Information Technologies of Active Control of Complex Hierarchical Systems under Threats and Information Attacks

Volodymyr Sabat[a], Lyubomyr Sikora[b] Bohdan Durnyak[c], Olga Fedevych[b], Natalia Lysa[b]

[a] *Ukrainian Academy of Printing, 19, Pid Holoskom St., Lviv, 79020, Ukraine*
[b] *National University «Lviv Polytechnic», 12, Stepan Bandera St., Lviv,, 79000, Ukraine*
[c] *Ukrainian Academy of Printing, 19, Pid Holoskom St., Lviv, 79020, Ukraine*

Abstract

The effect of active information, system and resource threats on the printing technology structure with a hierarchical organization of production is complex, and therefore the identification of influence channels and methods of countering attacks is an important challenge. In order to solve problems of this type, it is necessary, in accordance with the hierarchical structure, to separate the processes of technological, informational, managerial and actual preparation of the printing production product. Accordingly, the primary threats can be made at the stage of document design (content distortion). Information threats and system attacks on the management of the production process have a complex structure and their detection is an important task, as it is necessary to identify sources of threats, channels of attacks and assess the level of risk if attacks occur.

According to the protection tasks analysis, the structural scheme of decision-making in technical and publishing systems is substantiated and developed. On the basis of the decision-making process studies, the model of man-made structure under threats on ACSPP resources is constructed.

Keywords

Threats, attacks, control of hierarchical systems

1. Introduction

The emergence of various situations dangerous to municipal structures, man-made system and the environment is objectively characterized by many interdependent factors, independent disturbances and threats that cause crises, emergencies and catastrophic situations, which accordingly complicates decision-making for control with limited information and material and energy financial resources. Practice shows that problematic situations arise and proceed with different dynamics provoked by threats and disturbances, incorrect management at the upper and middle levels of the hierarchy of automated human-machine systems and complexes (AHMS and C), as well as in the social environment of cities.

In printing production, two basic structures can be distinguished - the information system of document preparation (electronic version) on the basis of a text document and the production system, which provides the appropriate product quality according to the target order. These structures can be attacked in series and in parallel, depending on the strength of the information attack and strategic goals, which may be long-term. For this purpose, the basic structural schemes of production processes are developed, the technique of an estimation of invasion risk and level of protection is proved.

IntelITSIS'2022: 3rd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 23–25, 2022, Khmelnytskyi, Ukraine
EMAIL:v_sabat@ukr.net (Sabat V.); lssikora@gmail.com (Sikora L.); durnyak@uad.lviv.ua (Durnyak B.), olha.y.fedevych@lpnu.ua (Fedevych O), lysa.nataly@gmail.com (Lysa N)
ORCID: 0000-0001-8130-7837 (Sabat V.); [0000-0002-6650-2703] (Durnyak B); [0000-0002-7446-1980](Sikora L); [0000-0002-8170-3001] (Fedevych O); [0000-0001-5513-9614] (Lysa N)

Accordingly, a table has been developed to assess possible intrusion channels and failure criteria and the risk of destruction of system protection.

2. Control of complex hierarchical structures under threats and information attacks

Solving the problems of control of complex hierarchical structures under threats and information attacks requires forming a set of methods for each type of object and system and decompose the problem into subject-oriented components (Fig. 1) [1]:

- the localization of the main factors of influence and threats and attacks;
- the assessment of heterogeneities and uncertainties in the structural hierarchy of the system and levels of risk under threats;
- the physical and statistical analysis of factors of influence, disturbances, threats;
- the identification of cause-effect relationships in the system and the influence of factors on various components of the structure;
- the organizational and technological models of decision-making processes and management under uncertainty and risk;
- the identification of the structural organization of the system functioning (block diagrams, digraphs, topology), the analysis of resources and human potential;
- the identification of models of dynamics of the control object for normal and emergency modes, strategies of target management;
- the management and coordination strategies, calendar dynamic action plans for all levels of the hierarchy of corporate, municipal and educational systems.

