Multi-criteria security assessment of control and diagnostic data on the technological processes

Igor Kotenko^{1,2} and Igor Parashchuk^{1,2,*}

¹ St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), 199178, St. Petersburg, 14-th Linia 39, Russia

² St. Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), 197101, St. Petersburg, Kronverksky Pr. 49, Russia

Abstract. A mathematical model of the dynamics of changes in the state of security indicators of control and diagnostic data on the technological process is proposed. It is constructed using Markov chains and takes into account the probabilistic-temporal mechanism for changing the state of data protection indicators of this class. Based on this model, a methodological approach has been developed for multi-criteria assessment of the security of control and diagnostic data on the technological process. The approach is based on the analysis of current deviations of the values of data protection indicators from the requirements for them, takes into account and eliminates the uncertainty of the initial diagnostic information. The proposed methodological approach also allows one to take into account transients that affect security when introducing control over the structure, parameters and modes of collection and processing of control and diagnostic data about the technological process in various conditions.

1 Introduction

The key problem of optimal control of a complex technological process (TP) is the timely receipt by the automated control system (ACS) of reliable and undistorted control and diagnostic data on the state of the parameters of this process in dynamics [1, 2].

Various production technologies, using many different tools and equipment, collect and analyze large amounts of information characterizing the results of control measurements and diagnostics [1-4]. The accuracy and reliability of this information certainly affects the effectiveness of TP management. At the same time, this data is subject to threats that could violate their availability, integrity and confidentiality. That is why in the world so much attention is paid to data protection about various technological processes [5-7]. This is the key to the rational functioning of modern complex technological and cyber-physical systems, including systems of the “smart production” type.

One of the traditional methodological tools for making decisions on the effective management of this type of data protection, for analyzing the level of their security, is the

* Corresponding author: shchuk@rambler.ru

methodology for assessing the security of diagnostic and control data about the technological process. The results of this analysis allow one to quickly introduce adequate control actions aimed at searching, detecting and countering the security threats of control and diagnostic information (CDI). Assessing the level of information security of complex systems, processes and data arrays, including the security of control and diagnostic data on the technological process, requires a large amount of knowledge about the processes of their collection, storage and processing. This knowledge can be expressed quantitatively, on the basis of measurements (formalized), or can be experimental (obtained on the basis of models) and expert-based. As part of the TP management, there is always uncertainty associated with the source data necessary for both the intelligent analysis of the CDI itself and the analysis of its security. This is all the more relevant now, with modern security threats and algorithms of aggressive computer penetration into TP, when complex multi-step attacks and the "introduction" of false data into CDI are possible from the different categories of intruders [8, 9]. The first and main stage of the methodology for analyzing the security of complex systems and data arrays is always the stage of modeling the behavior of security indicators in dynamics. At the same time, to model the change of states of the security indicators of systems and data using the processing of uncertain knowledge, the probability-temporal models of changing the values of these indicators in the state space are increasingly used. An additional element in the models of this class is their use in conjunction with algorithms for eliminating the uncertainty of knowledge about these states.

The feasibility and relevance of solving such problems is obvious. Based on the model of this type, it is possible to use these methods in cooperation with each other and to carry out a multi-criteria assessment of the security of the control and diagnostic data, taking into account the uncertainty. In addition, it is possible to automatically "accumulate" knowledge about CDI security and make optimal decisions to counter threats CDI on the TP, based on the accumulated knowledge and the results of data security analysis of this class.

2 Relevant works

Many works have been devoted to the development of analytical models and methodological approaches to assessing the security of complex technical systems and data arrays. There are a number of particular methods for evaluating the effectiveness of protection, storage and analytical processing of information [10-21]. These works have a number of advantages, but the use of the models proposed in them to develop a method for multi-criteria assessment of the security of TP diagnostic and control data is inappropriate. The main causes for this inappropriateness are as follows:

(1) the need to take into account transients inherent in various states of CDI security indicators and the requirements for security analysis [10-12]. This forces one to formulate not only a vector, but also a multi-criteria problem of assessing the security of TP diagnostic and control data;

(2) the models and methods proposed in these works do not take into account the unique properties and specific modern technologies of collecting, processing and storing the TP control and diagnostic data, do not take into account the features of CDI security indicators that need to be evaluated [13-15];

(3) in fact, there are no dynamic models and analysis methods in dynamics; the assessment of the security of systems and data is designed for analysis either in a static mode or under local stationary conditions [16-18].

