Infrastructure Cybersecurity under Complex Man-Made Threats Conditions

Liubomyr Sikora[1], Nataliia Lysa[1], Olga Fedevych[1], Bohdana Fedyna[2]

[1]*Lviv Polytechnic National University, 12 Bandera Str., Lviv, 79013, Ukraine*
[2]*Ukrainian academy of printing, 19 Pid Goloskom Str., Lviv, 79000, Ukraine*

Abstract

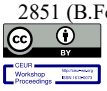
Making and implementing decisions in complex hierarchical systems, as a procedural part of management activity, has an applied nature, which is manifested in the performance of actions to respond to and influence threat factors on object, within the boundaries of relationship between management subject and object. In this context, the control system is provided by auxiliary computerized human-machine decision support systems (subsystems) that help intelligent agents perform decision-making actions and react to results of decision implementation. For effective adaptation and development of these systems, it is necessary to have a complete decision-making and implementation system. In the latter, there will be applied informational and algorithmic support for decision-making procedures implementation based on decision-making and implementation mechanism, taking into account management system integration, as a prerequisite for effective management of hierarchical systems. Such a complex need determines the necessity to develop the conceptual structure of the mechanism in connection with the decision-making and implementation system on the integration basis of building a management system.

Keywords

Cyber security, attacks, system, management, cognitive models, information technologies, strategies, risks, goal orientation, hierarchy.

1. Introduction

The decision-making and implementation mechanism is used based on the structure of hierarchical management system and its integration basis. Management system structure is represented by hierarchical system's composition and connections of the subsystems, which are based on information integration, in combination with other types of integration. Such a structure will be superimposed on the structure of mechanism itself, represented by composition and connections of components that embody the rules of managing a complex system through the processes of making and implementing management decisions. Therefore, integration concept

CITRisk'2022: 3rd International Workshop on Computational & Information Technologies for Risk-Informed Systems, January 12, 2023, Neubiberg, Germany
EMAIL: lssikora@gmail.com (L.Sikora); lysa.nataly@gmail.com (N.Lysa); olha.y.fedevych@lpnu.ua (O.Fedevych); fedynabogdana@gmail.com (B.Fedyna)
ORCID: 0000-0002-7446-1980 (L.Sikora); 0000-0001-5513-9614 (N.Lysa); 0000-0002-8170-3001 (O.Fedevych); 0000-0001-9487-2851 (B.Fedyna)


mechanism will involve combination of components on the structural-base model of integrated control system design.

2. State of the art

Management solution for managing a hierarchical system is an intelligent product created and used by the management system. Intellectual activity of this kind involves information operation about object characteristics with use by management subject of information-knowledge about the rules of operation, which explain how to influence or refuse to influence the object. That is, management is carried out through the information presentation of both the object and the subject's actions, taking into account the structure of a complex system with a hierarchical organization and various causes of emergency situations. Such situations can arise in the event of external threats and attacks on the object, and also in the preparation of project documentation, mistakes may be made during their development. Accordingly, active attacks, failures, malfunctions (reduction in system reliability and resources) can lead to a failure of the object's functioning. Also, one of the main reasons that can lead to a disaster and emergency situations in the facility's operation system is the intellectual and cognitive errors of the operational staff, which leads to its informational and target disorientation.

In accordance with goals that functioning system sets for itself, it is necessary to form requirements for its reliability and functionality of ACS (Automated Control System) units, management structure. Cybersecurity of a hierarchical structure is an urgent problem today, which includes information and intellectual support in the formation of adoption and implementation of purpose-oriented decisions in the conditions of threats, resource and structural and other types of attacks on infrastructure.

2.1. Related works

Works [1,2] are devoted to the problems of building procedures for making effective management decisions in technical and economic systems. Work [3] is devoted to large systems organization theory, in which the basic models of structure construction, functioning models, open management strategies, resource and strategic games, effective design problems are considered. Data processing methods, classification and forecasting methods as the basis for the formation of decision-making process are considered in [4,6]. Expert systems theory methods for use in complex systems in management decisions formation are considered in [7,8,9]. The theory of coordination in management processes is considered in [12-15]. Cognitive technologies for situation assessing are described in [21], risk models in [10,11] and the use of artificial intelligence and big data analysis in [16-20] accordingly.