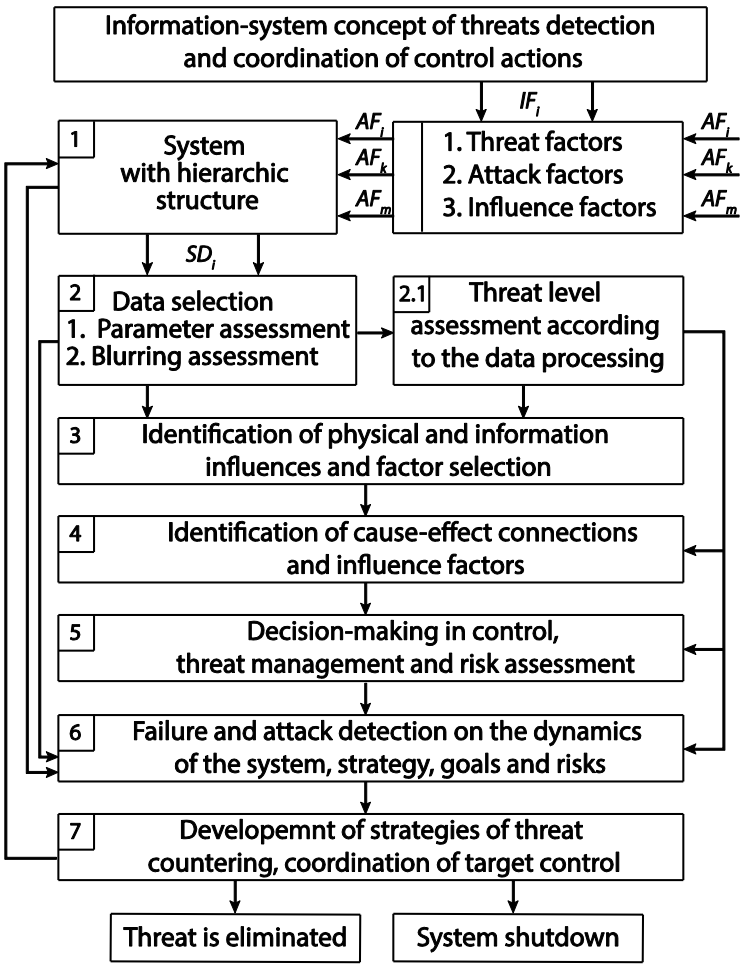

Figure 1: Structural and functional scheme of counteraction to attacks and active threats

Sustainable operation of permanent systems, taking into account the impact of a set of factors, is maintained by constant management influences based on decision-making and implementation, both automatic system and DM (DM – a decision maker) at different levels of the hierarchy of structural organization [2–5].

The decision, in a broad sense, means the choice of action mode to achieve the goals of the system control. The decision process has two components of activity [6] (Fig. 2):

1. Intellectual one (problem, goal, control, purposeful decision-making strategy);
2. Procedural, organizational and technological one (methods of implementing management actions).

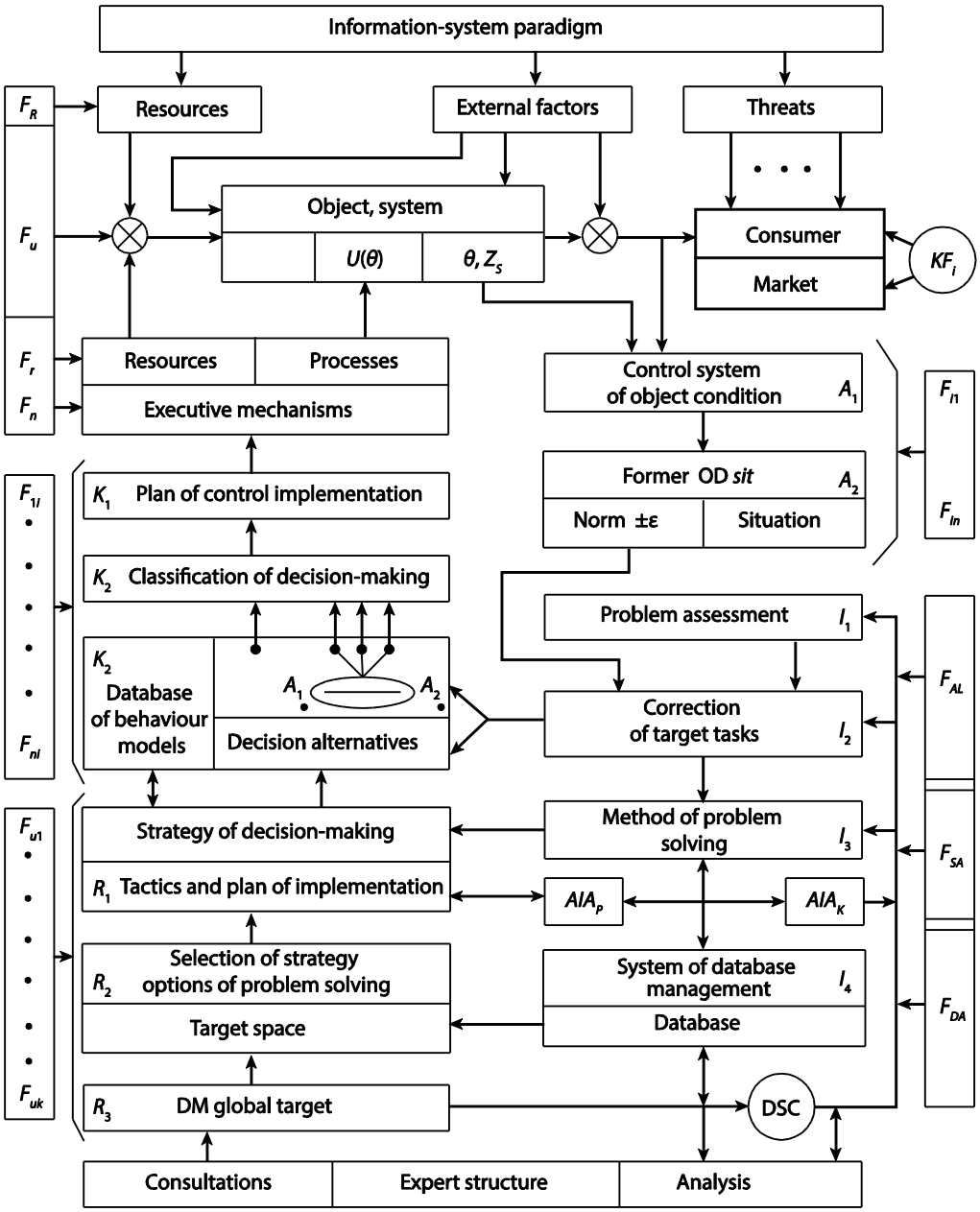

Figure 2: Block diagram of decision making in technological and publishing aggregate and integrated structures under risk

