Methods for assessing the risk of an emergency in the security system for the information complex of printing enterprises

Volodymyr Sabat[1,*,†], Lyubomyr Sikora[2,†], Bohdan Durniak[1,†], Vitalii Matsiuk[1,†], and Pavlo Hibey[1,†]

[1] *Ukrainian Academy of Printing, 19 Pid Holoskom Str., Lviv, 79000, Ukraine*
[2] *Lviv Polytechnic National University, 12 Stepan Bandera St., Lviv, 79000, Ukraine*

Abstract

The article analyzes the concepts of risk and security in a hierarchical automated control system (ACS) of a printing enterprise, presents the main algorithms for assessing the risk of emergencies in the technological process of an enterprise (TPE). Algorithms and methods of building information technologies for automatic determination of risk and security level of information complexes and systems of enterprise technological process control in view of active threats and attacks are substantiated and developed. The information and system technology for countering threats and attacks is proposed and the list of printing house assets in the order of decreasing risk exposure is given on the basis of experimental studies. The proposed approaches for determining the magnitude of risk and, accordingly, the level of security can be used for any enterprise with a hierarchical structure of technological process management.

Keywords

threats, attacks, risk, safety, hierarchical system management

1. Introduction

The analysis of the problem of emergencies in a hierarchical system of technological printing process control, under the influence of active threats and attacks, has shown the importance of building models for assessing the risk of emergencies due to cyber attacks on the hierarchical structure of the system. In the process of printing production, new threats arise related to critical infrastructure, power outages and the supply of necessary materials and tools for prompt system recovery after incidents and emergency production stoppages. All of this places new demands on the implementation of preventive protection measures and analysis of emergency risk situations in real-world conditions of military operations, without stopping the production process. Many works of both domestic and foreign scientists are devoted to the problems of risk assessment in protection systems, but these problems are of the greatest relevance nowadays, when emergency production stoppages can lead to the destruction of the entire infrastructure of critical technogenic energy-intensive enterprises.

Paper [3] investigates information technologies for controlling the occurrence of emergencies in complex hierarchical systems in the face of threats and information attacks. The risk assessment is based on determining the probability and frequency of threats and vulnerabilities to the assets of printing enterprises. Paper [2] investigates the relationships between risk, vulnerability, and threats

IntelITSIS'2024: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 28, 2024, Khmelnytskyi, Ukraine

* Corresponding author.
† These authors contributed equally.
v_sabat@ukr.net (V. Sabat); sikirdayuliya@ukr.net (L. Sikora); bohdan.durnyak@gmail.com (B. Durnyak); altentop17@yahoo.com (V. Matsiuk); pavlo.hibey@gmail.com (P. Hibey)
0000-0001-8130-7837 (V. Sabat); 0000-0002-7446-1980 (L. Sikora); 0000-0003-1526-9005 (B. Durnyak); 0009-0006-2283-5246 (V. Matsiuk); 0009-0008-2034-1060 (P. Hibey)

in the operation of metallurgical enterprises. The author points out the need to reassess the risk associated with changes in the structure of the control organization or security policy in the protection system. Means of counteracting external attacks are related to the concept of risk and require constant correction in the assessment process. The risk is associated with the reliability of the functioning of the studied control structure of nodes and units and affects their ability to function in accordance with the mode and goals of the production structure in various industries and hierarchy levels with an acceptable risk assessment. The scientific article [11] presents an educational information model and software for risk assessment of the airport network and information systems based on the application of the fuzzy logic method in the air transport environment. However, the proposed model is not able to assess the systemic negative impact on the management of the technological process in the face of threats and attacks. Paper [12] investigates the magnitude of the risk and the level of safety of subway passengers in cases of malicious technological incidents. The paper emphasizes the importance of protecting passengers to improve safety and avoid emergencies, using the example of the Athens metro system. Based on the research, the author points out the vulnerability of hierarchical systems to man-made disasters under the influence of external attacks and internal threats. The scientific article [13] proposes the use of an object-oriented Bayesian network to assess the risk of emergency scenarios for ships. A model for determining the key factors of hazardous situations has been developed that captures the dynamic dependencies and interdependencies between the main variables and establishes the degree of their influence on the probability of an accident. Methods of vector (multi-criteria) optimization in the development of a protection system are presented in [14]. Particular attention is paid to the process of assessing the correctness of decisions made in solving information security problems for a particular object. In [15], a study of risk analysis methods for various enterprises and organizations was conducted. Four methods of analyzing information security risks using ontologies based on hybrid risk assessment management models are proposed: reliability, availability, maintainability, and security for critical systems. These methods were developed for analyzing cybersecurity risks for industrial control systems and for the development of ISO/IEC 27.005, 2018 security standards to provide a step-by-step understanding of the meaning of security concepts and their relationships.

