Analysis of the Impact of Information Security on the Performance of Decision Management Process

Andrey I. Kostogryzov[1]

[1] *Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, 44/2 Vavilova Street., Moscow, 119333, Russia*

Abstract

The approach for analyzing an impact of a violation of information security requirements on the performance of decision management process in terms of predicted risks is proposed. The use of the proposed approach helps to identify "bottlenecks", reduce risks in decision management process, taking into account the requirements for system information security, and justify conditions and period, in which guarantees of risks retention within admissible limits are maintained. The usability of the approach is illustrated by examples.

Keywords

Analysis, system information security, model, risk, decision management process

1. Introduction

The main goal of decision management process is to provide an analytical basis for definition, characterizing and evaluating a variety of alternative decisions, choosing the most preferred decision and the ways of practical actions at any stage of the system life cycle. In the conditions of existing uncertainties, various risks arise that require rational management, including risks associated with violation of system information security requirements. Despite many works on risk management for different application areas (see, for example, [1-20]) the problems associated with the analysis of various impacts on the performance of decision management process and on output results in terms of predicted risks continue to be relevant.

In this paper an universal methodological approach to do the probabilistic analysis of an impact of information security on the performance of decision management process is proposed. It includes a description of general propositions, review and recommendations for probabilistic modeling (considering [1-20]), the approach to the estimation of integral risk, examples connected with decision management process in application to ISO 15704 "Enterprise modelling and architecture — Requirements for enterprise-referencing architectures and methodologies" and interpretation comments about a calculated impact of a violation of information security requirements on the performance of architectural decisions.

2. General propositions

In general, the main output of decision management process are:
- decisions that require alternative system analysis;
- the alternative ways of actions;
- preferred decisions and the ways of actions;
- the documented rationale of decisions, conditions and assumptions made during the process.

In the life cycle of systems, both the reliable performance of decision management process itself and the system information security proper to this process should be ensured.

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: akostogr@gmail.com
ORCID: https://orcid.org/0000-0002-0254-5202

To predict proper risks the approach for modeling decision management process is proposed below. According to ISO Guide 73 risk is understood as effect of uncertainty on objectives considering consequences (an effect is a deviation from the expected — positive and/or negative).

3. The recommendations for modeling

To predict the risks for a given prognostic time T it is proposed to use the following quantitative probabilistic measures:

$R_{\text{rel}}(T)$ – the probability of failure to reliable perform decision management process without consideration of threats to system information security;

$R_{\text{sec}}(T)$ – the probability of violating system information security requirements;

$R_{\text{int}}(T)$ – the integral probability of failure to reliable perform decision management process considering system information security.

To calculate the risk measures, the entities under study can be considered as a system of simple or complex structure. Models and methods for risks prediction use data obtained "upon the occurrence of events", according to the identified prerequisites for the occurrence of events, and data collected and accumulated statistics and possible conditions for their implementation of the process.

A simple structure system for modeling is a system consisting of a single element or a set of elements logically combined for analysis as a single element. The analysis of a simple structure system is carried out according to the «Black box" principle, when the inputs and outputs are known, but the internal details of the system operation are unknown. A system of a complex structure for modeling is represented as a set of interacting elements, each of which is represented as a «Black box" operating under conditions of uncertainty.

In general case the modeling is based on using concept of the probabilities of "success" and/or "unsuccess" (risk of "failure" considering consequences) during the given prognostic time period. There are recommended some «Black box" models for which probabilistic space (Ω, B, P) is created (see for example [1, 3, 6, 7, 13, 15] etc.), where: Ω - is a limited space of elementary events; B – a class of all subspace of Ω-space, satisfied to the properties of σ-algebra; P – is a probability measure on a space of elementary events Ω. Because, $\Omega=\{\omega_k\}$ is limited, there is enough to establish a reflection $\omega_k \to p_k = P(\omega_k)$ like that $p_k \geq 0$ and $\sum_k p_k = 1$. Using these probabilistic models the measures $R_{\text{rel}}(T)$ and $R_{\text{sec}}(T)$ can be estimated considering uncertainty conditions, periodical diagnostics, monitoring between diagnostics, recovery of the lost integrity for «Black box".

Applicable models for predicting such different risks, including the ways for generating models for complex system with parallel or serial structure, see in [1, 3, 6, 7, 13, 15]. These models can be used for analyzing the impact of information security on the performance of decision management process.