2.1. Analysis of the decision-making process

Characteristic features of the decision-making process are respectively [7-13] (Fig. 3):

- the ability to choose how to act on a variety of alternatives (action plans) according to a goal-oriented strategy;

- the goal (clear or blurred by the situation) that needs to be realized under threat factors;
- the need for a willful act of DM in choosing the method of solving the problem and the corresponding mental determination to target actions;
- the timeliness, according to the stages of development and analysis of the situation, solving the problem of overcoming the crisis of the control system;
- the authority of DM to act within its rights and powers;
- the specificity of the procedure for choosing the method of the control implementation;
- the constructiveness – taking into account the cost of changing the situation and the quality of management actions in relation to the target based on the analysis of the situation;
- targeting of executive mechanisms of both ACS and DM;
- the implementation of strategies and management plans in accordance with the goal;
- the terminality of time for decision-making and implementation of actions in normal and emergency situations caused by active threats.

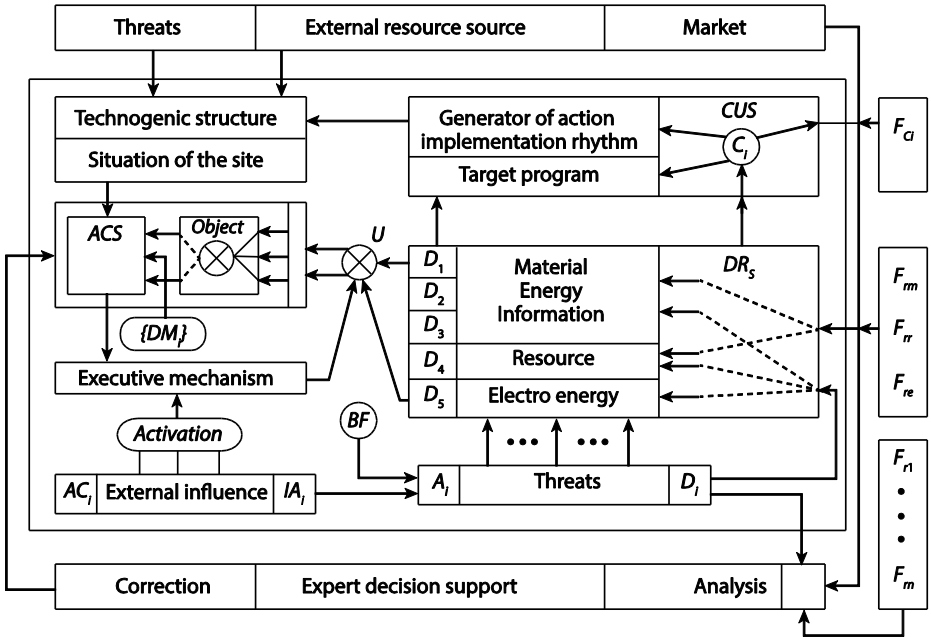

Figure 3: Model of man-made structure under the influence of threats to resources

Thus, the situational control in hierarchical human-machine local and distributed systems is a method of forming control actions based on strategies for predicting hazards and analyzing their destructive factors, symptoms and strategies to reduce negative consequences, maintaining the functional structure and technological modes with limited resources and acceptable product quality (Fig. 4) [8].

Accordingly, all actions are formed on a set of control cycles, which corresponds to the allowable terminal time of their implementation $T_{цi}$ ® $\left\{t\,|_{j=1,m}\right\}$ on the axis $T_{цi}$. Each cycle corresponds to:

- time markers $(t_i, i = 1,k)$ on the axis of the decision-making interval;
- time intervals of operations and actions on $T_{цi}$ ® $\left\{t_i\,|_{j=1,m}\right\}$ for every control act $\{A_i\}$, performed by the agent-operator.

Terminal time is divided into intervals $\left\{t_i, t_i\,|_{i=1,m}\right\}$ (Fig. 4).

- the assessment of the situation in the system and threats based on data processing;
- the formation of a model for the situation solving according to the object condition;
- the generation of action plans and acts in accordance with the goal and situation;
- the distribution of tasks for intelligent and automatic implementation;

- decision-making and its implementation by an active intelligent agent-operator for block management.

In this case, the balance condition of real and terminal time on the control cycle, which is formed by the ACS operator [9], must be met, respectively:

$$\forall T_{ui} \; MT_F \left\{ e \sum_{i=1}^{m} t_i \; J \; e \sum_{i=1}^{m} t_{iT} \right\},$$

where t_{iT} — is a terminal time interval $(t_{iT} \; OT_F)$ for the operation implementation.

