The Estimation of Probabilistic Risks for the Performance of System Human Resource Management Process

Andrey I. Kostogryzov[1], Roman Yu. Avdonin [1] and Andrey A. Nistratov [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 estimation of probabilistic risks for the performance of system human resource management process considering information security requirements is proposed. The recommended models for risks prediction are described. The use of the proposed approach helps to identify "bottlenecks", reduce risks in system human resource management process, justify conditions and period, in which guarantees of risks retention within admissible limits are maintained, taking into account the requirements for system information security. The usability of the approach is illustrated by examples.

Keywords

Analysis, system information security, model, risk, human resource management process

1. Introduction

The main goal of the human resource management process is to equip the system with the necessary specialists in a timely manner and maintain their competence at a level sufficient to ensure the required quality of the system being created and the efficiency of its operation. In the conditions of existing uncertainties, various risks can be associated with objective and subjective factors, with the uncertainty of responsibility, as well as with deliberate deviation from the established norms and rules of work. Despite many works on risk management for different application areas (see, for example, [1-21]) the problems associated with the estimation of predicted risks, taking into account the requirements for system information security, continue to be relevant. 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).

In this paper an universal approach to do the estimation of probabilistic risks for the performance of system human resource management process considering information security requirements is proposed. It includes a description of general propositions, review and recommendations for probabilistic modeling (considering [1-21]), the approach to the estimation of integral risk, examples connected with human resource management process in application to IEC 62508 "Guidance on human aspects of dependability" and interpretation comments about a calculated probabilistic risks.

2. General propositions

In general, the main output of the human resource management process are information and non-material results. The information results of management include plan for managing system human resource and personnel selection plans, personnel database, employment contracts, plans and reports on the implementation of projects. In turn, the non-material results include directly qualified and motivated personnel assigned to the relevant positions, acquired skills, publicly available knowledge, staff satisfaction with work, the level of staff turnover that meets the needs of the enterprise in employees, an acceptable socio-psychological climate at the enterprise, the required level of safety,

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: akostogr@gmail.com (A.1), ft.99@yandex.ru (A.2), andrey.nistratov@gmail.com (A.3)
ORCID: 0000-0002-0254-5202 (A.1), 0000-0002-5572-2727 (A.2), 0000-0002-0688-4156(A.3)

quality and efficiency of the system and the innovative potential of the enterprise (connected with human resource) etc.

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

To predict proper risks the approach for modeling human resource management process is proposed below.

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:

$R_{\text{human}}(T)$ – the probability of failure in reliable perform human resource management process without consideration of system information security;

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

$R_{\text{int}}(T)$ – the integral probability of failure in reliable perform human resource 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.

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, 8, 14, 16] 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 $R_{\text{human}}(T)$ 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 in the part of system human resource management process, see in [1, 3, 6, 8, 14, 16]. These models can be used for an estimation of the probabilistic risks proposed.

4. Estimation of measures

From engineering point of view the modelled system may be presented as "Black box" an as complex system composed from «Black box" elements. There may be two cases for estimating the probability of failure in "successful" operation of the j-th composing element ($j \geq 1$) during given prognostic time: the case of observed repeatability and the case of assumed repeatability of random events [1, 6, 8, 14, 16].

4.1. The observed repeatability

According to observed repeatability the inputs for the calculations of $R_{\text{human } j}(T)$ and/or $R_{\text{sec } j}(T)$ (denoted below as $R_{\text{fail } j}(T_j)$) use statistical data. Failure to perform the necessary actions of the j-th composing system is a threat of possible damage. From the point of view of the composition of actions and/or the severity of possible damage, all varieties of the actions can be divided into K groups, $K \geq 1$ (if necessary). Based on the statistical data, the probability of failure to perform the actions of the j-th composing system element for the k-th group for a given time (it also may be related to $R_{\text{human } j}(T)$ or $R_{\text{sec } j}(T)$) may be calculated by the formula

$$R_{\text{act } jk}(T_{jk}) = G_{\text{failure } jk}(T_{\boldsymbol{jk}})/G_{jk}(T_{\boldsymbol{jk}}), \quad (1)$$

where $G_{\text{failure } jk}(T_{\boldsymbol{jk}})$, $G_k(T_{\boldsymbol{jk}})$- are accordingly, the number of cases of failures when performing the necessary actions of the j-th composing system element and the total number of necessary actions from the k-th group to be performed in a given time $T_{\boldsymbol{jk}}$.