2.2. Research purpose

On the basis of system analysis and their information and logic-cognitive technologies, determine and justify indicators for identifying the causes of crisis and emergency situations in complex man-made integrated systems with hierarchical infrastructure when threats and attacks affect process and management goals, which is necessary to ensure effective methods of countermeasures and high cyber security level.

2.3. Research object

Hierarchical system, goals and dynamics of complex man-made systems in a complex of spatially distributed integrated production facilities.

3. Main results

3.1. Complex man-made system coordination processes between infrastructure hierarchy levels as a method for increasing resistance to attack actions

Analysis of complex ACS-TP systems developed during the (3-4) development stage of information and management technologies, which were used in complex production energy-active complexes with a continuous process, showed that at the current stage they do not meet the requirements for ensuring resistance to attacks of the system approach at their design.

Number of tasks that were solved in the management process was large, but the inconsistency of methods of solving technical, functional, algorithmic and organizational tasks and the procedures for their solution complicated the process of goal-oriented management due to the complexity of harmonizing technological requirements, management methods, data processing tools and decision-making strategies in the conditions of threats and information attacks.

Main reason for the low level of management efficiency in the event of resource and information threats at different levels of the hierarchy was that the behavior of operative personnel at different management levels was not coordinated with the production infrastructure possibilities and resources provision.

3.2. Man-made systems integration processes into complex strategic-level infrastructure for effective countermeasures against threats

At the fourth stage of the development of energy-active objects complex management systems in production management continuous process, to the fullest extent arose the need to combine individual automated systems and subsystems of the infrastructure into a complex goal-oriented system based on information and intellectual technologies.

A complex integrated infrastructure with a management system, which is oriented towards strategic goals, includes and will combine into a single the next goals:

- $\{MO_i /_{i=1}^{n}\}$ - management objects of passive and active type;
- $\{(\text{ACS - TP})_{i=1,n}\}$ - automatic facility management systems;
- $\{ACYI_n\}$ - automated systems with a hierarchical management structure;
- $\{\text{IIASC}_\text{R}\}$ - information intelligent management systems with coordinating management strategies;

- $\{\mathrm{DSS_R}\}$ - decision support systems with coordination and expert technologies to counter attacks and active threats;
- $\{OCIC_Y\}$ - operational systems of intellectual, cognitive and creative management;
- $\{RSU_{pi}\}$ - technological flows resource management systems;
- $\{SE_Z\}$ - environmental protection systems.

The theoretical foundations of such systems construction are considered in fundamental works [3, 11-15, 19-21].

On the basis of the conducted research, a structural-functional scheme of production structures coordination-integration game into infrastructure was developed based on agreement of global goal (Fig. 1.)

Markings on Fig. 1.:

- FR_m - factors affecting the ecosystem - material;
- FR_E - factors of energy impact on the environment;
- CF_Z - strategy of environmental protection systems;
- GG_i - global infrastructure goals;
- $GCiU$ - management goals at the operational level;
- CUS - goal oriented management of production system;
- $F(AtakCi)$ -attacks factor on the entire system – operational level;
- $I(Strat)$ - systems integration strategy at the upper level;
- $Strat(SKCi)$ - management coordination strategy according to the goal;
- $\{OYi\}$ - management objects (active passive conversion, mixed type);
- $\{Di, Dn\}$ - information and management – executive data flows;
- $\{FRi, FR_E, FR_S\}$ - factors influencing resource flows, energy, structures of the object.
- Integration processes during the structural game take place at the levels of the system hierarchy (SR5, SR6, SR7), coordination of goals and strategies occurs at levels (SR3, SR4, SR5).