In addition, in a number of works [19-21], the authors were forced to use (within the techniques of data protection efficiency analysis) the multi-dimensional joint probability densities of the values of security indicators. But this requires the collection and processing

of a large amount of statistical data, which is not always possible within the real TP. All this emphasizes the urgency of the tasks of developing existing techniques and searching for new mathematical methods for assessing the security of the TP diagnostic and control data within the framework of a probabilistic approach. In other words, a methodological approach is needed to reduce the dimensionality of the task of multi-criteria dynamic assessment of CDI security that allows one to quickly analyze the effectiveness of security mechanisms for control and diagnostic data from the point of view of optimal process control.

3 Theoretical part

In the paper we propose an approach that aims to develop existing techniques in terms of dynamic multi-criteria security assessment of CDI. This approach, unlike the existing ones, is based not on stationary probabilistic models of CDI on the TP security indicators to be monitored, but on probability-temporal models of these indicators. For this, controlled Markov chains are applied, the dynamics of the change of states in which is described using stochastic equations in finite differences. Analytical models of the process of changing the security states of the TP control and diagnostic data, which based on the mathematical apparatus of controlled Markov chains in the form of difference stochastic equations, are, in fact, probabilistic-temporal models of changing the states of CDI security indicators.

They, unlike the known ones, make it possible to take into account the dynamics of the probabilistic-temporal mechanism for changing the state of CDI security and the correlation of its estimates at the neighboring l -th steps of the TP. Then the probabilistic-temporal model of the process of changing states of a single CDI security indicator (the physical meaning is the deviation $\Delta \mathbf{w}$ of a security indicator from the required values within the TP), based on the mathematical apparatus of controlled Markov chains in the form of difference stochastic equations, has the form:

$$\Delta \mathbf{w}(l+1) = \mathbf{G}^T(l+1) \mathbf{Q}(l+1); \quad (1)$$

$$\mathbf{Q}(l+1) = \mathbf{M}^T(l+1, l, u) \mathbf{Q}(l) + \mathbf{v}(l); \quad (2)$$

$$\mathbf{v}(l) = [\mathbf{v}^T(l) \mathbf{Q}(l)] \mathbf{v}'(l+1); \quad (3)$$

$$\mathbf{K}(l+1) = \mathbf{H}(l, \mathbf{w}(l)) \mathbf{Q}(l+1) + \boldsymbol{\omega}(l+1), \quad (4)$$

where the expression (1) is the equation of state of the process $\Delta \mathbf{w}$ at the $(l+1)$ -th step of the TP (in our case, this is the deviation state of some CDI security indicator), $\mathbf{G}^T(l+1)$ – the transposed matrix-row of possible values of the security indicator deviations, $\mathbf{Q}(l+1)$ – an auxiliary vector of state indices of security indicators in the form of deviations, the elements of which take values

$$Q_m(l+1) = \begin{cases} 1 & \text{at } \Delta \mathbf{w}(l+1) = \Delta \mathbf{w}_m, \\ 0 & \text{in other cases.} \end{cases}$$

