevhen I. Tsikalo[2]
and Olga Yu. Fedevych[1,*]

[1]*Lviv Polytechnic National University, Lviv, Ukraine*
[2]*Ivan Franko Lviv National University, Lviv, Ukraine*
E-mail: liubomyr.s.sikora@lpnu.ua; nataliia.k.lysa@lpnu.ua;
yevhen.tsikalo@lnu.edu.ua; olha.y.fedevych@lpnu.ua
[*]*Corresponding Author*

Received 31 October 2022; Accepted 02 February 2023;
Publication 16 May 2023

Abstract

The complication of technological processes due to the modernization of complex technological processes aggregates with a distributed spatial infrastructure requires the use of new control systems and computer and information network technologies. Accordingly, this poses the problem of revising the basic concepts of information-measuring systems building, developing software and hardware for the implementation of the target management process. This requires development of new approaches to presentation, processing, and display of data about the aggregates state of energy-active objects and the entire information structure. For management under threat conditions, it is necessary to take into account the features of the information infrastructure, data selection and processing methods, methods and algorithms for classifying the situation, which are formed from blocks of data obtained from each unit and the technological process as a whole.

Information about the current state of system and infrastructure is necessary for the formation, adoption and implementation of management

Journal of Cyber Security and Mobility, Vol. 12_3, 389–414.
doi: 10.13052/jcsm2245-1439.123.7

decisions which is the basis for coordination strategies synthesis. Appropriate target orientation, reasonable indicators of real process trajectories divergence from the target state determine the probability of object attack. Knowledge and decision-making procedures for the coordination of managerial actions is based on the strategic target orientation of the structure, their professionalism and the level of intellectual, cognitive and scientific training which is the basis for correct situation interpretation of countermeasures against threats formation.

In the event of active threats complex on man-made systems in a certain region (resource, cognitive, system, information) and natural disasters or military operations, the threats lead to active destruction or failure of the production process. In order to functionally withstand related production structures, when loyal to the industrial relations concept, they need to integrate at the strategic management level on common goal basis to reduce risks. If necessary, to increase sustainability, they can be integrated at operational management level using interconnections at the production and resource levels. To do this, it is necessary to develop a strategic and goal-oriented management system behaviour line, which requires informational and intelligent data processing at the highest level using cognitive creative methods.

For each level of the infrastructure hierarchy, oriented towards strategic goals in the global infrastructure dynamic environment, methods of assessing the situation to detect failures and the actions of attacks have been developed, based on which countermeasures are formed depending on the type of threats.

Keywords: Cyber security, infrastructure, system, management, cognitive models, information technologies, strategies, risks, target orientation, hierarchy.

1 Introduction and Problem Structure

Modern analysis stage of dynamics and goals of whole-oriented hierarchical systems infrastructure functioning with corporate and other types of management shows that current crisis and emergency situations arise due to past design errors. Uncertainty and undefined clarity of goals, underestimation of resources, selection of unclear strategies and main goals, under the influence of cognitive failures in decision-making conditions, insufficient qualification of personnel, failure to take into account external threats, inability to predict active events for a long period of time. Determining threats level at the expense of a low level of management training, respectively, leads to the collapse of infrastructure (region, state and local systems) in active aggressive threats conditions of structural, resource, information type, which cannot be predicted in management cycle terminal time.

The problematic situation is that modern management methods do not sufficiently use logic-cognitive models of person who makes the decisions (cognitive intelligent agent), and even more so, little attention is paid to team's formation due to achieve effective management in threats conditions (man-made structures cyber security cognitive components with hierarchy in terms of attacks resistance integration).

The urgency of solving the problem. In modern production and socio-communal structures, telecommunication and communication systems and management of complex systems with a hierarchical organization, the causes of extreme and emergency situations can be both embedded errors in projects and, accordingly, in goals and strategies. Active attacks, failures, malfunctions (decreased reliability and resources) lead to a functioning failure. If production aggregate level produces increasing functional reliability problems then at the upper levels of control hierarchy, information and cognitive type failures and threats leads to accidents. Intellectual and cognitive errors of operative personnel cause (become) the cause of disasters or emergency situations in which the system loses its intended functionality, and informational and targeted disorientation of strategic-level personnel destroys the infrastructure.

In accordance with system goals, it is necessary to form reliability and functionality requirements of units, management structure which would take into account possible types of threats and attacks. Operational personnel's knowledgeable intellectual and cognitive characteristics and a way of their thinking determine the ability to make strategic creative decisions in emergency situations, which require a new approach to selection of operational and strategic management personnel. Cyber security as strategic security of infrastructure management is an urgent problem of ensuring functional stability according to the target tasks and is based on high-quality information and intellectual support of situations assessment in the formation, adoption and implementation of goal-oriented decisions in the conditions of threats, resource and structural and other types of attacks on infrastructure.

