Selection and Justification of Information Security Indicators for Materials Processing Systems

Igor Kotenko[1], *Igor* Parashchuk[1,*], and *Didier* El Baz[2]

[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS). St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), 199178, St. Petersburg, 14-th Liniya 39, Russia

[2] LAAS-CNRS, Université de Toulouse, Toulouse, France

Abstract. The paper examines an approach to formulating the composition of a non-redundant and rational set of information security indicators for modern materials processing systems. The approach is focused on taking into account the hierarchical relationships that exist between the processes and subsystems responsible for protecting information, taking into account the features and boundaries of modern requirements for the availability, integrity and confidentiality of information, and also takes into account the variety of factors affecting the information support of materials processing processes. A variant of the system of information security indicators for materials processing systems is proposed. Practical implementation of the approach to the selection and substantiation of information security indicators will improve the efficiency of security control of information support procedures for modern materials processing processes.

1 Introduction

Modern threats to information security for materials processing systems (MPSs) are complex and cyber-physical in nature, and security events are often correlated [1, 2]. These threats affect all cybernetic and physical levels, all multifaceted aspects of the activities of systems of this class, they are dangerous and difficult to predict. Therefore, the problems of protecting MPSs from various threats, the problems of monitoring integrated security in MPSs and the problems of information security management continue to be relevant [3].

An important feature is the fact that typical MPSs in the course of their activities carry out automated collection and processing of information necessary to optimize the control of technological equipment and materials processing processes. At the same time, for the collection and automated processing of information, for information communication of all MPS subsystems, industrial telecommunication networks are used. Networks of this class are traditionally controlled by the main processor of an industrial controller and contain special network interfaces, network and application software, as well as various computing,

* Corresponding author: shchuk@rambler.ru

automated sensor systems and other devices, united into a unified network based on wireless technologies [4].

In other words, along with a variety of traditional resources consumed by MPSs, information is one of the key resources. This, in turn, emphasizes the importance of ensuring the information security within the MPSs and the processes they implement. That is why the tasks associated with the search for new methods and means of managing the protection of information stored and processed in MPS continue to remain important, and the results of solving such problems are in demand.

One of the main stages of managing the protection of information stored and processed in MPSs is the stage of security analysis, i.e. the stage of assessing the quality and efficiency of the information security subsystem of MPS and the process it implements - the protection process [5, 6]. This stage makes it possible to form reliable, accurate and timely assessments of security indicators, and therefore, in turn, to formulate on their basis accurate and adequate control actions aimed at maintaining the information security of the MPS. It is assumed that timely, reliable, adequate, and, ultimately, efficient control actions will minimize the damage caused by malefactors.

The solution to the problem of MPS security analysis is a further development of approaches to the multi-criteria assessment of the level of information security of complex controlled production and information systems. This problem requires the introduction of additional conditions and restrictions, as well as the construction of fundamentally new models of the information security process in MPSs. Therefore, the regularization of the formulation and solution of the MPS security analysis problem is associated with the implementation of all those stages that are typical for assessing the level of information security in conditions of local temporary stationarity, but developed for the case of current assessment, which opens up the possibility of taking into account the dynamic nature of the change in the states of the information security subsystem and the information security (IS) process it implements.

All this emphasizes the importance of solving the problem of choosing and justifying a set of indicators of MPS information security, allowing one to take into account the dynamic and probabilistic nature of the process of functioning of the MPS information security subsystem and the process of protecting information in general, especially when the MPS interacts with production and information systems of general use. The paper examines a methodological approach aimed at obtaining a compact, non-redundant, but full-fledged set of information security indicators for MPSs in the interests of a reliable and complete assessment of the information security level of systems of this class.

2 Related works

A number of works [7-21] are devoted to the problems of selection and substantiation of information security indicators circulating in complex controlled production and information systems. They are aimed at increasing the reliability and adequacy of assessing the security level within the information security management of systems of this class.

For example, the works [7, 8] are known, in which it is stated that the algorithms for information security testing and monitoring for complex systems, as well as the algorithms for synthesizing optimal systems of security indicators can be implemented on the basis of expert assessments. At the same time, this approach requires large organizational, time and computational costs for collecting and processing data characterizing expert opinions.

There is a classical approach to assessing the information security on the basis of generalized (complex) and private security indicators [9]. But this approach is aimed at analyzing the vector indicators of network security, including the security indicators of network nodes, routers and individual links. Moreover, the analysis of such vector security

indicators requires the calculation of weight coefficients and the construction of probability density functions, which does not correspond to the general operational tasks facing the procedure for assessing the MPS information security.