4. Estimation of integral measure

The integral probability of failure to reliable perform decision management process considering system information security $R_{\text{int}}(T)$ for the period T is proposed to be calculated by the formula:

$$R_{\text{int}}(T) = 1 - [1 - R_{\text{rel}}(T)] \cdot [1 - R_{\text{sec}}(T)]. \quad (1)$$

Here the probabilistic measure $R_{\text{rel}}(T)$ is the probability of failure to reliable perform decision management process without consideration of threats to system information security and $R_{\text{sec}}(T)$ is probability of violating system information security requirements. They are estimated according to recommendations of section 3 considering the possible damage (the condition of independence between the random time before failure in performing the decision management process and the random time before violating system information security requirements is supposed).

5. Examples
5.1. General

Without deviation from the general understanding of the proposed approach, the examples are given with reference to the standard decision management process in application to ISO 15704 “Enterprise modelling and architecture — Requirements for enterprise-referencing architectures and methodologies”. The examples demonstrate the proposed approach to analyzing the impact of information security on the performance of decision management process.

Let some enterprise of hazardous production form a complex of architectural decisions according to the recommendations ISO 15704 on the general architecture of the enterprise. Separately, they define: architectural and organizational decisions focused on people; process-oriented architectural decisions; architectural decisions focused on the applied technologies.

Without going into the details of the considered architectures, the complex structure of architectural decisions for modeling is presented by Figure 1.

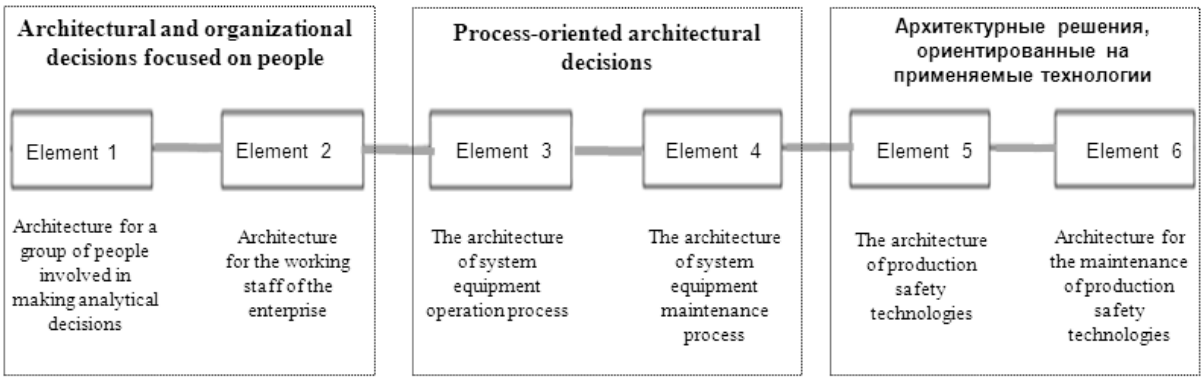

Figure 1. The complex structure of the architectural decisions

The elements of the modelled system are:

1st element - architecture for a group of people involved in making analytical decisions;

2nd element - architecture for the working staff of the enterprise;

3rd element - the architecture of system equipment operation process;

4th element - the architecture of system equipment maintenance process;

5th element - the architecture of production safety technologies;

6th element - architecture for the maintenance of production safety technologies.

According to definition reliable perform the necessary actions of decision management process (without consideration of threats to system information security) is provided during a given period, if during this period the actions needed are reliable performed "AND" for the architectural and organizational decisions focused on people (by elements 1, 2), "AND" for process-oriented architectural decisions (by elements 3, 4), "AND" for architectural solutions focused on the applied technologies (by elements 5, 6). The given prognostic period itself for an individual element can be interpreted as referring both to the stage of creation (for threats inherent in this stage) and to the stage of operation in the future (for potentially possible threats). By modeling the acceptability of architectural decisions and guarantees of risk retention within admissible limits are confirmed.

Let taking into account possible damages, the objectives of risk prediction are formulated by the company's management as follows:

- to quantify the risks of violating the reliability of the process performance without taking into account the requirements for system information security (both piecemeal and for a complex of architectural decisions);
- quantify the risks of violating system information security requirements (both piecemeal and for a complex of architectural decisions);

- quantify the risks of violating the reliability of the process performance, taking into account the requirements for system information security (entirely for the complex of architectural decisions);
- estimate such a period during which the guarantees of retaining risks within admissible limits are maintained;
- identify critical conditions in the development of various threats.