2 References Analysis

Articles [1, 2] are devoted to the problems of building procedures for making effective management decisions in technical and economic systems. The work [3] is devoted to the large systems organization theory, in which the basic models of structure construction, functioning models, open management strategies, resource and strategic games, problems of effective design are considered. The data processing, classification and forecasting methods as the basis for the formation of the decision-making process are considered in works [4, 6]. Methods of expert systems theory for use in complex systems in the formation of management decisions are considered in works [7–9]. Theory of coordination in management processes is considered in the works [10]. Cognitive technologies of situation assessment are shown in [11], risk models in intellectual strategies formation in [13]. Intellectual agent activity method based on ontology is considered in [12]. In [14] problem of management in situation change conditions under the influence of decision-making process violations is considered. The work [15] substantiates system analysis methods of decision-making process in social, organizational, and technological structures. Works [16, 18] disclose methods of complex systems designing and protecting them from attacks as well as system strategic security. The monograph [17] examines information wars types. The research results used in [19] are devoted to information technologies analysis, the concept of their development, platforms and standards, software and expert systems, fuzzy logic.

3 Aim and Object of Study

On the basis of system analysis, information and logic-cognitive technologies, determine and justify indicators for identifying the causes of crisis and emergency situations in complex integrated man-made systems with hierarchical infrastructure. In the event of threats and attacks on the process and management goals of each related industries infrastructures, an important means of their stability is integration as informational, intellectual resource component for development of a strategic line to counter threats, which is necessary to ensure effectiveness of countermeasures methods and high cyber security level.

Object of study. Infrastructure, goals and dynamics of complex man-made systems in the complex of spatially-distributed integrated production and economic components and resources of national economy of the region.

The tasks of management in complex systems dynamics researching under integrated conditions of threats:

- Based on system analysis and theory of hierarchical structures substantiate cognitive principles of coordination and information support of formation and decision-making process in the attacks conditions on the terminal time intervals of the infrastructure functioning against the action of active threats various types;

- Based on information technology and intellectual data processing prepare justification of ACS (Automated Control System) strategy support against attacks and threats in the current time period and their heterogeneity as well as strategic coordination and infrastructure integration.
- To justify the logic-cognitive method of situations expert analysis in ACS under the influence of threats and informative attacks for making effective, robust decisions for goal-oriented management and cyber security based on highly qualified expert's knowledge, who have high scientific and industrial qualifications and extensive professional experience in this field;
- To justify the method of intelligent data processing for assessing situations in the control object under structural and informational threats and attacks on the ACS, which are based on logic-cognitive methods of choosing of making goal-oriented decisions using complex methods of infrastructure cyber security;
- To develop a method of evaluating the effectiveness of information, cognitive and intellectual operations in the formation of management decisions under the conditions of active threats and complex attacks, based on the use of highly qualified expert's knowledge.

4 An Overview of the Main Material on Managing Complex Systems Under the Conditions of Resource Threats and Information Attacks Problem

4.1 The Cognitive Principles of Information Support are Necessary for the Construction of Procedures and Algorithms for Cognitive and Logical Situational Conclusions with Incomplete Data on the Dynamic State of Technological Systems Under Threat Conditions

The current state of technologies for managing complex objects development in the information structure of integrated hierarchical systems is characterized by the presence:

- automated control systems for managing technological processes in aggregated energy-active technological objects included in the structure as components with a certain (physical-thermodynamic, energy, resource, electrical, information-management) purpose according to the production type;

- management hierarchy general infrastructure (aggregate control, operational management, administrative-financial, local tactical and strategic command management of the lower level of the hierarchy);
- goal-oriented management with coordination strategies for harmonizing behaviour corporate rules in the formation of local and global goals;
- systems of a complex of cyber security methods and tools.

In accordance with the goals of production and the external situation in which the investigated infrastructure with a control complex is located, it is necessary to determine the roles and methods of behaviour (ACS) of the automated control system in interaction with the operational control team (constructive agents). It is necessary to evaluate the system interaction at all levels of the infrastructure:

- IS_1 – combined man-machine integrated systems of operational management of a complex of objects and units;
- $IS_{2,1}$ – operational-administrative strategic goal-oriented management at all levels of spatial infrastructure hierarchy;
- $IS_{2,2}$ – coordination management of integrated infrastructure in state and private production systems;
- IS_3 – systems of operational round-the-clock mode management and service maintenance of technological facilities.

This requires a high level of professional training, intellectual psychological stability, and professional maturity from the personnel to counter the threats.

In critical decision-making moment of control and management, when threats and attacks on the infrastructure occur, the staff must have appropriate goal-oriented and motivated behaviour that depends on the cognitive abilities of individuals and their informativeness and powers. According to cognitive characteristics, the following basic types of thinking of an operational worker can be distinguished, which are necessary for him during effective and constructive processing of data, when forming management decisions to counter threats.

- KM_1 – with a scenario-based imagination of events development in the system and imaginative thinking when forming decisions based on subconsciously accumulated knowledge and acquired professional experience;

- KM_2 – with analytical structured thinking, based on the events analysis, synthesis of strategies and action plans using ordered basic knowledge about the structure and dynamics, the purpose of the functioning of the hierarchy and each technological system unit;
- KM_3 – creative logic-systemic thinking characterizes the ability to take an integrated approach when forming solutions in extreme and emergency situations, the search for non-standard solutions to stabilize the functions of the integrated infrastructure and its cyber security.

Accordingly, at the top level of the hierarchy, decisions should be made by individuals of the second type KM_2, but with vagueness and incompleteness of data on the situation at different levels of the hierarchy and from information systems of ACS-TP and laboratory control operators, experts with a third type of thinking should be connected. These individuals with a high level of intelligence provide a complete analysis of data about the situation due to a high level of knowledge, the ability to model and interpret the situation in a hierarchy, to form operative actions to prevent emergency situations at objects, blocks, units of technological systems (Figure 1). Functional stability of the hierarchy in crisis situations in the integrated infrastructure can be provided by operative management workers with creative thinking $\{KM_1, KM_2, KM_3\}$, which are the core team of goal-oriented management of the process and cyber security of the infrastructure.