The probability $R_{\text{fail } j}(T_j)$ of failure in "successful" operation of the j-th composing system element during a given prognostic period T_j is proposed to be estimated for the option when only those cases are taken into account for which the actions were not performed properly (they are the real cause of the damage):

$$R_{\text{fail } j}(T_j) = 1 - \sum_{k=1}^{K} W_{jk}[1 - R_{fail\,jk}(T_{jk})]\, I(\alpha_k)/\sum_{k=1}^{K} W_{jk}, \quad (2)$$

where T_j is the maximum time for the j-th composing system element operation, including all particular values T_{jk} for the entire set of actions from different groups, taking into account their overlaps;

W_{jk} – is the quantity of actions for the j-th composing system element from the k-th group taken into account for multiple performances of the actions.

For the k-th group the requirement to perform the actions using the indicator function $I(\alpha_k)$ is taken into account:

$$I(\alpha) = \begin{cases} 1, & \text{if condition } \alpha \text{ is peformed,} \\ 0, & \text{if condition } \alpha \text{ isn't peformed.} \end{cases}$$

The condition α used in the indicator function is formed by the analysis of different specific conditions, proper to the j-th composing system element operation (defined in terms of system quality, safety, effectiveness etc.). It allows to take into account the consequences associated with the failure to perform the necessary actions – see (1), (2). Condition α_k means a set of conditions for all process actions, subject to quality, safety, effectiveness etc. and time constraints within the given time $T_{\boldsymbol{k}}$ for performing the necessary actions from the k-th group.

4.2. The «Black box» formalization

As modelled system (concerning a formalization of human resource management process) there are considered as «Black box" with virtual random events affecting system operation – for estimating $\boldsymbol{R_{\text{human}}}(\boldsymbol{T})$ and/or $\boldsymbol{R_{\text{sec}}}(\boldsymbol{T})$ in modelled system, presented as one element.

In general case "successful" modelled system operation is connected with counteraction against various dangerous influences on system integrity - these may be counteractions against human failures or "human factors" events in actions on time line.

There are proposed the formalization for the general technology of counteraction against various dangerous influences on system integrity. The technology is based on periodical diagnostics of system integrity, that is carried out to detect danger sources penetration into a system or consequences of negative influences (see Figure 1). The lost system integrity can be detected only as a result of diagnostics, after which the system recovery is started. Dangerous influence on system is acted step-by step: at first a danger source penetrates into the system and then after its activation begins to influence. The system integrity can't be lost before penetrated danger source is activated. A danger

for “successful” operation is considered to be realized only after a danger source has influenced on the modelled system.

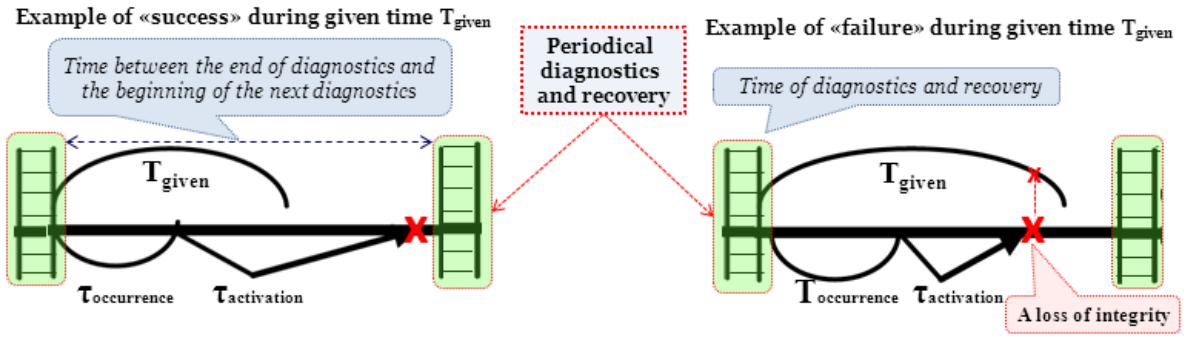

Figure 1. Some accident events in modelled system (left – correct operation, right – a lose of integrity during prognostic period T_{given})