By analyzing the above scientific works, methods and means of protecting automated document management systems with a hierarchical management structure for printing enterprises were developed.

The system of protection of the information complex of printing enterprises is based on the analysis and assessment of the risk value to build optimal protective measures and operation of the information system in a stable mode of protection against possible attacks. At the same time, risk assessment can be carried out using classical methods based on the analysis and identification of possible threats and vulnerabilities to the assets of a printing enterprise, as well as appropriate protective measures implemented to counter possible attacks in the security system. However, among the available literature sources, there is little information on the availability of risk models that would automate this process of assessing the risk in the information complex security system for hierarchical enterprises in real time of their operation. Given the relevance of these problems for building optimal protection systems, especially in our time of increasing cyberattacks on strategic management objects, the paper proposes new approaches to assessing the risk and level of security of the printing enterprise in the face of active threats and attacks.

2. Analysis of the concepts of risk and safety in the event of emergencies in hierarchical management systems of a printing enterprise

In contrast to risk, the security level indicates how dangerous the situation in the relevant information system or management system is in terms of possible losses. Let's consider some

differences between risk and security that justify the expediency of using the risk value in addition to the security level (Fig. 1). [1].

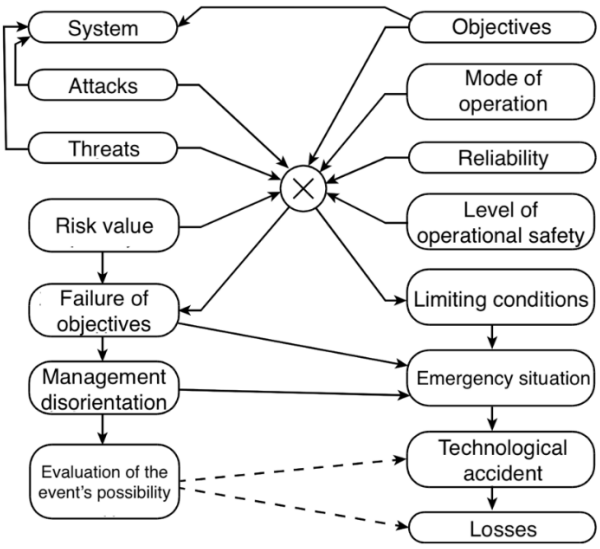

Figure 1: Categorical diagram of the relationship in terms of safety risk emergency situation due to threats, attacks.

The first difference between the risk parameter and the security parameter is the presence of some forecasting, which characterizes the concept of risk itself. Risk implies an assessment of a certain future, as opposed to a statement of fact, which provides an idea of the level of security.

The second feature of risk is the assessment of an event that should or may occur in the future, and the risk in this case determines what consequences the relevant event may lead to, taking into account its negative effect, and the risk in this case is directly related to the relevant event.

Risk, in terms of its interpretation, is a quantity used to measure losses resulting from the negative impact of an event. In this regard, risk is usually measured as a relative value, for example, as a percentage or as the amount of losses that may result from a particular event. [2]

In view of these features, it should be noted that the amount of risk cannot be precise and its determination should be based on the use of approximate methods and probable data. Risk is generally interpreted as an assessment of the negative characteristics of a certain reality. In general, it can be assumed that risk is used to assess events that may occur and have a negative interpretation. Therefore, the purpose of risk management is to determine the necessary actions that lead to its reduction or elimination of the risk in general. Risk is never used if there is no need to apply negative assessments of some events that should occur in the future. [3]

Given the above features of the interpretation of the concept of risk, it can be argued that the synthesis of risk models with the information security system is to assess the possibility of reducing the level of security of the system, provided that such a reduction is negative. The need to take this condition into account is determined by the fact that the concept of risk is associated with negative phenomena that are expected to be evaluated. The need to use this condition is based on the fact that the value of the security level Bz_i can not only increase but also decrease. In the second case of a change in the value of Bz_i, the interpretation of this change may be positive. This is due to the fact that ensuring a certain level of security of Bz_i requires appropriate costs, and security, which we will call protection, is required only if there are external attacks on the information management system IMS that reduce the level of security. If there are no such attacks on IMS, it is not advisable to invest in maintaining the security level of $Bz_i = \alpha$, but it can be reduced to a certain level: $Bz_i =$

β, where $\beta < \alpha$. At the same time, the reduction of the level Bz_i cannot be interpreted as a change in the risk value $R(t)$ of the functioning process IMS. [4]

For the correct implementation of the process of synthesizing $R(t)$ and of the Bz_i IMS, we accept the following conditions:

Condition 1. The risk value of $R(t)$ shall be calculated on the basis of statistical data or probable parameters characterizing the factors in relation to which it is calculated.

Condition 2. The calculation of risk should be based on the use of forecasting methods.

Condition 3. The amount of risk should relate to events or changes in the conditions of the facility's operation that may occur in a certain period of time ΔT.