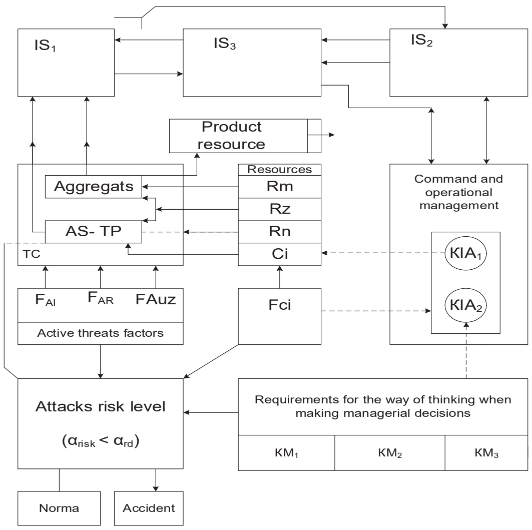

Figure 1 Systemic – informational interaction of threats and ACS – cognitive agent.

Notation: IS – hierarchical structure, Ci – goals, $\{\text{Fi}\}$ – disturbance factors, KIA – cognitive intellectual agent, $\{\text{KMi}\}$ – cognitive thinking type, α_r – emergency risk level, $\{\text{Ri}\}$ – resource flows.

Given scheme of system-information threats is the basis for building categorical logic-cognitive diagrams of management data flows and interaction.

5 Expert Analysis of the Situation when Threats Affect the Management Process

5.1 Intelligent Operations in Target Decision-making Procedures

The most complex element of the management process is the intellectual actions of processing information and making management decisions by the operator (cognitive agent). Information systems as part of ACS-TP should be oriented for the selection of non-standard operational and technological data from the hierarchical structure, their algorithmic processing and classification according to the specified characteristics, which provides the team (agents – managers) with an intellectual basis for the formation of strategies for exiting the crisis on the basis of a creative selection of permissible strategies using informational and intellectual combinations of operations.

In complex systems with a hierarchical infrastructure, with the command method of decision-making at the operational, administrative and strategic corporate levels, under the threat of active information attacks, decision support systems (DSS) are used for the whole oriented management.

The DSS include in their structure experts who, on the basis of knowledge engineering for each subject area, form a knowledge base necessary to support decision-making in the dialogic mode of implementing management in crisis conditions and emergency situations of infrastructure operation.

Accordingly, experts should specialize in areas of knowledge and technology – resource, aggregate – technological, operational management and information – measurement systems, administrative and strategic management.

Coordinating management in complex man-made situations of threats and accidents is based on team decision-making methods by experts under the leadership of a leader who, in the mode of dialogue with the strategic level of the hierarchy, takes measures to eliminate threats based on a situation assessment.

Intellectual thinking and operations of forming strategic goal-oriented coordination solutions provide relevant expert assessments:

- logical-cognitive processing of situations images formed on the basis of information technologies, to assess the position of the system in the space of goals;
- events development scenario analysis relative to the target state of the system and determination of the deviation degree;
- on the basis of the divergence degree, form a procedure for the strategies synthesis, tactics and action plans, which are translated into teams of consecutive targeted actions;
- on the basis of an assessment of changes in situations, if the goals are not achieved, move to coordination strategies.
- Information operations in the decision-making procedures for the management of the IACS (Intellectual ACS):
- data flow processing, information-algorithmic, for assessing situations in the space of states and building an image of situations in an energy-active object;
- analysis of the behaviour trajectory of the object's mode parameters relative to the specified loading and performance coordinates;
- determination of the state trajectory deviation degree from the given mode;
- if the target area is not reached due to the implemented strategy, under the condition of approaching the limit mode, the new situation is assessed as non-standard.

5.2 Terminal Defense Against Infrastructure Hierarchy Attacks

According to the target tasks, the production system includes the hierarchy management levels, the technological aggregate structure of the energy-active system (Figure 2):

- aggregated technological line in which the products production process (automated control) takes place;
- (IMS) – an information-measuring system for data selection and transmission to ACS-TP for forming control commands (automatic mode);
- automatic technological process control system (ACS-TP);
- an operational management unit with a display and panel complex for displaying information and means and a mechanism for executing management and coordinating commands (human resources) (OMU-MC);
- unit for administrative and technological management of the production plans implementation (human resources) (UA-TM);

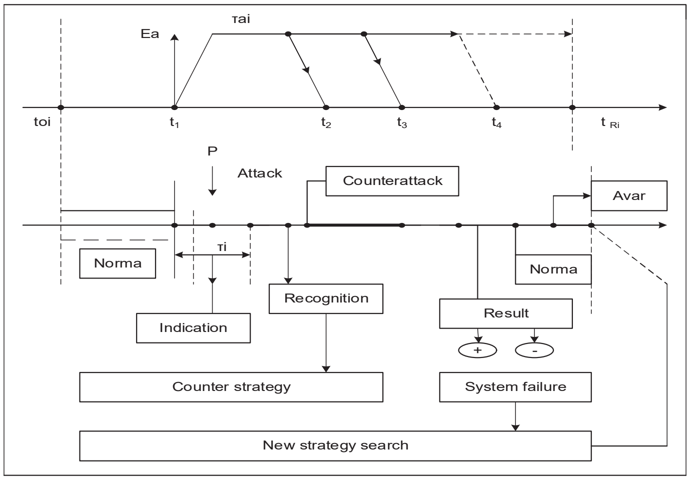

Figure 2 Terminal counter attack diagram.