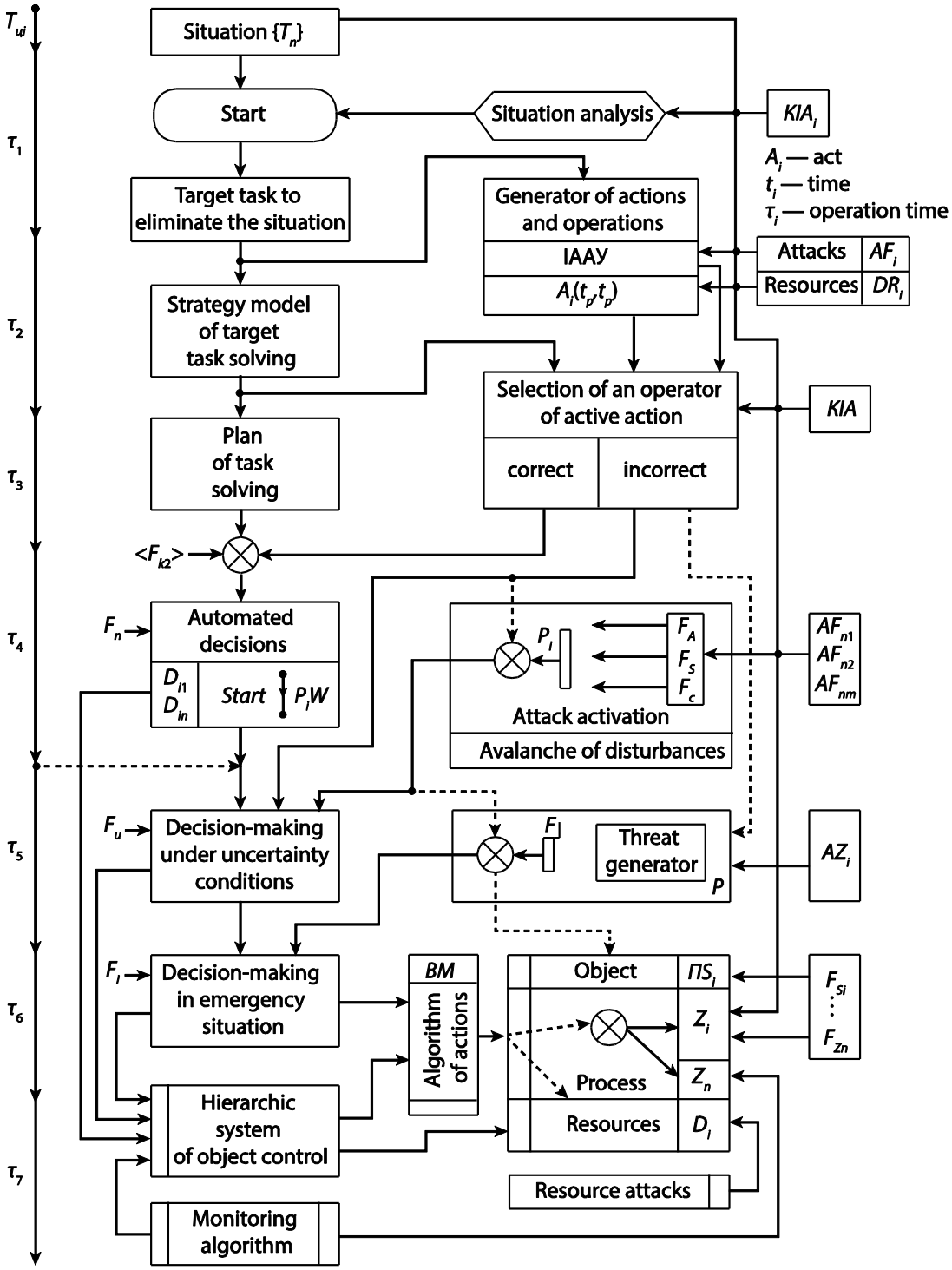

Figure 4: Block diagram of the situational management scenario model under threats to the system in the terminal cycle T_{ui}

The main symbols in Fig. 4: A_i — are acts of actions that are formed on the time interval of decision-making process; $\langle (t_{os}, t_{oa}, t_r), t_p, (t_{pr}, t_l, t_{la}) \rangle$ — are time markers needed to complete cycles of decision-making procedures according to the situation and the target task; *BM* – is an executive mechanism; *ПS* – is a state space of the object; T_m — is the terminal time of the decision cycle (formation and action); F_a, F_B, F_c — are factors of influence, probability of occurrence of disturbances and information attacks and threats to infrastructure; DA_i — is the flow of aggregate data on the control objects condition; $(t_{os}, t_o, t_{sr}, t_{pr}, t_{os}, t_{ad}, t_{lk})$ — are time intervals of operations implementation when making decisions on the management cycle under threats and attacks on the object; *CUS* — is a goal-oriented system that implements the management strategy.

3. Threats and crisis situations in hierarchical structures

Factors of internal and external influence can be the causes of crisis problem situations. Such factors include:

- natural phenomena (storms, typhoons, floods) threats;
- production and technical processes that went out of normal operation due to loss of reliability of units;
- political and economic situation;
- insufficient level of the operational staff skills;
- instability of the functional and structural system, random deviations, engineering errors in the design, system);
- intentional provocative actions of external threats of the target type;
- loss of design documentation as a basis for the formation of action chains in decision-making and project errors;
- conflict situations in the management team (leadership);
- equipment failures and breakdowns due to active intervention.

The above factors can negatively affect the decision-making process itself, as well as the functioning of the hierarchical structure as a whole. Therefore, they need to be analyzed in detail and their level of risk should be studied in the formation of protection systems, as well as in the process of functioning of complex hierarchical structures, in particular those located in high-risk areas. It is necessary to take into account both the losses that may result from the occurrence of negative factors of external and internal influences, and methods of restoring the information system due to the occurrence of such factors.