An auxiliary vector of indices $\mathbf{Q}(l+1)$ containing elements $Q(l+1)$ is introduced into the system of equations for the convenience of recording the dynamics of transitions of the security indicators. The equation (2) is the equation of state of the auxiliary index vector, where $\mathbf{M}^T(l+1, l, u)$ – the transposed matrix of probabilities of the transition of the process, causing the change of the state of CDI security indicators, $\mathbf{Q}(l)$ – the vector of

values of the state indices in the previous step, $\mathbf{v}(l)$ – a vector of compensation additives, the elements of which are designed to compensate the non-integer part of equation (2) and are obtained as a result of analysis and correction of the initial excitation noise. The excitation noise is considered as additive white Gaussian noise. Equation (3) explains the physical nature of the calculation of the elements of the vector $\mathbf{v}(l)$ of compensation additives. Moreover, in equation (3): $\mathbf{v}^T(l)$ – the transposed diagonal block matrix of compensation additives, the elements of which are designed to compensate the integer part in equation (2); $\mathbf{v}'(l+1)$ – the vector of values of the modified exciting noise that determines the values $\mathbf{Q}$ at the $(l+1)$ -th step. The equation for observing the process $\Delta \mathbf{w}$ at the $(l+1)$ -th step of the TP (in our case, this is the deviation state of some CDI security indicator) is described by expression (4).

The suggested model is a basis of the methodological approach on the multi-criteria assessment of security of the TP control and diagnostic data. In other words, the use of controlled Markov chains in the form of difference stochastic equations allows one to build the analytical models of functioning and life support of complex technological systems. It also allows one to build the models of ensuring the security of such systems and (or) data arrays collected for optimal management.

These models are formed taking into account the dynamic and probabilistic nature, non-stationarity and uncertainty of the processes of functioning of complex systems [22], their management processes, and the processes of ensuring the security of control and diagnostic data. From the point of view of multi-criteria security assessment of the TP control and diagnostic data, the application of the theory of state variables allows expressing in the form of difference stochastic equations (based on dynamic models of CDI security indicators) both private security processes and the subsystems that implement them within the TPs. That is why the generalized, multi-criteria CDI security indicator can and should include the sub-indicators of protection against computer attacks, against entering unwanted information ("spam"), against copying, intercepting and destroying of CDI, against access by personnel not participating in the TP (unauthorized, illegal use), against legal user errors and others. Account of the diversity of CDI threats and their physical heterogeneity allows one to get the values of the current particular security indicators (PSI) of the TP CDI and the current generalized multi-criteria security indicator (MSI) of the TP control and diagnostic data. They are formulated in the form of a joint probability to meet the requirements of modern production technologies for protection of this class data at the $(l+1)$ -th step of the TP:

$$\begin{aligned}
 p_{\text{csr CDI}}(l+1) &= p(l+1)[(\mathbf{Y}_{\text{csr CDI}}(l+1) \leq \mathbf{Y}_{\text{csr CDI}}^{\text{req}})/(\mathbf{Y}_{\text{TP}}^{\text{req}})] = \\
 &= p_{\text{ca}}(l+1)[(\mathbf{Y}_{\text{ca}}(l+1) \leq \mathbf{Y}_{\text{ca}}^{\text{req}})/(\mathbf{Y}_{\text{sp}}(l+1) \leq \mathbf{Y}_{\text{sp}}^{\text{req}}) \cap (\mathbf{Y}_{\text{cid}}(l+1) \leq \mathbf{Y}_{\text{cid}}^{\text{req}}) \cap \\
 &\cap (\mathbf{Y}_{\text{st}}(l+1) \leq \mathbf{Y}_{\text{st}}^{\text{req}}) \cap (\mathbf{Y}_{\text{ue}}(l+1) \leq \mathbf{Y}_{\text{ue}}^{\text{req}})] \times p_{\text{sp}}(l+1)[(\mathbf{Y}_{\text{sp}}(l+1) \leq \mathbf{Y}_{\text{sp}}^{\text{req}})/ \\
 &/(\mathbf{Y}_{\text{cid}}(l+1) \leq \mathbf{Y}_{\text{cid}}^{\text{req}}) \cap (\mathbf{Y}_{\text{st}}(l+1) \leq \mathbf{Y}_{\text{st}}^{\text{req}}) \cap (\mathbf{Y}_{\text{ue}}(l+1) \leq \mathbf{Y}_{\text{ue}}^{\text{req}})] \times \\
 &\times p_{\text{cid}}(l+1)[(\mathbf{Y}_{\text{cid}}(l+1) \leq \mathbf{Y}_{\text{cid}}^{\text{req}})/(\mathbf{Y}_{\text{st}}(l+1) \leq \mathbf{Y}_{\text{st}}^{\text{req}}) \cap (\mathbf{Y}_{\text{ue}}(l+1) \leq \mathbf{Y}_{\text{ue}}^{\text{req}})] \\
 &\times p_{\text{st}}(l+1)[(\mathbf{Y}_{\text{st}}(l+1) \leq \mathbf{Y}_{\text{st}}^{\text{req}})/(\mathbf{Y}_{\text{ue}}(l+1) \leq \mathbf{Y}_{\text{ue}}^{\text{req}})] \times p_{\text{ue}}(l+1)[(\mathbf{Y}_{\text{ue}}(l+1) \leq \mathbf{Y}_{\text{ue}}^{\text{req}})],
 \end{aligned} \tag{5}$$