- strategic management unit using operational and expert support (high-level human resource) (SMU);
- the information model of the production process, as a basis for the formation of management decisions according to the dynamic situation (IMS functioning benchmark), (databases and knowledge bases, DSS, experts).

In accordance with the structure of the system and target tasks, technologies for acquiring and using knowledge to solve management tasks in automatic and operational mode are being formed (Figure 2).

Accordingly, the infrastructure of production complexes can include a certain number of technological systems with appropriate corporate management, which are united by the products type, priorities in the foreign market, strategic goals, financial resources, which provides with production and functional stability at the intersystem level.

Accordingly, expert analysis on the terminal interval is carried out according to the diagram of countering attacks on the interval.

In accordance with the target task, a team of expert systems (experts) is used to counter cyberattacks on infrastructure (Figure 3), which includes relevant persons specialized in areas of knowledge complex:

- resources protection;
- an expert on the structuring of technological line units;
- experts in information and measurement systems and data processing;

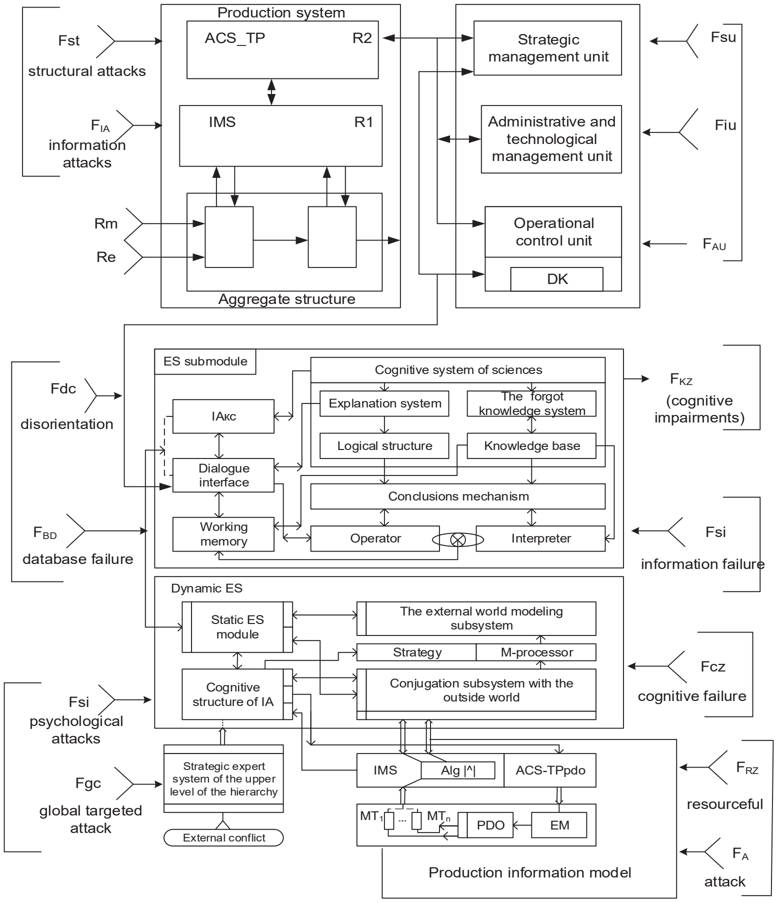

Figure 3 Hierarchy scheme of management systems expert team of the production structure with potentially dangerous aggregated infrastructure objects.

- experts in assessing situations and identifying indicators of possible types of threats (management, resource attacks, informational and intellectual, logical-systemic, cognitive and psychological);
- experts in strategic management of goal-orientation;
- experts in integration coordination methods in solving integrated infrastructure cyber security problems.

PDO – a potentially dangerous technologically active object (reactor); MT – measuring transducer; EM – executive mechanism; IMS – information and measurement system; ASC-TP – automatic technological process control system; ES – expert system; IA – intelligent agent-expert; IAκc – a team of intelligent expert agents, $\{\tau_i\}$ – factors of active attacks on the ACS system, attacks $\langle F_{b\imath e\ldots}F_{gS}\rangle$ – resource and information.

5.3 Hierarchy of Information and Intellectual Management Support

Hierarchy of information and intellectual support includes the following structures that implement the management process:

- production system structure, which includes the aggregated structure of the management object, the information and measurement system (IMS), the automated technological process control system (ACS-TP) and, accordingly, the three-level system of operational management, administrative technological management and strategic management, which is connected with an expert decision support system;
- expert system structure, which includes the sub-module of logical inference and the sub-module of the dynamic expert system, while the decision-making process is based on the cognitive ordered logical structure of the system of technical sciences and on the logical block (explanation system, logical structure of conclusions construction, knowledge base and knowledge interpreter);
- expert management support structure, the dynamic set of the expert system, the cognitive structure of the intelligent agent as a generator of strategies for targeted decisions, the quality of which depends on the intellectual level of the staff and their creativity while making decisions in extreme situations;
- database and knowledge base about the production process and its structural organization.