Example 1 is devoted to prediction the risk of violating the reliability of the process performance without taking into account the requirements for system information security. Example 2 is devoted to prediction the risk of violating the requirements for system information security. Example 3 illustrates the prediction of the integral risk of violating the process performance taking into account the requirements for system information security.

5.2. Example 1

The risk of violating the reliability of the process performance without taking into account the requirements for system information security is estimated for modelled structure of Figure 1. At the same time, the threats associated not only with the causes of human errors at the decision-making levels, but also hypothetical threats associated with the consequences of these errors at the stage of the enterprise's operation are taken into account. The generated input data for modeling, which cover each of the 6 composite elements, are presented in Table 1.

Table 1

Example 1 input for modeling complex structure by the model (see models in [13, 15])

Input for the model	Values and comments		
	for 1st /2nd elements	for 3rd /4th elements	for 5th/6th elements
σ - frequency of the occurrences of potential threats	1 time in a year / 1 time in a year (there are threats of human errors or due to health problems of the staff)	1 time in a year (this is commensurate with the equipment failure frequency during operating time) / 1 time in 5 years (this is due to rare failures in the process of maintaining the system equipment)	1 time in 2 years (this is commensurate with the frequency of technological failure during operating time) / 1 time in 5 years (this is due to rare failures in the process of maintaining the technological safety)
β - mean activation time of threats	2 weeks (this is commensurate with the time of mathematical modeling for making decision) / 5 years (this is commensurate with the mean time between failures in decisions implementations)	12 months (this is commensurate with the mean time for gradual failure considering equipment maintenance) / 6 months (this is complained of capabilities to operate in outdated environment)	1 month (this is commensurate with the mean time for gradual failure considering the maintenance of technological safety) / 6 months (this is complained of capabilities to operate in outdated environment)
T_{betw} - time between the end of diagnostics and the beginning of the next diagnostics	8 hours / 8 hours (this time is determined by the regulations for monitoring the readiness of personnel)	1 hour / 1 month (this time is determined by the regulations for control, except technological safety)	1 hour / 1 month (this time is determined by the regulations for technological safety control)

Input for the model	Values and comments		
	for 1st /2nd elements	for 3rd /4th elements	for 5th/6th elements
T_{diag} - diagnostics time	10 minutes / 10 minutes (this is the mean time of medical personnel examination before work)	30 seconds/30 seconds (this is commensurate with the automatic equipment integrity monitoring)	30 seconds/30 seconds (this is commensurate with the automatic monitoring of technological safety)
T_{recov} - recovery time	1 hour / 1 hour (this is the mean time to replace a person with a stand-in)	30 minutes (including system reinstallation) / 1 week (including the search for new contractors to system maintenance)	1 day (including recovery of technological operation) / 1 week (including the search for new contractors to system maintenance)
T - given prognostic period	From 6 months to 2 years (to estimate such a period during which the guarantees of retaining risks within admissible limits are maintained)		

Probability of failure to reliable perform decision management process without consideration of threats to system information security is estimated by the model [..]. The analysis of calculation results showed that during a year this probability will be about 0.040 for all complex of decisions - see Figure 2. If the prognostic period is increased from six months to 2 years, the risk increases from 0.018 to 0.083 (see Figure 3). For an acceptable risk at the level of 0.05, a period of up to 15 months is justified, in which guarantees of risk retention within admissible limits are maintained in the conditions of the example 1 (see Table 1).

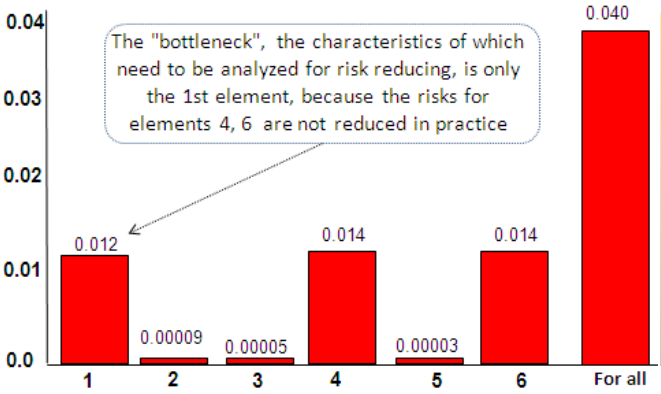

Figure 2. The probability of failure to reliable perform decision management process during a year without consideration of threats to system information security - $R_{\mathrm{rel}\,i}\,(T = 1\mathrm{year})$

