Volume XXV, 49 – No.2, 2023, DOI: 10.35116/aa.2023.0009

RISK ASSESSMENT OF AN AUTOMATED DOCUMENT MANAGEMENT SYSTEM IN A HIERARCHICAL MANAGEMENT SYSTEM

Volodymyr SABAT[1*], Bohdan DURNYAK[1*], Taras DYTKO[2], Oleksandr ONUFREI[2]
[1] Ukrainian Academy of Printing, 79020, Pid Goloskom Street, 19, Ukraine.
[2]Uzhhorod National University, 88000, Narodna Square, 3, Ukraine.
**Corresponding author.* E-mail: v_sabat@ukr.net, bohdan.durnyak@gmail.com

Abstract. The functioning of any document management system in the infrastructure of a hierarchical process control system is to ensure uninterrupted work with documents at all stages of their use for the system's subjects, from designers, administrators to users and executors. Only with a well-established security system with an authorization management system can an automated document management system (ADMS) achieve efficient operation. In its turn, the security system of the automated document management system is based on the developed security policy and risk management system. The paper considers the infrastructure of an automated document management system, methods for assessing risk levels, which determine the choice of security tools and determining the level of security for a hierarchical management system. The proposed research results have been tested in the functioning of security systems at airports with a hierarchical structure of process control.

Keywords: information security systems, airports, risk assessment, automated document management systems, hierarchical process control systems.

1. INTRODUCTION

Today, most document management systems contain paper documents in addition to electronic documents, which also have a specific procedure for their functioning in the information system. However, effective work with large amounts of information contained in documents is only possible when switching from paper to electronic documents with the subsequent implementation of an automated electronic document management system.

The joint use of electronic document management systems, the Internet and internal local networks with servers for document databases and archival repositories allows information to be structured by specific areas, research fields and topics. This makes it easier to search for information contained in documents, analyze and process it, which is necessary to support decision-making by a hierarchical management system.

The analysis of the problem of emergency and risk situations in a hierarchical process control system, under the influence of active threats and attacks, showed the importance of building models of attack penetration channels and methods of attacking the hierarchical structure of the system.

The work [1] presents the basics of information security, the monograph [2] discusses methods for determining threats and levels of security; in the collective work of scientists [3] and [4] highlighted the main provisions of risk assessment and management, in particular the use of quantitative and qualitative assessment methods, the application of game theory. In the work [5], a theoretical study was conducted on the development of a mathematical hybrid model for assessing the risks of the functioning of information modules of critical infrastructure objects in different modes in order to actively support the decision-making process. The proposed model can assess the risks of functioning of information modules, uses the intellectual analysis of experts' knowledge, reveals the ambiguity of input estimates and increases the validity of the process of making further management decisions based on the obtained results. In this study [6], an educational information model and software were

developed, which are designed to assess the risks of the airport network and information systems. These resources are primarily aimed at providing aviation education and training of specialists to ensure safe and sustainable air transport. In the works by [7] and [8], a method of risk assessment in cases of man-made incidents was developed, and permissible risk norms were determined when making decisions by the operator in the control system. These studies reveal the essence of hierarchical systems and their vulnerability to man-made disasters under the influence of external attacks and internal threats. Modern developed methods for analyzing general industrial control systems for hierarchical technogenic structures are presented in the works of scientists [9] and [10], and for complex risk management systems, they are given in [11]. In the research in [12-13], a model-based methodology for hybrid risk assessment management for critical systems is proposed. The result is a method for analyzing cybersecurity risks for industrial control systems.

Nevertheless, to date, there has been no thorough systematic analysis of risk assessment in automated document management systems with a hierarchical management system under the influence of active threats of resource, information and cognitive types based on categorical models of channels of influence on the management process.

The aim of the study is to develop a methodology for risk assessment in hierarchical process control systems under the influence of active threats and attacks.

2. RISK MANAGEMENT IN ADMS

In order to assess the risk in modern ADMS in the structure of hierarchical technological systems, it is necessary to identify the main vulnerabilities and threats at the stages of the electronic document life cycle, as well as to investigate countermeasures in security system for the selection and processing of control data.