Some solutions for the synthesis of a system of information security indicators are proposed in [10, 11], but here the choice and justification of the controlled parameters of information security is carried out for socio-cyber-physical systems and for monitoring of security incidents in conditions of uncertainty.

There are approaches that describe the methodology for choosing and justifying the scope and nomenclature of the set of estimated security parameters of complex systems and focused on mathematical (optimization) methods of decomposition, reduction and evolution. Their essence lies in the selection and justification of such a system of security indicators, which would be small, compact, but informative.

In particular, the options for setting and solving the parametric decomposition problem in the interests of optimizing the set of controlled parameters of information networks and indicators of their information security are formulated in [12, 13]. In [14], simple heuristic algorithms based on combinatorial solutions are proposed. The tensor approximation and ranking of tensors in [15] is proposed to be used in order to reduce the complexity of combinatorial decomposition algorithms, but tensor models applied to the problems of choosing and justifying information security indicators for MPSs do not guarantee a high solution accuracy. In [16] and [17], the approaches based on reduction methods are presented, including step-by-step scaling and reduction of the dimension of controlled indicators for complex systems and processes. However, these procedures are considered in these works under the condition of symmetry of the analyzed dynamical systems and processes, which significantly narrows the scope of these methods.

A variant of application of the reduction method is considered in [18]. The approach uses parametric reduction based on the approximating the ranks of various groups of indicators for a system or process. The advantages of the approach are obvious, but within the framework of the selection and justification of security indicators for materials processing systems, these methods require additional study of a variety of auxiliary (accompanying) parameters, which is often difficult for real MPSs.

In our opinion, the works [19-21] deserve special attention; they prove the necessity of synthesizing the optimal set of controlled indicators of complex systems and processes. In [19], it is argued that the input of control actions is impossible without the development and application of synthesis algorithms for a system of monitored and evaluated quality indicators, and these algorithms must operate in real time. In [20], it is said that reducing the number of monitored indicators is an important prerequisite for optimization. It allows you to reduce the cost of procedures for analyzing and managing complex systems (for example, an information security subsystems) and processes, such as the process of ensuring information security. In [21] the great importance of the problem of choosing and justifying security indicators (moreover, based on the availability, confidentiality and integrity of information) is noted for assessing the degree of security of control and diagnostic information about technological processes. This approach will be considered in our paper as well. It is the basis for the selection and justification of security indicators, but this paper does not consider the possible composition of the set of information security indicators for systems like MPSs.

Thus, the analysis of relevant works shows that the direct application of the results obtained in these works for the practical solution of the problems of choosing and justifying information security indicators for MPSs is impossible. Therefore, the unified approach proposed in the paper to solving the problem of formulating a hierarchical, non-redundant system of information security indicators, based on the interconnection of individual functioning processes and the information protection process as a whole, is relevant.

3 General formulation of the problem

The analysis of relevant works allows us to conclude that for assessing the security of information within the MPS framework, the system of security indicators (SSI) is applicable, formed using mathematical methods of the decomposition theory [12-15]. For a number of features, such as the presence of a large number of interrelated elements and processes, the possibility of splitting into subsystems and subprocesses, the complexity and versatility of the information security (IS) process in MPSs, active interaction with the external environment, the presence of automated control of the information security subsystem (ISS), the information security subsystem of the MPS can be related to complex systems, and the IS process - to complex processes.

Under these conditions, the generally accepted approach for complex systems and processes of the IS is applicable. It consists in the development of the main dominant SSI (DSSI) and the formulation of such a set of secondary local non-dominant SSI (NSSI), which corresponds to the totality of the properties of the IS process and the set of properties of the ISS that affect the performance of the task of ensuring the information security within the MPS. In this case, the DSSI, which characterizes the general, basic and unified task facing the ISS and the IS process, is obtained by combining the original NSSI in the materials processing systems.

In our case, within the framework of the general formulation of the problem of choosing and justifying information security indicators for MPSs, a method for forming a typical system of security indicators is proposed, which is somewhat different from traditional methods. It is proposed, based on the mathematical methods of the theory of decomposition (factorization, functional and parametric decomposition), instead of defining the NSSI of a low level of the hierarchy and then combining them into the DSSI, to consider the problem of ensuring information security within the framework of the MPS as a whole.

With this approach to assessing the MPS information security, the dimension of the problem being solved increases, since not one DSSI is formulated, but a set of hierarchically related NSSI. But on the other hand, the constructiveness of the solution to the problem of assessing security is ensured and the real current probabilistic characteristics of the ISS and the IS process are taken into account. The completeness and uniqueness of such an SSI is based on the fact that the initial data for its formulation are the requirements imposed by the user on the ISS and the IS process, mathematically correctly decomposed in the interests of their further use.

