Methodical rationale of system solutions to reduce risks and retain them within acceptable limits for knowledge management process

Andrey Kostogryzov[1], Roman Avdonin[2], Andrey Nistratov[3]

[1]Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia, e-mail: Akostogr@gmail.com
[2]Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia, e-mail: ft.99@yandex.ru
[3]Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia, e-mail: andrey.nistratov@gmail.com

Abstract

An approach to the formalization of the standard knowledge management process is proposed, taking into account the requirements for information protection. The approach has been developed to the level of methodical approach for estimation and rationale system solutions to reduce risks and/or retain risks within acceptable limits for various threats scenarios. The use of the approach allows to estimate the impact of various threats on knowledge management process performance by probabilistic measures (including threats to the violation of information protection requirements). The usability of the proposed methodical approach is demonstrated by examples.

Keywords: analysis, engineering, information protection, knowledge, model, prediction, risk, system

1. Introduction

Modern enterprises widely use the standard system process of knowledge management (see, for example, the descriptions of the standard process in ISO/IEC/IEEE 15288 "Systems and software engineering — System life cycle processes"). This concerns to both developing and operating systems, their subsystems and processes. In particular, the enterprise may be considered as a system interested in knowledge management about itself. The purpose of the system knowledge management process is to improve the quality and/or security and/or effectiveness of the system or related systems through the acquisition, creation, distribution, timely application and storage of useful knowledge in lifecycle. In turn, the knowledge itself serves as the basis for extracting latent effects and preventing possible errors during creation, operation of systems and their decommissioning.

Note. Knowledge means the volume of comprehensions and skills that are invented by people.

In the process of knowledge management, new knowledge is created and acquired, knowledge bases and centers (KnC) are formed. This explains the importance of the problem of storing acquired knowledge in the conditions of heterogeneous threats, including threats to the information protection. There are many works on risk analysis, see for example [1-22]. In [20] a qualitative risk

assessment is carried out using a general method of analogy, the essence of which is to analyze a set of data on similar projects. In [21] risk analysis, risk factors identification and systematization are based on spatial structuring in the coordinate plane, including development trends and features of the territory, taking into account its own possibility, the ability for innovations and competent risk management. In [22] the risks identification, the definition of priority strategies for reducing risks in supply chain is carried out using the supply chain Performance Standard (SCOR), Fuzzy Failure mode and Effect analysis (Fuzzy FMEA) and Fuzzy Analytical Hierarchical Process (FAHP). 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). However despite a lot of works, the issue of risks prediction, choosing system solutions to reduce risks and retain them within acceptable limits continues to remain relevant.

In comparison with the existing approaches, the proposed approach allows to estimate the impact of various threats on the effectiveness of the knowledge management process (including threats to the violation of information protection requirements), allows us to predict risks taking into account the complexity of the modelled system and measures to counter threats in each element, determine the reliability of the process and required information protection. It is expected that the use of the proposed approach in knowledge management processes in modern KnC will help both to increase the effectiveness of the process itself, and to choose and apply the rational measures to reduce risks and/or retain risks within acceptable limits for various threats scenarios.

2. General

It is proposed the approach to assess the integral risk of violation of the knowledge management process performance, taking into account the requirements for information protection and the particular risks (concerning the actions performance and the generalized risk of unreliability of knowledge management process performance).

It is proposed to characterize particular risks by the probabilities of corresponding events (in comparison with possible consequences):

- the probability of violating the reliability of the knowledge acquisition process performance without taking into account the requirements for information protection;
- the probability of violating the reliability of creating useful knowledge without taking into account the requirements for information protection;
- the probability of violating the reliability of the distribution of acquired or created useful knowledge without taking into account the requirements for information protection.

In turn, the reliable distribution of acquired or created useful knowledge means their application in time.

The generalized risk of unreliability of the system knowledge management process performance takes into account all the listed particular risks .