1. Vulnerabilities of the ADMS are identified by experts from the security services based on the analysis of the LDC vulnerabilities and monitoring of all security procedures at the stage of creation, routing and use of documents. It is necessary to determine the availability of possible access points to information (both in electronic and physical form) and the reliability of the systems in the organization. Such procedures may include: Internet connection; remote access points; connections to other organizations; physical access to the organization's premises; user access points; access points via wireless network.

For each point, you need to assess the information and systems and identify ways to access them. In addition, it is necessary to make sure that this list includes all known vulnerabilities of operating systems and applications, management and data processing systems (Fig. 1).

2. The main goal of ADMS security is to protect the information contained in documents from threats. Threats are assessed according to the amount of damage that may be caused to the EDMS as a result of the realization of the relevant threats. Damages may include loss of public trust or lowering the image of the organization of the EDMS in the society, liability before the law, threatening the safety of personnel, etc. However, they ultimately boil down to financial losses. The possibility of a threat being realized is characterized by the level of risk, which in turn depends on the vulnerability of the system. In other words, to protect documents and the information contained in them, it is necessary to reduce their vulnerability to an acceptable limit. At the same time, the cost of measures aimed at reducing the vulnerability of the ACS should not exceed the amount of damage that may be caused by the implementation of threats.

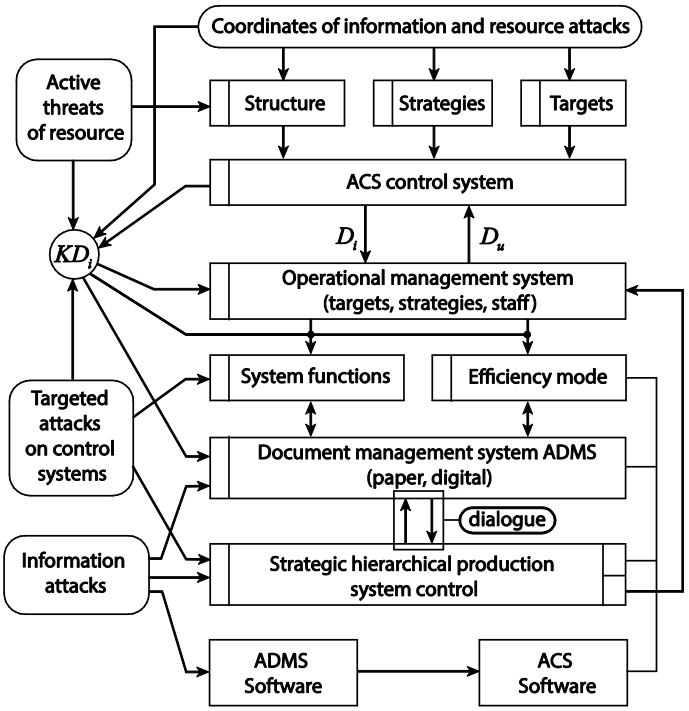

Figure 1. Coordinates (access points) in the ADMS integrated ACS in the implementation of information and resource attacks

3. An ADMS in an information system (IS) which is considered as one of the assets of an enterprise or organization. In turn, the ADMS consists of other assets and units that also need to be protected. Since the intended use of an ADMS is important for the organization's operations, it requires a detailed risk analysis.

A detailed analysis of the overall risk to IS involves identifying all risks and assessing their level of impact on the management process (integrated ACS).

Establishing possible boundaries for risk consideration is intended to clearly define which resources should be considered when considering the results of the risk analysis. When considering the risks of the ADMS, it is necessary to take into account the following factors that characterize management activities (Fig. 2):

- AF_i are information technology assets (hardware, software, information contained in documents), as they form the software and hardware basis for the functioning of the ADMS;
- KF_j is a the staff of the organization (working with and servicing the ADMS) as a source of possible threats and conflicts, and regime failures;
- RF_n are conditions of production activities, as they affect the normal functioning of the automated data processing system, failure of the regime and management;
- DF_k is a business activities, which is the main purpose of the ADMS.

For the purpose of detailed risk analysis, we will present the ADMS as a set of three components: information part, organizational work with personnel and hardware part. The functioning of the ADMS is impossible if at least one of its components does not function, i.e., disruption of the normal operation of at least one of them will lead to disruption of the operation of the other components and the entire system. Let us consider in more detail each of the components of the ADMS in the system of information support for the processes of formation and decision-making at the levels of the hierarchy of the cyber-technogenic production system according to Fig. 2.