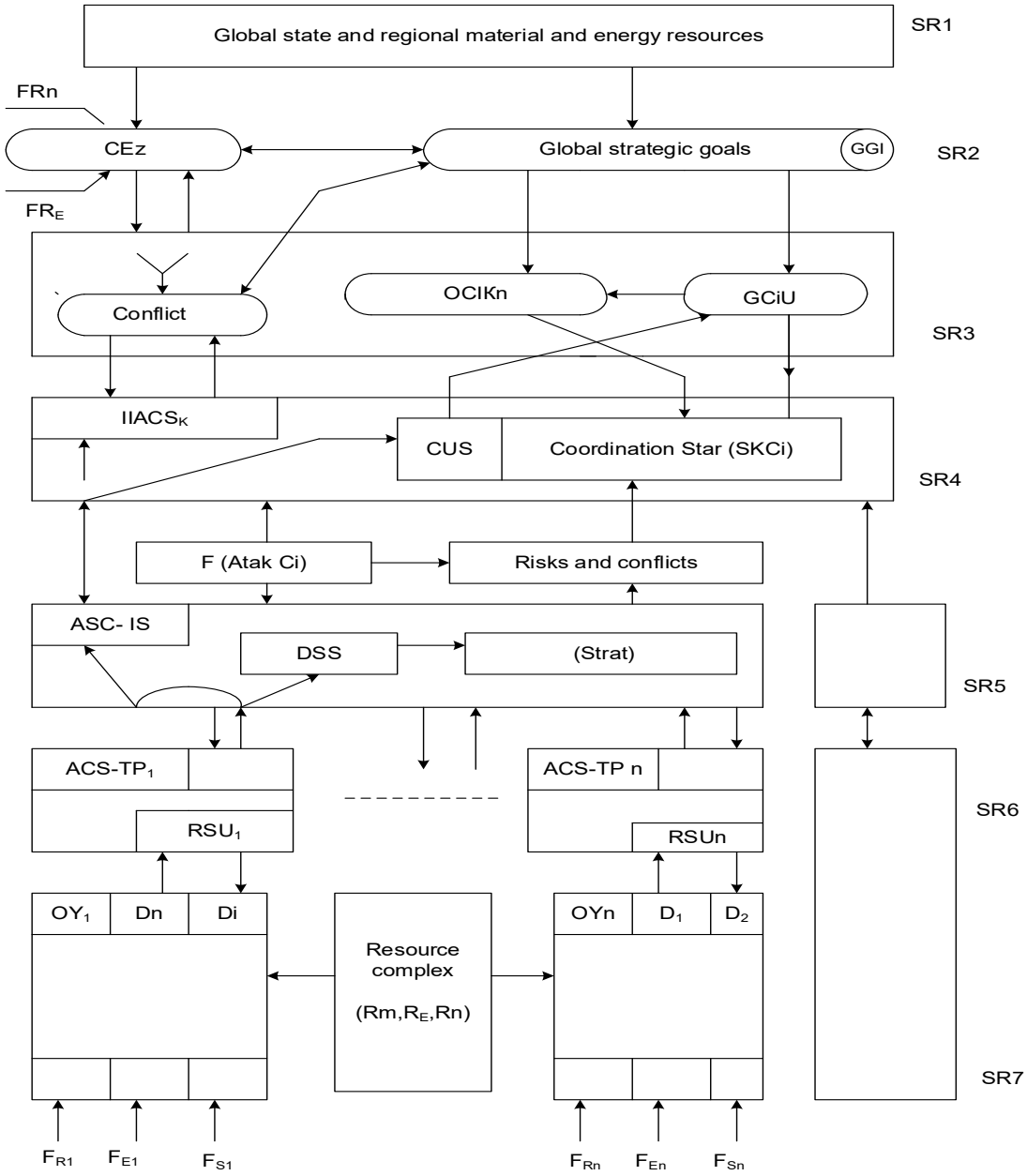


Figure 1: System's coordination-integration game structural-functional scheme

The global game is formed by the participants of ((SR1, SR2, SR3) $\otimes$ SR4) levels on the basis of infrastructure of corporate management goals and strategies agreement, which with full risk probability may be formed.

3.3. Procedures for integrating systems into the infrastructure with goal-oriented management strategies

In order to increase the stability of their infrastructure functioning, it is necessary to perform a constructive component analysis of technological aggregated system capabilities for production infrastructure in interaction with automated control system (human-machine interaction), taking into account intellectual capabilities of managers at all levels of hierarchy and service-operational maintenance. Assess possible risks of failure and shutdown of emergency situations under resource threats conditions and information attacks on goal-oriented management process (Fig. 2.).

