UDC 655.41:004

ANALYSIS OF AUTHORITY MANAGEMENT SYSTEMS IN AUTOMATED DOCUMENT MANAGEMENT SYSTEMS

Durnyak B.V.
Dr. Sc., Professor, Honoured Worker of Science and Technology of Ukraine,
Rector of Ukrainian Academy of Printing, Lviv, Ukraine
Sikora L.S.
Dr. Sc., Professor, Full Member of the Engineering Academy of Ukraine,
Professor of the Department of Automated Control Systems of the Institute of Computer Sciences and Information Technologies, Lviv, Ukraine
Sabat V.I.
Ph.D., Associate Professor, Associate Professor of the Department of Information Multimedia Technologies
of Ukrainian Academy of Printing, Lviv, Ukraine
Kuhot V.O.
graduate student of the Department of Information Multimedia Technologies
of Ukrainian Academy of Printing, Lviv, Ukraine

Abstract. *The article examines the features of the construction of the authorization management system for automated document management systems (ADMS), which is integrated into the structure of the hierarchy of organizations under the conditions of active attacks and threats to the information system. Based on the analysis of the terminal cycle of the technogenic hierarchy management process under the conditions of the risk of threats and attacks, the use of a conditional-modified authority management system is substantiated, which would take into account the specifics of the functioning of automated document management systems and would have the ability to respond to any negative changes or factors.*

Keywords: *THREATS, ATTACKS, AUTHORITY MANAGEMENT SYSTEMS, AUTOMATED DOCUMENT MANAGEMENT SYSTEMS.*

Introduction

Authorization management systems are basic from the point of view of the security of any organization when granting access rights to confidential information, as well as when determining the degree of confidentiality of documents that function in hierarchical production systems. Documents that mainly contain information about management actions and are aimed at managing technological processes are very vulnerable to intrusions by unauthorized persons or persons without sufficient rights. Therefore, the development of an authority management system for automated document flow systems in the hierarchical structure of production organizations is the main issue of security for their reliable and uninterrupted functioning. This issue is especially relevant in the context of attacks and threats to the management system.

The article substantiates that authorization management systems are best synthesized with an automated document flow system, which gives advantages in the efficiency of any changes related to the access rights of the subjects of the production process to the production facilities, determination of the levels of secrecy of documents, as well as control over the execution of documents and making operational and strategic decisions by operators in the process of managing technogenic processes in hierarchical structures in conditions of threats and information attacks.

The purpose and objectives of the research

The purpose of research is the development of information technology means of protection of document circulation systems in complex hierarchical structures based on the use of authority management mechanisms. In accordance with the formed paradigm of building a system of authority management in ADMS in the structure of a hierarchical organization, it is necessary to solve the following tasks: develop a structural and functional scheme for managing access to ADMS; propose the implementation of a security policy for the authorization management system; determine the ranking of the importance of data for making operational and strategic decisions by the operator in the management process, forming the level of confidentiality of documents.

Main part

The protection and reliability of automated document management systems is primarily based on the overlapping work of all subsystems and security services, the main of which is the service of access to information in documents that are formed during the functioning of integrated hierarchical systems of various functional purposes [1].

According to such ADMS there are data on:

– structural and functional organization of the system, database and knowledge;

– functions and goals, target-functional purpose of the system, blocks, objects, aggregates, decision-making and management strategies;

– technological processes and their parameters, organization of the production process, standards and regimes (normal, extreme, emergency);

– systems of data selection and processing in order to control the functioning of blocks and aggregates (informational and intellectual assessment);

– system and management processes (strategic, operational, automatic) at both technological and operational levels;

– plans, tactics, strategy of technological and operational management;

– data exchange system, according to the level of hierarchy, authority for management commands (operational level $\{KIA_i\}$, technological level $\{KIA_t\}$,

strategic level $\{KIA_s\}$) for the process of formation and decision-making, goal-setting and global level [2].

According to the concept of active target orientation of a technogenic cyber-physical system with a hierarchical structure of a strategic level, a structural-terminal cyclic scheme of the management process under conditions of risk during the action of attacks was developed (Fig. 1).

Designation on the diagram of Fig. 1: $\{R_i\}$ is hierarchy levels of the organizational structure; $AktD_i$ – threat activator; GC_i – generator of attack targets; LC_i – terminal local targets; $\left(X,Y,S\left(z,t\right)\right)$ – parameters of situation signs; KL_w – classification of the situation by risk level; $\left(\Pi Z_i\right)$ – problematic situational task; MS – information model of the situation, in the event of an active attack $\left(A \to x\right)$; I_k – an indicator of the influence of a cognitive agent $\left(KIA\right)$ on decision-making; $\{U_i\}$ – management action; $\left(I_k, I_i\right)$ – quality criteria.

Integrated hierarchical systems with different types of functional goal-oriented purpose are divided according to rank criteria of hierarchy levels [3]:

– $Rang1$ – SAR – systems of automatic regulation of the tracking type;

– $Rang2$ – ACS-TP – systems of automatic control of technological processes;

– $Rang3$ – ACS-OAP – systems of automated control of organizational administrative processes;

– $Rang4$ – IACS (Opt, Adap) – integrated optimal adaptive control systems;

– $Rang5$ – IHACS (Coord Ci) – integrated hierarchical intellectual systems with coordination;

– $Rang6$ – PIIACS – purposefull intelligent systems.

