Date of publication MAR-29, 2021, date of current version FEB-19, 2021.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.20.1.2088

Specification of Quality Indicators for Security Event and Incident Management in the Supply Chain

IGOR V. KOTENKO, IGOR B. PARASHCHUK
St. Petersburg Federal Research Center of the Russian Academy of Sciences, 14-th Liniya, 39, St. Petersburg, 199178, Russia,
(e-mail: ivkote@comsec.spb.ru, parashchuk@comces.spb.ru)

Corresponding author: Igor V. Kotenko (e-mail: ivkote@comsec.spb.ru).

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.

ABSTRACT The paper proposes an approach to a formalized description of the process of changing the values of quality indicators of decision support for managing security events and incidents in the supply chain. The approach is based on the analysis of the functioning processes of modern quality control systems for information security in supply chain. In addition, it is based on an analysis of decision support processes. We use controlled Markov chains, represented by difference stochastic equations. The considered version of the analytical description of the state change in dynamics allows one to formalize, structure, and mathematically describe the process of this class from a uniform perspective. It is important to note that with this representation of the dynamics of state transitions, the requirements for operativity (timeliness), reliability, secrecy and resource costs for supporting decision-making to control information security in the supply chain are taken into account.

KEYWORDS cyber attacks, security event and incident management, decision support, quality indicator, Markov chain, difference stochastic equation.

I. INTRODUCTION

MODERN technological solutions and promising trends within the framework of the Industry 4.0 concept directly affect the field of digital supply chains (SCs). This is not only about the digitalization of the Supply Chain Management process, which provides management at the level of movement of raw materials, materials, components and finished products [1-3]. Along with the management of logistics functions, digital SCs represent a digital transformation of the entire enterprise infrastructure to ensure the interconnection of procurement, production and sales systems. The goal is to plan and implement operations more efficiently, to ensure digitalization and integration of processes within the company as a whole: from product development to production, procurement, sales (sales), logistics and services [4-7].

In essence, this is another development step, the transition from an organizational strategy for ERP (Enterprise Resource Planning) to a new philosophy of integration of production, finance and asset management. This is already being implemented on the basis of new information and digital technologies, the postulates of “digital transformation”, and “smart production”. At the same time, “smart manufacturing” is often understood as a cyber-physical production system (CPS). The properties of such cyber-physical systems can also be possessed by enterprises and industries focused on digital SCs. They are able to provide a high level of productivity (ensure operation without interruption), reduce costs and shorten the turnover time of a product unit within the system.

CPSs, using digital SCs algorithms, have a complex distributed structure. Operations that examine various aspects of integration and performance in supply chains, as well as the control of these processes, are also complex. However, information security processes and systems, in particular the systems for attack detection and prevention, play a special and very important role on a variety of objects and technologies that occur in systems of this class [8]. These systems consist of various components (detectors, analyzers, databases, servers, workstations, security facilities), and also include officials (personnel). Such equipment elements are formed to provide security requirements in the digital SCs. The purpose of these systems is to reduce casualties due to an infringement of the confidentiality, integrity and availability of information stored, processed and transmitted during the implementation of digital SCs.

Information security processes and systems for attack detection and prevention, as well as methods for their analysis and modeling, are characterized by some features [9-13]. Almost all of the information security processes studied today and the information security systems used in practice are based on the implementation of complex algorithms of security incident and event management (SIEM), including to counter multilevel cyber attacks [14-16]. At the same time, intelligent mechanisms of decision support process (DSP) are embedded in the SIEM processes and systems. The key problem connected with the realization of rational DSPs consists in the problem of accurate and adequate quality control of information protection when implementing digital SCs. This control is carried out with the help and in the interests of the DSP of SIEM. The main means of research and optimization of DSP for SIEM in the implementation of digital SCs are mathematical models and methods.

This determines the relevance of the tasks of DSP modeling for SIEM in the implementation of digital SCs. These tasks are designed to carry out: analysis of the key features of DSP; definition of the place and role of formal models in the regulation and control tasks of DSP for SIEM in the realization of digital SCs; assessment of new, promising formal tools and methods for DSPs; building the dynamic models of DSP for SIEM when implementing digital SCs.

The dynamical model of DSP for SIEM, when implementing digital SCs, will consider the important properties of DSP and will model the probability-time transformation on the values of the process quality indicators (QIs). In addition, the model should take into account probabilistic transients when managing the DSP architecture, operating modes, and parameters in different conditions of SIEM and the implementation of digital SCs.

The paper formulates and substantiates a new look at the mathematical description of the transformation on the values of QIs of DSP for SIEM in the implementation of digital SCs. The approach proposed in the paper is based on the use of the mathematical apparatus of controlled Markov chains and relies on a detailed analysis of the functioning processes of systems for attack detection and prevention and analysis of DSPs to manage the modes of their operation, their parameters and structure to monitor the quality of information protection in SCs. This paper is a logical, mathematical (from the point of a model view) and experimental development of some provisions and hypotheses expressed by the authors at the international conference MIM 2019 in Berlin [17]. These hypotheses and provisions within the framework of the paper have been revised and comprehensively expanded. All the results of the analysis of relevant works were rethought, rewritten and supplemented in a new way, the depth and range of methodological foundations and models were significantly expanded. The experimental part is supported by the results of new computational experiments.

The paper consists of six sections. Section II is devoted to the related work analysis. Section III presents the methodological (theoretical) essence of the proposed approach to DSP modeling. Section IV illustrates the experiments provided. Section V is devoted to a short discussion of the results, and section 6 concludes the paper.