where $p_{\text{ca}}(l+1)$, $p_{\text{sp}}(l+1)$, $p_{\text{cid}}(l+1)$, $p_{\text{st}}(l+1)$ are the conditional probabilities of fulfilling the requirements for CDI protection against computer attacks, against entering unwanted information ("spam"), against copying, interception and destruction, and against access by personnel not participating in the TP (unauthorized, illegal use) at $(l+1)$ -th step of the TP, determined under condition that the requirements for the current CDI security

indicators considering legal user errors are met; $p_{ue}(l+1)$ – the unconditional probability of meeting the requirements for CDI security considering the legal user errors at the $(l+1)$ -th step of the TP.

The conditional and unconditional probabilities of fulfilling the requirements to security indicators, described in equation (5), contain the ratio of the true (real) $\mathbf{Y}$ and required $\mathbf{Y}^{\text{req}}$ values of the vector of the security indicators considering computer attacks $\mathbf{Y}_{ca}(l+1)$, the vector of the security indicators considering entering unwanted information ("spam") $\mathbf{Y}_{sp}(l+1)$, the vector of the security indicators considering copying, interception and destruction $\mathbf{Y}_{cid}(l+1)$, the vector of the security indicators considering the access of illegal personnel $\mathbf{Y}_{st}(l+1)$ and the vector of the security indicators considering errors of the legal user $\mathbf{Y}_{ue}(l+1)$, respectively.

It is important that particular security indicators have the same physical meaning as in [23–25], but are developed for the case of a dynamic multi-criteria security assessment of the TP control and diagnostic data.

4 Methodological part

The content and physical meaning of the stages of the suggested methodological approach should be formulated in more detail.

Obtaining the current probabilistic-temporal PSI is an important distinguishing feature (in addition to reducing the dimension of the analysis task) of the proposed methodological approach. The essence of obtaining the PSIs is to integrate the current one-dimensional probability densities of the values of the security indicators. They are formed on the basis of estimated values of the numerical characteristics of the CDI security indicators considering computer attacks, entering unwanted information ("spam"), copying, interception and destruction, illegal personnel access and legal user errors.

At the same time, the assessment of a specific PSI of CDI is supposed to be carried out using optimal filtering algorithms (Kalman filter) of the observed components of this security indicator. Estimated values of a specific PSI are used to form the current probability density of the values of this indicator, followed by integration of the obtained density over threshold values. As a result, in accordance with the expression (5), the obtained PSIs are convolved into the stepwise MSI values of CDI. Let us formulate in detail the essence of the stages of the methodological approach to multi-criteria assessment of the TP control and diagnostic data security:

I. Modeling (or collection of statistics based on the results of the real TP) of the change in the state of the security indicators values for the observation period (a step of the TP):

$$\begin{aligned}\mathbf{Y}_j(l+1) &= f(\Delta y_1(l+1), \dots, \Delta y_i(l+1), \dots, \Delta y_N(l+1)); \\ \mathbf{K}_{\mathbf{Y}_j}(l+1) &= \{k_{\Delta y_1}(l+1), \dots, k_{\Delta y_N}(l+1)\}^T = \\ &\quad \|\mathbf{H}(l+1)\| \mathbf{Q}(l+1) + \boldsymbol{\omega}(l+1),\end{aligned}\tag{6}$$

where $\mathbf{Y}_j(l+1)$ – the vector of CDI security indicators considering the j -th threat at the $(l+1)$ -th step of the TP; $\Delta y_i(l+1)$ – deviations of the i -th component of the j -th vector of security indicators or other CDI security indicators from the required values at the same step; $\mathbf{K}_{\mathbf{Y}_j}(l+1)$ – a vector of observations of $\mathbf{Y}_j(l+1)$, containing observations of

deviations of individual i -th CDI security indicators; $\|\mathbf{H}(l+1)\|$ – a matrix of observations of the state $\mathbf{Y}_j(l+1)$; $\boldsymbol{\omega}(l+1)$ – a vector of noises of observation of the state transition process.

II. Kalman (optimal according to the standard deviation minimum) filtering of the values of indicators (conditional averages) of the observed process of changing the states of CDI security indicators $\mathbf{Y}_j(l+1)$:

$$\{\Delta\hat{y}_1(l+1), \dots, \Delta\hat{y}_i(l+1), \dots, \Delta\hat{y}_N(l+1)\}^T;$$

$$\Delta\hat{y}_i(l+1) = \mathbf{M}\{\Delta\hat{y}_i(l+1)/k_{\Delta\hat{y}_i}(l+1)\}; \|\mathbf{D}\|, i = \overline{1, N}, \quad (7)$$

where $\Delta\hat{y}_i(l+1)$ – the estimated deviation of the i -th CDI security indicator at the $((l+1)$ -th step of the TP. The estimated value $\Delta\hat{y}_i(l+1)$ is defined as the conditional observation value of the moments – the mathematical expectation (the matrix $\mathbf{M}$) and variance (the matrix $\mathbf{D}$) of the process of changing the state of the i -th security indicator at this step of the TP.

III. Calculation of the estimated value of the j -th current particular security indicator $\hat{\mathbf{Y}}_j(l+1)$ based on the estimated values of its components:

$$\hat{\mathbf{Y}}_j(l+1) = f\{\Delta\hat{y}_1(l+1), \dots, \Delta\hat{y}_i(l+1), \dots, \Delta\hat{y}_N(l+1)\}. \quad (8)$$

IV. Determination (identification) of the parameters of the conditional by observations probability density $\hat{W}(\hat{\mathbf{Y}}_j(l+1))$ of particular security indicators using estimates of its moments:

$$\mathbf{M}\{\Delta\hat{y}_i(l+1)/k_{\Delta\hat{y}_i}(l+1)\}; \|\mathbf{D}\|.$$

V. Formation of estimated values of the j -th PSI at the $(l+1)$ -th step of the TP:

$$\hat{p}_j(l+1)[(\hat{\mathbf{Y}}_j(l+1) \leq \mathbf{Y}_j^{\text{req}})] = \int_0^{\mathbf{Y}_j^{\text{req}}} \hat{W}(\hat{\mathbf{Y}}_j(l+1)) d\mathbf{Y}_j. \quad (9)$$

VI. Obtaining the estimated value of the MSI at the $(l+1)$ -th step of the TP in accordance with the equation (5):

$$\hat{p}_{\text{csf CDI}}(l+1) = f\{\hat{p}_1(l+1), \hat{p}_2(l+1), \dots, \hat{p}_j(l+1), \dots, \hat{p}_J(l+1)\}. \quad (10)$$

5 Results and discussion

The recurrent form of representation of the PSI and MSI allows one to get their estimate in real time.