When an emergency situation (ES) occurs, the process of technogenic hierarchy management can be divided into three main stages: 1) recognition of ES; 2) decision-making process; 3) management.

At the first stage of recognition of an emergency situation, the process of identifying a problematic situation and comparing it with already known attack scenarios based on models of representations of a situation when the level of permissible risk increases to a high level over a certain period of time, occurs, takes place, passes. At the same time, there is a process of assessing risks, possible damages and consequences of an emergency situation. While the attack is taking place, it is also necessary to determine the local target at which it is directed [4].

At the second stage, a decision-making task is set based on the formation of the appropriate model according to the ES, updating the target of the attack, which leads to the selection of alternative means of countering the development of the attack, drawing up decisions and action plans.

At the third stage, the management process directly occurs, which prevents the development of the attack and allows you to assess its consequences and the results of achieving the goal (fig. 1).

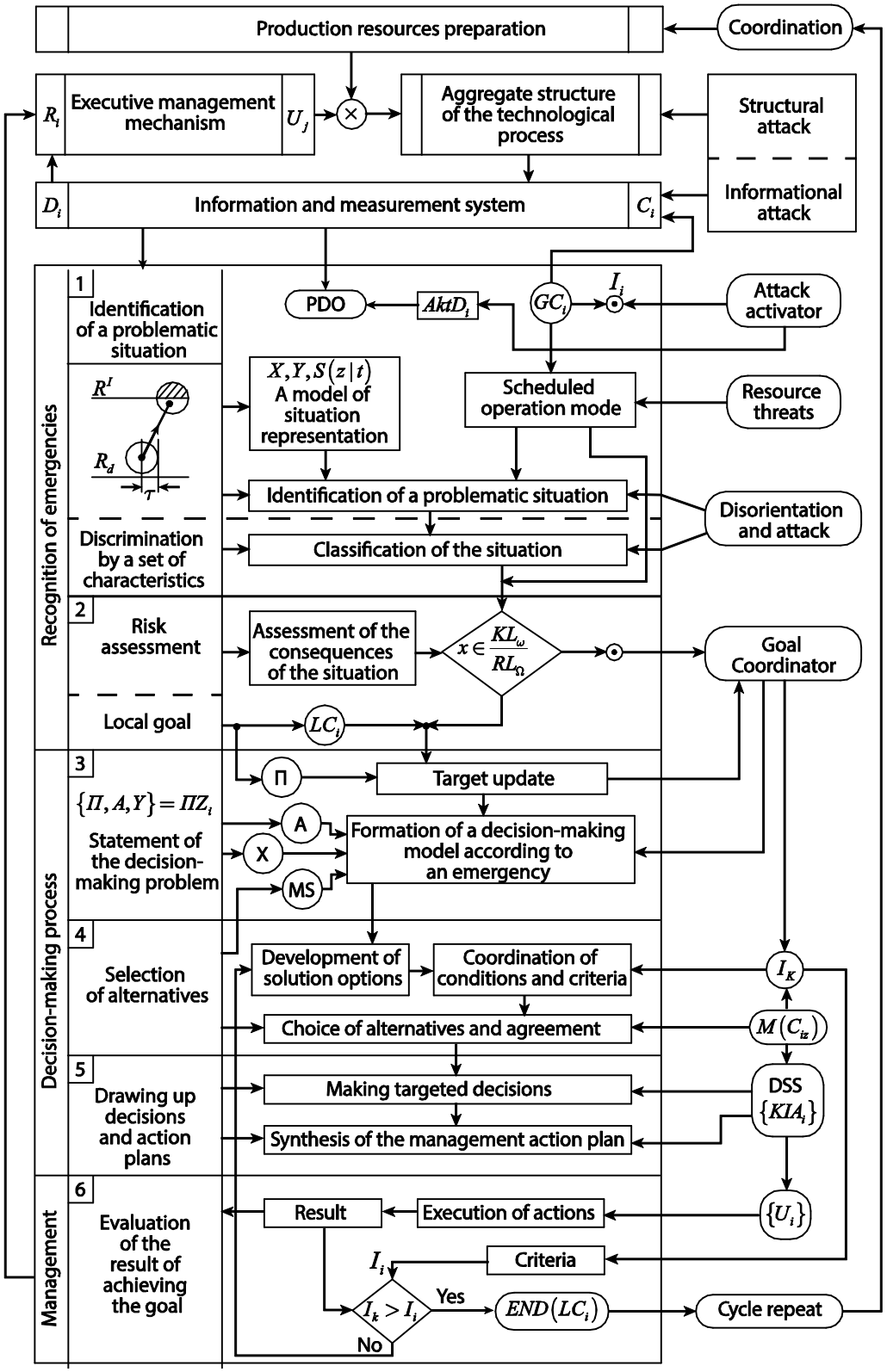

Figure 1 – Structural terminal cyclic diagram of the technogenic hierarchy management process under conditions of risk of threats and attacks

To ensure the stability of an integrated system with a hierarchy, it is necessary to introduce a set of authorizations, both for access to the decision-making process and for access to production data, standards, plans, current and strategic information (fig. 2).