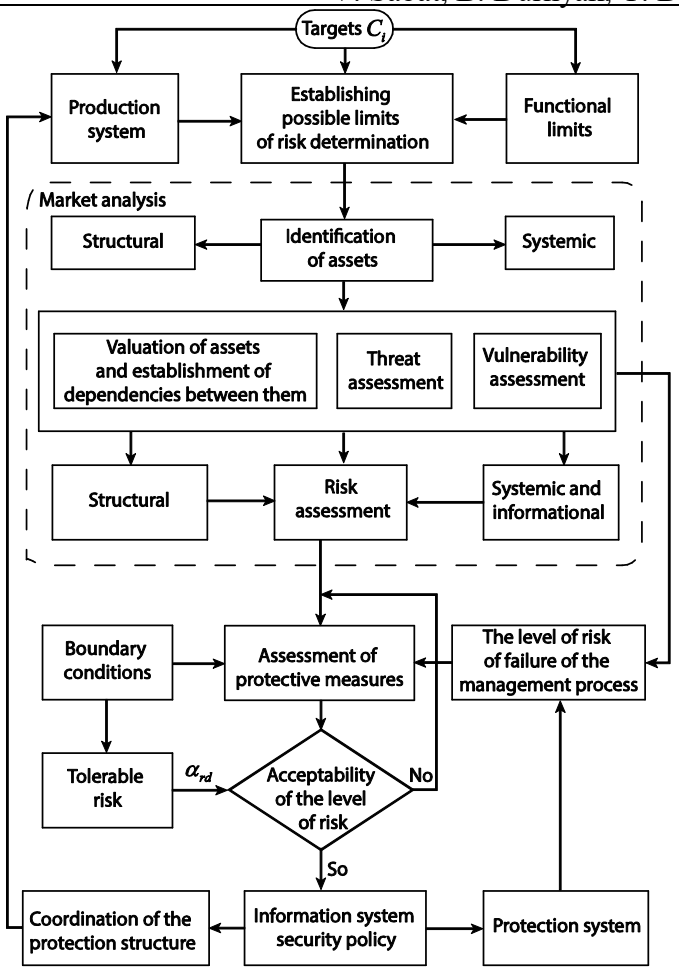

Figure 2. Functional diagram of risk management information technology based on the method of intelligent analysis of data flows in the integrated ACS

The system has the following levels of functioning in the context of countering threats:

- R_1 is a method for assessing risk limits;
- R_2 is a systematic identification of risk types;
- R_3 is assessment of the level of threats;
- R_4 is assessing the level of risks from attacks;
- R_5 is assessment of the system security level;
- R_6 is a level of security strategy development.

3. THE INFRASTRUCTURE OF THE ADMS

I. The information component of the automated document management system combines all the information that operates within the automated document management system, as well as incoming and outgoing information flows of documents, which corresponds to the method of representing the situation in the form of a categorical diagram of information processes in the automated document management system - man-made infrastructure (Fig. 3).

To analyze the information infrastructure of the automated document management system, a structural diagram of connections was developed on the basis of functional and categorical diagrams of data flows distribution.

The notation in Fig. 3: SU_d is a document management system; KIK are commands; F_{Ri}, F_{Sj} are external factors of information and structural risks; $\{A_i\}$ are attack triggers.

According to the scheme shown in Fig. 3, the functions of a typical automated data processing system are presented in the form of a hierarchical structure of information blocks that perform data processing operations necessary for making management decisions:

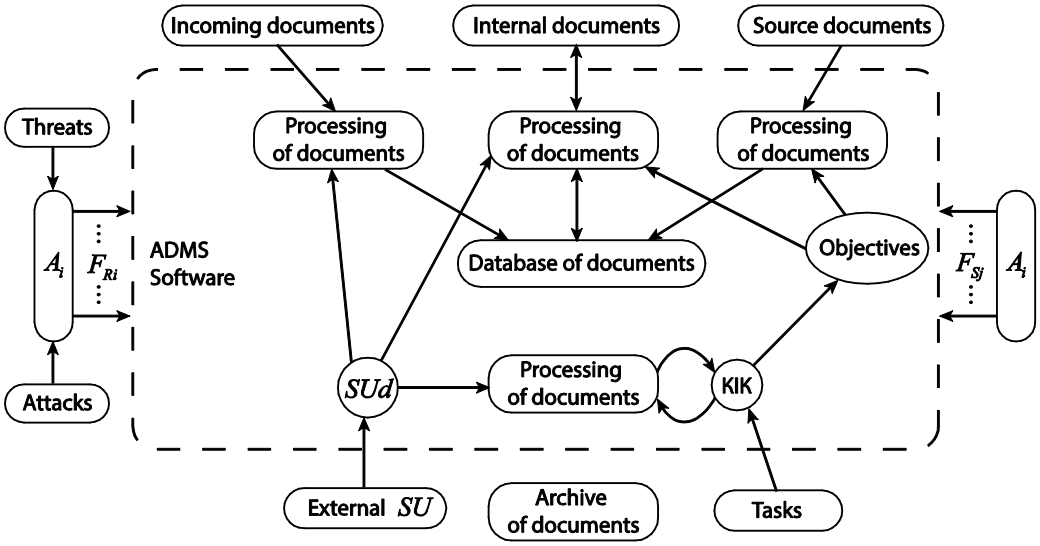

Figure 3. Categorical diagram of the ADMS information component

1. Input information (various incoming documents and their details, commercial information), process flows of parametric data and control commands.

2. Financial accounting data are processed by the program modules of the ADMS and entered into the central database (DB), which is managed by the ADMS;

3. In the process of work, various internal divisions of the enterprise access the central database through the relevant program modules - internal information exchange takes place as a basis for high-quality operational management;

4. During the operation of the automated data processing system, the relevant modules generate initial information (requests for materials, documents, operational accounting data) required at both the operational and strategic levels;

5. To ensure the reliability of work, the information of the central database is periodically archived and protected.

II. Software is a separate integral part of the information component of the automated data and information system. The software is used to create, transfer and transform information that operates in the ADMS. Software can be conditionally divided into main and auxiliary software.

The main software includes software modules for creating and processing information that operates in the ADMS, as well as the central database (DB) - the core of the ADMS. It can store a wide variety of information required in the process of working on documents.

Auxiliary software ensures the operation of the main software. This includes the operating system, drivers, various utilities, etc.

3.1. Hierarchical structures of operational and strategic levels

When determining software risk levels, we take into account its compliance with security requirements. The use of unlicensed software or third-party applications increases the risk of virus attacks through exploits, which are vulnerabilities in the software. This requires compliance with software updates of operating systems and all security software (including antivirus programs and other security components).

III. Hardware of the ADMS. The hardware of the ADMS includes devices that provide information exchange between components within the IS, as well as between the ADMS and the external environment, namely

- resources: servers, workstations, mobile computers;
- peripheral equipment: printers, scanners, webcams, etc;
- equipment for communication: networks and network equipment;

devices for communication with production equipment: controllers.

A server is an information structure - a resource that contains valuable information and requires controlled access. Accordingly, a workstation of the structure system is a resource that contains valuable information and to which only authorized access is possible, a mobile computer is a resource that contains valuable information and can be taken by the user outside the organization. [7]

To determine the levels of risk associated with the operation of the ADMS hardware, it is necessary to take into account not only the possibility of physical access to them, but also the possibility of remote control and remote access via external networks. Therefore, it is necessary to properly configure access modules on firewalls. As a result of scanning the network through a packet filtering firewall, more vulnerabilities are usually displayed than when scanning through an application layer firewall. It is also necessary to take into account the threat of access to confidential information when using wireless communication.

IV. Personnel. The term "personnel" refers to people - professionally trained intelligent cognitive agents serving the ADMS (for example, system administrators), as well as users, administrators and performers. When developing the infrastructure security policy, organizational work among the staff on improving the security of work in the ADMS within the framework of integrated ACS security is taken into account. Each employee should have appropriate knowledge and skills of working with documents, fulfil his/her official duties to comply with all procedures developed in the security policy. The greater the level of access of a particular subject of the security system to protected documents and objects of the ADMS, the greater the requirements for compliance with the rules and procedures of the security policy. At the same time, all services of the security system should be involved and control and monitor the production process, because due to the lack of security awareness of personnel, or the so-called "human factor", the most devastating and unpredictable attacks on IS are carried out, which end in emergencies and accidents.