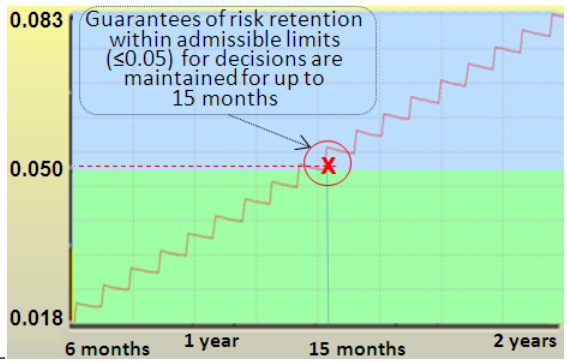

Figure 3. Dependence $R_{\mathrm{rel}}\,(T)$ on the prognostic period T lasting from 6 to 24 months

At the same time, the "bottleneck", the characteristics of which need to be analyzed for risk reducing, is only the 1st element - this is the architecture for a group of people associated with making analytical decisions (for managers, designers, designers, engineers, analysts, integrators). The identification of this "bottleneck" becomes the reason for an additional system analysis to reduce the risk. The simplest option is to combine efforts in solving the same problem on the part of several persons involved in making analytical decisions. These efforts imply mutual control and coordination of activities. And from the point of view of modeling, instead of the 1st element, the 1st subsystem appears in the structure, represented as two parallel elements – see Figure 4.

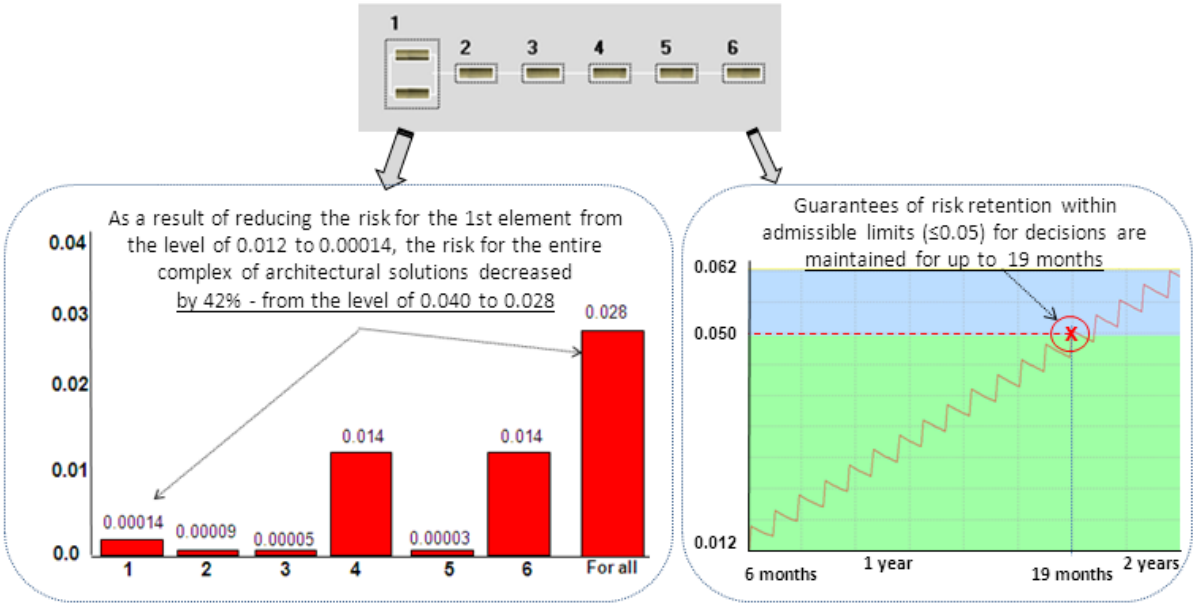

Figure 4. The risk of failure to reliable perform decision management process (without consideration of threats to system information security) is decreased (left), and guarantees of risk retention within admissible limits (≤0.05) are increased (right)

All the input data for each of the parallel combined elements of the 1st subsystem are the same as for the 1st element from Table 1. As a result of additional modeling, it was revealed that due to the measures taken, a 42% reduction in the risk of violating the reliability of the process performance without taking into account the requirements for system information security and an increase by 27% of the period for which guarantees of risk retention within acceptable limits are preserved (from 15 to 19 months – see Figure 4). In practice, it is these measures (combining the efforts of several persons in the parallel solution of one task with mutual control and coordination of the prepared solutions) that lead to the reliable performance of the process under consideration. The example shows only a quantitative estimation of such measures in terms of predicted risks (for each element).