Possible ways to reduce risks that can be quantitatively justified are itself the mechanisms for directly managing risks in the knowledge management process performance:

- for the risk of violating the reliability of the knowledge management process performance without taking into account the requirements for information protection, this is the fulfillment of the necessary conditions with the completion of all the actions taken by the processes of acquiring knowledge and creating useful knowledge (compliance with the delivery dates of acquired knowledge and created useful knowledge and the acceptable level of defects in them);
- the risk of violating the requirements for information protection in the process of knowledge management – this is a reduction in the frequency of occurrence of sources of threats to the violation of information protection requirements in the process of knowledge management (if possible), an increase in the time of threat development before the violation (if possible), optimization of the time

period between system diagnostics, reducing the duration of system diagnostics and system recovery time after a violation, choosing a prognostic period when effective preventive management actions are possible;

- the integral risk of the violation of the knowledge management process performance, taking into account the requirements for information protection, is a balanced action to ensure the reliability of the knowledge management process performance and information protection in the process, aimed at risks retention within acceptable limits.

The following statement are to be considered:

- analyzed objects for risks prediction in the knowledge management process performance;
- propositions on formalization;
- measures;
- the procedure for risks prediction;
- calculation methods, examples, interpretations.

3. Analyzed objects for risks prediction in the knowledge management process performance

To predict the risks it is proposed to define:

- the composition of the output results and performed actions of the knowledge management process and the assets used in this process;
- a list of potential threats and possible scenarios of the occurrence and development of threats for the output results, the actions performed by the process and the assets used in this process;
- technologies for countering threats used in the process of managing knowledge in given system application environment;
- formalized requirements or conditions for completing the necessary actions of the knowledge management process, meeting the deadlines for the delivery of knowledge, the absence of defects in the acquired and created knowledge, the distribution and application of useful knowledge.

To calculate typical risk measures, the analyzed entities are considered as a modelled system of simple or complex structure. In the models and methods of system analysis, in relation to such modelled systems, data obtained after the occurrence of events, according to the identified prerequisites for the occurrence of events, and data collected and accumulated statistics on the process and possible conditions for its implementation are used [1-8], [13-14].

Depending on the goals of risk prediction, models are presented in the form of a «Black box» or in the form of a complex structure. For separate elements of a complex system or for its rough modeling, a «Black box» models are used. To obtain more accurate results of risk prediction, a complex modelled system is decomposed to the level of composite system elements characterized by their parameters and operating conditions and combined to describe the integrity of the modelled system by the logical conditions "AND" and "OR". At the same time, the integrity of the modelled system (or system element) during specified prognostic period means such a state of this system (or system element) that during this prognostic period corresponds to the intended purpose of the applied model.

Notes

1 The logical condition " AND" for two elements connected by this condition is interpreted as follows: the modelled system of two sequentially connected elements is in a state of integrity when " AND" the first element, " AND" the second element are in a state of integrity.

2 The logical condition "OR" for two elements connected by this condition is interpreted as follows: a system of two elements connected in parallel is in a state of integrity when "OR" the first element, "OR" the second element is in a state of integrity (in particular, when the execution of separate actions is duplicated to increase reliability).

4. Proposition for formalization

To solve the problems of system analysis, a modelled system can be: a set of output results and/or assets, a set of actions of the knowledge management process, united by a purpose in the interested system.

For each of the elements of the modelled system, depending on the goals set, their own system analysis tasks can be solved. In general, the modelled system is represented as a «Black box» or as a complex system, the elements of which are combined sequentially or in parallel. At the same time, each element may be characterized by its own heterogeneous threats and the technologies used to control, monitor and recovery the violated integrity – see, for example [1-8], [13-14].

For each of the elements and for the modelled system as a whole, a space of elementary states is introduced (taking into account the logical relationships of the elements with the conditions " AND", "OR").

For example, in the application to predicting the risk of violation of information protection requirements, the space of elementary states on the time axis can be formally defined by two basic states:

- "Compliance with the requirements for information protection in the process of knowledge management is ensured", if the requirements for information protection are met during entire prognostic period, i.e. from the point of view of mathematical modeling, their non-compliance leads to damage;
- "Compliance with the requirements for information protection in the process of knowledge management is violated" - otherwise.