3.1. Classification and assessment of threats, research methodology

The threat, as a potential opportunity for attacks, has the ability to damage the IS and its assets. If the threat is realized, it can interact with the IS and cause unwanted incidents that adversely affect the system. Threats can be based on both natural and human factors, they can be realized accidentally or intentionally. Sources of both accidental and intentional threats should be identified and the probability of their implementation assessed [5-9]. The general classification of threats by type, action, source and object of action is presented in Fig. 5 [10]. A specialized IS threat catalog developed by Digital Security[2], one of the leading Russian consulting companies in the field of information security, as well as in the field of assessing the compliance of IS with the requirements of ISO 27001/ISO 17799[3], was used to assess threats. In the course of the work, a survey was conducted among system administrators of printing companies of Ukraine in order to increase the reliability of assessment of criticality, probability of implementation and frequency of threats. Respondents were sent a chart of the relationships between ACSPP assets, a table listing ACSPP assets and threats, and asked to assess the criticality, probability, and frequency of threats to each ACSPP asset, taking into account the relationships between assets. A scale from 0 to 3 was used for the assessment, where “0”

[2] Official website — http://www.dsec.ru.
[3] https://www.iso.org/isoiec-27001-information-security.html

is the absence of criticality, probability or frequency of threat to the asset, and “1”, “2” and “3”, respectively, “low”, “medium” and "high" level of these indicators. The survey involved 10 respondents working in 10 printing companies. In order to cover the widest possible risks of ACSPP, the analysis of the results was carried out on the principle of "maximum assessment", i.e. the highest value was selected from a number of assessments of one indicator.

To conduct research, a scheme of possible types of threats that operate in the control system of the technological process in printing on the basis of the system concept of classification of threats by type, action, source and object of action was developed.

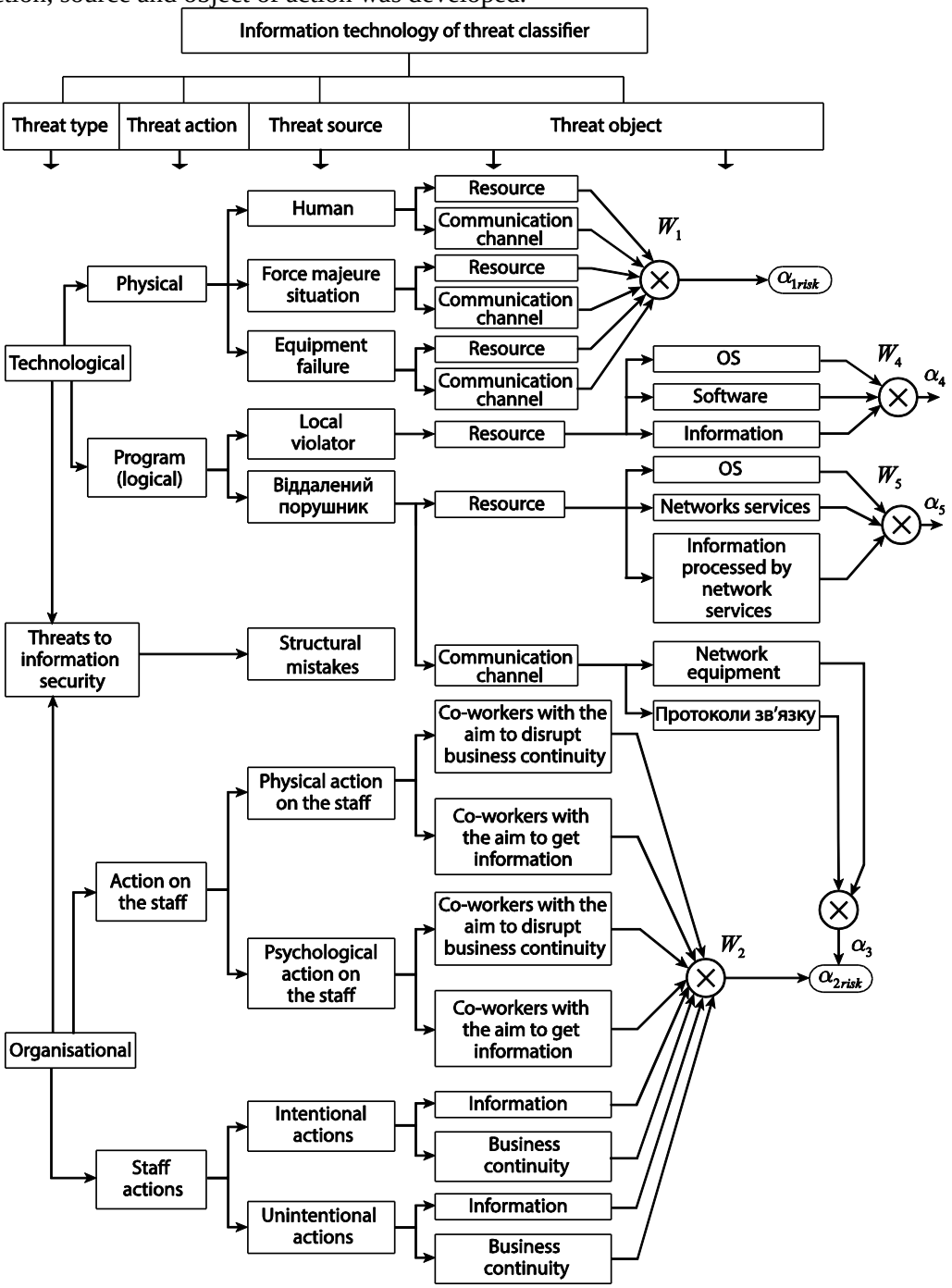

Figure 5: System concept of threats classification by type, action, source and object of action

3.1.1. Critical threat assessment methodology, which act on the management information and aggregate structure of the technological system

Examining the assets of automated control systems for printing production (ACSPP), it can be concluded that the objects of threats may be one or more assets of ACSPP. Tables 1 – 5 present a list of possible threats to ACSPP, according to the classification (Fig. 5), as well as the criticality of the threats implementation to ACSPP assets.