5.3. Example 2

Additionally the real and hypothetical threats to system information security are considered – see Figure 5 and input data in Table 2.

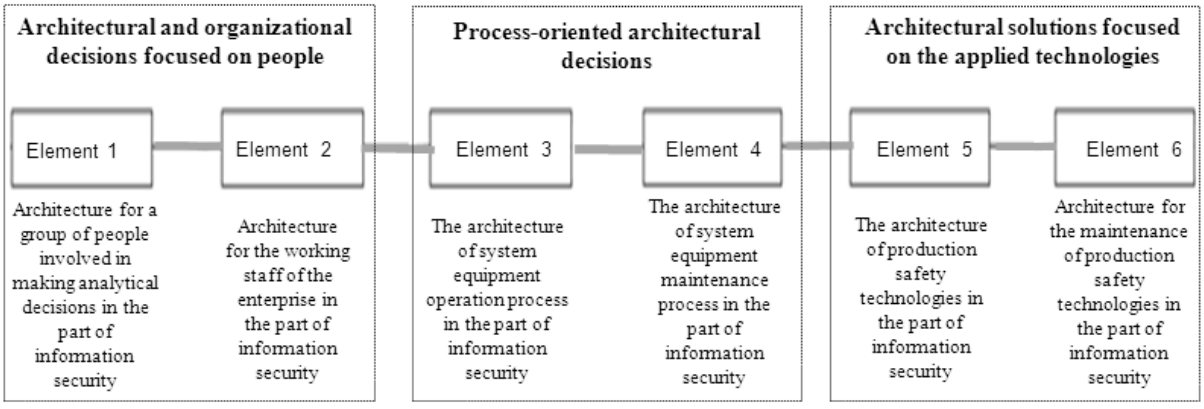

Figure 5. The structure of the simulated system in the form of a complex of architectural solutions in terms of accounting for information security requirements

Table 2

Example 2 input for modeling complex structure by the model [13,15]

Input for the model	Values and comments		
	for 1st /2nd elements	for 3rd /4th elements	for 5th/6th elements
σ - frequency of the occurrences of potential threats to information security	1 time in a year / 1 time in a year (there are threats to information security from the staff)	1 time in a year (this is commensurate with the equipment failure frequency during operating time) / 1 time in 5 years (there are threats to information security in the process of maintaining the system equipment)	1 time in 2 years (this is commensurate with the frequency of technological failure during operating time) / 1 time in 5 years (there are threats to information security in the process of maintaining the technological safety)
β - mean activation time of threats up to violation of information security	2 weeks (this is commensurate with the time of using vulnerabilities in the part of information security) / 5 years (this is commensurate with the mean time between failures connected with information security)	1 day / 1 day (it is assumed that due to masking, the sources of threats are not activated immediately, but with a certain delay of at least 1 day)	1 day / 1 day (it is assumed that due to masking, the sources of threats are not activated immediately, but with a certain delay of at least 1 day)
T_{betw} - time between the end of diagnostics and the beginning of the next diagnostics connected with information security	1 day / 1 day (this time is determined by the regulations for monitoring the readiness of personnel)	1 hour / 1 hour (this time is determined by the regulations for software and assets control in the part of information security, except technological safety)	1 hour / 1 hour (this time is determined by the regulations for technological safety control in the part of information security)
T_{diag} - diagnostics time	30 seconds/30 seconds (automatic control of personnel according to information security requirements)	30 seconds/30 seconds (automatic control of software and assets according to information security requirements)	30 seconds/30 seconds (automatic technological safety control according to information security requirements)
T_{recov} - recovery time after information security violation	5 minutes / 5 minutes (including system reinstallation)	5 minutes / 5 minutes (including system reinstallation)	5 minutes / 5 minutes (including system reinstallation)
T - given prognostic period	From 6 months to 2 years (to estimate such a period during which the guarantees of retaining risks within admissible limits are maintained)		

The analysis of the calculations results showed that in probabilistic terms, the risk of violating information security requirements during the year will be about 0.071 for the entire complex of

architectural solutions (see Figure 6), amounting to 0.034 for the 1st element ("bottleneck"), 0.021 for the 3rd element, and no more than 0.010 for the 2nd, 4th, 5th and 6th elements.