It is supposed that used diagnostic tools allow to provide necessary integrity recovery after revealing danger sources penetration into modelled system or the consequences of influences. Using the probabilistic models (described in details in [1, 6, 8, 14, 16] the measures can be estimated in terms “success” or “failure” considering uncertainty conditions, periodical diagnostics, monitoring between diagnostics, recovery of the lost integrity for «Black box”. The next universal input data for probabilistic modeling are:

σ - frequency of the occurrences of potential threats (or mean time between the moments of the occurrences of potential threats which equals to 1/frequency);

β - mean activation time of threats;

T_{betw} - time between the end of diagnostics and the beginning of the next diagnostics;

T_{diag} - diagnostics time;

T_{recov} - recovery time

T - given prognostic period.

4.3. The formalization for complex structure

For a complex system estimation with parallel or serial structure existing models can be developed by usual methods of probability theory. For this purpose in analogy with reliability it is necessary to know a mean time between losses of integrity for each element. Let's consider the elementary structure from two independent series elements this means logic connection “AND” and for two parallel elements this means logic connection “OR”. Let’s probability distribution function (PDF) of time between losses of j-th element integrity is $B_j(t) = P(\tau_j \le t)$, and random values τ_1, τ_2 are independent, then:

1) time between losses of integrity for system combined from series connected independent elements is equal to a minimum from two times τ_j: failure of 1st or 2nd elements (i.e. the system goes into a state of lost integrity when either 1st, or 2nd element integrity will be lost). For this case the PDF of time between losses of system integrity is defined as

$$B(t) = P(\min(\tau_1,\tau_2) \le t) = 1 - P(\min(\tau_1,\tau_2) > t) = 1 - P(\tau_1 > t)P(\tau_2 > t) = 1 - [1 - B_1(t)][1 - B_2(t)]. \quad (3)$$

2) time between losses of integrity for system combined from parallel connected independent elements (hot reservation) is equal to a maximum from two times τ_j: failure of 1st or 2nd elements (i.e. the system goes into a state of lost integrity when both 1st and 2nd element integrity will be lost). For this case the PDF of time between losses of system integrity is defined as

$$B(t) = P(\max(\tau_1,\tau_2) \le t) = P(\tau_1 \le t)P(\tau_2 \le t) = B_1(t)B_2(t). \quad (4)$$

Note. The same approach is developed also by Prof. E.Ventcel in 80th and by others researchers, see [1, 3, 6, 7, 8, 16] .

Thus, an adequacy of probabilistic models is reached by the consideration of real processes of control, monitoring, element recovery for complex structure. Applying recurrently expressions (3) –

(4), it is possible to receive PDF of time between losses of integrity for any complex modelled system with series and/or parallel structure.

4.4. The integral measure

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

$$R_{\text{int}}(T) = 1 - [1 - R_{\text{human}}(T)] \cdot [1 - R_{\text{sec}}(T)]. \quad (5)$$

Here the probabilistic measure $R_{\text{human}}(T)$ is probability of failure in reliable perform human resource management process without consideration of 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 and subsections 4.1-4.3 considering the possible damage.

Note. The condition of independence between the random time before failure in performing the human resource 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 human resource management process in application to standard IEC 62508 "Guidance on human aspects of dependability".

Let some enterprise implement a set of actions for human resource management. According to the recommendations of IEC 62508, devoted to the analysis of the influence of the human factor on the system dependability, the main actions of the enterprise should be: the formation of human resources; the use of human resources; the development of human resources; the evaluation of efficiency related to human resource management.

Without going into the details of the considered aspects, the structure of actions set for receiving results of human resource management process is presented by Figure 2. For example 1 the actions set of system human resource management process is considered as complex modelled system. The approach of 4.3 is applied (because the approaches of 4.1, 4.2 are more simple, for them many aspects of system human resource management process are not considered).