Here, the NSSI of a lower level of the hierarchy detail the internal properties of the ISS and the information security process, and the DSSI describes the external (user) properties of the ISS and the IS process in MPSs. This is due to the really existing dominant value of one process in the ISS - the process of information protection itself, over another process - the information security management process in MPSs.

In addition, in our opinion, modern international standards in the field of information security management, for example, ISO/IEC 27002:2013/COR 2:2015 and ISO/IEC 27000:2018 [22, 23], should serve as the most important criteria when choosing and justifying a system of information security indicators for MPSs.

Thus, using the hierarchy that characterizes the stage-by-stage decomposition of the general tasks of the functioning of complex systems [12, 13], it is possible to form a hierarchical system of security indicators for MPSs. From the point of view of the formulation of the general task of choosing and justifying information security indicators for MPSs, this hierarchy of indicators can and should include the DSSI and a number of hierarchical interconnected NSSI. This NSSI is the main non-dominant SSI - the system of indicators of the process of ensuring security (information protection process), as well as the NSSIs for information security management process.

4 Formulation of a variant of the information security indicators

Let us formulate and justify the composition of the DSSI and the main one of the NSSI - the system of indicators of the process of information protection.

The composition of the DSSI for the MPS developed for the case of security analysis is as follows:

$$\vec{Y}_{\text{SoI}}(k) = [\bar{t}_{\text{acc}}(k);\ K_{\text{loss reli}}(k);\ K_{\text{misr}}(k);\ K_{\text{konf}}(k);\ \vec{R}_{\text{SoI}}(k)]^{\text{T}}, \quad (1)$$

where $\bar{t}_{\text{acc}}(k)$ - the average time of accessing the authorized users (people and subsystems) of the MPS to the protected information resource at the *k*-th step of the functioning of the MPS ISS, which characterizes such a property of means and technology for secure processing of technological information as availability; $K_{\text{loss reli}}(k)$ - the coefficient of information reliability loss and $K_{\text{misr}}(k)$ - the coefficient of distortion characterizing the integrity property - the ability of the MPS ISS to keep information in a reliable and undistorted form, despite the presence of threats and vulnerabilities; $K_{\text{konf}}(k)$ – the coefficient of information confidentiality at the *k*-th step of the functioning of the MPS ISS, which characterizes the property of the ISS to keep information secret from subjects that do not have the authority to access it; as well as the vector of resource costs $\vec{R}_{\text{SoI}}(k)$ for the construction of the ISS and the implementation of the process of protecting information circulating in the MPS.

Among the NSSIs in the MPS, the leading system is the system $\vec{Y}_{\text{isp}}(k)$ of indicators of the information protection process, which includes: the vector $\vec{Y}_{\text{avail}}(k)$ of indicators of the availability of authorized users (people and subsystems) of the MPS to the protected information resource; the vector $\vec{Y}_{\text{cont}}(k)$ of indicators of the continuity of the IS process; the vector $\vec{Y}_{\text{integ}}(k)$ of information integrity indicators during the implementation of the IS process; the vector $\vec{Y}_{\text{conf}}(k)$ of information confidentiality indicators during the implementation of the IS process, as well as the vector $\vec{R}_{\text{isp}}(k)$ of resource costs for the implementation of the IS process at the *k*-th step of its implementation:

$$\begin{gathered}\vec{Y}_{\text{isp}}(k) = [\vec{Y}_{\text{avail}}(k);\ \vec{Y}_{\text{cont}}(k);\ \vec{Y}_{\text{integ}}(k);\ \vec{Y}_{\text{conf}}(k);\ \vec{R}_{\text{isp}}(k)]^{\text{T}} = \\ = [\bar{t}_{\text{acc}}(k);\ \bar{t}_{\text{wait}}(k);\ \lambda_{\text{doa}}(k);\ \bar{t}_{\text{doa}}(k);\ \bar{t}_{\text{co}}(k);\ K_{\text{co}}(k);\ K_{\text{loss reli}}(k);\ K_{\text{misr}}(k); \\ K_{\text{auth}}(k);\ K_{\text{ident}}(k);\ K_{\text{log}}(k);\ N_{\text{phy res}}(k);\ I_{\text{inf res}}(k);\ M_{\text{staff res}}(k); \\ U_{\text{ser costs}}(k);\ V_{\Sigma\ \text{isp}}(k);\ \alpha_{\text{pat isp}}(k)]^{\text{T}}.\end{gathered} \quad (2)$$