In the application to the prediction of the integral risk of violation of the process performance, taking into account the requirements for information protection, the space of elementary states on the time axis can be formally defined by the other two basic states:

- "The reliability of the knowledge management process performance and the fulfillment of the requirements for information protection in the system are ensured", if during entire prognostic period the reliability of performing certain actions of the process for obtaining output results and the fulfillment of certain requirements for information protection are ensured;
- "The reliability of the system knowledge management process performance and/or the fulfillment of the requirements for information protection in the system is violated" – otherwise.

In general, it is possible to expand or rename the elementary states themselves, the main thing is that they form a complete set similar to the sets presented above.

The use of the risk prediction helps to justify acceptable risks. In fact, for each analyzed object there are its own conditions of acceptability in the intended use. The priority is to choose the criterion of acceptable risk based on the precedent principle. The essence of the precedent principle is that as a norm for information protection, such a value of acceptable risk is established, which was chosen as acceptable based on the results of modeling various past events. For the specified prognostic period, the calculated risk values that are characteristic of the violations that have taken place are determined as unacceptable, and those that are smaller than those that are unacceptable are determined as acceptable (these risk values correspond to the precedent absence of violations of information protection requirements).

As measures to counter threats that can reduce the calculated risks when they are applied, more frequent (compared to the time of threat development) system diagnostics or control with the restoration of normal operation (of the system, process, system element) can act. When using the specified limits of acceptable risk, predictions for real cases of violations of the norm "before" and "after" the occurrence of violations allow (when using the quantified limits of acceptable risk) to perform an analytical rationale of proactive measures to reduce or retain risks within acceptable limits and/or reduce costs and / or possible damages under the specified restrictions. The reasoned determination of balanced system measures and actions that prevent the occurrence of damage

under restrictions on resources and acceptable risks, as well as the assessment and rationale of effective short-, medium - and long-term security plans are carried out by solving independent optimization tasks using the calculated values of the predicted risks.

5. Measures

In application to modeled system, which can be represented as a «Black box» or a complex logical structure, the next measures are proposed:

$R_{\text{gen}}(T_{\text{spec}})$ — the risk of unreliability of the knowledge management process performance during specified prognostic period T_{spec} without taking into account the requirements for information protection;

$\boldsymbol{R_{\text{sec}}(T_{spec})}$ — the risk of violating the requirements for information protection in the process of knowledge management during specified prognostic period $\boldsymbol{T_{\text{spec}}}$;

$R_{\boldsymbol{int}}(T_{spec})$ — integral risk of the violation of the knowledge management process performance, taking into account the requirements for information protection during specified prognostic period T_{spec}.

The integral risk of the violation of the knowledge management process performance depends on unreliability of the process performance or on the violation of requirements for information protection, or both, with the severity of possible consequences.

6. The procedure of risks prediction

To predict the risks, it is proposed to perform the following steps:

1) to define the modelled system and set the analyzed objects of risk prediction;

2) to set the specific goals of risk prediction;

3) to create a list of possible threats. The decision is made to represent the modelled system in the form of a «Black box» or in the form of a complex structure decomposed to composite elements. They form the space of elementary events for each element and the modelled system as a whole;

4) to select calculated measures and suitable mathematical models and methods (including methods to increase their adequacy).

7. Calculation methods, examples, interpretations

The proposed methods to rationale system solutions, to reduce risks and/or retain them within acceptable limits are presented in combination with examples and the practical interpretations of the calculation results concerning some problems of Arctic development.

To achieve the main goals in the Arctic development for the period up to 2035, numerous problems must be systematically solved in the areas of social and economic development, development of the infrastructure of the Arctic zone, development of science and technology in the economic interests, environmental safety, development of international cooperation, ensuring the protection of the population and territories of the Arctic zone from natural and man-made emergencies, ensuring information protection. The system solution of the entire set of tasks is based on knowledge management, based on the analytical processing of heterogeneous monitoring data and providing for the improvement, accumulation and timely application of emerging knowledge.