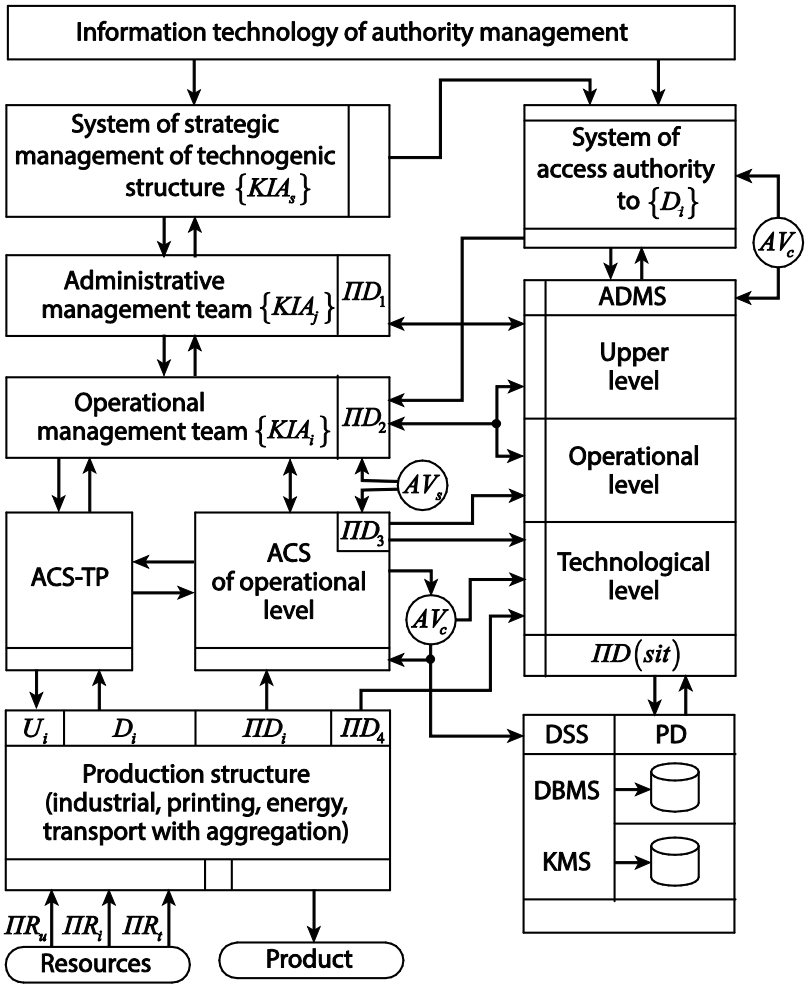

Figure 2 – Structural and functional scheme of management of access rights to ADMS of technogenic integrated system

The set of authorizations for access to the process of management and document circulation is implemented through the structure of the authority management system in the automated document circulation system [5].

The authorization management system (AMS) provides access to commands and blocks the action of active agents from intruding into the function and process of managing the integrated structure.

The authorization system provides access to information contained in documents (objects) and its connection with the user identification service (subjects) in ADMS. The operation of the access service is based on the AMS, developed by specialists in the field of security, and coordinated with the administration of ADMS.

The structure of the repetition management system can be described at the physical and logical levels. The physical mapping of an AMS occurs in the defined relationships not only of objects with ADMS subjects, but also of the possible functional interactions between the objects themselves and their components. This implementation is especially important at the stage of designing documents and agreeing on their parameters (identification code, level of secrecy, document structure, etc.). Within the framework of physical components, a number of logical connections can be implemented, which are described by logical components. In

general, the structure of AMS in ADMS can be described by such universal schemes as static, dynamic and conditionally modified [6].

The static structure of AMS in ADMS is characterized by the fact that the relationships between individual components do not change during the functioning of the system. The existence of relationships between components does not mean that there is a functional relationship between them. Such systems may have different logical and functional structures not interconnected within the ADMS system.

The functional structure of AMS in ADMS can change according to the predetermined time period of its operation. Changes in the work of the authority management system can also occur based on the analysis of the results of its work during a given period of time ΔT .

Condition 1. If, over a certain period of time, the level of secrecy of documents in AMS changes, and accordingly their level of protection in ADMS, this involves the introduction of corrections in granting access rights to the specified documents for all subjects of ADMS.

Such a time interval ΔT is determined by the period of solving the basic tasks of the authority management system in ADMS, and the analysis of the functioning of the system during time ΔT is implemented by means of the interpretation of the results obtained by the application task in ADMS. When analyzing the operation of the authority management system, attention should be paid to the following main factors [1]:

– connection of the results of solving the applied problem with the ADMS functioning process in period ΔT ;

– analysis of the parameters characterizing ADMS regardless of the interpretation used in processing of its functioning;

– analysis of development or changes in the structure of AMS;

– determination of the level of risk that may change upon completion of ΔT .

Conditionally modified structure of the authority management system is a structure that can be modified at any time ΔT of ADMS operation. Its modification may occur for one of the following reasons: registration of events with a negative interpretation; output of parameters that characterize AMS beyond permissible limits; initiation of changes in the system as a result of counteracting detected attacks in ADMS. Any changes in the components of AMS can also lead to changes in its structure and strategy optimization. Therefore, for organizations with a hierarchical structure of production process management, the conditioned and modified AMS structure is most suitable, able to quickly react in the conditions of threats and attacks.