II. RELATED WORK

Problems of DSP modeling and different variants of models of security processes are actively explored by modern authors. So, for example, in the works of [18-21], examples of the typical statement and solution of the tasks of modeling the sophisticated management processes, decision making and decision support for information security are given. These examples differ in the depth (level) of the models, in the set of studied process parameters and in the essence of approaches to the decomposition of modeling stages. However, the models proposed in these papers are too complex, difficult to formalize and implement with mathematical expressions. These models are not invariant for various specific decision support processes and information security processes in general.

In [22], to reduce the complexity of the statistical assessment of the intensity of cyber attacks, it is proposed to use the methods of the theory of queuing. But these methods are not able to ensure the high adequacy of the mathematical specification of a specific DSP model, do not allow one to talk about the sufficient (acceptable) accuracy of the DSP model for SIEM when implementing digital SCs.

In [23, 24] the approaches to the modeling of quality indicators (and reliability) of security systems and processes are proposed based on probabilistic algorithms (by analyzing the intensity of events and incidents) and reduction (ranking) algorithms. These are parametric approaches; they investigate groups of parameters of modeled processes. But in our conditions, we need statistics on the values of auxiliary parameters characterizing the DSP for SIEM indicator groups. It is almost impossible to collect such statistics in the framework of digital SCs implementation.

An interesting approach to modeling is considered in [25, 26]. Here, the models are mathematically specified spaces of threats, events, vulnerabilities, and incidents. However, the definition of boundaries and the scaling of such spaces in these papers is considered without taking into account the features of modern intelligent DSPs, which does not allow their direct use in SIEM tasks in the implementation of digital SCs, and also narrows their scope. In [27, 28] the game methods to model the processes of information security are used. But the implementation of game algorithms in this case should be supported by techniques and methods of simulation, and almost in real time. In addition, the drawback of this paper is its focus on traditional database models, which is not entirely compatible with the DSP for SIEM models when implementing digital SCs.

The hypothesis of building a model based on the general theory of systems was proposed in [29]. But the typical model of a protected system in this paper is described as the relationship of transcendental, non-specific operators. This does not allow full use of such a model for the formalized description of specific algorithms of DSP and threats for SIEM in the implementation of digital SCs.

In [30, 31] the models of complex controlled processes based on stochastic differential equations were proposed. However, these models require large expenditures for collecting source data statistics, do not support the unification and usability requirements of the models, and are time consuming and inaccurate in terms of describing the dynamics of SIEM when implementing digital SCs.

Articles [32, 33] investigate dynamical models of complex processes based on Markov chains. These approaches are also used in our work with respect to the description of the current changes in time of OIs of DSP. With the help of Markov chains one can describe such complex processes, and they can act as a mathematical platform for modeling, but in these papers the issues of estimating the joint probability distribution density of different in physical meaning QI of DSP is not considered.

The analysis of relevant works shows that there are no ready-made solutions to building DSP models for SIEM when implementing digital SCs. Moreover, the existing DSP models are mostly either static or use local stationarity to describe the dynamics, i.e., dynamic models are less common; they do not take into account the probabilistic and current in time nature of the parameters of this process under various conditions of interaction with other processes and systems [34, 35]. Almost all of them have parametric and functional limitations, these models are complex, inadequate, laborious, and for their practical implementation a lot of additional data is needed. In addition, the sets (systems) of QI of DSP do not unsubscribe all the basic properties of these processes, they are excessively large, i.e., may contain many unimportant, secondary quality indicators [36, 37].

The relevance and novelty of the unified approach to DSP modeling for SIEM proposed in the paper when implementing digital SCs, in addition to the results of the analysis of related works, is also confirmed by the fact that it is based on the formulation of probabilistic-time, dynamic models of DSP state transitions in the state space. This approach has a theoretical novelty, since it can serve as the basis for fundamentally new solutions to the development of SIEM algorithms within the framework of digital SCs. It can serve as a basis for modeling a dynamic, complex, multi-level and controlled DSP with the required quality and for the actual operating conditions of digital SCs.

III. ANALYTICAL MODEL

It is known that the basic properties of DSP are: operativity of decision support (DS), reliability of DS, stealth of DS and the volume (quantity) of management system resources spent on DSP. A private property of a DSP may be its level of automation. In accordance with the proposed approach, the analytical model of DSP for SIEM in the implementation of digital SCs in the mathematical and physical sense does not differ from the traditional mathematical model of the decision making. The key difference is the content of the vector of quality indicators that characterize this process. And the analytical model is a formalized analytical description of the probability-time conversions in the QIs of DSP values in the state space.

The system of QIs of DSP for SIEM, when implementing digital SCs, may include: the duration $t_{\text{ds}}(k)$ of the DS cycle; risk coefficient $K_{\text{swd}}(k)$ of making the wrong (an erroneous, false) decision; coefficient $K_{\text{sec dsp}}(k)$ of secrecy of DSP and vector $\vec{R}_{\text{dsp}}(k)$ of resource expenses on DSP:

$$\vec{Y}_{\text{dsp}}(k) = (t_{\text{ds}}(k);\, K_{\text{swd}}(k);\, K_{\text{sec dsp}}(k);\, \vec{R}_{\text{dsp}}(k))^{\text{T}}. \quad (1)$$

The composition of the QI elements (1) is determined by the traditional basic requirements for DSP in terms of: timeliness, i.e., duration of the DS cycle; reliability (accuracy, adequacy) of decisions, described by the risk coefficient of making a wrong decision; security, specified by the DSP secrecy factor, and also takes into account the cost of resources.