Table 1

Human physical threats aimed at IS resources

Threat	Criticality of the threat to the asset of ACSPP							
	Networks	Servers	Mobile PC	Workstations	Software modules of ACSPP	Auxiliary software	Central database	Internal data
1	2	3	4	5	6	7	8	9
Human physical threats aimed at IS resources								
Reading valuable information from paper and video terminal PC devices	0	0	0	0	0	0	0	0
Modification of valuable information on paper	0	0	0	0	0	0	0	0
Destruction or damage of media with valuable information	0	0	0	0	0	0	0	0
Replacement of media with valuable information	0	0	0	0	0	0	0	0
Media theft	0	0	0	0	0	0	0	0
Theft of mobile and handheld PCs	0	0	3	0	0	0	0	0
Theft of used materials (garbage, destroyed documents)	0	0	0	0	0	0	0	0
Unauthorized use of equipment	0	3	3	3	3	3	3	3
Damage or intentional change of equipment operation modes	3	3	3	3	3	3	3	3
Installation of devices for removal of electromagnetic oscillations	0	0	0	0	0	0	0	0
Installation of means for listening to conversations	0	0	0	0	0	0	0	0
Installation of means for video surveillance by the violator	0	0	0	0	0	0	0	0
Installation of noise generators and other devices by the violator to create interference	0	0	0	0	0	0	0	0
Disclosure, transfer or loss of access restriction attributes	0	3	3	3	3	3	3	3
Obtaining confidential information without the use of special tools	0	0	0	0	0	0	0	0
Human physical threats at IS communication channel								
1	2	3	4	5	6	7	8	9
Cable damage	3	0	0	0	2	2	2	2
Unauthorized wireless connection to the cable line	0	0	0	0	0	0	0	0
Unauthorized wired connection to the cable line	0	0	0	0	0	0	0	0
Installation of noise generators and other devices by the violator to create interference	0	0	0	0	0	0	0	0
Unauthorized connection to wireless networks	0	0	0	0	0	0	0	0

The criticality[4] of the threat is assessed on the scale described above. Dependencies between assets are also taken into account in the assessment. [13] Determination of criticality coefficients was carried out at various enterprises of the printing and publishing industry from 2019 to 2021. The research was conducted with the aim of product quality, and became the basis for the development of methods to combat information attacks in the workplace.

Table 2
Global and local physical threats aimed at IS

Threat	Criticality of the threat to the asset of ACSPP							
	Networks	Servers	Mobile PC	Workstations	Software modules of ACSPP	Auxiliary software	Central database	Internal data
Disaster	3	3	3	3	3	3	3	3
Technogenic disaster	3	3	3	3	3	3	3	3
Military action	3	3	3	3	3	3	3	3
Revolution	3	3	3	3	3	3	3	3
Terrorist act	3	3	3	3	3	3	3	3
Local physical threats aimed at IS								
Fire	3	3	3	3	0	0	0	0
Lightning strikes	3	3	3	3	0	0	0	0
Cross-reference	3	3	3	3	0	0	0	0
Failure of external energy sources	3	3	3	3	0	0	0	0
Failure of internal (reserve) energy sources	3	3	3	3	0	0	0	0
Sharp voltage fluctuations in the power grid	3	3	3	3	0	0	0	0
Ventilation system failure	2	2	2	2	0	0	0	0
Air conditioning system failure	3	3	3	3	0	0	0	0
Heating system failure	0	0	0	0	0	0	0	0
Violation of the circuit of closed systems near IS objects	2	2	2	2	0	0	0	0
Physical threats related to the equipment failure								
Loss of information as a result of data carrier failure	0	3	3	3	3	3	3	3
Defective data carriers	0	3	3	3	3	3	3	3
Reduction of equipment reliability after the end of its service life	2	2	2	2	0	0	0	0
Data loss or system malfunction due to overflow of storage devices	0	3	3	3	2	3	3	2

[4] The criticality of the treat is a measure of damage caused by this threat in its implementation.