Unavoidable uncertainties in the specifics of applications for a given prognostic period are taken into account when solving practical problems using mathematical modeling, risk prediction, system analysis and optimization at various meta-levels.

Given the complexity and versatility of the practical tasks being solved for the development of

the Arctic region, the creation of one or more KnC is inevitable. In the conditions of real and potential threats to the security of critical information infrastructure, information protection in the KnC is of priority importance. Without going into the details and specifics of the heterogeneous knowledge to be integrated and applied, some practical problems to the use of this methodic approach are concerning:

- to solve the profile tasks of ensuring environmentally safe marine exploration, production and transportation of various types of minerals in extreme natural and climatic conditions (profile tasks of the 1st type);
- to solve specialized tasks of ensuring integrated safety of operations on the continental shelf, including monitoring and forecasting of extreme situations of natural and man-made nature (profile tasks of the 2nd type);
- to solve the specialized tasks of preventing and eliminating emergency oil spills in ice conditions, including the creation of technologies for detecting oil under ice (profile tasks of the 3rd type);
- to solve the profile tasks of developing technologies for integrated hydrometeorological and environmental monitoring of natural hazards in the Arctic regions (profile tasks of the 4th type);
- to solve the profile tasks of developing technologies for remote sensing of the Earth, including environmental monitoring, resource estimation and forecasting of the state of the Arctic environment (profile tasks of the 5th type).

The methodic approach is illustrated by the examples of the predictions:

- the risk of unreliability of the knowledge management process performance without taking into account the requirements for information protection;
- the risk of violating the requirements for information protection;
- the integral risk of the violation of the knowledge management process performance, taking into account the requirements for information protection.

For certainty from the point of view of system engineering for information protection, two options are considered: the creation and operation of five autonomous specialized KnC, each of which specializes in solving its own profile tasks (option 1), and the addition of a single KnC integrating the capabilities of all autonomous KnC (option 2). Taking into account possible consequences, the objectives of risk prediction are formulated as follows. In the conditions of existing uncertainty:

- to quantify the risk of unreliability of the knowledge management process performance without taking into account the requirements for information protection;
- quantify the risk of violating requirements for information protection (both piecemeal for each KnC, and for a complex of all KnC);
- identify critical conditions in the development of various threats;
- to quantify the integral risk of violating the reliability of the knowledge management process performance, taking into account the requirements for information protection;
- to determine such a period in which guarantees of non-excess of acceptable risks are maintained.

Examples 1-3 show an assessment of the risk of unreliability of the knowledge management process performance (without taking into account the requirements for information protection). Assuming the commensurability of possible consequences, the examples assess the probabilities of unreliability of acquiring and creating useful knowledge and the probability of unreliability of the distribution of acquired or created useful knowledge and their timely application.

7.1. Example 1

The example shows an assessment of the risks of unreliability of the knowledge acquisition process performance.

When assessing the risks of unreliability of the knowledge acquisition process performance, the methods of system analysis are adapted in terms of assessment:

- the risk of incomplete performance of the necessary actions for the supply of acquired knowledge;
- the risk of violation of the delivery dates of acquired knowledge;
- the risk of an unacceptable defects level in the acquired knowledge (analytical errors, descriptions, unsubstantiated conclusions and/or recommendations).

From the point of view of calculations, the models for assessing the above risks are identical, since when assessing each of the risks, the calculated probabilistic measures are compared with the possible consequences proper due to non-fulfillment of the conditions for acquiring knowledge.

The example below shows an estimation of the violation of the reliability of the timely delivery of acquired knowledge. The estimation of the incompleteness of performing the necessary actions to supply the acquired knowledge and the presence of an unacceptable defect in the acquired knowledge (analytical errors, descriptions, unsubstantiated conclusions and/or recommendations) is done by analogy.