Condition 4. In contrast to forecasting tasks, the risk value should be closely related to a change in a parameter, a factor or other events that directly cause a change in the risk value $R(z)$.

In order to separate the concept of a system's security measure from the concept of risk assessment, we accept the following conditions.

Condition 5. The security measure of the system Bz_i reflects the security level available in the system at the current time.

Condition 6. The Bz_i security measure is measured on the basis of data that reflects the security of the system.

Let's accept the following notation for the parameters:

- $Bz(IMS)$- security level of the management information system;
- $Sh(\alpha_{Bi})$ - safety factor scale $[0 \div 1]$;
- $\alpha_i(u, a_i)$ - the effectiveness of a successful attack;
- $\beta(a_i)$ - the effectiveness of any attack on $\tau_i \in T_m$.

For the sake of argument, let's assume that the security level of Bz_i is measured by the ratio of the number of successful attacks to the number of all attacks that were realized against IMS.
The number of successful attacks is determined based on the analysis and detection of anomalies resulting from such attacks and on the audit of the system for which Bz_i is determined. Thus, the value of Bz_i can be determined according to the ratio:

$$\forall ISU, \exists \mu(BZ_i): \langle BZ_i = \sum_{i=k}^{k}(\alpha_i(ua_i))/\sum_{j=1}^{n}\beta_j(a_j)\rangle \rightarrow SA_{risk}\begin{matrix}\nearrow \max \alpha_{risk} \\ \searrow \min \alpha_{risk}\end{matrix} \quad (1)$$

where α_i is the effectiveness ratio of a successful attack ua_i; k is the number of successful attacks; β_J is the effectiveness of any attack a_i, depending on the type of attack and the type of attack target; a_j is a separate attack, $\mu(BZ_i)$ is a security measure, SA_{risk} is an attack countermeasure. The number of neutralized or canceled attacks, which are mostly recorded, is described by the ratio at the interval of the terminal cycle of the attack and when countering threats:

$$\forall t_i \in T_{mi}, \exists Strat(U/PAt): \langle va_i = \left(\sum_{j=1}^{n}\beta_j(a_j)\right) - \left(\sum_{i=1}^{k}\alpha_i(ua_j)\right)\rangle \rightarrow \underbrace{\min \alpha_{risk}}_{\dot{T}}. \quad (2)$$

Let's look at the types of security. Each of the security types B_v, B_u, B_g and B_i is caused by the corresponding attacks. For example, B_v is determined by the failure of hardware components, B_u is safety due to control errors, B_g is safety due to emergency shutdowns, and B_i is safety due to emergency situations. On the one hand, the failure of a hardware component can be interpreted as an attack. In this case, the relevant attack is an event that is not caused by external factors. This type of attack can be activated by external factors, but we will not consider this possibility in order to ensure complete unambiguity among the set of attacks. Obviously, such a failure can also occur

with respect to software components. While in the first case the failure may be caused by physical processes occurring in the software components, in the second case the failure may occur due to the fact that the program contained an error that was not noticed at the stage of testing the finished software product. In the first case, the attack is described by the reliability parameters of hardware elements, and in the second case, by parameters that characterize the probability that a certain number of errors remain in the program after testing. An example of a model that describes the presence of errors remaining in a program system after testing is the following ratio:

$$f_0 = \ln(N/U) + \sum_{i=1}^{t} N_i \ln N_i + \sum_{i=1}^{t}(N - N_i)\ln(N - N_i) - N\ln N, \quad (3)$$

where N is the total number of errors in the program; U is the sum of errors detected by t independent tests, and it is assumed that, $U < N$, N_i is the number of errors detected by i [5]. In the first and second cases, the events that lead to failures are probabilistic in nature. It should be noted that if the probability estimates of these events do not change, their occurrence corresponds to a certain level of security BZ_i. Risk assessment occurs when there is a prerequisite for changing the corresponding probability estimate of random processes that lead to a change in the security of the system BZ_i. Such prerequisites may include not only the occurrence of external negative factors, but also changes that occur within the framework of the system IMS. An example of such changes may be a change in the mode of operation IMS, associated with the need to change the structures of the enterprise's technological process. This may be due to the need to launch new products and other *TPE-related* factors. The above example illustrates one of the cases when, in addition to the value of BZ_i of a certain system, it is necessary to calculate the value of risk $R(t)$