With an increase in the prognostic period from six months to 2 years, the risk increases from 0.040 to 0.140 (see Figure 7). For an acceptable risk at the level of 0.05, a period of up to 8 months is justified, in which guarantees of risk retention within acceptable limits are maintained in the selected architectural solutions characterized by the conditions of the example from Table 2.

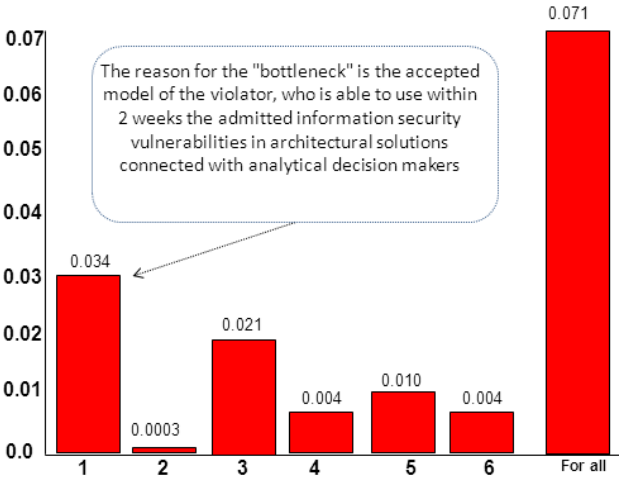

Figure 6. The probability of violating system information security requirements - $\boldsymbol{R_{sec\,i}\,(T = 1year)}$

Figure 7. Dependence $\boldsymbol{R_{sec}\,(T)}$ on the prognostic period $\boldsymbol{T}$ lasting from 6 to 24 months

The "bottleneck" is connected with element 1. The reason for the "bottleneck" is the accepted model of the violator (see Table 2, the value for β - mean activation time of threats up to violation of information security), who is able to use within 2 weeks the admitted information security vulnerabilities in architectural solutions connected with analytical decision makers.

5.4. Example 3

In continuation of Examples 1 and 2, the integral probability $\boldsymbol{R_{int}\,(T)}$ of failure to reliable perform decision management process considering system information security is calculated using the recommendations of section 4.

Considering that $\boldsymbol{R_{rel}\,(T = 1year)} = 0.028$ and $\boldsymbol{R_{sec}\,(T = 1year)} = 0.071$, by formula (1)

$$\boldsymbol{R_{int}\,(T = 1year)} = 1 - (1 - 0{,}028)\cdot(1 - 0{,}071) \approx 0{,}097.$$

For commensurate damages in resulting value of integral risk 0.097 the risk of violating system information security requirements (0.071) is 2.5 times higher than the risk of failure to reliable perform decision management process without consideration of threats to system information security. Comparing with the admissible level of 0.05, we can state that the calculated risks exceed the acceptable risk (in probability value). It means the rationale that the system decisions are not balanced and the improvement of decision management process is needed (connected with architectural and organizational decisions focused on people, process-oriented architectural decisions, architectural decisions focused on the applied technologies). And the main goal is to reduce the risk of violating information security requirements.

Thus, the examples 1-3 demonstrate the impact of information security on the performance of decision management process by risks measures.

6. Conclusion

The proposed methodological approach allows to analyze an impact of a violation of information security requirements on the performance of decision management process. It uses the measure for uncertainty conditions – the integral probability of failure to reliable perform decision management process considering system information security. Considering threats to system information security the approach use helps to confirm that the planned or applied system decisions are balanced (or not), to identify "bottlenecks" and the ways to reduce risks in decision management process, and justify conditions and period, in which guarantees of risks retention within admissible limits are maintained, taking into account the requirements for system information security.

7. References

[1] A. Kostogryzov, G.Nistratov and A.Nistratov. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management. Total Quality Management and Six Sigma, InTech, 2012: 127-196. DOI: 10.5772/46106

[2] A. Barabanov, A. Markov, V. Tsirlov. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls, Journal of Theoretical and Applied Information Technology, 2016, vol. 88, No 1, pp. 77-88

[3] M. Eid, and V. Rosato. Critical Infrastructure Disruption Scenarios Analyses via Simulation. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, 2016: 43-62.