The probability $R_{\text{td}\,i}(T_{\text{spec}\,i})$ of violation of the terms of a single delivery for knowledge of i-th type for a given time $T_{\text{spec}\,i}$ is calculated by the formula

$$R_{\text{td}\,i}(T_{\text{spec}\,i}) = N_{\text{sec}\,i}(T_{\text{spec}\,i})/N_i(T_{\text{spec}\,i}), \quad (1)$$

where $N_{\text{sec}\,i}(T_{\text{spec}\,i})$ and $N_i(T_{\text{spec}\,i})$ – accordingly, the number of violations and the total number of deliveries in a given time $T_{\text{spec}\,i}$ to the knowledge of i-th type statistics.

The delivery time fulfillment indicator for k-type knowledge is defined as follows

$$Z_{\text{term}\,i}\,(T_{\text{spec}\,i}) = \begin{cases} 0, \text{ if the conditions of delivery terms are met;} \\ R_{\text{td}\,i}(T_{\text{spec}\,i}) \text{ according to the formula (1), if the conditions are not met or not specified.} \end{cases} \quad (2)$$

The condition for fulfilling the terms of the knowledge delivery of k-th type is defined as the condition for not exceeding the maximum acceptable level $R_{\text{add.св}\,i}(T_{\text{spec}\,i})$, set for the probability of violating the terms of a single delivery. This condition is expressed in the form:
$R_{\text{td}\,i}(T_{\text{spec}\,i}) \le R_{\text{add.td}\,i}(T_{\text{spec}\,i})$. In the expression for the generalized risk the execution rate of the delivery terms for the acquisition of knowledge of i-th type $Z_{\text{term}\,i}\,(T_{\text{spec}\,i})$ is marked as $Z(\text{acq})_{\text{term}\,i}\,(T_{\text{spec}\,i})$.

The probability of violation of delivery dates for the entire set of knowledge of various types implemented in the process according to statistical data, taking into account the multiplicity of deliveries characterized by the input data for each of the types of knowledge, is calculated by the formula

$$R_{\text{td}}\,(T_{\text{spec}}) = 1 - \sum_{i=1}^{I} M_i[1 - R_{\text{td}\,i}\,(T_{\text{spec}\,i})] \Big/ \sum_{i=1}^{I} M_i; \quad (3)$$

where T_{spec} – is the specified total delivery time of the entire set of knowledge of various types, including all the particular values of $T_{\text{spec}\,i}$ taking into account their overlaps, M_i – is the number of deliveries of knowledge of the i – th type taken into account for multiple deliveries, in the expression for the generalized risk in relation to the acquisition process , the designation M(acq) i , i = 1,…,I(acq) is used.

In accordance with the tasks set for the development of the Arctic region, it is planned to acquire several types i of knowledge. The acquisition of all types of knowledge, with the exception of one, takes place without violating the delivery dates, i.e. in this case $Z_{\text{term}\,i}\,(T_{\text{spec}}) = 0$**.** Therefore, the risk assessment takes into account only the type of acquired knowledge for which the delivery dates are violated.

Taking into account the statistical data on the development of the Arctic, for certainty, it is conditionally assumed that for a given time $\boldsymbol{T_{spec\,i}}$ = 1 year for type *i* of knowledge, the total number of deliveries N_i = 100, the number of violations of delivery dates $\boldsymbol{N_{sec\,i}}$ = 3, which is 3% of the total number of deliveries, and the number of multiple deliveries M_i = 1.

The results of the estimation of the violation of the reliability process performance of creating useful knowledge are completely identical to this example.

7.2. Example 2

The example illustrates the assessment of the risks of violating the reliability process performance of distributing useful knowledge. The methods for calculations see in [13-14].

Let's assume that, taking into account statistical data, the frequency of a significant change in the usefulness of knowledge about Arctic conditions in the system's knowledge base will be no more than one change per 10 years, i.e. **ξ** = 10 years. The average time for acquiring or creating and placing new knowledge in the knowledge base of the system (from the creators or distributors of knowledge) will be about three months, i.e. $T_{\text{knowledge base}}$ = 3 months, which, translated to the same units of measurement, is 0,25 years. Updates from the KnC are delivered to the system consumers on a monthly basis, i.e. q = 1 month or 0,083 years. In addition, a restriction is imposed on the probability of violating the reliability of the distribution of useful knowledge from above: this probability should not exceed the maximum allowable level $R_{\mathbf{add.dist}}(\boldsymbol{T_{spec}})$ = 0,10.