Figure 1 shows an example of the results (obtained by modeling and the computational experiment) of a step-by-step calculation of estimated values of the PSIs. It represents the graphics of the dependencies of the estimated values of the probability of satisfying the requirements to the deviations of various PSIs on the TP step for various security threats.

Fig. 1. The dependencies of the estimated values of the probability of satisfying the requirements to the deviations of various PSIs on the TP step for various security threats

Obtaining the real-time estimated values allows one to increase the efficiency of the CDI security management cycle within the TP [22-25].

In addition, the transition from the stationary analytical models of security indicators to the models based on Markov chains made it possible to investigate the transients in the dynamics of changing the level of security of the TP control and diagnostic data as a whole.

The proposed methodological approach can be used to solve the problems of direct dynamic multi-criteria security assessment of the TP diagnostic and diagnostic data as a whole, as well as to solve the inverse problem, i.e. the justification of CDI security requirements, optimization of algorithms for ensuring of this class data security in different realizations of the technological process.

6 Conclusion

The paper suggested the mathematical model of the process of changing the states of CDI security indicators based on Markov chains. The model serves as the basis of the methodological approach (methodology) for multi-criteria assessment of the security of the TP diagnostic and control data. It considers the elimination of the uncertainty of the source data and takes into account the probabilistic-temporal mechanism for changing the security state of the technological process in dynamics. The paper described the stages of the methodological approach (methodology) of multi-criteria (vector) assessment of the effectiveness of this class data protection. This methodology is based on the analysis of the current deviations of the values of the CDI security indicators from the requirements for them are.

This approach can be useful for technical and design bodies responsible for the development of information security systems for technological processes. It allows one to analyze the contribution to the security of such processes of new technical principles for constructing algorithms, tools and complexes for detecting and countering CDI threats.

In addition, this methodological approach can find its application in the development of an investment plan in the industrial and financial sector, which is responsible for realizing content security control and management systems necessary to implement modern “smart” high-tech industries.

New, promising areas for the further development of the CDI security assessment methodology are related to creating the methods for optimal management of this class data protection. The proposed methodological approach is not “closed”, it suggests the possibility of supplementing and expanding the list of security indicators studied (different in class and physical sense). It can be the basis of a vector dynamic analysis of security of any other information (data) for any technological processes as well as complex information-analytical and computing systems. In addition, a multi-criteria assessment of the security of diagnostic and diagnostic data can be implemented in the interests of operational security policy management structures of promising technological and cyber-physical systems such as “smart city”, “smart healthcare”, “smart transport” and others.

This research is being partially supported by the grants of the RFBR (projects No. 16-29-09482, 18-37-20047, 18-07-01488, 18-07-01369 and 18-29-22034), and by the budget (the project No. 0073-2019-0002).