Markings on Fig.2.:

- Target requirements: V1.1 - goals definition, V1.1a – goals coordination, V2.1 – internal and external factors affecting goals, V2.1a – structured goals, V1.2 – coordination of goals with management, V1.2a – functioning duplication;
- Functional requirements: V2.2 – functional structuration, V2.2a – management functions;
- Organizational management requirements: V1.3 – structure consistency, V 1.4 – actions coordination, V 1.5 – throughput, V 1.6 – system stability, V2.3 – elements organization, V2.4 – elements fixing, V2.5 – load distribution, V2.6 – control, V 1.7- active actions;
- Cognitive requirements: V 1.8 – professional qualities, V2.7 – regulation, V2.8 – professional compliance, V1.9, V1.15 – consistency, V1.10 – sharing usage, V1.11 – information duplication, V1.13 – information compatibility, V1.14 – information aggregation, V2.9 – information provision, V2.10 - single database, V2.11 – information duplication, V2.13 – information transformation, V2.14 – accounting of method, – consistency, V1.16 – risk assessment, V1.17 – feasibility;
- Management integration: V2.15, V2.16 – indicators, V2.17 – methods, V1.18 – management process, V1.19 – process safety, V1.20 – conflicts occurrence, V2.18 – goals achievement, V2.19 – control means, V2.20 – information technology tools.

To increase robustness of information and management systems, networks and channels of transmission and dial exchange in the management process, under the conditions of information, psychological and cognitive attacks, it is necessary to analyze (both in existing and newly designed) all infrastructure components for stability. At the same time, it is necessary to take into account that components have, according to the type of systems and dynamics functions $\left\{ \forall x_{ij} \in X_i ; \exists y_{ik} \in Y_K ; X_i \xrightarrow{A_{ij}} Y_y \mid C_i \right\}$ and displaying actions $\left\{ A_{ij} \right\}$ in the target area defined at strategic level.

Interaction between systems during the integration process can take place between energy-active, informational, resource and management infrastructure components.

Decision-making levels:

- V_1 - (object - control) – (control $\left(OY_i \xrightarrow[A_i]{\xleftarrow{Si}} BM_i \right)$);

- V_2 - (object - control) – (resource source $\left(OY \xleftarrow{Ai} \Pi R_i \mid \Pi R_i \subset D\,\mathrm{Re}\,s \right)$);
- V_3 - (object - control)– (information system $\left(OY_R \xrightarrow{K} IBC \right)$);
- V_4 - (information system) – (system (ACS-TP) management $\left(OY_R \xrightarrow{S} IBC \xrightarrow{Di} SUi \right)$);
- V_5 - (ASC-TP) – (operational management system $(KRIAi)$ with operational cognitive agents team).