Let us consider these indicators in more detail. Indeed, the internal aspects of the property of information security in the MPS, which characterize the quality and efficiency of the MPS process in terms of the degree of satisfaction of the user of the MPS with the services provided to him (her) for the MPS, are: the availability of authorized users of the MPS (people and/or subsystems) to the protected information resource during the implementation of the IS process, the IS continuity, the integrity of information (its reliability) during the implementation of the IS process, the confidentiality of information during the implementation of the IS process, as well as the cost of resources for the implementation of the IS services provided to the consumer at a certain level of hierarchy.

The analytical relationship of individual security indicators as part of the NSSI of the IS process is determined by a number of relationships. Let us consider the composition of these vectors from the point of view of information security analysis for MPSs.

The vector $\bar{Y}_{\text{avail}}(k)$ of indicators of accessibility of authorized users (people and/or subsystems) of MPS to the protected information resource during the implementation of the IS process is one of the most important in the structure of security indicators. And the indicators included in this vector are designed to quantitatively describe the ability (property) of the information protection process to provide MPS users with the services of secure access to protected information when they need it and for the required time (duration of service provision) with the required quality.

Temporary availability or timeliness is one of the main properties of the IS process for MPSs, which is considered as the ability of the IS process to provide access to the protected information resources of the system and the provision of the required list of secure services to them in a timely manner. The indicator of the timeliness of access of MPS authorized users to the protected information resource can be expressed in terms of the average access time $\bar{t}_{\text{acc}}(k)$ or in terms of the average waiting time $\bar{t}_{\text{wait}}(k)$ for access to the service. An analytical expression for determining the value of the average waiting time for access to a service, which characterizes the property of temporary accessibility of users to the information protected, within the framework of the MPS, has the form:

$$\bar{t}_{\text{wait}}(k) = (\bar{t}_{\text{req trans}}(k) + \bar{t}_{\text{proc req}}(k) + \bar{t}_{\text{req impl}}(k)), \tag{3}$$

where $\bar{t}_{\text{req trans}}(k)$ is the average time spent by the MPS user on the formation and transmission of a request for the provision of information services at the *k*-th step of the implementation of the IS process, $\bar{t}_{\text{proc req}}(k)$ is the time spent by the IS process to check the authority of the MPS terminal or the MPS user (authentication, identification, authority, priority), and processing of a user's request for the provision of an information service at the *k*-th step of the implementation of the IS process within the framework of the MPS, $\bar{t}_{\text{req impl}}(k)$ is the time spent by the IS process to ensure the secure implementation of the request within the requested information service or to transmit a signal to the MPS user about the impossibility of ensuring the secure implementation of the request within the requested services at the *k*-th step of the implementation of the IS process within the MPS.

In addition, the temporary availability of legal MPS users to the protected information resource can be quantitatively characterized by the intensity $\lambda_{\text{doa}}(k)$ of access denials caused by failures (errors) during the implementation of the IS process, as well as the average time $\bar{t}_{\text{doa}}(k)$ between access denials. So, for example, the intensity of denials in access of legal MPS users to the protected information resource can be defined as the ratio of the number of MPS users (people and/or subsystems) received through the fault of the IS process by MPS users (people and/or subsystems) of denials in access to the total number of MPS requests for access to the protected information resource:

$$\lambda_{\text{doa}}(k) = \frac{N_{\text{doa}}(k)}{N_{\text{acc req}}(k)}. \tag{4}$$

Thus, the vector indicator of security, which characterizes the internal property of the IS process within the MPS framework - the temporary availability of legal (authorized) MPS users to the protected information resource, contains the following indicators (parameters):

$$\vec{Y}_{\text{avail}}(k) = [\bar{t}_{\text{acc}}(k); \bar{t}_{\text{wait}}(k); \lambda_{\text{doa}}(k); \bar{t}_{\text{doa}}(k)]^{\text{T}}. \quad (5)$$

The vector $\vec{Y}_{\text{cont}}(k)$ of indicators of the continuity of the IS process characterizes the property of this process to continue for the required time.

The continuity indicator can be expressed in terms of the average time $\bar{t}_{\text{co}}(k)$ of continuous (uninterrupted) implementation of the IS process when providing information services to MPS users. In addition, the continuity of the IS process in the MPS can be described using the continuity coefficient of the IS $K_{\text{co}}(k)$, which is the ratio of the average time of the continuous implementation of the IS process to the total time of the implementation of the material processing process (the time of the MPS operation):

$$K_{\text{co}}(k) = \frac{\bar{t}_{\text{co}}(k)}{T_{\text{f MPS}}(k)}, \quad (6)$$

moreover, this coefficient should tend to unity.