One method of determining the assessment of the local component of $R_i(t) \in GR_i(t)$ risk $R(t)$ can be used in the following case. Let's assume that *TPE* uses IMS, which can be affected by external and internal factors. To ensure a certain functional stability, the control system IMS must provide a given level of safety of Bz_i. We will not consider other components of the *TPE* system. If external or internal reinforcing factors occur by chance, but the estimates of these probable events are stable, then the IMS protection means, based on known estimates of the probability of reinforcing factors, can activate the means of monitoring and counteracting the negative impact of the relevant factors on IMS. If there are known prerequisites for changing such assessments, it is necessary to calculate the risk of reducing the level of safety Bz_j, where $Bz_j < Bz_i$ or the risk value described by the ratio: $R(t) \leq Bz_i - Bz_j$, which means a decrease in the level of security. In order to calculate the value of $R(t)$, the data on the relevant preconditions will be denoted by $H(h_i)$, where h_i are certain parameters of the precondition H. <If such a precondition H were fully known, there would be no need to calculate the risk $R(t)$>, and new probabilistic parameters of the factors that affect the level of security could be calculated immediately. Based on such estimates, the discipline of monitoring the relevant attacks could be modified and the appropriate defenses could be activated, which determine the components of overall security B_v, B_u, B_g and B_i. Then it is advisable to define a parameter by which the overall characteristic for all components can be assessed. [6]

In probability theory, the concept of parameter estimation is used for such purposes. [7] Such estimates are described by the following characteristics: unbiased estimation; estimation efficiency; and estimation validity.

1. The non-displacement of the estimate means that the $\hat{\theta}$ estimate of the θ parameter corresponds to the ratio $\mu(\hat{\theta}) = \theta$, where μ is the mathematical expectation.
2. If the unbiased estimate has the smallest variance among all estimates of θ, then this estimate is effective.

3. If the inequality corresponding to the law of large numbers is fulfilled for the estimate of $\hat{\theta}$, or the following ratio is available: $\lim_{n\to\infty}\{P|\hat{\theta}-\theta|<\varepsilon\}=1$ then the estimate of $\hat{\theta}$ is called reasonable.

One common parameter estimate is a random variable equal to the sum of the squares n of independent random variables u_i, each of which follows a normal distribution law with parameters $\mu=0$ and $\sigma^2=1$ and is called a random variable with distribution $\aleph^2$, and is described by the relation:

$$\aleph^2=\sum_{i=1}^{n}u_i^2, \tag{4}$$

where $u_i^2=(\omega/\sigma_i)^2$, $\omega^2=(\aleph_i-\mu)^2$, μ, σ are the mathematical expectation and variance, respectively, $\aleph_i$ is a series of independent observations, each of which follows a normal distribution law. The differential distribution function $\aleph^2$ with k - degrees of freedom is written in the form:

$$f(\aleph^2)=L(n)\cdot\aleph^{n-2}e^{-x^2}/2, \tag{5}$$

where $L(n)$ is a coefficient that depends on the sample size; $\aleph$ is the current variable; n - number of items in the sample.

If the parameter c^2 is greater than the accepted limit, it means that it is not permissible to use all the factors that cause the risk increase together, since each of the causes will have a distribution of random values that may dominate other distributions.

R_v, R_u, R_g to do this, it is necessary to calculate the risks of unacceptable situations separately for each of the reasons that lead to deviations from the current values of the safety levels, which were referred to as B_v, B_u, B_g and B_i, and which in this case will determine the respective components of the risk values and R_i.

The overall risk of R_z is determined as a function of the above components for each type of system (ACS and IAS) and type of attack:

$$\forall F_m, \exists Strat(U/B_i): \langle R_z=f(R_v,R_u,R_g,R_i)\rangle \to \underbrace{\min\sum_{T}\alpha_{risk}^{s}}. \tag{6}$$

One of the features of the $R(t)$ risk assessment is the assessment of changes that may be reflected in the system in the event of activation of an event by external factors. At the level of qualitative interpretation, this means that it is necessary to assess the risk that the situation in the system will deteriorate when a particular action is taken on the system. Since the system is affected by external factors that lead to a decrease in the level of security Bz_i, in the case of using risk assessment, an event and, accordingly, an external factor may occur that differs from the already known negative factors for the security systemBz_i. [8]

In order to distinguish these events from each other, we will introduce the following definitions of situation and event.

Definition 1. Events that adversely affect a certain object, protection against which is realized by means of protection under the control of the security system Bz and are mostly known to the security system, will be called regular negative factors RNF.

Definition 2. Events that may adversely affect the object of protection, which are one-time in terms of their impact on the relevant system, will be called single negative factors ONF.

Let's define the overall risk of a threat situation through the components of active influence on system objects:

$$\alpha_{risk} = \langle R_z(t_i \in T_m, \tau_i)\rangle; \tag{7}$$

then, accordingly, the multiplicative model has the form (Fig. 2):

$$R_z = f\left(R_v, R_u, R_g, R_i\right) \rightarrow \otimes_{i=1}^{n} A(R_i) \cdot W_i, \tag{8}$$

where $A(R_i)$ is a multiplicative attack operator;
α_{risk} - a multiplicative threat operator;
R_v - risks of transition to the marginal regime;
R_u - risks associated with management errors;
R_g - risks of emergency shutdown;
R_i - risks of an emergency situation;
$\langle t_i, t_i, T_m \rangle$ - terminal marker.