4. METHOD OF RISK ASSESSMENT OF THE MANAGEMENT PROCESS

To assess the risk, it is necessary to identify document vulnerabilities at all stages of the PLC. However, the mere existence of document vulnerabilities does not cause damage to the ADMS, as this requires the existence of a corresponding threat to the document. The existence of a vulnerability in the absence of such a threat does not require protective measures, but the vulnerability should be recorded and further verified in case the situation changes. Security safeguards that are not used correctly or do not function properly can themselves become sources of vulnerabilities. Vulnerability assessments are conducted only for critical threats in the ADMS, as there is no point in assessing vulnerabilities for non-critical threats, as well as for those that are very unlikely to occur.

The probability of vulnerability realization and, accordingly, the level of risk in the process of managing complex hierarchical structures can be assessed on different scales. This conditional division can be considered for different modes of functional load of the system.

Klymenko S. M. and Dubrova O. S. distinguish four risk zones: risk-free zone, zone of acceptable risk, zone of critical risk, and zone of catastrophic risk [4]. In addition, they substantiate in their work that in order to make managerial decisions, it is necessary to take into account the acceptability and feasibility of risk, as well as the likelihood that possible losses that may arise in a risky situation will not exceed a certain level and are within the tolerance, that is, the $R = p\left(x \le x_0\right)$, where x_0 is a the limit value of a certain level of loss. V. V. Vitlinsky and G. I. Velykoivanenko consider this indicator to be the main one in risk assessment [7]. The described methodology in most scientific works is called the "method of analyzing possible losses" [8].

To determine the strategy of sustainable management, we present a diagram of risk scaling in a system with a hierarchical structure, taking into account such factors as reliability, stability, robustness, and controllability of the system under different modes of its functional load and performance (Fig. 4).

The designations in Fig. 4: $\{V_{ri}\}$ is a defined areas of risk intervals; $\{P_{zi}\}$ is intermediate zones of transition of risk values when the load changes or under the influence of attacks; α_{risk} is a risk factor $\alpha_{risk} \in [0 \div 1]$; P_n is a load mode power; $\{I_i\}$ is a intervals for splitting the state space and load mode.

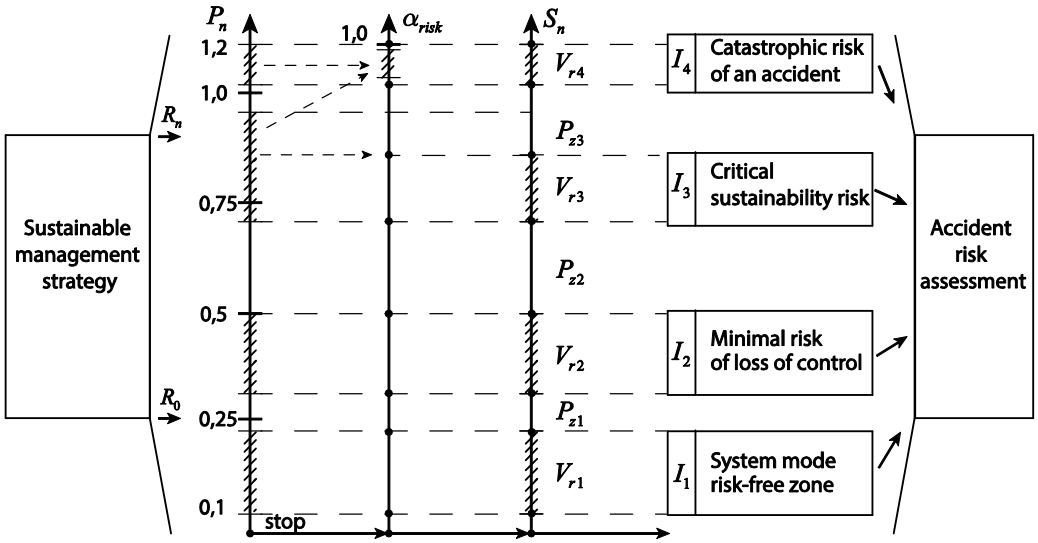

Figure 4. Scaling the risk zone in a system with a hierarchical structure (reliability, stability, robustness, controllability) under different modes of functional load (performance)