At the same time, the operativity of this process refers to the ability of the operators and means of DSP to develop a set of decision variants for potential solutions, analyze these variants and report the analysis results to the security administrator in a timely manner. Operativity of the DSP characterizes QI – the duration $t_{\text{ds}}(k)$ of the cycle of DS for the *k*-th stage of the DSP, which can be determined using the expression:

$$t_{\text{ds}}(k) = \sum_{u=1}^{U_{\text{var}}} t_{\text{dv}\,u}(k) + t_{\text{av}\,u}(k). \quad (2)$$

In expression (2) $t_{\text{dv}\,u}(k) = Q_{\text{op dv}\,u}(k) / J_{\text{dv}\,u}(k)$ – the time, required to form the *u*-th decision option (variant) out of the total number of possible options. This time is found as the ratio of the number of computational operations, necessary to develop a solution $Q_{\text{op dv}\,u}(k)$, to the performance of computing tools for developing the solutions $J_{\text{dv}\,u}(k)$. A separate component $t_{\text{dv}\,u}(k)$ may be the reaction time of the security administrator.

The variable $t_{\text{av}\,u}(k)$ in expression (2) is the time for validation (analysis) of the *u*-th decision option (variant), defined as the ratio $t_{\mathrm{av}\,u}(k)=Q_{\mathrm{op\,av}\,u}(k)/J_{\mathrm{av}\,u}(k)$: the number of computational operations necessary for analyzing the solution variant $Q_{\mathrm{op\,av}\,u}(k)$ and the performance $J_{\mathrm{av}\,u}(k)$ of the computing tools for analyzing the solution variants (and the reaction time of the data protection specialist). The dynamics of the model, as the dynamics of the change of states of the formulated QIs in the DSP process, allows you to implement the *k* coefficient in the model (for the *k*-th stage of DSP).

The coefficient $K_{\mathrm{swd}}(k)$ of the risk for making the wrong (an erroneous, false) decision can be an IQ characterizing the reliability of DS:

$$K_{\mathrm{swd}}(k)=\frac{m_{\mathrm{sol}}^{\mathrm{real}}(k)}{m_{\mathrm{sol}}^{\mathrm{req}}(k)}\left[2\Phi_{\mathrm{o}}\left(\frac{\varepsilon(k)}{\Delta(k)}\right)\right]^{u(k)-\mu(k)-\rho(k)}. \qquad (3)$$

In expression (3), $m_{\mathrm{sol}}^{\mathrm{real}}(k)$ – the number of really analyzed solution variants for the *k*-th stage of the DSP; $m_{\mathrm{sol}}^{\mathrm{req}}(k)$ – the number of all possible solutions that need to be analyzed based on the features and conditions of the organization of SIEM in the implementation of digital SCs; $\Phi_{\mathrm{o}}(*)$ – the Laplace integral, with the help of which the probability is estimated that for the *k*-th stage of the DSP the index of the objective function DS will deviate from the optimal value to an acceptable level, is estimated; $\varepsilon(k)$ – the maximum allowable deviation among the QIs, which determines the effectiveness of the DSP and is caused by errors in the DS analytical models used; $\Delta(k)$ – the standard deviation of the performance indicator of DS from the required value at the *k*-th stage of DSP; $u(k)$ – the number of individual QIs that determine the quality of the DS at the *k*-th stage of DSP; $\mu(k)$ – the number of non-optimizable parameters of model for assessing the objective function of DS quality; $\rho(k)$ – a set of parameters fixed (pinned) by the data protection specialist in the model at the *k*-th stage of DSP.

The model should describe the dynamics of the QIs of DSP values in the state space. It is proposed to describe the dynamics in the form of controlled Markov chains, represented by stochastic difference equations (MCC-DSE). Moreover, the model is a complex of equations of state and observation for individual QIs of DSP, as described in [38].

Then the model of state change of the operativity indicator of DS, which can be expressed through QI – the duration $t_{\mathrm{ds}}(k)$ of the DS cycle, takes the form:

$$\vec{t}_{\mathrm{ds}}(k+1)=\mathrm{C}_{t_{\mathrm{ds}}}^{\mathrm{T}}(k+1)\,\vec{\Theta}_{t_{\mathrm{ds}}}(k+1); \qquad (4)$$

$$\vec{\Theta}_{t_{\mathrm{ds}}}(k+1)=\varphi_{t_{\mathrm{ds}}}^{\mathrm{T}}(k+1,k,u)\,\vec{\Theta}_{t_{\mathrm{ds}}}(k)+\Delta\vec{\Theta}_{t_{\mathrm{ds}}}(k+1); \qquad (5)$$

$$\vec{z}_{t_{\mathrm{ds}}}(k+1)=H_{t_{\mathrm{ds}}}(k,\vec{x}(k))\,\vec{\Theta}_{t_{\mathrm{ds}}}(k+1)+\vec{\omega}_{t_{\mathrm{ds}}}(k+1). \qquad (6)$$

In the system of equations (4)-(6), in the expressions for the MCC-DSE, the formula (4) is the equation of state of the operativity indicator of DS for the (*k*+1)-th stage of the DSP. Here $\vec{t}_{\mathrm{ds}}(k+1)$ – is a vector-column of the values of the operativity indicator of DS for the (*k*+1)-th stage of DSP, in it, all elements are equal to 0, except one; $\mathrm{C}_{t_{\mathrm{ds}}}^{\mathrm{T}}(k+1)$ – the diagonal quadratic (of order *n*) matrix of the allowed values of the operativity of DS for the (*k*+1)-th stage of DSP, the number *n* (rows and columns) are defined by a set of allowed states (depth of modeling); $\vec{\Theta}_{t_{\mathrm{ds}}}(k+1)$ – an auxiliary column vector of state indicators of the operativity indicator of DS at the (*k*+1)-th step of the DSP, introduced for the convenience of recording the dynamics of the transition of this indicator from one state to another state.