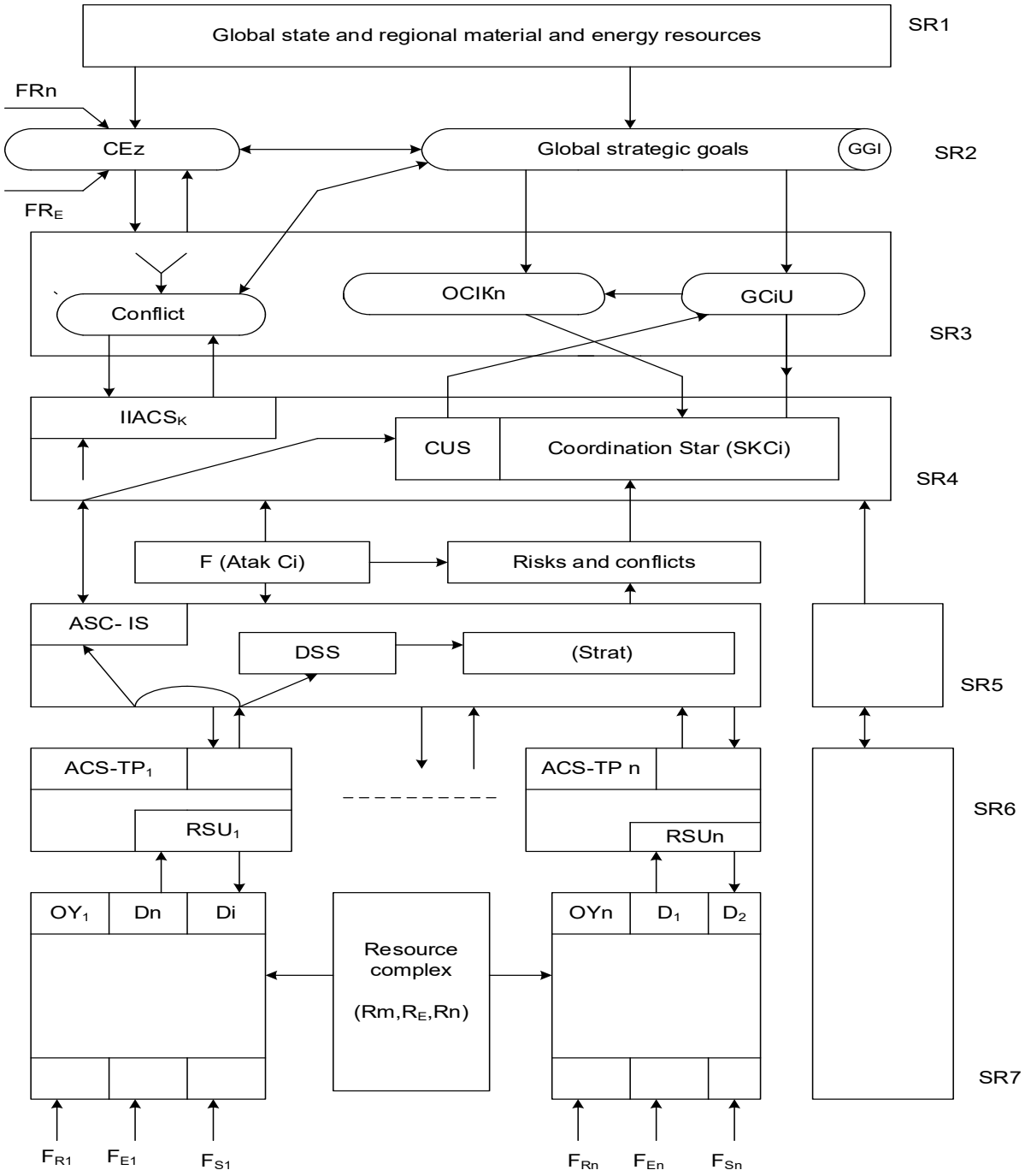


Figure 2: Risks scheme in the event of uncoordinated requirements for system integration

The interaction and integration game concept of infrastructure, between production, information, management type subsystem is the basis for describing process of active countermeasures against threats.

If take into account that management structure includes an automatic system for implementation of object management process (ASU-TP-ASU) and a team of management operators (cognitive agents) so behavior of such a structure has a high risk of failure under threats influence.

Accordingly, let's provide a list of active threat attacks on the man-made system, both internal and external (Table 1).

Table 1

Active threats and attacks on man-made systems

№	Type of threats	α_r
1.	Threats and information-intelligent attacks on infrastructure destruction.	0,01-0,95
2.	Target threat structures to block technological process.	0,01-0,3
3.	Resource attacks to disrupt technological process.	0,01-0,2
4.	Information attacks in the data transmission network to distort situation image in object.	0,1-0,5
5.	Structural attacks on production system organization.	0,1-0,35
6.	Complex attacks on ACS – TP.	0,01-0,95
7.	Attacks on target disorientation.	0,5-0,75
8.	Attacks on hierarchy of authority.	0,5-0,9
9.	Strategic management attacks.	0,6-0,95
10.	Attacks on processor systems of ACS control complex.	0,5-0,95
11.	Attacks on changing of energy-active objects mode.	0,01-,3
12.	Information-mental attacks on personnel to change stress resistance and goal orientation.	0,3-0,9
13.	Complex attacks on hierarchical management structure and internal	0,01-0,2

	conflicts.	
14.	Attacks on complex destruction of man-made system.	0,01-0,95

In accordance with situation in external and internal infrastructures, let's form a target integration process (Fig. 3).

Markings on Fig. 3.:

- $\left\langle F_{I}, F_{Z}, F_{c} \right\rangle$ - active influence factors on information, knowledge, goal-oriented factors of integration process.
- System $OY\left(RIAi \mid_{s=n,1} \right)$ - operational administrative management system $\left(\left\langle KIA_{i} \mid_{i=1,n} \right\rangle \xrightarrow{Di} \left\langle A \cup U_{K} \right\rangle \right)$;
- Strategic goal-oriented management system with all levels of infrastructure hierarchy $\left\langle э\ Koord\left(Strat\left(U \mid Ci\right)\right) : \left\langle SStratCu \right\rangle - Leve \cup IS \right\rangle$ on the basis of goal-oriented coordination management.