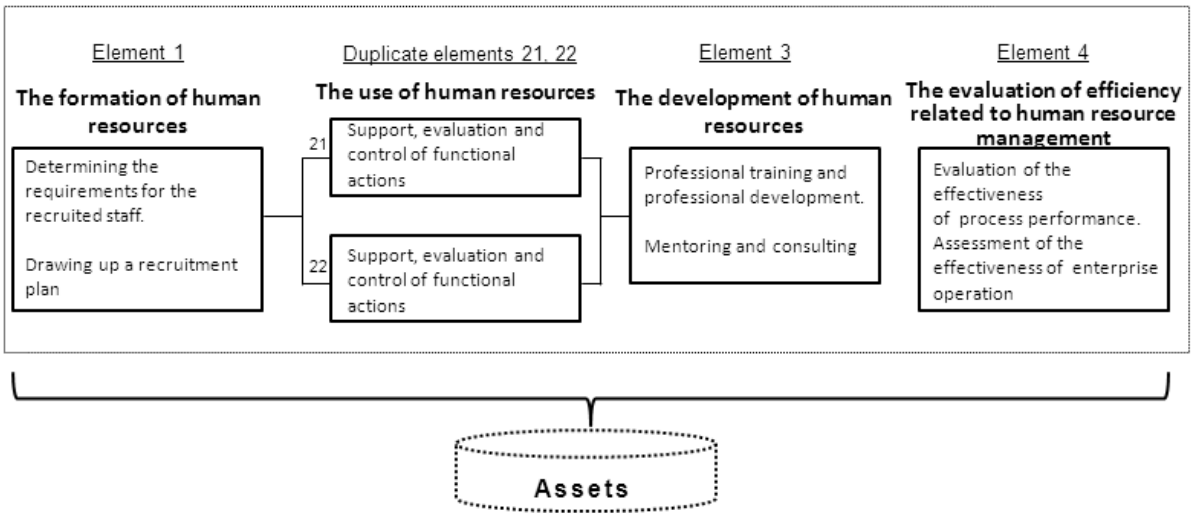

Figure 2. The formal structure of actions set for example 1

The elements of the modelled system are:

1st element (subsystem) - the actions of the formation of human resources;
2nd subsystem (elements 2.1 and 2.2) - the actions to use of human resources;
3rd element - the actions to the development of human resources;
4th element - the actions to the evaluation of efficiency related to human resource management.

Subsystem 2 is designated in the modelled system as two duplicate elements of the system - elements 21 and 22. Duplication in practice means that actions are performed by more than one performer, one of whom is a person, the functions of another performer can be performed either by another person (for example, a boss) and/or supported by a robot and/or some artificial intelligence system. From the point of view of elementary events, such interaction essentially means that actions will be performed by subsystem 2 if " OR " element 2.1 "OR" element 2.2 will be in the elementary state "The integrity of the element of the modeled system is retained".

By definition, the reliable performance of human resource management process in the modelled system is considered to be ensured during a given prognostic period, if during this period the "AND" actions of the process for the formation of human resources (according to element 1), "AND" for the use of human resources (according to element 2.1 "AND"/"OR" element 2.2), "AND" for the development of human resources (according to element 4), "AND" for the evaluation of efficiency (according to element 4) are reliably performed. The prognostic period itself for an individual element can be interpreted as referring to the stage of creation (for threats inherent in this stage), and to the stage of operation in the future (for potentially possible threats), modeling the acceptability of solutions and confirming guarantees that acceptable risks are not exceeded.

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. Many possible threats affecting the each of the structural elements of the modelled system have been identified. At the same time, not only health threats and the possibility of human errors are taken into account, but also hypothetical threats associated with the possible consequences of these errors at the stage of enterprise operation. The generated input data for modeling, which cover each of the composite elements, are presented in Table 1.

Table 1
Example 1 input for modeling complex structure (see models in [1, 6, 8, 14, 16])

Input for the model	Elements	Values and comments
σ - frequency of the occurrences of potential threats	1st element	1 time in 5 years (because of lost qualifications or knowledge for solving problems)
	Element 2.1	2 times in a year (because of insufficient qualifications or knowledge to solve problems or due to health problems of the staff)
	Element 2.2	The same as for element 2.1
	3rd element	1 time in 5 years (because of the violation of the necessary terms of professional training and advanced training)
	4th element	1 time in a year (because of the violation of the necessary deadlines or the quality of the periodic evaluation of the effectiveness of the process performance)
β - mean activation time of threats	1st element	3 months up to possible damage
	Element 2.1	2 months up to possible damage
	Element 2.2	2 months up to possible damage
	3rd element	6 months up to possible damage
	4th element	6 months up to possible damage