4.1. Models of scales for assessing the risk of emergency situations in automated document management systems

To select adequate protective measures, it is necessary to assess the magnitude of risks. The amount of risk in the ADMS depends on the value of the asset, the criticality of the threat, and the probability and frequency of the threat. The amount of risk will be determined by formula (1) based on a probabilistic approach:

$$R_{i,j} = V_j \times K_{i,j} \times P_{j,i} \times W_{j,i} \times Q_i^{\Sigma} \tag{1}$$

where: V_j is the value of the *j*-th asset; $K_{i,j}$ is a criticality *i*-th threat for *j*-th asset; $P_{j,i}$ is occurrence probability of an *i*-th threat for *j*-th asset; $W_{j,i}$ is a the frequency of occurrence of the *i*-th threat to the *j*-th asset during the year; Q_i^{Σ} is the total value obtained as a result of the vulnerability assessment for the *i*-th threat.

Vulnerability assessment, as opposed to risk level, is determined by a ratio:

$$Q_i^{\Sigma} = \sum_{q=1}^{n} P_q^T \tag{2}$$

where: P_q^T is the probability of vulnerability *q* for the *i*-th threat; *n* is the number of vulnerabilities exploited by the *i*-th threat.

The value of the total risk for the *i*-th threat is determined according to Eq:

$$R_i^{\Sigma} = \sum_{j=1}^{s} R_{i,j}, \tag{3}$$

where s is a total number of threats.

As a result of risk assessment, a numerical value is determined for each threat, which characterizes the degree of risk caused by this threat in the ADMS. In this way, it is possible to rank threats in order of decreasing risk caused by them and to create adequate protective measures in the security system to counteract the relevant threats. This method allows to develop a risk management system in the security system not only for the ADMS, but also for any organization and system that needs to protect its assets, structure, functions.

Accordingly, risk scales are built that reflect the situation in the system:

1. Percentage scale of risk assessment:

$$\min_{T_w}\left|\alpha_{risk}\left(t_i,T_m\right)\right| \equiv P_{rob}\left[\frac{\Delta n_a\left(t_i\right)}{N_T}\times 100\% \to 0\right] = 1,$$

where: n_a is a successful attacks on the structure and dynamics of the system in a timely manner T_m.

2. *Relative risk scale* based on an assessment of the probability of transition to the emergency area of the system under the influence of threats:

$$\max_{T_w}\left|\alpha_{risk}\left(t_i,T_m\right)\right| \equiv P_{rob}\left[\frac{\Delta n_a\left(sit\right)}{N_a} \to 1, \forall t \in T_n\right],$$

where: Δn_a is a successful attacks on the system over time T_n; N_a is a the total number of attacks implemented.

3. *An absolute index scale for assessing the level of risk*:

$$\max_{T_w}\left|\alpha_{risk}\left(t_i,T_m\right)\right| \equiv \min_{T_w}\left[\Delta p_n = \left|P_d - P\left(t,T_m\right)\right|\right],$$

where P_d is a the permissible level of functional load (Fig. 5).

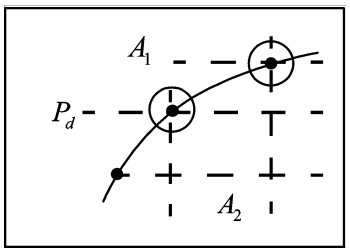

Figure 5. Determining the permissible level of functional load

4. The risk scale is related to the mode of loading and operation of the units:

$$\max_{T_w}\left|\alpha_{risk}\left(t_i,T_m\right)\right| \equiv P_{rob}\left(y\left(t,T_m / C_i\left(u\right)\right) \geq L_d^+\right) \to 1,$$

at $L_d^+ \subset M\left\{L_{\min}^+, L_i^+, L_n^+, L_g^+, L_d^+, L_A^+\right\}$ is a designation of the mode lines when splitting the state space and the target space into alternative regions:

$$V_{ai} \subset \left|L_{i+1}, L_i\right|, \dim\left|L_{i+1}, L_i\right| > 0 + \Delta,\ \forall L_i \subset StratIIS_{AS}.$$

Accordingly, based on the procedure for recognizing the situation in the system, the rank of trajectory deviation is determined by the state parameter $\left\{Rang\,|+\Delta_i\,|-\Delta_j\,|\right\}$ and an appropriate management decision is made.