Designation for the category diagram of the management process (Figure 4): $\{Ci\}$ – system goals, ACS – automated control system,

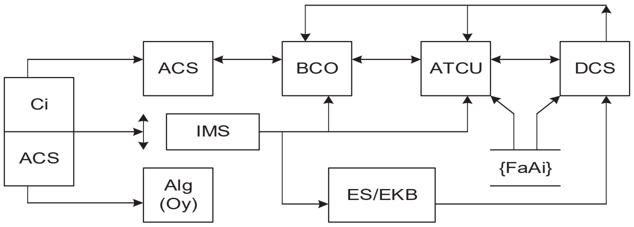

Figure 4 Categorical diagram of the intelligent management process.

BCO – basic control object, ES/EKB – an expert system with a knowledge base for expert assessment of situations, ATCU – object automatic technological control unit, DCS – decision coordination system.

6 Informational and Intellectual Provision of Data Flow Processing for Expert Conclusions About Object Dynamics and Selection of Purposeful Management Strategies

In technological structures, it is impossible to manage processes without data selection, their processing, and in case of incompleteness – replenishment due to the knowledge of experts. Let's consider the expert system functioning stages, the management knowledge base, which is formed due to the totality of knowledge and awareness of production and management personnel, their intellectual actions based on an operations complex (Figure 5):

- Stage 1. Formation of a strategic target task;
- Stage 2. The choice of ES mode strategies for a specific subject area;
- Stage 3. Identification, in which tasks are grouped into classes, that must be solved first of all in order to clarify the target tasks and identify risk factors;
- Stage 4. Conceptualization, during which a meaningful analysis of the subject area related to production technology is carried out;
- Stage 5. Main concepts and their interrelationships are highlighted, methods and strategies for solving problems that arise during the technological process in real time are defined;
- Stage 6. Formalization, i.e. languages for presenting data and tasks, software tools are selected, methods of knowledge presentation are developed;
- Stage 7. The main concepts are being formalized, which ensures the perception of the situation by operational personnel;
- Stage 8. Development of rules for structuring the hierarchical organization of infrastructure.

So, the role of a person is reduced to that of an expert:

- IA_1 – processes data and knowledge of the subject area;
- IA_2 – in accordance with the target task chooses a scheme, procedure, algorithm and strategy for its solution based on the risk factors identification;

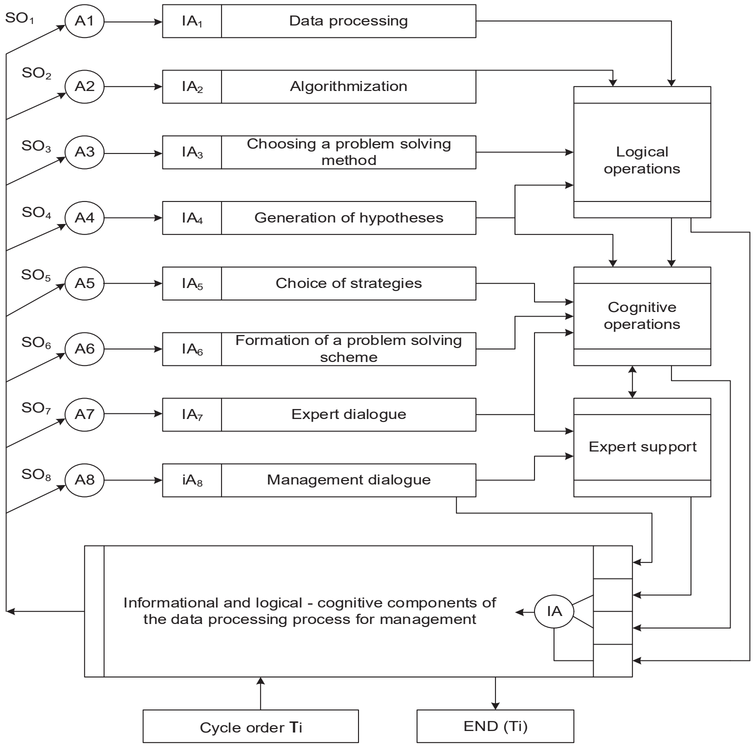

Figure 5 Diagrams of logic-cognitive procedures for processing data from objects using information technologies and a set of system operations (SOi).

- IA_3 – lack of data and incomplete knowledge searches for methods of supplementing their knowledge within the framework of the basic theory;
- IA_4 – based on heuristics, generates hypotheses about problem solving schemes;
- IA_5 – chooses procedures or algorithms according to functioning reference models of the production system and goal-oriented strategies;
- IA_6 – finding the appropriate scheme for solving the task (problem), the expert describes problem area in the form of a set of facts and rules (proof, solution);
- IA_7 – fills ES with new knowledge (as the basis of ES self-learning process);
- IA_8 – transmits data to operational personnel for decision-making.

- Accordingly, the appropriate stages of searching for a method of solving management problems in dialog mode are developed with the appropriate sequence, to the target task and the problem situation;
- IA_9 – generation of strategic and local goals for infrastructure functioning.
- R1 – ES client consultation mode – IA: during the operator-intelligent agent dialogue (IA) with ES, the solution of the problem in the subject-oriented area is provided, using the formed knowledge base and DB, ES, and situational data of a certain level of reliability;

ES awareness mode of its own essence of the cognitive component through self-testing includes decision-making procedures based on logical explanation schemes, scheme mechanisms, proof procedures when solving test problems (self-diagnosis) in the structure of the production system – a system involved in strategic management.