T_{betw} - time between the end of diagnostics and the beginning of the next diagnostics	For all elements	1 time in a week
T_{diag} - diagnostics time	1st element	1 hour - this average time is required to monitor the performance of functions related to determining the requirements for the recruited staff and drawing up plans
	Element 2.1	15 minutes (a time of medical examination before work)
	Element 2.2	The same as for element 2.1
	3rd element	8 hours
	4th element	8 hours
T_{recov} - recovery time	1st element	1 day
	Element 2.1	1 hour (this is the mean time to replace a person with a stand-in)
	Element 2.2	The same as for element 2.1
	3rd element	1 week - this is the time to correct mistakes in providing professional development, organizing mentoring and consulting staff
	4th element	3 days - this is the time to correct mistakes in ensuring a timely and qualitative estimation of the effectiveness of the process performance and the organization operation
T - given prognostic period	For all elements	From 1 to 4 years (to estimate such a period during which the guarantees of retaining risks within admissible limits are maintained)

The analysis of the calculation results showed that in probabilistic terms, the risk of failure in reliable perform human resource management process without consideration of system information security for 2 years will be about 0.02 for the entire set of actions (see Figure 2). With an increase in the prognostic period from 1 year to 4 years (see Figure 3), the risk increases from 0.043 to 0.241. For an acceptable risk at the level of 0.05, a period of up to 14 months is justified, in which guarantees are maintained that the acceptable risk is not exceeded in the conditions of the example from Table 1.

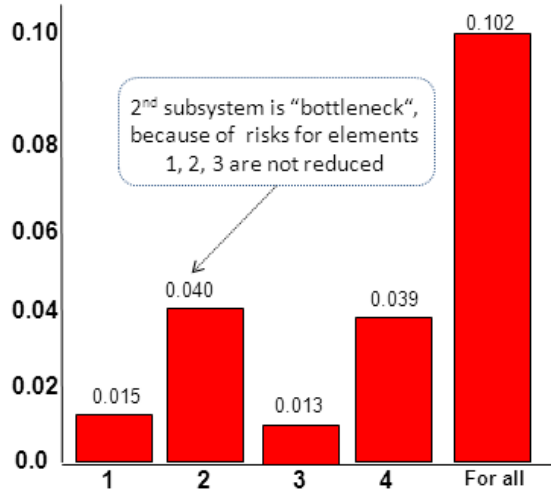

Figure 2. The probability of failure in reliable perform human resource management process during 2 years without consideration of system information security - $R_{\text{human } i}\,(T = 2 \text{ years})$

Figure 3. Dependence $R_{\text{human}}\,(T)$ on the prognostic period T lasting from 1 to 4 years

The" bottleneck", the characteristics of which it makes sense to analyze for risk reduction, is only subsystem 2 – this is a set of actions for the use of human resources related to functional support, estimation and control. The identification of this "bottleneck" forces an additional analysis to identify ways to reduce the risk. The simplest option is to combine efforts in the use of human resources. These efforts imply mutual assistance, including mutual control of activities, and from the point of view of modeling in the structure, instead of element 2.2 with characteristics identical to element 2.1, the use of element 2.2, for which the frequency of occurrence of sources of threats associated with ineffective functional support, evaluation and control of actions (σ) will not be 2 times a year (as in Table 1 for medium-qualified personnel), but 1 time every 2 years, i.e. 4 times less often. This is quite achievable due to the performance of functions by a more highly qualified human performer and/or a robot and/or with the support of some kind of artificial intelligence system. All other input for modeling are the same as shown in Table 1.

As a result of additional modeling, it was found that due to the measures taken, the risk of failure in reliable perform human resource management process without consideration of system information security was reduced to the level of 0.076 (i.e. by 34.2%) and an increase from 14 to 16 months of the period for which guarantees of non-excess of acceptable risks are retained (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 of the prepared solutions) that lead to success. The example shows only a quantitative estimation of the results of applying such measures.