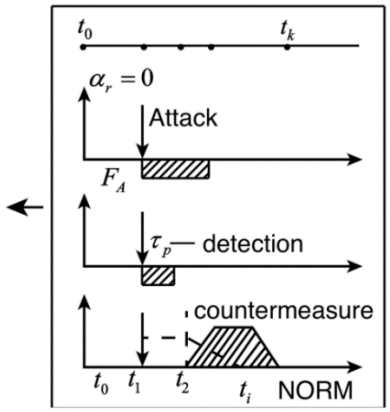

Figure 2: Diagram of countering attacks

Accordingly, the overall level of security is related to the level of risk through the operator $\delta(B_i)$, for which we have the corresponding balance.

If $\left[\underbrace{\max \delta(B_i/\forall t_i \in T_m)}_{T_m}\right]$ and $\left[\alpha_r(t_i \in T_m) \rightarrow \underbrace{\min \alpha_{drisk}}_{T_m}\right]$, that is, minimizing the active impact of threats on the system through a set of countermeasures leads to an increase in the security of the hierarchical system.

Single negative factors, if they are repeated with frequencies close to the repetitions of RNF, then becomes ONF, RNF and their effect is assessed by the Bz system, not by means of calculating the risk $R(t)$. The transition of individual factors from RNF to ONF is not considered, because by the time of such a transition, the Bz system has enough information about the functioning of factors of the RNF class, and therefore it makes no sense to talk about the risk of such a factor's impact on the system. [9]

In this case, a factor of the type ONF can be formed by the user in such a way that the corresponding factor has a positive effect on the system. IMS Before this factor is activated, it is studied within the system model, so that the nature of its impact on can be determined quite accurately and there is no need to determine the value of $R(t)$.

If some factor such as ONF is formed to act on IMS, but the way it acts may change in the process of its activation and it may become a negative factor NF, then in such cases it is relevant to determine the risk that the factor will cause negative changes as a result of its action on IMS, which will be interpreted as a decrease in the level of security.

If the active factor y_i is dependent on one or a small number of variables $x_1, \dots, x_k$, then the nature of the impact on IMS can be determined quite accurately and there is no need to determine the value of risk $R(t)$, which by definition has a negative interpretation.

Therefore, we will set the risk value only for factors y_i that are dependent on a significant number of arguments or independent variables.

Definition 3. Let the basic model for determining the value of R_i risk be a multiple linear regression, then we accept the following interpretation of the elements of the linear regression, which is described by the relation:

$$\pi(x) = a_0 + a_1 x_1 + \cdots + a_n x_n, \tag{9}$$

where a_i are the regression coefficients to be determined. Typically, such coefficients are determined by the least squares principle described by the following relation:

$$\{Q = \sum[y - (a_0 + a_1 x_1 + \cdots + a_n x_n)]^2\} \to Qmin, \tag{10}$$

We sequentially differentiate this equation for all n-coefficients and get a system of equations:

$$\begin{cases} na_0 + a_1 \sum x_1 + a_2 \sum x_2 + \cdots + a_n \sum x_n = \sum y\,, \\ a_0 \sum x_1 + a_1 x_1^2 + a_2 \sum x_1 x_2 + \cdots + a_n \sum x_1 x_n = \sum x_1 y\,, \\ \cdots \\ a_0 \sum x_n + a_1 \sum x_1 x_n + a_2 \sum x_2 x_n + \cdots + a_n \sum x_n^2 = \sum x_n y. \end{cases}, \tag{11}$$

The above system of equations is transformed in such a way that the calculation of regression coefficients is as simple as possible.

For the practical use of this approach, it is necessary to consider the interpretation of all elements of the model that would correspond to acceptable ideas about the risk and the purpose of using the calculated value $R(t)$. Within the IMS system, the Zz protection means are used, which are organized within the $Bz_i = \{Zz_i, \dots, Zz_n\}$ security system, and the means of determining the risk of the system R_i.

Bz thesystem is characterized by a security level, which will be further denoted as $\mu(Bz)$. The security level, as mentioned above, depends on the total number of attacks and attacks that have been eliminated by the security features of Bz. The more attacks were eliminated, the higher the level of $\mu(Bz)$. If the number of attacks initiated against IMS decreases, then the number of attacks that have been prevented by the security features will also decrease. Thus, $\mu(Bz)$ remains the same regardless of the number of attacks launched against IMS. Risk, by its interpretation, is the inverse of security. The interpretation of security is as follows. The value of the security level characterizes the current state of IMS 's capabilities in terms of the system's suitability for solving the main application tasks. This means that different classes of tasks that are solved in the TPE environment require different levels of security $\mu(Bz) = \alpha$. Therefore, the main task of the security system is to maintain a certain level of security of IMS and, accordingly, TPE, which is equal to $\mu(Bz) = \alpha_i$.