Table 3

Local and logical threats

Threat	Criticality of the threat to the asset of ACSPP							
	Networks	Servers	Mobile PC	Workstations	Software modules of ACSPP	Auxiliary software	Central database	Internal data
Change of the user privileges when running exploits that use local OS vulnerabilities	0	0	0	0	2	3	3	3
Local OS vulnerabilities that do not require an exploit to run the threat	0	0	0	0	2	3	3	3
Running files with viruses that affect the OS	0	0	0	0	2	3	3	3
Running the OS from external media	0	0	0	0	2	3	3	3
Modification of OS components	0	0	0	0	2	3	3	3
1	2	3	4	5	6	7	8	9
Failure to service the OS	0	0	0	0	2	3	3	3
Local logical threats aimed at software								
Change of the user privileges when running exploits that use local software vulnerabilities	0	0	0	0	2	3	3	3
Local application software vulnerabilities that do not require an exploit to run the threat	0	0	0	0	2	3	3	3
Opening files with macro viruses	0	0	0	0	2	3	3	3
Modification of application software	0	0	0	0	2	3	3	3
Failure to service the application software	0	0	0	0	2	3	3	3
Local logical threats aimed at information, stored and processed on the resource								
Unauthorized modification of information in the database stored on the resource	0	0	0	0	0	0	3	3
Unauthorized modification of information in the e-mail system stored on the resource	0	0	0	0	0	0	0	0
Unauthorized modification of electronic documents containing valuable information	0	0	0	0	0	0	0	3
Unauthorized reading of confidential information in the database stored on the resource	0	0	0	0	0	0	0	0
Unauthorized reading of messages in the e-mail system stored on the resource	0	0	0	0	0	0	0	0
Unauthorized reading of confidential information in electronic documents stored on the resource	0	0	0	0	0	0	0	0
Loss or violation of the integrity of information stored on the resource due to improper operation of the software	0	0	0	0	0	0	3	3
Unauthorized malicious use of e-mail by an infringer on behalf of a legal user	0	0	0	0	0	0	0	0
Deletion of valuable information stored in the database by the violator	0	0	0	0	0	0	3	3
Deletion of e-mails by the violator	0	0	0	0	0	0	0	0
Deletion of electronic documents containing valuable information by the violator	0	0	0	0	0	0	2	3

Table 4

Remote logical threats

Threat	Criticality of the threat to the asset of ACSPP							
	Networks	Servers	Mobile PC	Workstations	Software modules of ACSPP	Auxiliary software	Central database	Internal data
Collection of information about the OS	0	0	0	0	0	0	0	0
Collection of information about the OS	0	0	0	0	0	0	0	0
Launch of exploits that use remote OS vulnerabilities	0	0	0	0	3	3	3	3
Remote logical threats aimed at network services								
Network service failure due to internal software failure	0	0	0	0	0	0	0	0
Launch of exploits that use remote network service vulnerabilities and result in denial of service	0	0	0	0	0	0	0	0
Running exploits that use remote network service vulnerabilities and cause arbitrary code to run on a remote PC	0	0	0	0	0	2	2	2
User mailbox overflow	0	0	0	0	0	0	0	0
Selection of user authentication data	0	0	0	0	0	0	0	0
Remote collection of information about network services	0	0	0	0	0	0	0	0
Remote logical threats aimed at information, processed by network services								
Interception of information provided by network services using vulnerabilities in data transmission protocols	0	0	0	0	0	0	0	0
Logical threats aimed at network equipment								
Unauthorized access to the network device at the software level	3	0	0	0	3	3	3	3
Denial of service at the software level	3	0	0	0	0	0	0	0
Unauthorized connection to wireless networks	0	0	0	0	0	0	0	0
Remote logical threats to communication protocols								
Interception of network traffic at the logical level due to incorrect configuration of network devices or inability to differentiate traffic between network nodes	0	0	0	0	0	0	0	0

Table 5

Threats related to physical exposure to humans

Threat	Criticality of the threat to the asset of ACSPP							
	Networks	Servers	Mobile PC	Workstations	Software modules of ACSPP	Auxiliary software	Central database	Internal data
Unavailability of information due to incapacity of IS users who have this information	0	0	0	0	0	0	0	0
Improper functioning of IS due to the inability of the administrator	2	2	2	2	2	2	2	2
Reduced response to information security incidents due to administrator incapacity	2	2	2	2	2	2	2	2
Violation of business continuity due to physical action on the company employee	0	0	0	0	0	0	0	0
Threats related to psychological effects on humans								
Disclosure of confidential information as a result of psychological actions of third parties on the company employee	0	0	0	0	0	3	3	3
Substitution of information as a result of psychological actions of outsiders on the company employees	0	0	0	0	0	3	3	3
Modification or destruction of information as a result of psychological actions of third parties on the company employees	0	0	0	0	3	3	3	3
1	2	3	4	5	6	7	8	9
Unavailability of information due to incapacity of IS users who have this information	0	0	0	0	0	0	0	0
Improper functioning of IS due to the inability of the administrator	2	2	2	2	2	2	2	2
Reduced response to information security incidents due to administrator incapacity	2	2	2	2	2	2	2	2
Threats related to psychological effects on humans								
Disclosure of confidential information by the company employees	0	0	0	0	0	3	3	3
Modification or destruction of information by the company employees	0	0	0	0	0	3	3	3
Substitution of information by the company employees	0	0	0	0	0	3	3	3
Threats related to unintentional actions of the staff								
Violation of information confidentiality due to unintentional actions	0	0	0	0	0	3	3	3
Unintentional violation of information integrity	0	0	0	0	3	3	3	3
Unintentional deletion of critical information	0	0	0	0	3	3	3	3

As some threats are not critical to any of ACSPP assets, there is no need to provide further results of their assessment.