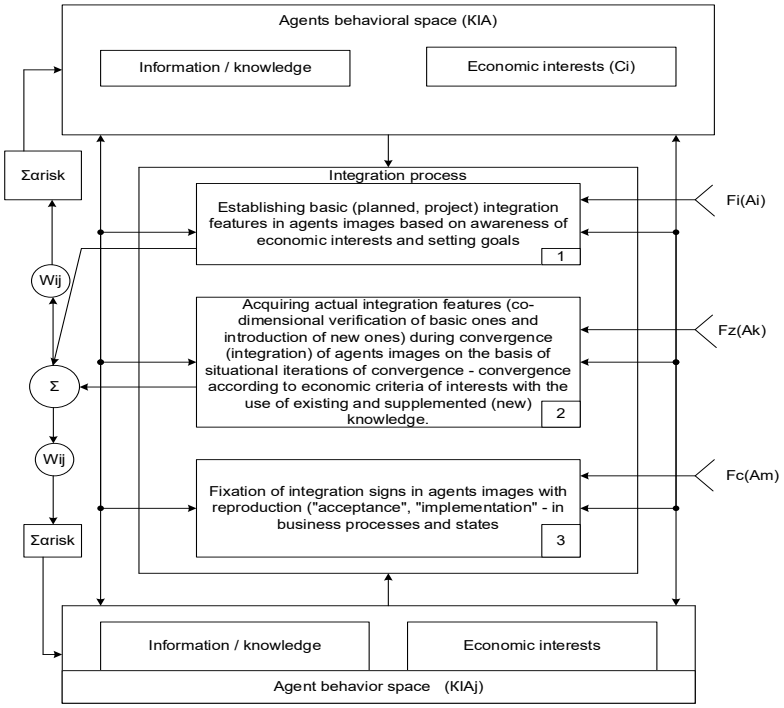


Figure 3: Implementation of an active integration process in systems structure in information interaction conditions of strategic level cognitive intellectual agent's teams

Main strategic management goal is the development of sustainable self-renewing methods process of production based on strategies of overall orientation, integration, and coordination under the conditions of active overall oriented threats.

Table 2

Infrastructure integration risk assessment

№	Component integration	CF	BD	αr_1	αr_2	αr_3
1.	goal orientation (V_{11}, V_{21})	<0.5	>0.9	0.85	0.8	>0.8
2.	there is no agreement of goals (V_{11}, V_{12})	0.95	0.9	>0.9	>0.9	>0.9
3.	goals and strategies coordination (V_{12}, V_{22})	0.95	0.85	<0.1	<0.2	0.15
4.	structure goal orientation (V_{12a}, V_{22a})	>0.8	>0.7	>0.2	>0.25	>0.3
5.	management's goal orientation (V_{13}, V_{23})	0.95	>0.9	<0.1	<0.15	>0.2
6.	management tactics (V_{14}, V_{24})	0.85	>0.95	<0.15	<0.1	<0.2
7.	management tactics dynamics (V_{15}, V_{25})	0.7	0.7	<0.2	0.3	<0.3
8.	resistance to attack factors (V_{16}, V_{26})	0.8	0.82	<0.3	<0.35	>0.35
9.	mode indicators analysis (V_{17}, V_{27})	0.83	0.85	<0.3	<0.3	<0.4
10.	integration project team	0.9	0.95	0.1	0.15	<0.2

11.	cognitive level (V_{18}, V_{28}) n-system structural integration generalized risks	$\mu_n(CF)$ $(0.7 \div 0.9)$	$\mu_n(Bd)$ $(0.7 \div 0.9)$	$\Pr ob$ $\alpha r_1(0.1 \div 0.9)$	$\Pr ob$ $\alpha r_2(0.1 \div 0.9)$	$\Pr ob$ $\alpha r_3(0.1 \div 0.4)$

3.4. Risks analysis in man-made systems

To analyze risks in man-made systems and build schemes and methods for their minimization and management, it is necessary to apply the risk analysis methodology, which is based on four components:

1. Risk factors source, structure models.
2. Scenarios of active actions and effects of factors on system functioning process.
3. Analysis of action results of active factors on system.
4. Attacks generators and activators.