Thus, the vector indicator of the continuity of the process of ensuring the protection of information within the framework of the MPS (continuity of the SI process), which characterizes the property of this process to continue for the required time, includes two indicators (parameters):

$$\vec{Y}_{\text{cont}}(k) = [\bar{t}_{\text{co}}(k); K_{\text{co}}(k)]^{\text{T}}. \quad (7)$$

The vector $\vec{Y}_{\text{integ}}(k)$ of information integrity indicators during the implementation of the IS process within the MPS contains indicators (parameters) that numerically characterize the accuracy, reliability and completeness of the protected information, as well as the security of the information stored, processed and transmitted in the MPS from possible unintentional and malicious distortions. In other words, this property of the IS process in MPS should be ensured without excessive deterioration, in compliance with the requirements (boundaries) for error-free and accurate (reliability) and undistorted information stored, processed and transmitted in MPS, i.e. in compliance with the requirements for the number of errors and distortions of information.

Thus, the integrity $\vec{Y}_{\text{integ}}(k)$ of information during the implementation of the IS process can include two components - reliability (accuracy, error-freeness) and non-distortion in the IS process during its storage, processing and transmission during the processing of materials.

Integrity, from the point of view of maintaining the reliability and accuracy of information during the implementation of the IS process in the MPS, can be assessed by the coefficient of loss of information reliability $K_{\text{loss reli}}(k)$, stored, processed and transmitted to the MPS. This coefficient, taking into account the multiservice information stored, processed and transmitted in the MPS, includes: loss of syllabic intelligibility $A(k)$ in the form of the number of lost (misunderstood, distorted beyond recognition) words and phrases $N_A(k)$ for IP telephony; the number $N_{\text{incorr ii}}(k)$ of incorrectly recognized images during the implementation of videoconferencing within the framework of MPS, as well as the number $N_{\text{err}}(k)$ of erroneously (distorted) received, processed, stored and transmitted data when implementing services within the framework of MPS, oriented to data transmission.

In general, taking into account the variety of real threats to information security $U_{\text{real}}^{thr}(k)$ for each specific service of the many information services $N_{\text{real}}^{thr}(k)$ implemented and provided to users within the MPS, the integral coefficient of information reliability loss can be represented as:

$$K_{\text{loss reli}}(k) = \sum_{n=1}^{N_{\text{real}}^{thr}(k)} \sum_{u=1}^{U_{\text{real}}^{thr}(k)} \alpha_u^n \, P_{\text{reli}}(k) \, N_{\text{err}}^n(k), \tag{8}$$

where α_u^n is the relative danger (difficulty of overcoming) the *u*-th threat when providing the *n*-th service at the *k*-th stage of the MPS functioning, and $N_{\text{err}}(k)$ represents either $N_A(k)$, or $N_{\text{incorr ii}}(k)$, or $N_{\text{err}}(k)$ depending on the type of the *n*-th service to be protected; $P_{\text{reli}}(k)$ – the probability of reliable information transmission during the functioning of the MPS under the influence of threats at the *k*-th stage of the implementation of the IS process.

The indicator of information non-distortion during the implementation of the IS process numerically characterizes the ability of this process to counter the modification or destruction of information stored, processed and transmitted and received in the MPS, and can be represented as a distortion factor (packets, data blocks, etc.). The physical meaning of this coefficient is the ratio of the amount of distorted data to the total number of stored, processed and transmitted data in MPS:

$$K_{\text{misr}}(k) = \frac{N_{\text{misr}}(k)}{N_{\text{total}}(k)}, \tag{9}$$

moreover, this coefficient should be minimal (should tend to zero).

Thus, the vector indicator of the information integrity preservation during the implementation of the IS process within the framework of the MPS includes an indicator of reliability (error-free, accuracy) and an indicator of undistorted information

$$\vec{Y}_{\text{integ}}(k) = [K_{\text{loss reli}}(k);\ K_{\text{misr}}(k)]^{\text{T}}. \tag{10}$$

The vector $\vec{Y}_{\text{conf}}(k)$ of indicators of information confidentiality preservation during the implementation of the IS process characterizes the property of this process to ensure the availability of information in the MPS only for those who have the appropriate authority (authorized users).