The problem of optimizing the security level of the authority management system

When the authorization management system is functioning in ADMS, the main aspect of its effectiveness is the determination of the optimal level of security. It is clear that the level of security should not exceed certain permissible limits in the security policy related to the determination of the level of risk and vulnerability of

ADMS [7]. When the security level in the AMS is close to zero, it will evolve into a Resource Management System (RMS), which also manages the tasks used and operated within the ADMS [8]. Therefore, the use of AMS in ADMS is appropriate only in those cases when ADMS documents require appropriate security (fig. 3).

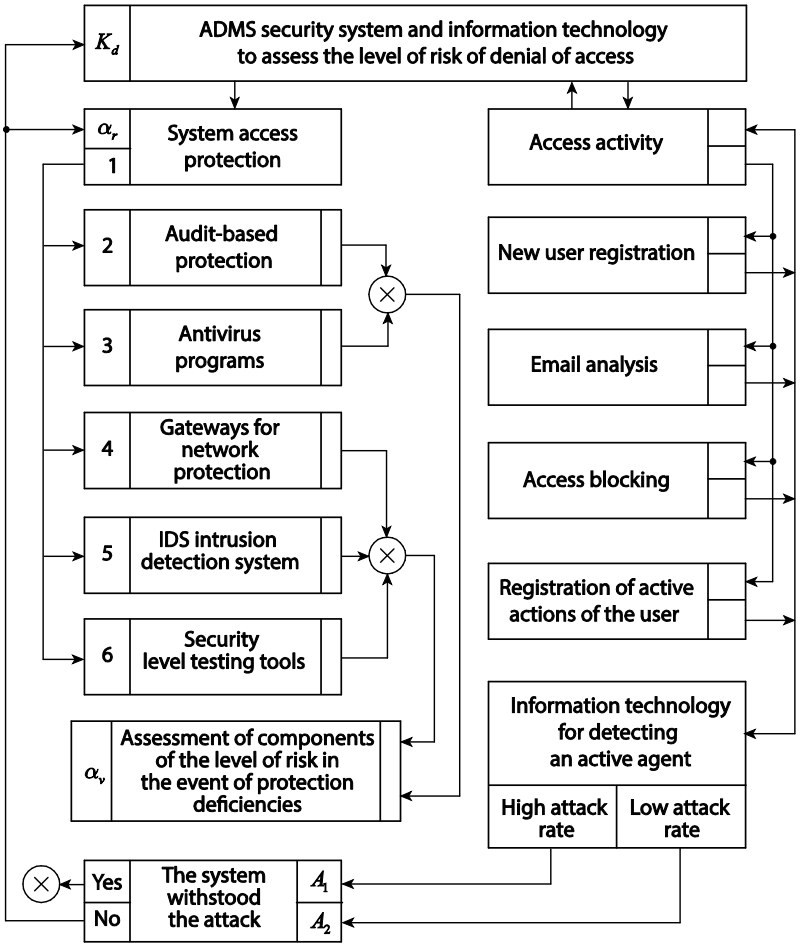

Figure 3 – Structural and functional diagram of the information technology of protection of access to ADMS for agents of different levels of the hierarchy

The main functions of AMS, developed in the security policy, include the following (fig. 4):

– F_1 – the ability of ADMS protection tools to detect and counteract external negative factors that prevent work with documents (access or modification attacks);

– F_2 – providing reliable access to information in ADMS to authorized users;

– F_3 – detection of internal errors and unauthorized intrusions into the system, which are registered in the event logs of the system administrator;

– F_4 – timely response to negative events according to the protection scheme.

The events associated with the implementation of attacks include events that are characterized by a change in the parameters of the access conditions in ADMS, especially when, before the occurrence of such events, access to ADMS was prohibited by the authorization management system. When ADMS attacks are detected, it is necessary to analyze the sequence of events that can be linked [9]. With such an analysis, it is possible to detect an attack, or the fact of its absence in the

current situation of the ADMS functioning process, in accordance with the security policy of the hierarchical management structure of technogenic or organizational-administrative systems adopted at the strategic level (fig. 4).