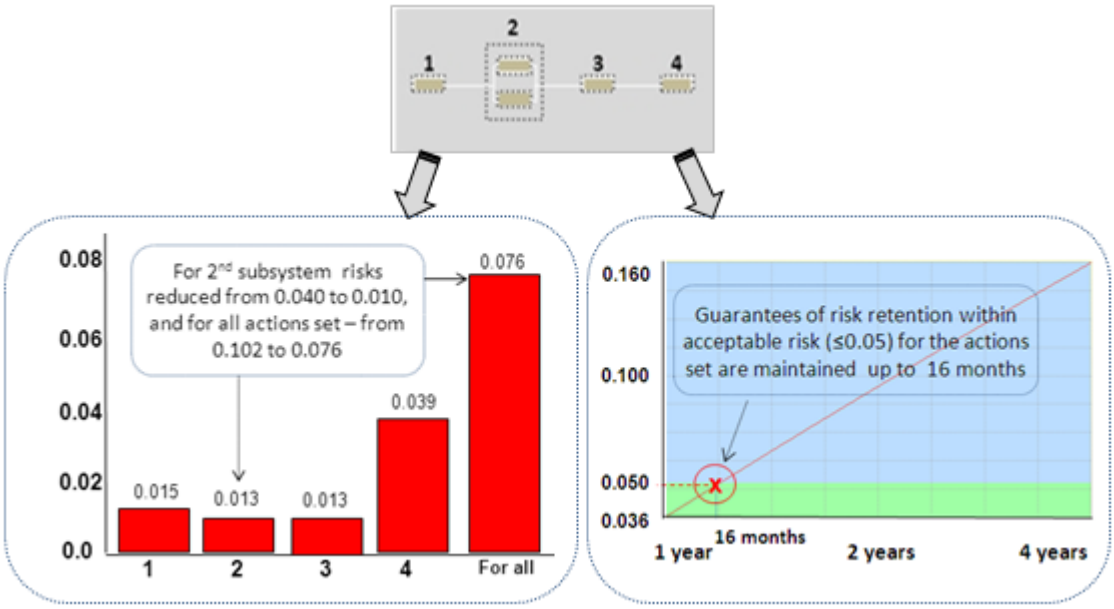

Figure 4. The risk of failure in reliable perform human resource management process (without consideration of system information security) is decreased (left), and guarantees of risk retention within admissible limits (≤0.05) are increased (right)

5.3. Example 2

Continuing Example 1, the prediction of the risk of violation of information security requirements is illustrated for a set of actions according to the recommendations of ISO/IEC 27002 (Section 8) in terms of ensuring the safety of personnel (see Figure 5). The actions set is considered as complex modelled system. Still the approach of 4.3 is applied (because the approaches of 4.1, 4.2 are more simple for modeling in the example).

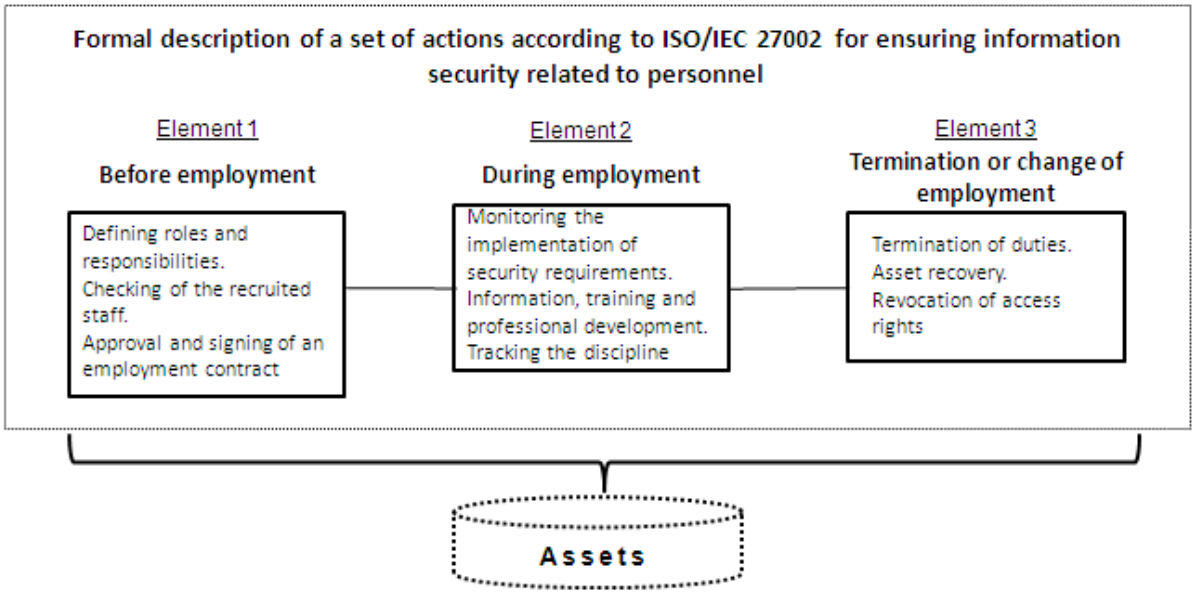

Figure 5. The formal structure of actions set for example 2

The input for each of the 3 constituent elements are presented in Table 2.