The equation of state (state transition) of the auxiliary vector $\vec{\Theta}_{t_{\mathrm{ds}}}(k+1)$ of indicators is represented by expression (5). Here $\varphi_{t_{\mathrm{ds}}}^{\mathrm{T}}(k+1,k,u)$ is the square (of order n) matrix of transition probabilities, which describes the probabilistic-temporal mechanism for changing the states of the operativity indicator of DS for the *k*-th stage of DSP for SIEM when implementing digital SCs; $\vec{\Theta}_{t_{\mathrm{ds}}}(k)$ – a column vector of the status indicators of the operativity indicator of DS in the previous step; $\Delta\vec{\Theta}_{t_{\mathrm{ds}}}(k+1)$ – a column vector of increments of the status indicator values. This vector provides for the missing (non-integer) part of the formula (5). Its elements are obtained on the basis of the results of the correction of the starting excitation noise with the mathematical expectation and dispersion for the starting (initial) state of the modeled process.

The formula for observing the process of transformation of the states of the operativity indicator of DS is the expression (6). Here, $\vec{\omega}_{t_{\mathrm{ds}}}(k+1)$ is the vector of white noises (observation noises) with zero mean and dispersion matrix $\delta_{\omega}(k+1)$, and $H_{t_{\mathrm{ds}}}(k,\vec{x}(k))$ is the diagonal quadratic (of order *n*) matrix of the observed values of this process.

Summing up the general formal description of a specific IQ, we note that, using expressions (4)-(6), a mathematical model of the transformation of this indicator states (i.e., the operativity indicator – the time $t_{\mathrm{ds}}(k+1)$ for cycle of DS) is presented. This model is described in terms of MCC-DSE.

By analogy with the system of equations of state and observation (4)-(6), we can imagine the model of reliability of DS. This model illustrates the dynamics of changing states of the DSP reliability indicator, i.e., the risk coefficient $K_{\text{swd}}(k+1)$ for making the wrong (an erroneous, false) decision:

$$\vec{K}_{\text{swd}}(k+1) = \text{C}^{\text{T}}_{K_{\text{swd}}}(k+1)\,\vec{\Theta}_{K_{\text{swd}}}(k+1); \tag{7}$$

$$\begin{aligned}\vec{\Theta}_{K_{\text{swd}}}(k+1) = \varphi^{\text{T}}_{K_{\text{swd}}}(k+1,k,u)\,\vec{\Theta}_{K_{\text{swd}}}(k) + \\ + \Delta\vec{\Theta}_{K_{\text{swd}}}(k+1);\end{aligned} \tag{8}$$

$$\begin{aligned}\vec{z}_{K_{\text{swd}}}(k+1) = H_{K_{\text{swd}}}(k,\vec{x}(k))\,\vec{\Theta}_{K_{\text{swd}}}(k+1) + \\ + \vec{\omega}_{K_{\text{swd}}}(k+1).\end{aligned} \tag{9}$$

Mathematical models of other quality indicators of the DSP for SIEM in the implementation of digital SCs can be represented in a similar way.

For example, the secrecy of DSP for SIEM in the implementation of digital SCs can be described through the dynamics of transformation of the states of the quality indicator – the DSP stealth coefficient $K_{\text{sec dsp}}(k+1)$:

$$\vec{K}_{\text{sec dsp}}(k+1) = \text{C}^{\text{T}}_{K_{\text{sec dsp}}}(k+1)\,\vec{\Theta}_{K_{\text{sec dsp}}}(k+1); \tag{10}$$

$$\begin{aligned}\vec{\Theta}_{K_{\text{sec dsp}}}(k+1) = \varphi^{\text{T}}_{K_{\text{sec dsp}}}(k+1,k,u)\,\vec{\Theta}_{K_{\text{sec dsp}}}(k) + \\ + \Delta\vec{\Theta}_{K_{\text{sec dsp}}}(k+1);\end{aligned} \tag{11}$$

$$\begin{aligned}\vec{z}_{K_{\text{sec dsp}}}(k+1) = H_{K_{\text{sec dsp}}}(k,\vec{x}(k))\,\vec{\Theta}_{K_{\text{sec dsp}}}(k+1) + \\ + \vec{\omega}_{K_{\text{sec dsp}}}(k+1).\end{aligned} \tag{12}$$

Through the dynamics of state changes of the elements of the vector $\vec{R}_{\text{dsp}}(k+1)$ of resource costs, the resource consumption model of DSP for SIEM in the implementation of digital SCs can be described.

Elements of this vector can be the values of the following indicators: temporary resource $t_{\text{dsp}}(k+1)$ provided by the DS for the $(k+1)$-th stage of the DSP; the resource $N^{\text{r}}_{\text{exp}}(k+1)$ of data protection specialists, as well as resources of computer systems for the automation of DSP (described by the performance coefficient of automation tools).