Main concepts are laid out in diagrams according to the target task of sustainable goal-oriented infrastructure management:

Table 1 Compliance of system characteristics with the requirements of given integration in the management system

	Integration Requirements		Integration Signs
	1. Targeted integration		
V 1.1	All-factor goals determination	V2.1	The goals disposition takes into account internal and external factors influencing their determination
V 1.1a	Non-contradiction and compatibility of goals	V2.1a	Objectives are structured as a result of decomposition
	2. Functional integration		
V 1.2	Functions coordination with management goals	V2.2	The functional system structuring corresponds to the target based on the decomposition
V 1.2a	Management functions duplication elimination	V2.2a	Management functions completed collapse
	3. Organizational integration		
V 1.3	Consistency of the organizational management structure with the target and functional structures	V2.3	In the system organizational elements (in subdivisions, subsystems), goals are fixed, management functions are localized, and target and functional tasks are defined.

(*Continued*)

Table 1 Continued

	Integration Requirements		Integration Signs
V 1.4	Regulation and inter-element coherence of actions in the management process.	V2.4	The distribution and consolidation (coordination is taken into account) of the actions organizational elements which are being performed in decision-making processes and implementation of them in the management system has been carried out.
V 1.5	Ensuring the throughput of control system elements	V2.5	The distribution of the load on the system elements is optimized
V 1.6	Resistance of the management system to destructive influences	V2.6	Control over the system integration parameters has been established and countermeasures against disintegration has been developed
4. Cognitive procedural activation			
V 1.7	Changes update during system functioning	V2.7	Procedures for self-regulation and system reengineering, taking into account the controlled parameters of integration, have been developed
V 1.8	Professional and cognitive qualities of developers and implementers of integrated solutions	V2.8.	Professional compliance and cognitive compatibility of personnel are achieved, which makes it possible to make and implement integrated decisions.
5. Information integration			
V1.9	Consistency of the information structure with target, functional, organizational structures ("info-structural" positioning)	V2.9	The information structure ensures the concentration and localization of information in the elements of the target, functional, organizational structures
V1.10	Information shared use in the management system	V2.10	Availability of a single information database corresponding to the functional management needs
V1.11	Elimination of unnecessary duplication of information in the management system	V2.11	The minimum necessary level information duplication

(*Continued*)

Table 1 Continued

	Integration Requirements		Integration Signs
V1.13	Information compatibility in elements of the management system	V2.13	Transformation of non-uniform information into uniform information for data comparison is provided
V1.14	Information aggregation about activities progress and results, management system state	V2.14	Availability of accounting methods, data synthesis and generalization means about system functioning
	6. Economic integration		
V1.15	Business entity management system structures and economic performance indicators consistency	V1.15	Economic effect indicator and effect-forming indicators are structured in accordance with management system structure and applied management concept and are representative for determining of economic entity state
V1.16	Integration risks assessment	V 2.16	System of economic indicators is hierarchically arranged, vertically and horizontally positioned and acceptable for economic performance coordinated management
V1.17	Ensuring actions economic expediency in the management process to achieve economically efficient performance of business entity	V2.17	Available methods and means of actions intellectualization (“knowledge economy”) for economic justification of management decisions regarding the impact on the economic effect and business entity state
	7. Instrumentally – applied management integration		
V1.18	Penetration of the management process by management levels on the basis of unification and standardization of information transformation processes	V2.18	Typicality, modularity and non-duplication of information technologies have been achieved
V1.19	Security of information storage and transformation processes. Compatibility of decision-making and implementation processes	V2.19	Available information control and protection means and processes of its transformation

(*Continued*)

Table 1 Continued

	Integration Requirements		Integration Signs
V1.20	Possibility of conflicts	V2.20	Available information technologies means for designing solutions, from monitoring of their implementation on a single design database and execution information with the use of unified information and process technologies