Thus, the risk assessment for the discipline of knowledge distribution immediately after its acquisition or creation is determined by the formula

$$R_{\text{dist}} = 1 - \frac{\xi}{\xi + T\text{knowledge base}} = 1\text{-}10/(10+0{,}25) = 0{,}024. \quad (4)$$

The risk assessment for discipline periodic distribution of knowledge regardless of the dates of their acquisition or creation, i.e. regulation (confirming the usefulness of existing stored knowledge in the absence of changes) is determined by the formula

$$R_{\text{dist}} = 1 - \frac{\xi^2}{q(\xi + T\text{knowledge base})}\left[1 - \exp\left(-\frac{q}{\xi}\right)\right] =$$

$$= 1\text{-}\ 102\cdot[1\text{-}\exp(\text{-}0{,}083/10)]/0{,}083\cdot(10+0{,}25) = 0{,}060. \quad (5)$$

Since the condition of not exceeding the maximum acceptable level of $\mathrm{R_{dist}}(T_{\text{spec}}) \le \mathrm{R_{add.dist}}(T_{\text{spec}})$, is met, this indicator can be neglected in further calculations, i.e. $\mathrm{Z}_{us}\,(T_{\text{spec}}) = 0$, the conditions for the distribution of knowledge are met, see formula (6). For the period T_{spec}, for which the input data ξ, Tknowledge base, **q**, is determined, the indicator of the reliability of the distribution of useful knowledge, assuming the timeliness of their subsequent application, is defined as follows

$$Z_{us}\,(T_{\text{spec}}) = \begin{cases} 0, & \text{if the conditions for the distribution and application of knowledge are met;} \\ R_{\text{dist}}(T_{\text{spec}}) & \text{according to formulas (4) and (5), if the conditions are not met or not specified.} \end{cases} \quad (6)$$

7.3. Example 3

The example presents an assessment of the generalized risk of the unreliability of the knowledge management process performance, which is determined by the formula

$$R_{\text{spec}}\,(T_{\text{spec}}) = 1 - [1 - Z_{us}\,(T_{\text{spec}})] \cdot$$

$$\cdot\{\sum_{k=1}^{K(acq)} W(acq)_k[1 - Z(acq)_{act\,k}(T_{\text{spec}\,k})] + \sum_{k=1}^{K(creat)} W(cr)_k[1 - Z(cr)_{act\,k}(T_{\text{spec}\,k})] + \quad (7)$$

$$+ \sum_{i=1}^{I(acq)} M(acq)_i[1 - Z(acq)_{term\,i}(T_{\text{spec}\,i})] + \sum_{i=1}^{I(cr)} M(cr)_i[1 - Z(cr)_{term\,i}(T_{\text{spec}\,i})] +$$

$$+ \sum_{j=1}^{J(acq)} L(acq)_j[1 - Z(acq)_{def\,j}(T_{\text{spec}\,i}) + \sum_{j=1}^{J(cr)} L(cr)_j[1 - Z(cr)_{def\,j}(T_{\text{spec}\,i})]\}$$

$$/\,[\sum_{k=1}^{K(acq)} W(acq)_k + \sum_{i=1}^{I(acq)} M(acq)_i$$

$$+ \sum_{j=1}^{J(acq)} L(acq)_j + \sum_{k=1}^{K(cr)} W(cr)_k + \sum_{i=1}^{I(cr)} M(cr)_i + \sum_{j=1}^{J(cr)} L(cr)_j],$$

where $\boldsymbol{T}_{\text{spec}}$ – is the specified total time, including all the partial values $\boldsymbol{T}_{\text{spec}\,k}$, $\boldsymbol{T}_{\text{spec}\,i}$, $\boldsymbol{T}_{\text{spec}\,j}$

$R_{\text{spec}}(T_{\text{spec}}) = 1\text{-}[1\cdot(1\text{-}0{,}03)+1\cdot(1\text{-}0{,}03)+1\cdot(1\text{-}0{,}03)+1\cdot(1\text{-}0{,}03)+1\cdot(1\text{-}0{,}03)+1\cdot(1\text{-}0{,}03)]/(1+1+1+1+1+1) =$
$=0{,}03.$

As a calculation result, the risk of unreliability of the system knowledge management process performance in the prognostic period of 1 year will be approximately 0,03.