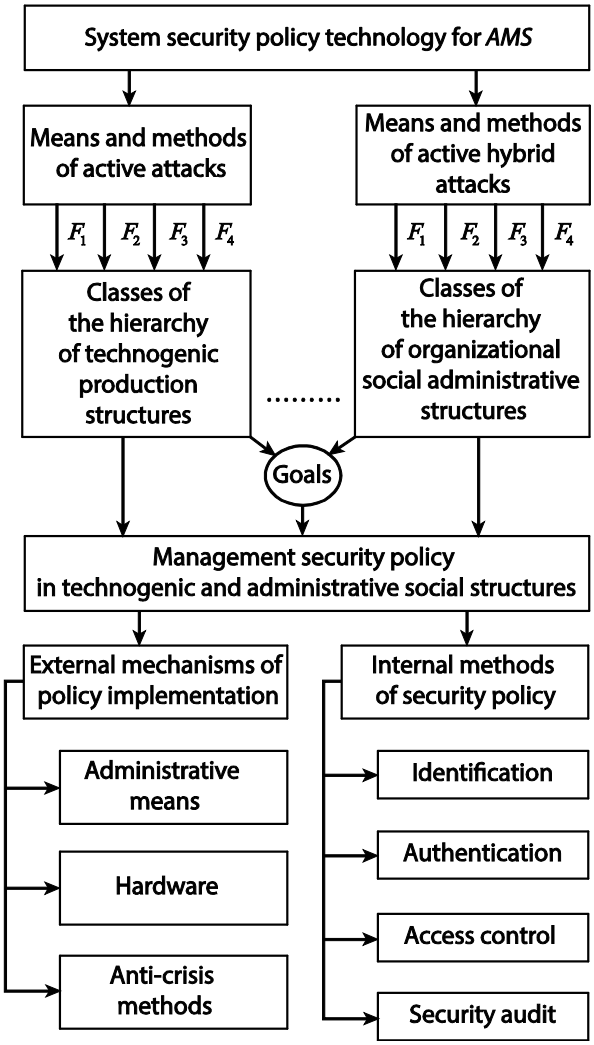

Figure 4 – Information technology and structural diagram of security policy implementation for the authority management system

In addition to detecting access attacks in ADMS, a conflict situation may arise in the access control system itself. Such situations are usually called anomalies in the process of functioning of the authorization management system, but they can also be attributed to attacks due to internal errors of the system. Examples of conflict situations include conflicting events of subjects on objects in ADMS, for example, when the authorization management system grants one user the authority to modify a document and another user the authority to delete all information in that document. In the functioning of the authority management system, it is also necessary to analyze not only the management of the granting of authority to subjects over objects, but also to control the implementation of appropriate non-contradictory actions over them [10].

Mathematical logic method for formal description of operational data access control systems

The presence or absence of authorities can be interpreted as discrete events. The conditions determining the possibility of the occurrence of certain events also allow for a discrete interpretation, since their nature in most cases is such that the condition is fulfilled or not fulfilled. Between the conditions leading to the occurrence of the event and between the events there are relationships that allow their logical interpretation. For example, for the occurrence of some event y_i a certain combination of events can be used, the connection between which, thanks to their discrete interpretation, is described by logical functions of narrow calculus $\{\&, \vee, \rightarrow, \neg\}$ [11]. The system of these functions, depending on the specific needs of the subject area of authority management tasks, can be extended by additional logical functions that will describe selected logical connections interpreted as axioms of a specific task, or specialized connections between individual variables that have their own interpretation in subject area, which is consistent with the generally accepted interpretation in mathematical logic [12].

The conditions describing the possibility of occurrence of certain events are formed by the users of the relevant information systems and are primarily determined by the interpretation of the relevant data and operations with this data. In order to be able to form certain data structures and their interpretations, it is necessary to create a system of data evaluations used in information systems (IS) [13]. Appropriate data evaluation techniques directly belong to certain groups of users. Therefore, the assessment methods represent a certain hierarchy based on the basic definitions corresponding to the Table 1 estimates of the level of importance in case of data loss in the hierarchy of management systems.

Table 1 – Ranking scales of assessments of the importance of data for making operational and strategic decisions by the operator[1]

№	LR_i	Availability class	R_z
1.	LR_1	Available data	$\leq 0,5$
2.	LR_2	Service data	$\leq 0,6$
3.	LR_3	Design and technological data	$\leq 0,7$
4.	LR_4	Personal data of operational personnel	$\leq 0,8$
5.	LR_5	Corporate data	$\leq 0,8$
6.	LR_6	Personal data of customers	$\leq 0,8$
7.	LR_7	Operational management and administration data	$> 0,8$
8.	LR_8	Closed administrative and financial data	$> 0,9$
9.	LR_9	Closed strategic level data	1,00

Markings in the Table 1: R_z is importance rank in case of data loss; $\{LR_i\} \rightarrow \left(I_v = \sum Shi\right)$ is rating scale diagram.

[1] The rank limits were determined on the basis of a year-long survey of specialists of ten printing enterprises in which the operation of the access control system and ADMS is established.

The problem of data evaluation is closely related to the choice of scale for appropriate evaluations. Information systems were based on the transfer of the latter from paper media to digital media and into digital computer systems that were formed as databases or as specialized data systems, then the methods of evaluating relevant data were also transferred from information systems that were formed on the basis of paper media information [14]. Limitations in *IS*, which were implemented in digital structures of means of protection:

– n_k – the number of assessments used was limited;

– n_s – the method of determining this or that assessment depended significantly on the subjective factors of the users;

– n_a – general analysis of a set of data that had different estimates was quite difficult to conduct, since interdependencies between different estimates were described by relatively simple relationships.

An example of such evaluations is the four-level evaluations known from the Bell-Lapaduli models and others and defined as «available data», «data for official use», «secret data» and «top secret data» [15]. When moving to *IS* implemented in digital systems, it becomes possible to use significantly more levels of assessments that can be defined within the chosen measurement scale. The use of a small number of gradations for data evaluations will be called a coarse-discrete evaluation system, and accordingly, the scale of their measurements will be called a coarse-discrete scale. Analyzing the well-known assessment models, we include scales in which the number of assessment levels $R\left(\widehat{O}\right)$ is no more than five, or: $R \le 5$. A peculiarity of the coarse-discrete scale is that each assessment is determined exclusively based on the subjective considerations of the user, who in most cases is the owner of the relevant data [16].