As elements of the vector of information confidentiality indicators in the implementation of the IS process in MPSs, indicators of security against unauthorized use of MPS resources can be used. They include parameters that numerically characterize the properties of the IS process to protect against unauthorized access to information in MPSs and unauthorized use of MPS equipment.

The implementation of these properties is carried out using the mechanism of authentication of MPS users and identification of MPS equipment. For example, using passwords and user authentication modules, an individual identification number of MPS equipment, a user privacy mechanism and the introduction of authorization mechanisms - priority control, excluding access to resources for MPS users of a lower hierarchy level, i.e. access control by priority, control of the authority of service objects. The indicators of the quality of the implementation of these properties within the framework of the IS process in the MPS can be:

user authentication factor $K_{\text{auth}}(k)$ that has a meaning inverse to the risk of compromising the algorithm and authentication data

$$K_{\text{auth}}(k) = 1 - P_{\text{compr auth}}(k), \tag{11}$$

where $P_{\text{compr auth}}(k)$ is the probability of compromising the algorithm and authentication data of the served MPS users at the *k*-th step of the IS process implementation;

coefficient $K_{\text{ident}}(k)$ of MPS equipment identification, which has a meaning inverse to the risk of compromising the equipment identification number (ID) embedded in each terminal of the MPS

$$K_{\text{ident}}(k) = 1 - P_{\text{compr ID}}(k), \tag{12}$$

where $P_{\text{compr ID}}(k)$ is the probability of compromising the identification number of the equipment of the MPS users at the *k*-th step of the implementation of the IS process;

authorization coefficient $K_{\log}(k)$, which has a physical meaning inverse to the risk of access of a user of a lower priority to information resources of the MPS, intended for the level of users of the system of a higher priority

$$K_{\log}(k) = 1 - P_{\text{hig priority}}(k), \tag{13}$$

where $P_{\text{hig priority}}(k)$ is the probability of access of a lower priority user to the information resources of the MPS, intended for the level of a higher priority user of at the *k*-th step of the implementation of the IS process.

Thus, the vector indicator of maintaining the confidentiality of information circulating in the MPS includes three indicators:

$$\vec{Y}_{\text{conf}}(k) = [K_{\text{auth}}(k); K_{\text{ident}}(k); K_{\log}(k)]^{\text{T}}. \tag{14}$$

The vector $\vec{R}_{\text{isp}}(k)$ of resource consumption indicators of the IS process is intended to quantitatively characterize the total costs of the implementation of this process in the framework of MPS. At the same time, the resource spent on the implementation of the IS process should be understood as something that has value for the MPS from the IS point of view (IS information, personnel, IS services, equipment for IS, materials for IS, etc.).

They distinguish between the types of resources spent on IS in MPSs: physical - objects of the MPS infrastructure, directly related to the IS during its storage, transmission and processing - premises, IS technical means, data transmission channels (internal and external); informational - documents on IS, IS software, human knowledge on IS; personnel assigned to implement the IS process; services for the provision of IS in the MPS - networks for the exchange of service data on IS, public key exchange services, electricity, air conditioning system, fire alarm, water supply, room access control system, etc.

Taking into account the peculiarities of the information protection process in MPSs, the vector of total resource costs for the implementation of this process can be represented as:

$$\vec{R}_{\text{isp}}(k) = [N_{\text{phy res}}(k); I_{\text{inf res}}(k); M_{\text{staff res}}(k); U_{\text{ser costs}}(k); V_{\Sigma\ \text{isp}}(k); \alpha_{\text{pat isp}}(k)]^{\text{T}}. \tag{15}$$

In expression (15), all elements have the physical meaning of the total costs of a certain type of resource. For example: $N_{\text{phy res}}(k)$ – the expenditure of physical resources for the IS

process at the *k*-th step of the MPS operation; $I_{\text{inf res}}(k)$ – the cost of information resources for the IS process at the *k*-th stage of its implementation; $M_{\text{staff res}}(k)$ – the number of personnel called upon to carry out the IS process on the *k*-th of its implementation; $U_{\text{ser costs}}(k)$ – total costs of services for the IS provision at the *k*-th stage of its implementation. In addition, the vector of resource consumption indicators can include the total resource of the computing power of the MPS $V_{\Sigma\ \text{isp}}(k)$, used in the interests of the IS process and expressed in the amount of observation information, signaling, etc., transmitted (processed) by the MPS ISS per unit time.

In addition, the vector of indicators of resource consumption of the IS process can include an indicator characterizing the costs of the computational resource of the automation tools of this process, which takes into account the increase in the capabilities of the MPS ISS with the introduction of promising information technologies and can be expressed through the coefficient of the automation means productivity of the IS process $\alpha_{\text{pat isp}}(k)$.