The magnitude of the risk in relation to its interpretation characterizes the possibility of negative changes in the object, and depending on these changes, the risk is measured. Therefore, to determine the risk, it is important to identify the object in which changes are expected and what the risk may be. Let's assume that the risk will be a decrease in the value of the security level $\mu(Bz)$. We will not consider further development of the interpretation of this aspect. Obviously, in this case, an increase in the value of the level of security is not a risk. To avoid duplicating the concept of risk with the concept of safety, let us assume that risk determines the amount of decrease in the level of safety $\mu(Bz)$. Then we can introduce the following definition:

Definition 4. Risk is an assessment of the possible magnitude of a negative change in the level of security.

In order to designate a security derivative, the function of changing the security level must be represented in a certain form.

Definition 5. Let us assume that in the process of functioning of IMS and, accordingly, the security management system (SMS) at each fixed moment of time t_i, the value $\mu(Bz_i)$ takes on certain values. This can be represented as the ratio $\mu(Bz_i) = \alpha_i$.

Accordingly, the level of security can be determined by the following ratio:

$$\mu(Bz_i) = \alpha_i = \sum_{i=1}^{k} At_i / At_i^n, \tag{12}$$

where At_i - attacks detected and neutralized during the operation of; SMS At_i^n - all attacks possible at the time of t_i that have been activated against IMS.

Using the selected approximation function, you can get an approximate description of the function of changing the value of the security level of $\mu(Bz)$ under the influence of threats and attacks:

$$\mu(Bz) = f(Bz, Bz_i, t), \tag{13}$$

where t is the time of operation of SMS.

Since $R(t)$ predicts the assessment of a negative change in the value of the security level, the event with which the risk is associated may belong to the factors of negative impact on IMS. These factors in this study belong to the category of attacks on IMS. Therefore, the event for which the risk value is supposed to be determined reduces the level of security of IMS, which can occur if a negative single event of the type occurs $At_i(ONF)$.

We define the conceptual system procedures for assessing the level of risk arising in a hierarchical automated control system under the influence of threats and the stages of their implementation.

Procedure I - predicting the occurrence of an event $At_i(ONF)$, which is focused on the impact of the management information system and the security management system.

Procedure II - determining the mechanism of action of $At_i(ONF)$ on IMS in order to calculate the amount of losses that may result from this event.

Procedure III - determination based on the synthesis of the forecast result with the amount of losses caused by activation $At_i(ONF)$.

Procedure IV - determination of the relationship between IMS, which is affected by $At_i(ONF)$, and SMS, which should counteract the relevant factor. Based on this analysis, the magnitude of changes that will occur in IMS, which, due to the protective functions of SMS, will be smaller compared to the changes in IMS that would occur if SMS were not used, is estimated.

Procedure V - the process of systematic formulation of an adequate interpretation of the risk value for IMS as a result of a possible action of $At_i(ONF)$ is performed.

An adequate interpretation of the accident risk assessment is to develop a method:

- determination of the amount of losses resulting from the resulting risk;
- selection of units of measurement of such losses;
- determining the probability of losses by combining the above interpretive descriptions.

The method of performing system procedures is implemented in a certain sequence. First, by applying regression models that use statistical samples of possible attacks, the task of predicting the

occurrence of $At_i(ONF)$ is solved. Forecasting provides information on when and under what conditions the predicted event may occur. [10]

Subsequently, the $At_i(ONF)$ recognition operation is performed based on modeling the effect of a possible attack on the system. The purpose of attack recognition is to determine the appropriate measure of protection for the SMS system. As a result, the negative impact of $At_i(ONF)$ on IMS can be reduced.

At the next stage, an assessment is made to determine the possible losses that, for example, can be projected onto the cost of products to be produced by TPE under the control of the IMS system. Thus, with the help of the described methods of solving the problem, it becomes possible to form an adequate interpretation of the value of the risk $R(t)$. In accordance with the definition of the risk, it is necessary to introduce certain protection measures that reduce the vulnerability of assets to various threats and make it impossible to carry out attacks. Thus, on the basis of detecting the magnitude of the risk, the protection system detects weak points in the security system and counteracts possible external attacks on the hierarchical management system.

3. Experimental research

To assess the risk in automated document management systems (ADMS) used to manage the technological process of printing enterprises, the main vulnerabilities and threats at the stages of the life cycle of both paper and electronic documents were identified, and countermeasures in the security system were investigated.