Thus, the model, that illustrates the dynamics of the state transition of the vector $\vec{R}_{\text{dsp}}$ of resource costs of DSP for SIEM in the implementation of digital SCs, has the form:

$$\vec{R}_{\text{dsp}}(k+1) = \text{C}^{\text{T}}_{\vec{R}_{\text{dsp}}}(k+1)\,\vec{\Theta}_{\vec{R}_{\text{dsp}}}(k+1); \tag{13}$$

$$\begin{aligned}\vec{\Theta}_{\vec{R}_{\text{dsp}}}(k+1) = \varphi^{\text{T}}_{\vec{R}_{\text{dsp}}}(k+1,k,u)\,\vec{\Theta}_{\vec{R}_{\text{dsp}}}(k) + \\ + \Delta\vec{\Theta}_{\vec{R}_{\text{dsp}}}(k+1);\end{aligned} \tag{14}$$

$$\begin{aligned}\vec{z}_{\vec{R}_{\text{dsp}}}(k+1) = H_{\vec{R}_{\text{dsp}}}(k,\vec{x}(k))\,\vec{\Theta}_{\vec{R}_{\text{dsp}}}(k+1) + \\ + \vec{\omega}_{\vec{R}_{\text{dsp}}}(k+1).\end{aligned} \tag{15}$$

There is another approach using a different form of MCC-DSE notation for specific individual cases of describing the process of transformation of the states of individual indicators inserted in the parameter vector $\vec{R}_{\text{dsp}}(k)$ of resource costs of DSP for SIEM when implementing digital SCs. Under these conditions, a system of equations is applied that includes three separate subsystems of equations.

Each subsystem of equations, at the same time, separately characterizes the dynamics of transformation of the state of the cost indicator: the resource $N^{\text{r}}_{\text{exp}}(k+1)$ of experts and security administrators, the temporary resource $t_{\text{dsp}}(k+1)$ allocated to DS for the $(k+1)$-th stage of DSP, as well as resources of computer systems for the automation, designed to perform DSP tasks for SIEM when implementing digital SCs. The resources of computer systems for the automation can be expressed in terms of the performance coefficient of automation tools used for the DSP.

It is known that the quality of DS largely depends on the amount spent in the interests of DSP for SIEM in the implementation of digital SCs of computing, temporary, energy, software and hardware and other types of resources.

However, there are methods to optimize or reduce the cost of resources used. One of these methods is based on finding the optimal (minimal, but sufficient in shape and size) state spaces and DSP observations. In turn, this requires defining time intervals for discretization of state variables and a sufficient number of gradations of these states for the considered simulation problems of DSP for SIEM when implementing digital SCs.

The purpose of this approach is to coordinate the number of gradations of these states of QIs for DSP with the threshold limits of the values of fundamental operational and technical indicators of this process based on algorithms for generating vector criteria for mathematical simulation and evaluating of QIs for DSP.

It must be remembered that the task of finding time intervals for discretization of state variables and a sufficient number of gradations of these states for the considered simulation problems of DSP for SIEM in the implementation of digital SCs will always be solved under a number of restrictions. These restrictions are associated with the need to fulfill the requirements for:

- stability of basic technical and operational indicators of DPS with respect to concerning disturbing influences (threats and security violations) in the implementation of digital SCs;

- deviation value (accuracy) of the quality assessment criterion of DSP;
- complexity of modeling and assessing the quality of DPS;
- essence (form) of the description of state spaces by users conducting modeling and quality assessment of DSP for SIEM when implementing digital SCs.

The stages of the general methodology for the synthesis of state spaces and observation for optimality criteria in the problems of constructing cyber-physical systems are described in detail in [38].

If we use these stages as a basis, the factors listed above and the limitations associated with the need to fulfill four groups of requirements must be taken into account as well as the features of DSP as an object of modeling, then we can formulate the essence and content of new algorithm steps. This will be an algorithm, designed to select the acceptable number of gradations of state spaces for models of state transition of QIs for DSP in the interests of SIEM when implementing digital SCs.

The content of the steps of the algorithm, designed to select the acceptable number of gradations of state spaces for mathematical models of state transitions of IQs of DSP for SIEM in the implementation of digital SCs is as follows:

Step 1. Formulation (selection) of the minimal but sufficient dimension of state spaces IQs of DSP $X = \{x_j\}$, $j = \overline{1, m}$.

Step 2. Calculation of the time intervals for discretization of state variables and a sufficient number of gradations of these states, based on the specified accuracy of modeling of DSP for SIEM when implementing digital SCs.

Step 3. Search for the time intervals for discretization of state variables and a sufficient number of gradations of these states, formed to meet the requirements for DSP stability to threats and violations of information security when implementing digital SCs.

Step 4. Determining the time intervals for discretization of state variables and a sufficient number of gradations of these states, taking into account the user's requirements for the difficulty of the DSP model in the interests of security management when implementing digital SCs.

Step 5. Optimization of the time intervals for discretization of state variables and a sufficient number of gradations of these states, with the restrictions of specified in steps 2-4 of the algorithm.

Step 6. Output of the results – the optimal time intervals for discretization of state variables IQs of DSP and a sufficient number of gradations of these states.

One of the possible and effective approaches to solving the problem of optimizing the time intervals for discretization of state variables IQs of DSP and a sufficient number of gradations of these states is the approach described in [38] and based on the traditional methods of the theory of sensitivity.

IV. AN EXAMPLE IMPLEMENTATION AND EXPERIMENTAL VERIFICATION

Consider the key source data needed to calculate an example implementation of the proposed algorithm. The initial data for the implementation of the model, using the MCC-DSE should be elements of the transition probability matrix.