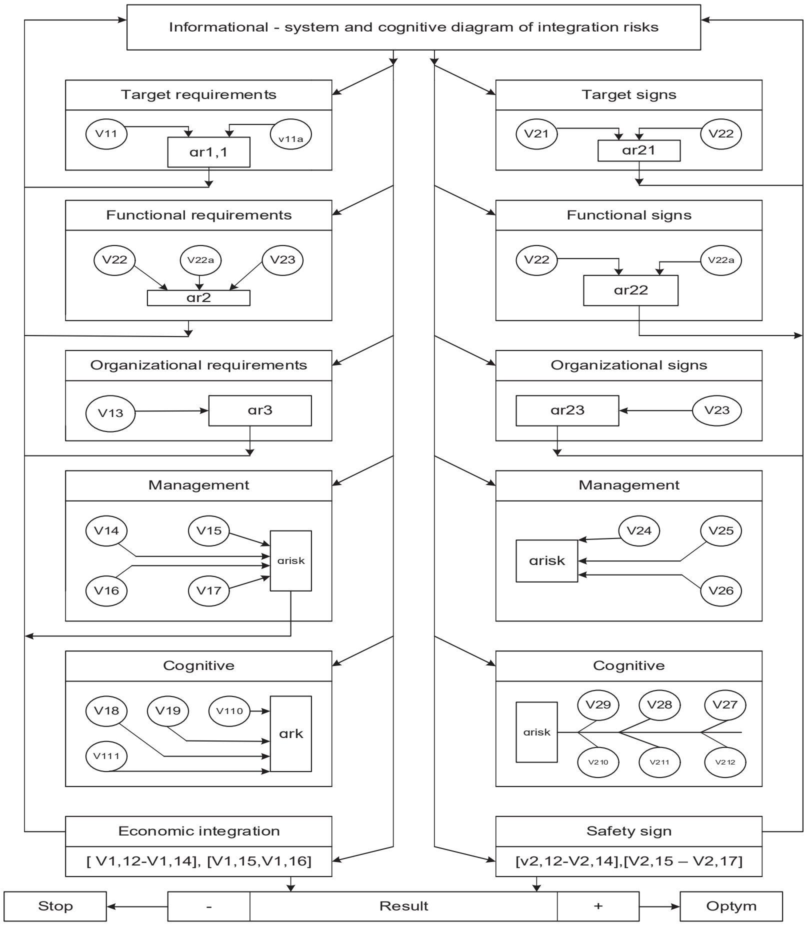

Figure 6 Uncoordinated requirements risks scheme for system integration.

Positions (Vij) – information requirements components and infrastructure integration features.

On the basis of above table, which was developed by a team of experts who meet the qualification requirements that ensure the system integration procedures at all levels, let's build a categorical risks scheme that arise in the event of errors in the integration procedure. Since systems of a hierarchical type in sense of structure of resource and financial opportunities management strategy are not homogeneous, it is difficult to ensure management efficiency from the point of view of possibility of forming management teams that would be non-conflict and professionally homogeneous. This would make it possible to ensure conflict-free management activities in the conditions of threats based on the definition of a team leader.

Possible risks assessment of complex state based on activity type combination and integration degree is based on Table 2, which is formed by expert analysis in real time of production and events in external environment in competition conditions.

Table 2 Complex state possible risks assessment based on a combination of the activity type and the integration degree

State Type	Activity Effect Change	Degree Integration Change	Complex State Components Evaluation	
			Economic Condition	Integration State
1	2	3	4	5
1.1	$\alpha_{r1} < \alpha_d$	$\alpha_{r1} < \alpha_d$	Planned and achieved	Planned and achieved
1.2	$\alpha_{r2} \leq \alpha_d$	$\alpha_{r2} < \alpha_d$	Weakened state for previously achieved planned integration state	Achieved as planned, but with a caveat about hidden disintegration
1.3	$\alpha_{r3} \leq \alpha_d$	$\alpha_{r3} \leq \alpha_d$	Reinforced state for planned integration state	Effective achieved planned state
1.4	$\alpha_{r4} = \alpha_d$	$\alpha_{r4} > \alpha_d$	Planned state in weakened integration state conditions	Weakened state with clear disintegration, which in general did not affect the economic state
1.5	$\alpha_{r5} \geq \alpha_d$	$\alpha_{r5} \geq 2\alpha_d$	Planned state under a weakened integration state	Weakened state with clear disintegration, which negatively affected the economic state

(*Continued*)

Table 2 Continued

State Type	Activity Effect Change	Degree Integration Change	Complex State Components Evaluation	
			Economic Condition	Integration State
1	2	3	4	5
1.6	$\alpha_{r6} \leq \alpha_d$	$\alpha_{r6} \leq 2\alpha_d$	A strengthened state in conditions of weakened integration state	Weakened state with clear disintegration, which did not prevent strengthening of economic state
1.7	$\alpha_{r7} < \alpha_d$	$\alpha_{r7} < 0,5\alpha_d$	Planned state under enhanced integration state	Strengthened state, which did not ensure economic state strengthening
1.8	$\alpha_{r8} \geq 3\alpha_d$	$\alpha_{r8} \to \max$	Weakened state with ineffective strengthening of integration state	Strengthened state that negatively affected the economic state due to hidden disintegration
1.9	$\alpha_{r9} \leq 0.5\alpha_d$	$\alpha_{r9} \to \min$	Enhanced state in the conditions of enhanced integration state	Strengthened state, which had a positive effect on the economic state

7 Conclusion

According to the target task of developing methods for solving infrastructure cyber security problems, the following were completed:

- Literature sources analysis on the issues of man-made infrastructure cyber security, resistance to attacks and recovery in the conditions of threats;
- Tasks that need to be solved to ensure the attack and threats management system countermeasures to the infrastructure and the system itself, the target management strategy were substantiated;
- Cognitive principles of information support necessary for the creation of active countermeasures strategies against attacks on the management structure based on coordination strategies and goal orientation were substantiated;

- An expert analysis of emerging situations in the event of threats was conducted and an operations diagram for detecting and countering attacks was constructed;
- Data flow processing methods information provision for determining the sign indicators by an expert system as the strategy basis for countering threats was substantiated;
- Process of interaction between operational and target, cognitive and automated decision-making levels of the management hierarchy was analysed;
- System concept of integration processes and coordination structure of goal-oriented management was substantiated.

Solving the above problems at the system and information level can help modernize the existing infrastructure and improve their design process to increase complex cyber security level.

References

[1] Ponomarenko, V.S. (2002) *Information systems and technologies in the economy.* Kyiv: Academy, 542 p.

[2] Konstantinov, S.M., Ponomarenko, Yu.L. (2010) *Information technologies of modern enterprise management.* Lviv: UAoP, Vol. 1., 368 p.