A variant of the system of information security indicators for MPS is proposed in Fig. 1.

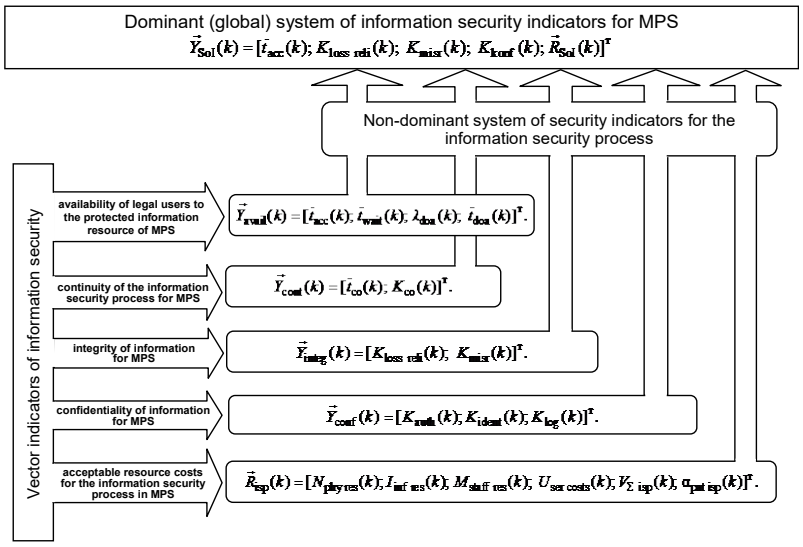

Fig. 1. A variant of the system of indicators of information security for materials processing systems.

The diagram in Fig. 1 and expressions (2)-(15) have the physical meaning of a complete, interconnected system of information security indicators for MPSs. It includes the DSSI, which characterizes the requirements of the supersystem (external, user-defined properties), and the key NSSI, which characterizes the set of properties of the IS process that affect the performance of the general task of ensuring the information security within the MPS.

The proposed system of indicators of information security for MPS is the initial data and will form the basis of the algorithm for evaluating the effectiveness of the IS of systems of this class. To implement the analytical method for the current assessment of the effectiveness of the IS for MPS, the necessary next stage is the approximation of the known analytical probability distribution densities of the real distribution densities of the values of the security indicators presented in Fig. 1. At the same time, a high level of a priori uncertainty regarding the statistical characteristics of the IS process and the impacts on it

from the opposing system (intruder) emphasizes the expediency of using the method of choosing and justifying approximate distribution models for solving the problem. This is due to the fact that obtaining accurate analytical ratios for the densities of the probability distribution of security indicators based on a rigorous consideration of the exact analytical model encounters a number of fundamental difficulties associated with the need for the most complete reproduction of all the specifics of stochastic processes in MPS and reflecting the objective complexity of information support for material processing processes.

5 Conclusion

The paper proposed an approach to the formulation (synthesis, selection) of the composition of a non-redundant, rational and hierarchically interconnected system of information security indicators for MPSs. The choice and justification of the volume and nomenclature of systems of information security indicators was carried out, firstly, in the interests of a formal parametric description of the essential properties of the information security process circulating in the MPS, and secondly, in the interests of the subsequent reliable assessment of the quality and efficiency of the MPS information security subsystem and the process it implements - the process of ensuring information security of such complex modern systems. Practical implementation of the proposed approach will, in our opinion, increase the efficiency of quality control for protecting the MPS information support procedures. This will happen by increasing the redundancy, reliability and accuracy of the obtained estimates and security forecasts, due to the rational redistribution of the costs of resources allocated in the interests of assessing only the demanded significant indicators. The direction of further research can be the solution for the problem of formulating the composition of the systems of security indicators, taking into account the uncertainty of the initial data due to external and internal disturbances inherent in both the information security process and the process of materials processing in general.

This research is being supported by the grant of RSF #21-71-20078 in St. Petersburg Federal Research Center of the Russian Academy of Sciences.