For example, for a model of transformation of the states of the duration $t_{\text{ds}}(k)$ of a DS cycle, these are the elements of the matrix $\varphi_{t_{\text{ds}}}^{\text{T}}(k+1, k, u)$. In addition, a starting vector is needed – the probabilities of the starting states of this process.

Let, as an example, the probabilities p_{ij} of a given QI from one state to another state (for three states, n = 3) and the probabilities of the starting states $p_i(0)$ be given and summarized in Table 1.

Table 1. Elements of the transition probability matrix

p_{ij} \ j i	1	2	3	p_i (0)
1	0.6	0.1	0.3	1
2	0.4	0.2	0.4	0
3	0.1	0.5	0.4	0

For the given, as an example, source data (3×3 matrix), the implementation of the simulated process in steps are obtained.

Fig. 1 shows that the QI value takes one of three states characterized by the values of auxiliary indicators $\vec{\Theta}_{t_{\text{ds}}}(k)$.

Fig. 2 illustrates an example of implementation by stages of a simulated process (the process can be in one of three states).

The formalized form of the transition probability matrix $\varphi_{t_{\text{ds}}}^{\text{T}}(k+1, k, u)$ for the model of the process of state transition has the form

$$\varphi_{t_{\text{ds}}}^{\text{T}}(k+1, k, u) = \begin{vmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{21} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{vmatrix}, \qquad (16)$$

and the values of the elements in this matrix are defined in accordance with Table 1 and normalized by row:

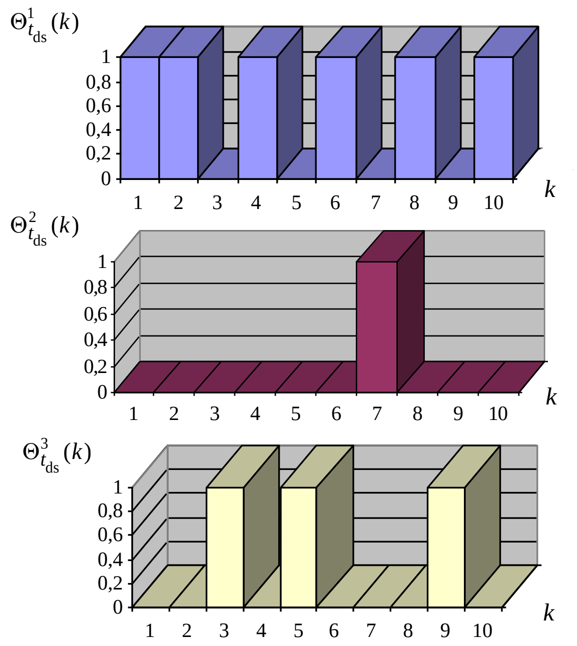

Figure 1. Implementations of the values of three auxiliary indicators of the state of the simulated process

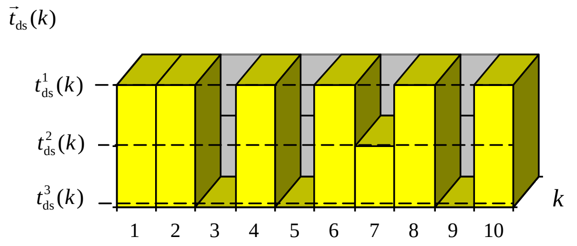

Figure 2. Implementations of a simulated process that takes one of three states of a quality indicator

$$\varphi^{\mathrm{T}}_{t_{ds}}(k+1,k,u)=\begin{vmatrix}0,6 & 0,1 & 0,3\\ 0,4 & 0,2 & 0,4\\ 0,1 & 0,5 & 0,4\end{vmatrix}. \qquad (17)$$

The simulation results are summarized in graphs (in Fig. 1), illustrating the implementations of the values of three auxiliary indicators of the state of the simulated process and are represented by the dependences of the values of additional indicators of three possible states ($\Theta^1_{t_{ds}}(k)$, $\Theta^2_{t_{ds}}(k)$ и $\Theta^3_{t_{ds}}(k)$), and in the graph (in Fig. 2), where the final results are shown – step-by-step values of the dependence of the operativity (timeliness) indicator $t_{ds}(k)$ of DS are simulated, i.e., the values of the corresponding elements of the vector $\vec{t}_{ds}(k)$ on the step of DSP for SIEM in the implementation of digital SCs.

The analysis of the obtained dependencies suggests that the considered modeling method allows one to obtain the sample values of QIs of the DSP for SIEM under digital SCs with a high – level of adequacy.

This approach, among other things, ensures that further analysis on the parameters of DSP (Bellman's dynamic programming method, theory of nonlinear and linear optimal filtering) is consistent with advanced mathematical methods, because it relies on Markov chains.

The undoubted advantage of this approach is that the investigation of processes taking into account exciting noise in the state space allows one to study the dynamics of any other stochastic processes of SIEM, taking into account possible computer attacks and other similar security threats when implementing digital SCs.

A computational prototype was implemented to fully test the adequacy and correctness of this model functioning. The calculations were carried out for various options of arbitrary arrays of input data (probability of the starting states, the values of matrix elements, etc.). The results of the given example (see Fig. 1 and Fig. 2) and the results of additional verification calculations confirm the hypotheses put forward in the article and prove the potential applicability of the proposed method.