Identification of *ACS* vulnerabilities began with an analysis of all security procedures: possible access points to information (both in electronic and physical form) and systems in the organization. These procedures 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, the cost of information and reliability of the systems were assessed and access methods were identified. In addition, the list included all known vulnerabilities in operating systems and applications. The analysis of vulnerabilities and threats to the assets of the printing enterprise was determined on the basis of surveys conducted among system administrators of Ukrainian printing enterprises in order to increase the reliability of the assessment of criticality, probability of implementation and frequency of threats [2,3]. The respondents were sent a diagram of dependencies between the assets of the automated printing production management system (APMS), a table with a list of assets and threats to the APMS, and were asked to assess the criticality, probability and frequency of threats for each APMS asset, taking into account the dependencies between the assets, as well as the vulnerability of these assets to critical threats.

A targeted threat is a combination of a specific agent with knowledge, access, and motivation and a specific event aimed at a specific target. Identifying all targeted threats is time-consuming and challenging. An alternative is to determine the overall threat level, which does not require knowledge of the targeted or specific threat addressed to the company's unit the agent is acting on (Figure 3).

When studying existing countermeasures, it is necessary to identify possible attack paths and protective measures when an attacker implements possible threats. Such countermeasures and protective measures include (Figure 3):

- K_1 - firewalls for all levels of the management hierarchy;
- K_2 - anti-virus software for ACS and ADMS;
- K_3 - access control to prevent intrusion into the system;
- K_4 - a two-factor authentication system for attack indicators;

- K_5 - identification card of the authorized agent;
- K_6 - biometrics for each management agent;
- K_7 - smart card readers at the entrance to the premises;
- K_8 - security - external, internal and systemic;
- K_9 - control of access to files in the database structure of the ACS, ADMS;
- K_{10} - encryption of data flows, schemes, and design solutions;
- K_{11} - training employees in the organization's security policy;
- K_{12} - intrusion detection systems based on attack indicators;
- K_{13}, K_{14} - automated receipt of updates from intrusion prevention in the structure and control system.

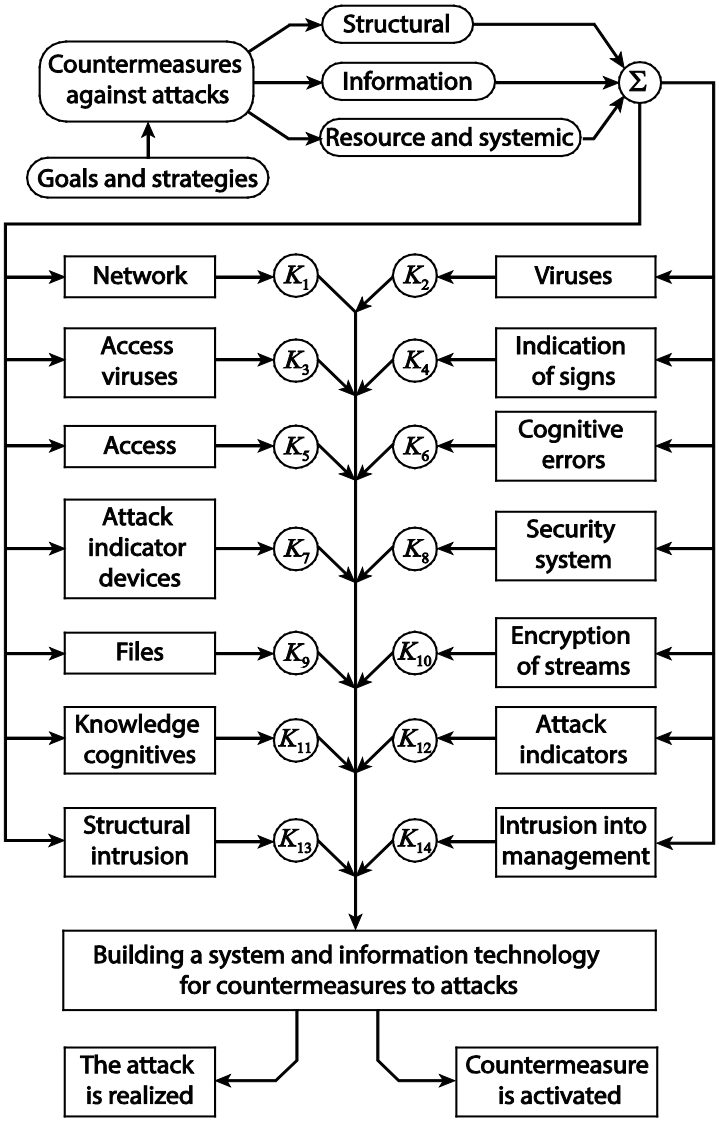

Figure 3: Information and system technology for countering threats and attacks

The study of vulnerabilities and threats conducted in this paper allowed us to determine the complex level of risk for the assets of the ACS in the order of ranking the level of risk for each asset (Table 1).