In the case of a fine-discrete rating system, or when using a fine-discrete scale (FDS), the following opportunities arise for the formation of signs of importance in case of data loss, which affect the possibility of documentary information attacks (table 1, fig. 5):

– m_1 – to automate the process of determining ratings based on factors that are interpretatively related to the corresponding ratings and which excludes the process of forming a certain interpretation by the user (the need for a separate rating with *FDS*);

– m_2 – the measure of DDH readings can be implemented in the direction of decreasing the value of a separate dimension in the rating scale, even if for the corresponding reading level, the interpretation of the corresponding rating levels is established, in an explicit form by the consumer;

– m_3 – when reducing the discretization level of *RO*, it is necessary to establish some limit of such reduction δ(*RO*), after which the reduction of *RO* cannot have a reasonable interpretation.

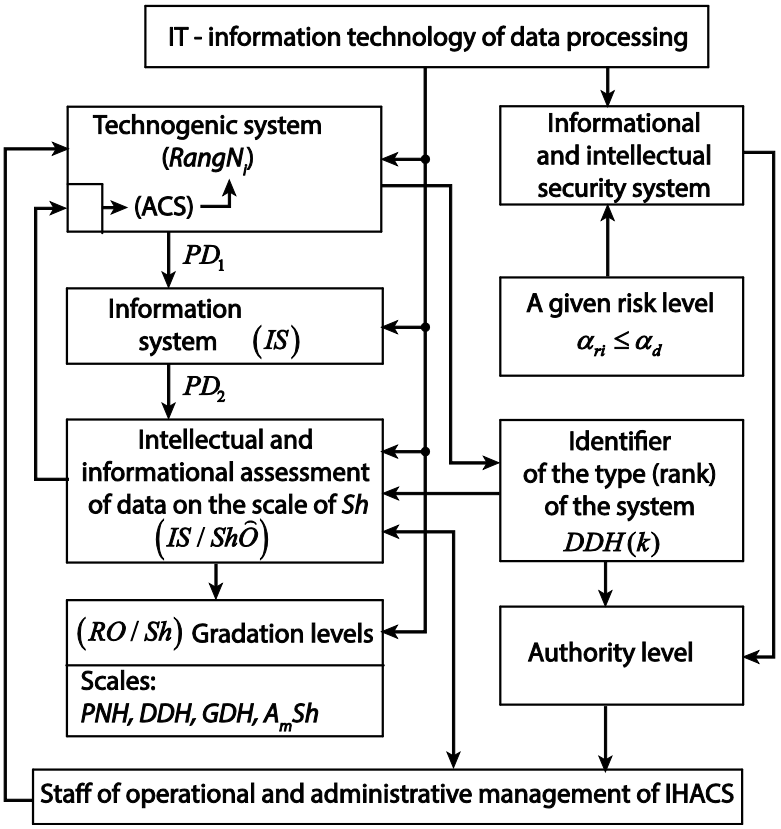

Figure 5 – Logical-cognitive structural diagram of formation of authorities of access to operational and strategic level data

When the FDS reaches the level of $Shr\left(\widehat{RO}\right)$, we have a pseudo-continuous data rating scale (*PCS*). We will refer to a scale of this type as a continuous scale from the point of view of the methods of analysis of the corresponding assessments. In order to determine the analytical features of the evaluation system, we will analyze at a qualitative level the reasons that determine the expediency of using the appropriate evaluations. The object of assessments should not be only data. The objects of assessments can be the processes operating in the information system (IS), individual programs and other components used to implement the functioning processes as a whole. Different objects are included in the classes of the system, they can be evaluated based on different interpretations. A separate system of scales $[Shi(\widehat{O})]$ must be used for each individual system. At the general level of evaluation of the information system, it is necessary to consider the methods of integration of evaluations in different systems. Let us denote rating systems by *FDS(K),* where *K* is the identifier of the system in which the rating is performed.

Consider the system of assignment of powers in which, to the maximum possible extent, the possibility of introducing subjective factors into the determination of powers related to the rights to use information in documents is excluded. For known object evaluation models, we will call them categories, and we will assign subjects to different classes [17]. As part of this approach, the authorization management system (AMS) consists of the following components (fig. 6):

– k_1 – managing the assignment of categories to each individual object;

– k_2 – the management component and definition of the class of the subject that can have certain powers in relation to the objects;

– k_3 – component of relationships between classes and categories;

– k_4 – component of defining the current category of a separate object;

– k_5 – component of defining the current category to a separate subject.