V. DISCUSSION

Based on the results of the analysis of relevant works and on the results of experiments, we can state that the proposed set of equations (4)-(6), (7)-(9), (10)-(12) and (13)-(15) is a mathematical model, describing the process of changing the values of main feature properties of DSP for SIEM when implementing digital SCs.

This model can be used to model and control the quality of information security in the supply chain and is described in terms of MCC-DSE.

In this case, the essential properties of DSP are expressed through the dynamics of transformation of the values of its QIs in the state space. This allows for a formalized mathematical specification of the state transition of DSP, taking into account the features of complex modern managed systems for detecting and eliminating threats of computer attacks, taking into account the peculiarities of digital SCs processes and the peculiarities of decision support for managing the supply chain operating modes, parameters and structure.

The proposed version of the mathematical description of the process of state change of DSP for SIEM in the implementation of digital SCs allows one to unify and structure the description of such processes, taking into account the requirements of operativity, reliability, secrecy and the amount of resources used.

As a result, it can be noted that it is advisable to use the proposed model in the form of MCC-DSE to control the quality of information security in the supply chain using a mathematical description of a stochastic managed decision-making process for managing security events and incidents in the interests of detecting and eliminating threats of computer attacks in the implementation of digital SCs. Moreover, while preserving the advantages of the traditional formalized representation of controlled Markov chains, the high degree of adequacy of which to the formed process has been tested. Model based on MCC-DSE works with probability-time characteristics and takes into account the exciting noise of the simulated process.

VI. CONCLUSION

The paper proposed models important for a formalized analytical description of the controlled processes occurring in cyber-physical systems and other complex software-hardware, which are processes of guaranteed information protection in the supply chain. The developed mathematical model allows one to describe the dynamics of transformation of the values of the fundamental properties of DSP for SIEM in the implementation of digital SCs. Moreover, the properties of DSP are expressed in terms of its quality indicators, formalized on the basis of the apparatus of MCC-DSE. Application of the developed model in practice will improve the quality of modeling by increasing the reliability and accuracy of the results obtained when they are used for evaluating and predicting the state of security control in the supply chain. Therefore, this will reduce the cost of time, financial and other management resources in the development (design), and operation of decision support systems. It will increase the degree of validity of decisions on the management of the operation modes, parameters and structure of quality control systems for information protection in the implementation of digital SCs.

The directions of further development and research are the implementation in practice of the proposed model and the modeling of DSP for SIEM when implementing digital SCs, based on real expert values of private QIs, parameter values set by security administrators in the supply chain, and existing characteristics of the real input data flow to develop options for solutions to control the information security in systems of this class.

References

[1] A. Robinson, *The Digital Supply Chain: The Landscape, Trends, Types and Application in Supply Chain Management*, 2019, [Online]. Available at: https://cerasis.com/e-book-digital-supply-chain/

[2] M. Alexander, P. Brody, J. Chadam, C. Cookson, J. Little, B. Meadows, *Digital supply chain: It's all about that data.* 2016 EYGM Limited. EY's Global Technology Sector. 2016, 16 p.

[3] M. Moon, "Digital supply chains for English language learning", *Journal of Digital Asset Management*, no. 4, pp. 2-4, 2008. https://doi.org/10.1057/dam.2008.8.

[4] P. Farahani, C. Meier and J. Wilke, "Digital supply chain management agenda for the automotive supplier industry," *Shaping the Digital Enterprise*. Springer. pp. 157-173, 2017. https://doi.org/10.1007/978-3-319-40967-2_8.

[5] *Industry 4.0: Global Digital Operations Study 2018*, 2018. https://doi.org/10.1016/S1365-6937(18)30176-X.

[6] *Logistics Trend Radar 2018/19: Delivering Insights Today, Creating Value Tomorrow*, 2018, [Online]. Available at: https://www.logistics.dhl/globalen/home/insights-and-innovation/insights/logistics-trendradar.html

[7] *Supply Chain 4.0 – the next-generation digital supply chain*, 2019, [Online]. Available at: https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-40-the-next-generation-digital-supply-chain

[8] V. Desnitsky, D. Levshun, A. Chechulin, I. Kotenko, "Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 7(2), pp. 60-80, 2016.

[9] Y. Sun, "Research on security issues and protection strategy of computer network," *The Open Automation and Control Systems Journal*, no. 7, pp. 2097-2101, 2015. https://doi.org/10.2174/1874444301507012097.

[10] P.L. Dordal, *An Introduction to Computer Networks*, Release 1.9.0, 2017, 745 p.

[11] J.M. Kizza, *Guide to Computer Network Security*, 3rd Edition. Springer, New York, 2015, 545 p. https://doi.org/10.1007/978-1-4471-6654-2_1.

[12] S. Watts, "Low-intensity computer network attack and self-defense," *International Law Studies*, vol. 87. pp. 59-87, 2011.

[13] S. Eckmann, G. Vigna, R. Kemmerer, "STATL: An attack language for state-based intrusion detection," *Journal of Computer Security*, vol. 10(1/2), pp. 71-104, 2002. https://doi.org/10.3233/JCS-2002-101-204.

[14] M. O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*, Apress, New-York, 2019, 1151 p. https://doi.org/10.1007/978-1-4842-4294-0.

[15] A. Salmon, W. Levesque, M. McLafferty, Applied Network Security: Proven Tactics to Detect and Defend Against all Kinds of Network Attack, Packt Publishing, Birmingham, 2017, 336 p.