References

1. J. Davis, T. Edgar, J. Porter, J. Bernaden, M. Sarli, *Smart Manufacturing, manufacturing intelligence and demand-dynamics performance.* Computers & Chemical Engineering, **47**, pp. 145-156 (2012)
2. I.V. Kotenko, D.S. Levshun, A.A. Chechulin, *Event correlation in the integrated cyber-physical security system.* Proceedings of the 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM-2016), IEEE, St. Petersburg, Russia, pp. 484-486 (2016)
3. I.B. Parashchuk, I.V. Kotenko, *Target functions of the conceptual model for adaptive monitoring of integrated security in material processing systems.* Materials Today: Proceedings. Elsevier. **38 (4)**, pp. 1454-1458 (2021)
4. B.R. Mehta, Y.J. Reddy, *Industrial Process Automation Systems: Design and Implementation*. (Elsevier Science. Amsterdam, Holland, 2014)
5. R.L. Krutz, *Industrial Automation and Control System Security Principles*. (International Society of Automation. Durham, US, 2016)

6. M. Lehto, P. Neittaanmaki (ed.), *Cyber Security: Analytics, Technology and Automation*. (Springer International Publishing Switzerland. Cham, Switzerland, 2015)
7. L. Johnson, *Security Controls Evaluation, Testing, and Assessment Handbook*. (Academic Press. New York, 2019)
8. R. Rogers, G. Miles, E. Fuller, T. Dykstra, *Security Assessment*. (Syngress Publishing. Amsterdam, Holland, 2004)
9. C. McNab, *Network Security Assessment*. Second Edition. (O'Reilly Media Inc., Sebastopol, US, 2008)
10. I.V. Kotenko, I.B. Parashchuk, *Synthesis of Controlled Parameters of Cyber-Physical-Social Systems for Monitoring of Security Incidents in Conditions of Uncertainty*. IOP Conf. Series: Journal of Physics: Conference Series (JPCS), **1069**, pp. 1-6 (2018)
11. I.B. Parashchuk, I.V. Kotenko, *Formulation of a system of indicators of information protection quality in automatic systems of numerical control machines for advanced material processing*. Materials Today: Proceedings. **19 (5)**, pp. 1835-1840 (2019)
12. W. Whitt, *Variability functions for Parametric Decomposition approximations of queueing networks*. AT&T Bell Laboratories, 1994, (online), Available: http://www.columbia.edu/~ww2040/parametric.pdf, Accessed on February 2021.
13. Y. Lu, R. Gadh, T. Tautges, *Volume decomposition and feature recognition for hexahedral mesh generation*. I-CARVE Lab, University of Wisconsin-Madison, 1998, (online), Available: https://www.osti.gov/biblio/14065, Accessed on February 2021.
14. H. Sakurai, P. Dave, *Volume Decomposition and Feature Recognition*. Part II: Curved Objects Computer-Aided Design 28, **6/7**, pp. 519-537 (1996)
15. N. Sidiropoulos, L. Lathauwer, X. Fu, K. Huang, E. Papalexakis, C. Faloutsos, *Tensor Decomposition for Signal Processing and Machine Learning* (Fellow, IEEE), 2016, (online), Available: https://arxiv.org/pdf/1607.01668.pdf, Accessed on February 2021
16. E. Hubert, G. Labahn, *Scaling Invariants and Symmetry Reduction of Dynamical Systems Cheriton School of Computer Science*, 2010, (online), Available: https://cs.uwaterloo.ca/~glabahn/Papers/focm.pdf, Accessed on February 2021
17. S. AbdusSalam, C. Burgess, F. Quevedo, *MFV reductions of MSSM parameter space*. Journal of High Energy Physics. 2015, (online), Available: https://www.researchgate.net/ /publication/267983062, Accessed on March 2021
18. G. Ciuprina, J. Fernandez, Z. Ioan, S. Ilievski, *Parameterized model order reduction*. CASA-Report. Eindhoven University of Technology, 2015, (online), Available: http://www.win.tue.nl/analysis/reports/rana15-08.pdf, Accessed on March 2021
19. A. Zecevic, D. Siljak, *Control of Complex Systems*. (Springer Science and Business Media, London, UK, 2010)
20. F. Golnaraghi, B. Kuo, *Automatic Control Systems*. Tenth Edition. (McGraw-Hill, London, UK, 2017)
21. I.V. Kotenko, I.B. Parashchuk, *Assessment of components to ensure the security of control and diagnostic information about technological processes*. MATEC Web of Conferences. **329** (**03005)**, pp. 1-10 (2020)
22. ISO/IEC 27002:2013/COR 2:2015. *Information technology – Security techniques – Code of practice for information security controls – Technical Corrigendum 2*, 2015, (online), Available: https://www.iso.org/standard/69379.html, Accessed on March 2021
23. ISO/IEC 27000:2018. *Information technology – Security techniques – Information security management systems – Overview and vocabulary*, 2018, (online), Available: https://www.iso.org/standard/73906.html, Accessed on March 2021