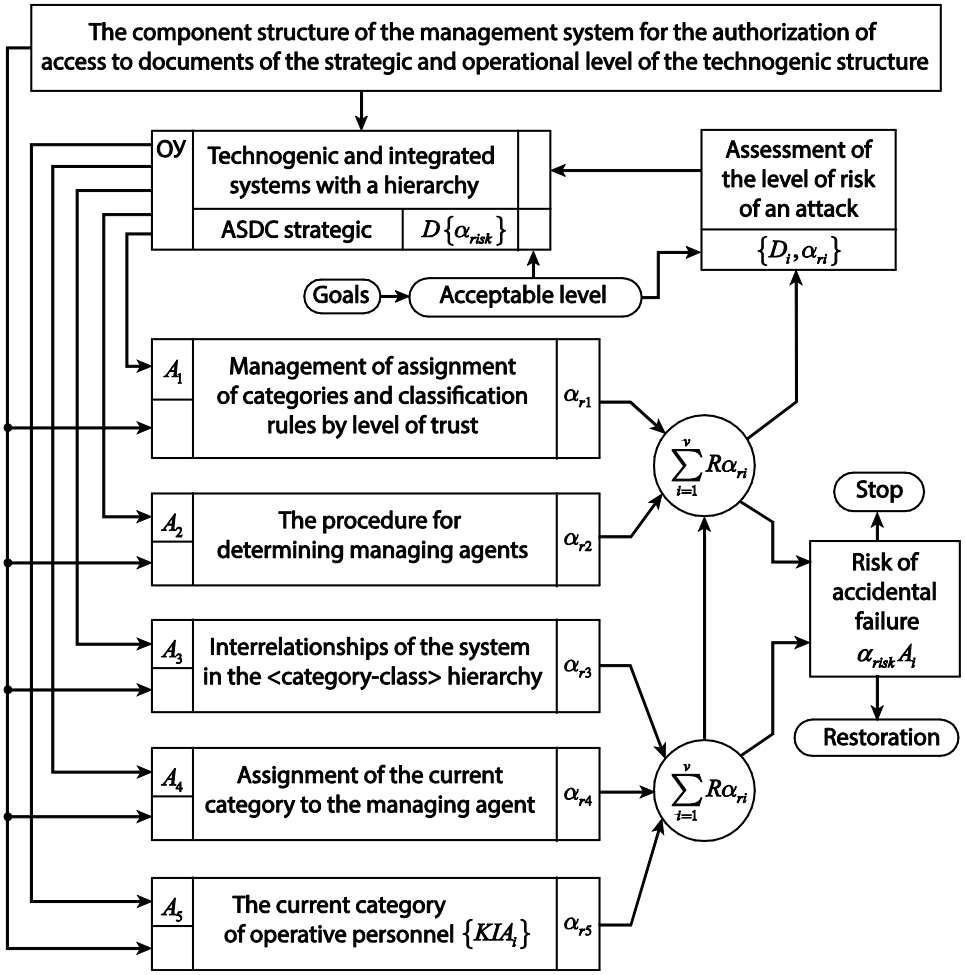

Figure 6 – Component structure of information technology for the ADMS access authority management system

At the initial stage of the formation of the authorization system, all objects and subjects that are known at the time of the installation of the authorization management system receive categories and classes according to the data on the subject area to which they belong [1]. At this stage, the degree of subjectivity is maximum for AMS, since the description of the subject area is formed by specialists who specialize in the relevant subject area, databases and knowledge(W_i, BD, BZ).

At the following stages of the operation of the authority management system, authority management is implemented in accordance with the following factors of executive actions:

– F_{p1} – a change in the class of subjects, which is caused by events that take place in W_i and are the processes of authentication of subjects;

– F_{p2} – on the basis of data obtained as a result of monitoring the access rights of individual subjects to the relevant objects;

– F_{p3} – based on events occurring in W_i and associated with objects and subjects;

– F_{p4} – based on category changes in objects;

– F_{p5} – based on data on attacks on the data system, which is a component (W_i – a class of system description ontologies).

Let's consider the theoretical basis of the description and research of methods of managing the assignment of categories to each individual object or group of objects. Since there can be quite a lot of individual objects, we will consider not individual objects but their classes, and we will move to individual objects based on individual conditions, which we will call conditions of detailing.

We will introduce the principle provisions that determine the methods of assigning a category to an object x_i, which will be formally denoted by $x_i\left(k_j\right)$, where x_i is the object; k_j is the *j-th* category of the object x_i.

According to the known estimates, we will assume that the categories are mutually dependent. Such a dependence corresponds to the growth of the category number, which can be formally written as follows:

$$K = \left\{k_1 < k_2 < k_3 < \ldots < k_n\right\}.$$

In this case, the interpretation of different categories is fundamental. We will interpret the category k_i as a measure of secrecy. This means that if $t_i < t_j$ exists, the secrecy level of k_j will be higher than the secrecy level of k_i.

Since the categories for objects x_i within the authority management system must change automatically, it is necessary to decide on the criteria used to determine k_i for x_i. For this purpose, we introduce the following definitions.

Definition 1. The degree of secrecy $\mu_i\left(k / x\right)$ of the category k_i of the object x_i is higher, the smaller the number of subjects y_i has the authority to use the object x_i.

If we assume that $\left\langle x_i\left(k_i\right)\right.$ and $x_j\left(k_j\right)$, then $\left.k_j > k_i\right\rangle$, then $\left\langle \sum_{i=1}^{n} y_i > \sum_{j=1}^{n} y_j \right.$, where $y_i = f_i\left(x_i\right)$, and $\left.y_j = f_j\left(x_j\right)\right\rangle \Rightarrow \left(\min \alpha_{risk}\left(f_i \in F\right)\right)$, where f_i is a function describing the types of powers relative to x_i (similarly for f_j).

Accordingly, a categorical diagram of the degree of secrecy of the object with respect to the system is constructed (Fig. 7). In this case, there may be a situation when x_i is an object that is not functionally needed by subjects of class y_i and therefore the latter do not use x_i.