[16] I. Kotenko, A. Chechulin, "Computer attack modeling and security evaluation based on attack graphs", *Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems* (IDAACS'2013), Berlin, 12-14 September 2013, pp. 614-619. https://doi.org/10.1109/IDAACS.2013.6662998.

[17] I.V. Kotenko, I.B. Parashchuk, "An approach to modeling the decision support process of the security event and incident management based on Markov chains," *Proceedings of the 9th IFAC/IFIP/IFORS/IISE/INFORMS Conference "Manufacturing Modelling, Management and Control"* (MIM 2019). 28-30 August 2019, Berlin, Germany. IFAC-PapersOnLine. 2020.

[18] T. Gh. Dobre, J. G. Sanchez Marcano, *Chemical Engineering: Modelling, Simulation and Similitude*, Wiley-VCH, Weinheim, 2007, 568 p. https://doi.org/10.1002/9783527611096.

[19] A. Quarteroni, "Mathematical models in science and engineering," *Notices of the AMS*, vol. 56, no. 1, pp. 9-19, 2009.

[20] M. Stamp, *Information Security Principles and Practice*, San Jose State University, San Jose, 2005, 381 p.

[21] M.S. Merkow, J. Breithaupt, *Information Security: Principles and Practices*, second ed., Indianapolis, 2014, 341 p.

[22] I.A. Shuvalov, E.A. Semenchin, "Mathematical model of impact of threats on information system of processing of personal information," *Fundamental Research*, no. 10, pp. 529-533, 2013.

[23] A.I. Pereguda, D.A. Timashov, "Mathematical model of reliability of security information systems", *Information*, no. 8, pp.10-17, 2009.

[24] P.Y. Ryan, "Mathematical models of computer security," in: R. Focardi and R. Gorrieri (Eds.): FOSAD 2000, LNCS 2171, 2001, pp. 1-62.

[25] *Security Trends & Vulnerabilities Review Corporate Information Systems*, 2017, [Online]. Available at: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Corp-Vulne-rabilities-2017-eng.pdf.

[26] A.V. Zadorskii, N.P. Romashkina, Information Security. Threats during Crisis and Conflicts of the XXI century, IMEMO, Moscow, 2016, 133 p. https://doi.org/10.20542/978-5-9535-0461-4.

[27] V. Pham, C. Cid, *Are we compromised? Modelling security assessment games.* in: Decision and Game Theory for Security, Springer, 2012, pp. 234-247. https://doi.org/10.1007/978-3-642-34266-0_14.

[28] C. Scheau, A. Arsene, G. Dinca, "Phishing and e-commerce: an information security management problem," *Journal of Defence Resources Management*, vol. 7, No. 1(12), pp. 129-140, 2016.

[29] L.J. La Padula, *Secure Computer Systems: A Mathematical Model*. in: MTR-2547, vol. 1, The MITRE Corporation, Bedford: Massachusetts, 1993, 33 p.

[30] D.J. Higham, "An algorithmic introduction to numerical simulation of stochastic differential equations," *SIAM Review*, vol. 43(3), pp. 525-546, 2001. https://doi.org/10.1137/S0036144500378302.

[31] S. M. Iacus, *Simulation and Inference for Stochastic Differential Equations, with R Examples*, Springer Verlag, 2008, 214 p. https://doi.org/10.1007/978-0-387-75839-8.

[32] S.N. Ethier, T.G. Kurtz, *Markov processes*, in: Wiley Series in Probability and Mathematical Statistics: Probability and Mathematical Statistics, John Wiley & Sons Inc., New York, 1986, pp. 214-234. https://doi.org/10.1002/9780470316658.

[33] D. Bini, G. Latouche and B. Meini, *Numerical Methods for Structured Markov Chains*, in: Oxford University Press, New York, 2005, 215 p. https://doi.org/10.1093/acprof:oso/9780198527688.001.0001.

[34] M. Rashidi, M. Ghodrat, B. Samali and M. Mohammadi, "*Decision Support Systems, Management of Information Systems*", IntechOpen, 2018. https://doi.org/10.5772/intechopen.79390.

[35] S.V. Belim, N.F. Bogachenko, Y.S. Rakitskiy, A.N. Kabanov, "Using the decision support algorithms combining different security policies," *Cryptography and Security*, Cornell University, 2018, [Online]. Available at: https://arxiv.org/abs/1812.08030v1.

[36] J.P. Shim, M. Warkentin, J.F. Courtney, D.J. R. Power, R. Sharda and C. Carlsson, "Past, present, and future of decision support technology," *Decision Support Systems*, vol. 33(2), pp. 111-126, 2002. https://doi.org/10.1016/S0167-9236(01)00139-7.

[37] S.N. Medvedev, K.A. Aksyonov, O.P. Aksyonova, "Application of a decision support system in an industrial enterprise", *IOP Conf. Series: Materials Science and Engineering*, 709, article ID 044026, pp. 1-5, 2020. https://doi.org/10.1088/1757-899X/709/4/044026.

[38] 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), vol. 1069, no. 012153, pp. 1-6, 2018. https://doi.org/10.1088/1742-6596/1069/1/012153.

IGOR V. KOTENKO, *Doctor of Technical Sciences, Professor; Head of the Laboratory of Computer Security Problems in St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Areas of scientific interests: information security, artificial intelligence, machine learning, data mining, telecommunications.*

IGOR B. PARASHCHUK, *Doctor of Technical Sciences, Professor; Leading Researcher of the Laboratory of Computer Security Problems in St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Areas of scientific interests: computer network security, automated information systems, data storage and processing.*

•••