Table 1
List of assets in order of decreasing risk exposure

No. s/n	Asset	Risk appetite
1.	Prestige of the organization	19035
2.	Services	19035
3.	Internal data	15669
4.	Central database	13506
5.	Source files	12177
6.	Auxiliary software	11454
7.	Program modules of the ACS	7098
8.	Servers	4527
9.	Workstations	3834
10.	Hard copies	3704
11.	Networks	3465
12.	Mobile PCs	3288
13.	Archives	947

To assess the risk, we determined the damage caused to the organization if the attack is successful. This took into account the fact that the risk cannot be completely eliminated - it can only be managed to minimize losses from attacks and threats based on an assessment of the level and probability of negative impact $\{F_{ai} \rightarrow K_i\}$ for each impact factor.

4. Conclusions

An analysis of the concepts of risk and security in the face of threats and attacks on the information system of technological processes of enterprise is carried out. On the basis of the category diagram, a scheme of functional relationships of concepts that affect the levels of security and risk in the event of emergencies due to threats and attacks is built, which allows creating models for assessing the magnitude of risk.

The conditions for calculating the amount of risk and differences in approaches to assessing the security of information management systems are determined. It is proved that the measure of security is determined on the basis of the ratio of the number of successful attacks to the total number of attacks on the system at the terminal cycle of technological process control, and the risk assessment should be made when changing the corresponding probabilistic assessment of random processes that lead to a change in the security of the system.

The parameters that affect the risk value and lead to deviations in the current values of the levels of different types of security are identified. The author defines regular negative factors known to the security system and one-time negative factors. In the first case, such factors are assessed by the safety system and do not relate to the concept of risk, and in the second case, they require the introduction of tools for calculating the risk of emergencies.

The value of the security level that characterizes the state of the system to solve the main technological tasks in the face of threats and attacks, and different levels of security must be provided for different stages and technological objects.

To assess the risk, it is important to identify the objects in which changes occur in the terminal control cycle that lead to a decrease in the level of security. According to the above

algorithms and procedures, it is possible to develop information technologies for automatic determination of the risk and safety level for information complexes and process control systems.

The results of the research can be implemented in the design of a management and security system not only for printing enterprises, but also for any complex systems with a hierarchical structure in the face of threats and crises.

References

[1] Marvin Rausand, Stein Haugen, Risk Assessment: Theory, Methods, and Applications, 2nd Edition. John Wiley & Sons, Inc., 2020.

[2] V. Sabat, B. Durnyak, L. Sikora, V. Polishchuk, Research on the assessment of the risk situations emergence for automated control systems of the metallurgical industry companies. Acta Montanistica Slovaca, (2023) 201-213. doi:10.46544/AMS.v28i1.16

[3] V. Sabat, L. Sikora, B. Durnyak, N. Lysa, O. Fedevych, 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, Ukraine, 25–27.05 (2022): 305-318.

[4] M. Modarres, T. Zhou, M. Massoud. Advances in multi-unit nuclear power plant probabilistic risk assessment. Reliab Eng Syst Saf, (2017) 87-100. doi:10.1016/J.RESS.2016.08.005

[5] J.-M. Bruel, M. Mazzara, B. Meyer. Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment. Lecture Notes in Computer Science, 5-6.05 (2018). doi.org/10.1007/978-3-030-06019-0

[6] V. Domeh, F. Obeng, F. Khan, N. Bose, E. Sanli, Risk analysis of man overboard scenario in a small fishing vessel. Ocean Engineering, 229, (2021): 108979. doi:10.1016/j.oceaneng.2021.108979.

[7] Rick Durrett. Probability: Theory and Examples. Cambridge University Press, 2019.

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

[9] T. Zhou, M. Modarres, E.L. Droguett, Multi-unit nuclear power plant probabilistic risk assessment: a comprehensive survey. Reliab Eng Syst Saf, 213 (2021) 107782, doi:10.1016/J.RESS.2021.107782

[10] Lawrence Leemis. Mathematical Statistics. Ascended Ideas, 2020.

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

[12] Ch. Milioti, K. Kepaptsoglou, A. Deloukas, E. Apostolopoulou, Valuation of man-made incident risk perception in public transport: The case of the Athens metro, International Journal of Transportation Science and Technology, Volume 11, (2022) 578-588, doi:10.1016/j.ijtst.2021.07.003.

[13] V. Domeh, F. Obeng, F. Khan, N. Bose, E. Sanli, Risk analysis of man overboard scenario in a small fishing vessel. Ocean Engineering, Volume 229, (2021) 108979. doi:10.1016/j.oceaneng.2021.108979.

[14] V. Khoroshko, M. Brailovskyi, M. Kapustian, Multi-criteria assessment of the correctness of decision-making in information security tasks. International scientific journal «Computer systems and information technologies», 4 (2023) 81-86. doi:10.31891/csit-2023-4-11

[15] V.A. Agrawal. Comparative study on information security risk analysis methods. J Comput (Taipei), (2017) 57-67. doi:10.17706/jcp.12.1.57-67