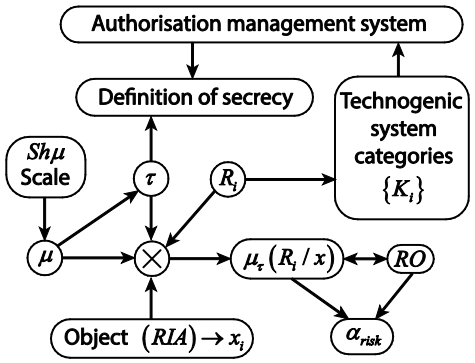

Figure 7 – Categorical diagram of the formation of the degree of secrecy of the object in relation to the authority management system

To avoid the corresponding contradiction, we assume that all objects x_i from X, where $X \subset W_i$, are functionally required by all of y_i from Y, where $Y \subset W_i$. Such a condition is justified if we take into account that all objects X and all subjects Y are components of one system, and the tasks solved within the framework of the relevant information system are closely related to each other.

This condition means that both ($x_i \in X$ i $y_i \in Y$) are functionally homogeneous within the framework of the information system. Accordingly, in the case where x_i and y_i from IS are not functionally homogeneous and individual subjects use only their functionally necessary objects x_i, then the task of introducing and using concepts about categories k_i for x_i and, accordingly, introducing and using concepts of classes for y_i would not be relevant.

Research results

With the help of mathematical logic methods for the formal description of management systems for access to operational data and the use of ranking scales, a method of ranking the importance of data for making operational and strategic decisions in hierarchical structures, which affects the management process, has been developed.

A categorical diagram of the formation of the degree of secrecy of the object in relation to the authority management system and the information system in general has been developed, which allows creating a model of authority management for technogenic hierarchical management systems.

A survey of specialists and system administrators of automated authority management systems (AAMS) was conducted in order to increase the reliability of the assessment of the level of importance of data loss in the hierarchy of management systems. Based on the studied data, a table of ranking scales of the importance of data loss is given.

Research results can be implemented in the design of the management and protection system not only for AAMS, but also for any complex systems with a hierarchical structure in the conditions of threat and crisis situations.

Conclusions

An analysis of the information support of the authorization management system, which is based on the functioning of automated document management systems with a hierarchical structure in the conditions of threats, was carried out, on the basis of which a structural-terminal cyclic scheme of the technogenic hierarchy management process was developed and substantiated in the conditions of the risk of threats and attacks.

The structural and functional scheme for managing access rights to the ADMS of the technogenic integrated system is substantiated and developed, the set of powers for the management process and document flow based on the access rights management system is described, the structure of the construction and functioning of the AMS is considered.

The problems of optimizing the security level of authority management in hierarchical production structures were analyzed, as a result of which a structural-functional scheme of information technology for protecting access to ADMS for agents of different levels of the hierarchy was proposed.

The main functions of AMS, developed in the security policy for any organization with a hierarchical structure, events related to the implementation of access attacks were studied, on the basis of which the information technology and the structural scheme of the implementation of the security policy for the authority management system were developed.

References.

1. Durnyak, B.V., Sabat, V.I., & Shvedova, L.E. (2016). Authority management in information protection systems: Monograph. UAP.

2. Veres, O.M. (2010). Decision support technologies. (In general ed. V.V. Pasichnika). Lviv Polytechnic.

3. Sikora, L.S. (1998). Systemology of decision-making and management in complex technological structures. Kamenyar.

4. Sikora, L., Lysa, N., Tkachuk, R., Sabat, V., & Fedevych, O. (2021). Information Technology of Risk Assessment for Automated Control Systems of Printing Production. CITRisk'2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, 1-15. https://sci.ldubgd.edu.ua/bitstream/123456789/9708/1/4_St_2021.pdf.

5. Kunchenko-Kharchenko, V.T. (2015). Information and management documentation in hierarchical systems: Concepts of information protection. UAP.

6. Pavlov, A.A., Grisha, S.N., Tomashevsky, V.N., Sinyavsky, E.P. et al. (1991). Fundamentals of system analysis and design of automated control systems. (Under total ed. A. A. Pavlova). Vyschaya shk.

7. Sabat, V., Sikora, L., Durnyak, B., Lysa, N., & Fedevych, O. (2022) Information technologies of active control of complex hierarchical systems under threats and information attacks. The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2022), (3156), 305-318. http://www.scopus.com/inward/record.url?eid=2-s2.0-85133627478&partnerID=MN8TOARS.

8. Domarev, V.V. (2001). Safety of information technologies. Methodology of creation of protection systems. TID "DS".

9. Kobozeva, A.A., Machalin, A.A., & Khoroshko, V.O. (2010). Security analysis of information systems. DUIKT.

10. Vasylenko, V.O., & Shostka, V.T. (2003). Situational management. KTSUL.

11. Vertuzaev, M.S., & Yurchenko, O.M. (2001). Protection of information in computer systems against unauthorized access. European university.

12. Boolos, J., & Jeffrey, R. (1994). Computability and logic. Mir.

13. Hrytsunov, O.V. (2010). Information systems and technologies: teaching manual for students studying "Transport technology". KhNAMG.

14. Sergienko, I.V. (1985). Mathematical models and methods of solving discrete optimization problems. Naukova dumka.

15. Androshchuk, G.A., & Krainev, P.P. (2000). Economic security of the enterprise: protection of trade secrets. In Yure.

16. Tymchenko, A.A. (2000). Fundamentals of system design and system analysis of complex objects. Lybid.

17. Ushakova, I.O., & Plekhanova, G.O. (2009). Information systems and technologies at the enterprise. Ed. Khneu.