Table 2

Example 2 input for modeling complex structure by the model (see models in [1, 6, 8, 14, 16])

Input for the model	Values and comments		
	for 1st element	for 2nd element	for 3rd element
σ - frequency of the occurrences of potential threats to information security	1 time in 5 years (these are threats related to subjective factors before employment)	1 time in a year (these are threats of damage during the employment of personnel)	2 times in a year (these are threats of damage caused by previous mistakes or due to dissatisfaction of dismissed personnel)
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)	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 (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 week (this time is determined by the regulations for monitoring assets related to recruited staff)	1 hour (this time is determined by the regulations for monitoring assets related to staff)	1 hour (this time is determined by the regulations for monitoring assets related to staff)
T_{diag} - diagnostics time	30 seconds/30 seconds (automatic control information security conditions)	30 seconds/30 seconds (automatic control information security conditions)	30 seconds/30 seconds (automatic control information security conditions)
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 1 to 4 years (to estimate such a period during which the guarantees of retaining risks within admissible limits are maintained)		

Analysis of the calculation results showed that in probabilistic terms, the risk of violating the requirements for information security within two years will be about 0.130 for the entire set of actions, amounting to 0.014 for the 1st element, 0.041 for the 2nd element, 0.080 for the 3rd element ("bottleneck"). With an increase in the prognostic period from a year to 4 years, the risk increases from 0.067 to 0.243. For an acceptable risk at the level of 0.050, a period of up to 8 months is justified, in which guarantees are maintained that the acceptable risk is not exceeded in the selected set of actions characterized by the conditions of the example from Table 2.

A "bottleneck" has been identified – it is the preservation of the ability of a person who has stopped or changed his duties to use the information received (element 3). At the same time, the cause of the "bottleneck" is a violator who is able (according to the accepted information security model) to use this hypothetical vulnerability during a day - see Table 2, the value for β - mean activation time of threats up to violation of information security.

5.4. Example 3

In continuation of Examples 1 and 2, the integral probability $\boldsymbol{R_{int}}\ (\boldsymbol{T})$ of failure in reliable perform human resource management process considering system information security is calculated using the recommendations of section 4. Considering that $\boldsymbol{R_{human}}\ (\boldsymbol{T = 2\ years})$ = 0.076 and $\boldsymbol{R_{sec}}\ (\boldsymbol{T = 2\ years})$ = 0.130, by formula (5)

$$\boldsymbol{R_{int}}\ (\boldsymbol{T = 2\ years}) = 1 - (1-0.076)\cdot(1-0.130) \approx 0.196.$$

For commensurate damages in resulting value of integral risk 0.196 the risk of violating system information security requirements (0.130) is 1.7 times higher than the risk of failure to reliable perform human resource management process without consideration of 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 human resource management process is needed. And the main goal is to reduce the risk of violating information security requirements.

Thus, the examples 1-3 demonstrated a usability of the approach.

6. Conclusion

The proposed approach allows to estimate probabilistic risks for the performance of system human resource management process considering information security requirements. It uses the measure for uncertainty conditions – the integral probability of failure in reliable perform human resource management process considering system information security. Considering system information security the approach application helps to identify "bottlenecks" and the ways to reduce risks in human resource 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] Kostogryzov A., Stepanov P., Nistratov A., Nistratov G., Klimov S., Grigoriev L. (2017). The method of rational dispatching a sequence of heterogeneous repair works. Energetica. Vol.63, 4, 154-162. www.lmaleidyka.lt/ojs/index.php/energetika/index
[7] 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.
[8] 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.
[9] 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
[10] 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
[11] 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.
[12] 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
[13] 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
[14] 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
[15] 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
[16] 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
[17] 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
[18] 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
[19] 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
[20] 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

[21] 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