[4] A. Markov, A. Fadin, V. Tsirlov. Multilevel Metamodel for Heuristic Search of Vulnerabilities in the Software Source Code, International Journal of Control Theory and Applications, 2016, vol. 9, No 30, pp. 313-320.

[5] Zegzhda, P., Zegzhda, D., Pavlenko, E., Dremov, A. Detecting Android application malicious behaviors based on the analysis of control flows and data flows. ACM International Conference Proceeding Series, 2017, pp. 280-286. DOI: 10.1145/3136825.3140583.

[6] V. Artemyev, Ju. Rudenko, G. Nistratov. Probabilistic modeling in system engineering. Probabilistic methods and technologies of risks prediction and rationale of preventive measures by using “smart systems”. Applications to coal branch for increasing Industrial safety of enterprises. IntechOpen, 2018: 23-51.

[7] V. Kershenbaum, L. Grigoriev, P. Kanygin, A. Nistratov. Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018: 55-79.

[8] A. Markov, A. Barabanov and V. Tsirlov. Probabilistic modeling in system engineering. Periodic Monitoring and Recovery of Resources in Information Systems. IntechOpen, 2018: Chapter 10. URL: http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

[9] I. Goncharov, N. Goncharov, S. Kochedykov and P. Parinov. Probabilistic modeling in system engineering. Probabilistic analysis of the influence of staff qualification and information-psychological conditions on the level of systems information security. IntechOpen, 2018: Chapter 11. URL: http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

[10] A. Barabanov, A. Markov, V. Tsirlov. Information Security Controls Against Cross-Site Request Forgery Attacks on Software Application of Automated Systems. Journal of Physics: Conference Series. 2018. V. 1015. P. 042034. DOI :10.1088/1742- 6596/1015/4/04203.

[11] A. Berdyugin, P. Revenkov. Approaches to measuring the risk of cyberattacks in remote banking services of Russia. 2019. Vol-2603. P. 23-38. URL: http://ceur-ws.org/Vol-2603/short2.pdf

[12] N. Korneev, V. Merkulov. Intellectual analysis and basic modeling of complex threats. 2019. Vol-2603. P. 23-38. URL: http://ceur-ws.org/Vol-2603/paper6.pdf

[13] A. Kostogryzov. Risks Prediction for Artificial Intelligence Systems Using Monitoring Data. 2019. Vol-2603. P. 29-33. URL: http://ceur-ws.org/Vol-2603/short7.pdf

[14] V. Varenitca, A. Markov, V. Savchenko. Recommended Practices for the Analysis of Web Application Vulnerabilities. 2019. Vol-2603. P. 75-78. URL: http://ceur-ws.org/Vol-2603/short16.pdf
[15] A. Kostogryzov, V. Korolev. Probabilistic methods for cognitive solving some problems of artificial intelligence systems. Probability, combinatorics and control. IntechOpen, 2020, pp. 3-34. URL: https://www.intechopen.com/books/probability-combinatorics-and-control
[16] V.A. Nadein, N.A. Makhutov, V.I. Osipov, G.I. Shmal', P.A. Truskov Hybrid modelling of offshore platforms' stress-deformed and limit states with taking into account probabilistic parameters. Probability, combinatorics and control. IntechOpen, 2020, pp. 73-116. URL: https://www.intechopen.com/books/probability-combinatorics-and-control
[17] I. Sinitsyn, A. Shalamov Probabilistic analysis, modeling and estimation in CALS technologies. Probability, combinatorics and control. IntechOpen, 2020, pp. 117-142. URL: https://www.intechopen.com/books/probability-combinatorics-and-control
[18] D. Neganov., N. Makhutov. Combined calculated, experimental and determinated and probable justification for strength of trunk oil pipelines. Probability, combinatorics and control. IntechOpen, 2020, pp. 143-164. URL: https://www.intechopen.com/books/probability-combinatorics-and-control
[19] N. Makhutov, M. Gadenin, Yu. Dragunov, S. Evropin, V. Pimenov Probability modeling taking into account nonlinear processes of a deformation and fracture for the equipment of nuclear power plants. Probability, combinatorics and control. IntechOpen, 2020, pp. 191-220. URL: https://www.intechopen.com/books/probability-combinatorics-and-control
[20] I. Goncharov, N. Goncharov, P. Parinov, S. Kochedykov, A. Dushkin Modelling the information-psychological impact in social networks. Probability, combinatorics and control. IntechOpen, 2020, pp. 293-308. URL: https://www.intechopen.com/books/probability-combinatorics-and-control