References

1. C.C. Wang, C.H. Ko, J.S. Shiau, W. Long, *Development of Monitoring and Diagnosis Technologies for Steel-Making Process in CSC*, Optomechatronic Technologies (ISOT), International Symposium on 5-7 Nov. (2014). Seattle: WA, USA. Access mode: <https://ieeexplore.ieee.org/document/7119397/>
2. B.A. Weiss, M. Helu, G. Vogl, G. Qiao, *Use Case Development to Advance Monitoring, Diagnostics, and Prognostics in Manufacturing Operations*, IFAC-PapersOnLine **49-31**, p. 13-18 (2016)
3. G. Qiao, B.A. Weiss, *Weiss Advance Measurement Science to Assessments, Diagnostics, and Prognostics for Manufacturing Robotics* Int J Progn Health Manag. **7** (2016); (Spec Iss on Smart Manufacturing PHM): 013
4. A.M. Pishchukhin, G.F. Akhmedyanova, *Multidimensional analysis of monitoring and diagnostic information on the technological process*. MATEC Web of Conferences **224**, 01022 (2018) ICMTMTE 2018; <https://doi.org/10.1051/mateconf/201822401022>
5. Y. Zhang, *Distributed intrusion detection system in a multi-layer network architecture of smart grids* / Y. Zhang, L. Wang, W. Sun, R.C. Green, M. Alam // IEEE Transactions on Smart Grid, pp. 796-808 (2011)
6. Data Protection Policy / Daimler AG Mercedesstraße **137** 70327 (2017). Stuttgart. Germany. 18 p. Access mode: <https://www.daimler.com>.
7. General Data Protection Regulation. (EU) 2016/679 // Official Journal of the European Union. No. **4, 5**, pp. L.119/1 – L.119/88 (2016)
8. I.V. Kotenko, A.A. Chechulin, D.A. Komashinsky, *Categorisation of web pages for protection against inappropriate content in the Internet* // International Journal of Internet Protocol Technology (IJIPT), **10** (1), pp. 61-71 (2017)
9. I.V. Kotenko, A.A. Chechulin, *Common Framework for Attack Modeling and Security Evaluation in SIEM Systems* // Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing (California: IEEE Computer Society), pp. 94-101 (2012)
10. R. Dorf, R. Bishop, *Modern Control Systems* (10th Edition, Prentice Hall, 2014)
11. A.I. Zecevic, D.D. Siljak, *Control of Complex Systems* (London, Springer Science Business Media, 2010)

12. K.S. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications* (Edition 2. John Wiley & Sons, Inc., Hoboken, New Jersey. USA. 2016)
13. S. Yuksel, *Control of Stochastic Systems* (Queen's University Mathematics and Engineering and Mathematics and Statistics. 2017)
14. R. Van Handel, *Stochastic Calculus, Filtering and Stochastic Control* (Springer, New York. 2007)
15. C.P. Pfleeger, S.L. Pfleeger, *Security in Computing* (New Jersey, USA. Prentice Hall. 2015)
16. L.A. Shuvalov, E.A. Semenchin, *Mathematical model of impact of threats on information system of processing of personal information*, Fundamental Research, **10**, pp. 529-533 (2013)
17. M. Stamp, *Information Security Principles and Practice* (San Jose State University. 2005)
18. A. Quarteroni, *Mathematical Models in Science and Engineering*, Notices of the AMS. Volume **56**, Number **1**. pp. 9-19 (2009)
19. A. Myers, *Complex System Reliability* (Springer Science & Business Media. Luxembourg. 2010)
20. N. Walliman, *Research methods: the basics* (Taylor & Francis. London, UK. 2011)
21. D.W. Oliver, T.P. Kelliher, J.G., *Engineering Complex Systems With Models and Objects* (McGraw-Hill Companies. New York, USA. 2007)
22. I.B. Parashchuk, *Parametrization principles of states space of Telecommunications network in the framework of formulation of problem of optimal adaptive networking monitoring*, Modern Science: Development Tendencies. VII Extramural International Science-Practical Conference. Part **II**. Krasnodar, pp. 142-144 (2014)
23. I.B. Parashchuk, *Decision Support at the Phase of Estimation of Telecommunication Network Functioning Efficiency*, IEEE/ICC2001, St. Petersburg International Conference on Communications. SPb.: SPbGTU «LETI», pp. 2-6 (2001)
24. I.V. Kotenko, I.B. Parashchuk, *Synthesis of Controlled Parameters of Cyber-Physical-Social Systems for Monitoring of Security Incidents in Conditions of Uncertainty*, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) / IOP Conf. Series: Journal of Physics: Conference Series (JPCS) Vol.**1069**, pp 1-6 (2018)
25. I.V. Kotenko, I.B. Parashchuk, T.K. Omar, *Neuro-Fuzzy Models in Tasks of Intelligent Data Processing for Detection and Counteraction of Inappropriate, Dubious and Harmful Information*, II International Scientific and Practical Conference «Fuzzy Technologies in the Industry» (FTI 2018), Ulyanovsk, Russia. / CEUR Workshop Proceedings (CEUR-WS). Vol.**2258**, pp. 116-125 (2018)