Risk source is related to consequences of active actions through the scenario - a chain of events related to risk implementation in system, under certain conditions, which leads to negative consequences and accidents.

Chains, paths are actually development scenarios of a dangerous situation from the point of view of different positions and describe what can happen to system under action of active factors generated by risk source.

4. Conclusion

According to target task of developing methods for solving infrastructure cyber security problems, it has been completed:

- Analysis of the literature sources on man-made infrastructure cyber security, issues resistance to attacks and recovery in threats conditions;
- Tasks that need to be solved to ensure counteraction of attack management system and threats to infrastructure and system, target management strategies are substantiated;
- Cognitive principles of information provision necessary for creation of active resistance strategies to attacks on management structure based on strategies of coordination and overall orientation are substantiated;
- Information provision data flow processing methods for determining indicators of signs by an expert system as of countering threats strategy basis is substantiated;
- Interaction process between operational and target, cognitive and automated decision-making levels of management hierarchy was analyzed;

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

References

[1] V.Ponomarenko, Information systems and technologies in economics, Kyiv, Academy, 2002

[2] S.Konstantinov, Yu.Ponomarenko, Modern information enterprise management technologies, Lviv, UAP, 2010

[3] V.Kondratiev, Large systems: Modeling of organizational mechanisms, Moscow, Science, 1989

[4] T.Hettmanserger, Statistical inference based on ranks, New York, 2ws, 1985

[5] E.Muschik, P. Muller, Entschidun – gspraxis, Berlin VEB Verlog Technik, 1990

[6] M.Davison, Multidimensional scaling, New York, IWss, 1988. DOI:10.1016/S0169-7161(03)22018-6

[7] M.Barankevych, Expert methods in decision making, Lviv, PC LNU named after I. Franko, 2008

[8] O.Belz, Basics of economic expert systems, Lviv, LNU, 2009

[9] A.Erina, Statistical modeling and forecasting, Kyiv, 2004

[10] L.Sikora, N.Lysa, R.Tkachuk, O.Fedevych, J.Krejčí, Cognitive and information decision-making technologies and risk assessment in technogenic systems in: Proceedings of the 2nd International workshop on computational & information technologies for risk-informed systems CITRisk 2021, Kherson, Ukraine, 2021, pp. 419-433

[11] J.Fesl, L.Tupychak, L.Sikora, N.Lysa, R.Tkachuk, O.Fedevych, Information technologies for operational staff training for man-made systems under threats and risks in: Proceedings of the 2nd International workshop on computational & information technologies for risk-informed systems CITRisk 2021, Kherson, Ukraine, 3101, 2021, pp.374-387

[12] Yu.Kunchenko, Polygons of approximation in space with a generating element, Kyiv, Science thought, 2005

[13] S.Demri, V.Goranko, M.Lange, Temporal Logics in Computer Science, Cambridge, Cambridge University Press, 2016. DOI:10.1017/CBO9781139236119

[14] F.Lyugger, Artificial intelligence: strategy and method of solving complicated problem, Moscow, Wiyams, 2003

[15] Mi.P.Groover, Automation, production systems, and computer-integrated manufacturing, Prentice Hall Press, 2007

[16] I.Hawryszkiewych, Introduction to system analysis and design, New York, 2000

[17] A.Miele, J.Damoulakis, J.Cloutier, J.Tietze, Sequential gradient-restoration algorithm for optimal control problems with nondifferential constraints, JOTA, 2, 1974, p.13

[18] W.Lynn III, Defending a new domain: the Pentagon's cyberstrategy, Foreing Affairs, 2010

[19] K.Mitnik, W.Simon, S.Wozniak, The art of deception, New York, Wiley, 2002

[20] P.Neumann, Computer-Related Risk, ACM Press/Addison Wesley, New York, 1995

[21] L.Sikora, N.Lysa, R.Tkachuk, V.Sabat, O.Fedevych, Information technology of risk assessment for automated control systems of printing production in: Proceedings of the 2nd International workshop on computational & information technologies for risk-informed systems CITRisk 2021, Kherson, Ukraine, 3101, 2021, pp. 404-418