Comparing the data from Table 1 - 5, it is possible to make the list of the most critical threats for typical ACSPP:

1. Human physical threats aimed at IS resources:
   - unauthorized use of equipment;
   - damage or intentional change of equipment operation modes
   - disclosure, transfer or loss of access restriction attributes;
2. Human physical threats aimed at IS communication channel:
   - Cable damage;
3. Global physical threats aimed at IS (full list of threats);
4. Local physical threats aimed at IS:
   - cross-reference;
   - failure of external energy sources;
   - failure of internal (reserve) energy sources;
   - sharp voltage fluctuations in the power grid;
   - air conditioning system failure;
5. Physical threats related to the equipment failure:
   - loss of information as a result of data carrier failure;
   - defective data carriers;
   - reduction of equipment reliability after the end of its service life;
   - data loss or system malfunction due to overflow of storage devices;
6. Local logical threats aimed at OS:
   - running files with viruses that affect the OS;
   - running the OS from external media;
   - modification of OS components;
   - failure to service the OS;
7. Local logical threats aimed at software:
   - opening files with macro viruses;
   - modification of application software;
   - failure to service the application software;

Thus, a list of critical threats to ACSPP is received, which may occur with a medium or high probability and cause significant damage to one or more assets, which will lead to serious violations in the work of ACSPP. For a more accurate analysis of threats in ACSPP, it is also necessary to analyze the probability of their detection and the frequency of recurrence over a period of time, which is planned to be done in future studies.

4. Conclusions

The analysis of information support of the complex system control process with a hierarchical structure under threats is done as well as the process of document circulation in the formation and decision-making process, based on which a structural and functional scheme is developed and substantiated to counter threats and attacks on the control process in the hierarchical structure.

The block diagram of decision-making in technical and publishing systems under risk is substantiated and developed.

The characteristic features of the decision-making process and parameters affecting this process are analyzed, as a result of which a model of technogenic structure under threats to resources is constructed.

Management actions on a set of control cycles to which the admissible time of their performance corresponds are studied and the block diagram of the scenario of situational management under threats on a terminal cycle is constructed.

The system concept of classification of threats and crisis situations in hierarchical structures by type, action, source and object of action, influencing the decision-making processes, is presented.

A survey of ACSPP system administrators is conducted in order to increase the reliability of assessing the threat criticality. Based on the studied data, the most critical threats to a typical automatic control system are presented.

The results of research can be implemented in the design of control and protection systems not only for automatic control systems, but also for any complex systems with a hierarchical structure under threats and crises.

5. References

[1] .B. Boyer, Countering Hybrid Threats in Cyberspace.Cyber Defense Review. Vol. 2 Ed. 3, 2015. 11.

[2] Groome, D., Brace, N., Edgar, G., Edgar, H., Eysenck, M., Gobet, F., Law, R., Manly, T., Ness, H., Pike, G., Scott, S., Styles, E.: An Introduction to Cognitive Psychology: Processes and Disorders. Routledge, 4th edn. (2021). https://doi.org/10.4324/9781351020862 Title Suppressed Due to Excessive Length 11

[3] Andonov, S. Safety Accidents in Risky Industries: Black Swans, Gray Rhinos and Other Adverse Events. CRC Press, 1st edn. (2021).https://doi.org/10.1201/9781003230298

[4] Boy, G.A.: The Handbook of Human-Machine Interaction: A Human-Centered Design Approach. CRC Press, 1st edn. (2011). https://doi.org/10.1201/9781315557380

[5] L. Sikora, R. Tkachuk, N. Lysa, I. Dronyuk, O. Fedevych, R. Talanchyk. Information-resource and cognitive concept of threat's influence identification on technogenic system based on the cause and category diagrams integration. IntellTSIS 2021. Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS Khmelnytskyi, Ukraine, March 24–26, 2021. Vol. 2853, pp. 398-416.

[6] L. Sikora, R. Tkachuk, N. Lysa, I. Dronyuk, O. Fedevych Information and Logic Cognitive Technologies of Decision-making in Risk Conditions. IntellTSIS 2020. Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. Khmelnytskyi, Ukraine, June 10-12, 2020. pp. 340-356. http://ceur-ws.org/Vol-2623/paper29.pdf

[7] Bhise, V.D.: Decision-Making in Energy Systems. CRC Press, 1st edn. (2021). https://doi.org/10.1201/9781003107514

[8] Kozlova, L.P., Kozlova, O.A.: Using of fuzzy set theory when designing technical systems. In: 2015 XVIII International Conference on Soft Computing and Measure-ments (SCM). pp. 193{194 (2015). https://doi.org/10.1109/SCM.2015.7190453

[9] Tattam, D.: A Short Guide to Operational Risk. Routledge, 1st edn. (2011).https://doi.org/10.4324/9781315263649

[10] Hovorushchenko T., Pavlova O. Method of Activity of Ontology-Based Intelligent Agent for Evaluating the Initial Stages of the Software Lifecycle. Advances in Intelligent Systems and Computing. 2019. Vol. 836. Pp. 169-178. doi:10.1007/978-3-319-97885-7_17

[11] Wiggins, M.W.: Introduction to Human Factors for Organisational Psychologists. CRC Press, 1st edn. (2022). https://doi.org/10.1201/9781003229858

[12] S. Demri, V. Goranko, M. Lange. Temporal Logics in Computer Science, Cambridge: Cambridge University Press. 2016. 752 p.

[13] Balyk, V.M., Thuong, N.Q. Statistical synthesis of the principle of ra-tional organization of a complex technical system. In: 2019 InternationalConference on Engineering and Telecommunication (EnT). pp. 1{4 (2019). https://doi.org/10.1109/EnT47717.2019.9030569.

[14] F.G. Hoffman. Hybrid Warfareand Challenges, Joint Forces Quarterly 52, 2009.