[3] Kondratyev, V.V. (1989) *Large systems: Modeling of organizational mechanisms.* Moscow: Science, 245 p.

[4] Hettmanserger, T. (1985) *Statistical inference Based on Ranks.* New York: 2ws, 335 p.

[5] Muschik, E., Muller, P.H. (1990) *Entschidun gspraxis.* Berlin: VEB Verlog Technik, 206 p.

[6] Davison, M. (1988) *Multidimensional scaling.* New York: IWss, 253 p.

[7] Barankevych, M.M. (2008) *Expert methods in decision-making.* Lviv: LNU, 214 p.

[8] Belz, O. (2009) *Economic expert systems basics.* Lviv: LNU, 238 p.

[9] Erina, A.M. (2004) *Statistical modeling and forecasting.* Kyiv: Academy, 170 p.

[10] Sikora L., Tkachuk R., Lysa N., Dronyuk I., Fedevych O., Talanchuk R. (2021) "Information-resource and cognitive concept of threat's influence identification on technogenic system based on the cause and category diagrams integration" in *Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information*

Security 2021, CEUR Workshop Proceedings 2853, CEUR-WS.org, 398–416.

[11] Sikora L., Tkachuk R., Lysa N., Dronyuk I., Fedevych O. (2020) "Information and logic cognitive technologies of decision-making in risk conditions" in *Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security 2020*, CEUR Workshop Proceedings 2623, CEUR-WS.org, 340–356.

[12] Hovorushchenko T., Pavlova O. (2019) "Method of activity of ontology-based intelligent agent for evaluating the initial stages of the software lifecycle" in *Recent Developments in Data Science and Intelligent Analysis of Information 2019*, Springer International Publishing 836, 169–178.

[13] Sikora L., Tkachuk R., Lysa N., Dronyuk I., Fedevych O., Navutka M. (2020) "Information technologies of formation of intellectual decision-making strategies under conditions of cognitive failures" in *Proceedings of the 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems 2020*, CEUR Workshop Proceedings 2805, CEUR-WS.org, 233–254.

[14] Demri, S., Goranko, V., Lange, M. (2016) *Temporal logics in computer science.* Cambridge: Cambridge University Press, 752 p.

[15] Lyugger, Dzh. F. (2003) *Artificial intelligence: strategy and methods of solving complex problems.* Moscow: Williams, 864 p.

[16] Khoroshchko V., Bobalo B., Dudykevych V. (2020) *Complex information protection systems design.* Lviv: LPNU Publishing, 320 p.

[17] Tsypanov V., Bukharin S. (2007) *Information wars in business and politics.* Moscow: Academic Project, 336 p.

[18] Mykytyn H., Dudykevych V., Bobalo Yu. (2019) *Strategic security of "object – information technology" system.* Lviv: LPNU Publishing, 580 p.

[19] Vendrov A. (2000) *Software design of economic information systems.* Moscow: Finances and Statistics, 352 p.

Biographies

Liubomyr S. Sikora received the bachelor's degree in trunk communication from Lviv Telecommunications Technical School of USSR Ministry of Communications in 1963, the master's degree in automation, telemechanics from Lviv Polytechnic National University in 1975, and the philosophy of doctorate degree in Information and Measurement Systems from USSR Academy of Sciences Institute of Physics and Mechanical Sciences in 1992, as well as Doctor of Technical Sciences from Ukraine Academy of Sciences State Research Institute of Information Infrastructure in 2001 respectively. He is currently working as a Full Professor at the Department of Automated Control Systems, Institute of Computer Science and Information Technologies, Lviv Polytechnic National University. His research areas include integrated hierarchical control systems, digital signal processing, management activity cognitive components, information technologies in complex systems.

Nataliia K. Lysa received the master's degree from Ivan Franko Lviv National University in 1994, the philosophy of doctorate degree in Information Technologies from Lviv Academy of Printing in 2012, and her Doctor of Technical Sciences from Lviv Academy of Printing in 2019 respectively. She is currently working as an Associate Professor at the Department of

Automated Control Systems, Institute of Computer Science and Information Technologies, Lviv Polytechnic National University. Her research areas include web cyber security, trend forecasting and process modelling analysis, information and telecommunication management technologies, information technologies in ecology and medicine.

Yevhen I. Tsikalo received the master's degree in economic information mechanized processing organization from Ivan Franko Lviv National University in 1975, and the philosophy of doctorate degree in Mathematical Methods and Application of Computer Technology in Economic Research, Planning and Management of the National Economy and its Branches from Ivan Franko Lviv National University in 1989. He is currently working as an Associate Professor of the Department of Accounting and Auditing at Ivan Franko Lviv National University. His research areas include integrated enterprise management technologies, mathematical methods and application of computer technology in economic research.

Olga Yu. Fedevych received the bachelor's degree in computer science from Lviv Polytechnic National University in 2013, the master's degree in computer science from Lviv Polytechnic National University in 2014, and the philosophy of doctorate degree in Information Technologies from Lviv Polytechnic National University in 2018, respectively. She is currently working as an Associate Professor at the Department of Automated Control Systems, Institute of Computer Science and Information Technologies, Lviv Polytechnic National University. Her research areas include web cyber security, trends forecasting, and process modelling analysis. She has been serving as a reviewer for many highly-respected journals.