5. SUMMARY AND CONCLUSIONS

Based on the study of the management system of hierarchical structures ensuring the technological process of production, it is concluded that for the effective operation of such systems it is necessary to use automated systems of document management and control over the execution of documents. This is primarily due to the fact that the information in the designed documents contains management actions aimed at performing certain processes of production at the terminal technological cycle, and due to the control over the execution of such processes, the document management system generates reporting documents on the completion of the process. Thus, the execution of documents ensures the smooth operation of the entire production process control system. However, like any information technology system, the ADMS is vulnerable to external negative influences and attacks.

The paper analyzes the way the ADMS-functions in the hierarchical structure of technological process control in the face of attacks and the ways to protect such systems. An analysis of the information infrastructure of the automated document management system is carried out, based on functional and categorical diagrams of data flow distribution, a structural diagram of connections is developed, on the basis of which a method of identifying access points with determining the coordinates of information and resource attacks on the automated document management system in the form of a functional diagram and a description of threats to the system is proposed.

An assessment of the level of vulnerability of the ADMS under the influence of threats to the hierarchical system and determination of the levels of acceptable risk to the system's functional load mode on their basis are carried out.

Structural diagrams of risk management information technologies, categorical diagrams of production processes, risk assessment scales were developed, which forms the basis for the further formation of system and information security technology.

Research results can be used to create and improve airport security and safety systems, but can also be used in any field of technological production with complex hierarchical management systems.

In the future, the authors set themselves the task of developing software for the possibility of practical use of the conducted research.

REFERENCES

[1] Andreev V.I., Khoroshko V. O., Cherednychenko V. S., Shelest M. E. (2009) Basics of information security. K.: DUIKT, 2009. 292 p. (In Ukrainian).

[2] Bobalo Y.Ya., Gorbaty I.V., Bondarev A. P. Information security. Lviv: Lviv Polytechnic University, 2012. 580 p. (In Ukrainian).

[3] Kravchenko M. O., Boyarinova K. O., Kopishinska K. O. Risk management / Study guide. Kyiv: KPI named after Igor Sikorsky, 2021. 432 p. (In Ukrainian).

[4] Klymenko S. M., Dubrova O. S. Justification of business decisions and risk assessment. Education manual. K.: KNEU, 2005. 252 p. (In Ukrainian).

[5] V. Polishchuk, Yu. Mlavets, I. Rozora, O. Tymoshenko (2023) A hybrid model of risk assessment of the functioning of information modules of critical infrastructure objects. Procedia Computer Science, Volume 219, pp. 76-83, https://doi.org/10.1016/j.procs.2023.01.266.

[6] M. Kelemen, V. Polishchuk, B. Gavurová, R. Andoga, S. Szabo, W. Yang, J. Christodoulakis, M. Gera, J. Kozuba, P. Kaľavský, M. Antoško (2020) Educational Model for Evaluation of Airport NIS Security for Safe and Sustainable Air Transport. Sustainability 12, 6352. https://doi.org/10.3390/su12166352.

[7] Vitlinsky V. V., Velikoivanenko G. I. Riskology in economics and entrepreneurship. Monograph. K.: KNEU, 2004. 480 p. (In Ukrainian).

[8] V. V. Lukyanova, T. V. Golovach Economic risk. Education manual K.: Akadem-publisher, 2007. 464 p. (In Ukrainian).

[9] F. Sicard, É. Zamai, J.M. Flaus (2019) An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems. Reliab Eng Syst Saf, 188 (2019), pp. 584-603, 10.1016/j.ress.2019.03.020

[10] A. Cormier, C. Ng. (2020) Integrating cybersecurity in hazard and risk analyses. J Loss Prev Process Ind, 64, Article 104044, 10.1016/j.jlp.2020.104044
[11] L. Vessels, K. Heffner, D. Johnson (2019) Cybersecurity risk assessment for space systems. 2019 IEEE Space Comput Conf (SCC), pp. 11-19, 10.1109/SpaceComp.2019.00006
[12] Jarmo Alanen, Joonas Linnosmaa, Timo Malm, Nikolaos Papakonstantinou, Toni Ahonen, Eetu Heikkilä, Risto Tiusanen (2022) Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems, Reliability Engineering & System Safety, Volume 220, Article 108270, 10.1016/j.ress.2021.108270.
[13] 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) Khmelnytskyi (In Ukrainian).

Received 09, 2023, accepted 12, 2023