7.4. Example 4

The example demonstrates the prediction of the risk of violation of information protection requirements in several autonomous KnC. Elements of the modelled system are elements 1-5, formally associated with assets and output results of solving profile problems of the 1st-5th types, respectively.

By definition, the absence of violations of information protection requirements in the modelled system is considered to be ensured during a given prognostic period if there are no violations in all autonomous data centers during this period. The prognostic period itself for an separate 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).

Performing step 3 of this methodic approach (see section 6), many critical threats were identified that affect the information protection of each of the structural elements of the modelled system. Hypothetical input data for each of the five elements of the modelled system with a brief rationale in the comments are presented in Table 1.

Table 1: *Hypothetical input data for predicting the risk of violation of information protection requirements*

Input data	Element #	Values and comments
σ – the frequency of occurrence of sources of threats to the violation of information protection requirements	1	four times a year, which is commensurate with the occurrence of threats associated with subjective factors and errors of intermediate-qualified IT specialists in solving problems of ensuring environmentally safe offshore exploration, production and transportation of various types of minerals in extreme natural and climatic conditions
	2	twice a year, which is commensurate with the time of failure of software and technical equipment to ensure comprehensive safety of operations on the continental shelf, including monitoring and forecasting of extreme situations of a natural and man-made nature
	3	once a year, which is commensurate with the emergence of threats related to the causes of human errors at the decision-making levels for

		the prevention and elimination of emergency oil spills in ice conditions, including the creation of technologies for detecting oil under ice
	4	once in two years, which is comparable with the emergence of threats from the use of undeclared capabilities of the software technology integrated hydrometeorological and environmental monitoring of natural hazards in the Arctic regions
	5	once in two years, which is comparable with the emergence of threats from the use of undeclared capabilities of the software in the technologies of remote sensing, including environmental monitoring, resource estimation and forecasting of the Arctic environment
β – the average time of threat development from the moment of the occurrence of threat sources to the violation of information protection requirements	1–5	1 day (it is assumed that due to the source of threats, they are activated not immediately, but with a certain delay of at least a day) – this is the time before possible damage after the occurrence of threat signs
T_{av}– the average time between the end of the previous and the beginning of the next diagnostics of the system's capabilities to meet the requirements for information protection	1	1 hour - it is determined by the regulations for monitoring the integrity of the KnC software and assets during shift work in terms of marine exploration, production and transportation of various types of minerals in extreme natural and climatic conditions
	2	1 hour - is determined by the regulations for monitoring the integrity of software and assets when monitoring extreme situations of a natural and man-made nature
	3	2 hours - it is determined by the regulations for monitoring the integrity of the KnC software and assets during shift work in terms of preventing and eliminating emergency oil spills in ice conditions
	4	1 hour - is determined by the regulations for monitoring the integrity of the KnC software and assets during complex hydrometeorological and environmental monitoring of natural hazards in the Arctic regions
	5	8 hours - it is determined by the regulations for monitoring the integrity of the KnC software and assets during shift work in terms of remote sensing of the Earth, including environmental monitoring, resource estimation and forecasting of the state of the Arctic environment
T_{diag}– the average time for diagnosing the state of assets and the system itself	1–5	30 seconds which is commensurate with the duration of automatic integrity control of the software and assets of the KnC
T_{rec} – the average recovery time of the required norm of information protection effectiveness after detection of violations	1–5	5 minutes including rebooting the software and restoring the KnC data
T_{spec}– the specified duration of the prognostic period	1–5	From 1 month up to 2 years (to determine the period during which guarantees are maintained that the acceptable risk of violating information protection requirements will not be exceeded)

The analysis of modeling results showed that in probabilistic terms, the risk of violating the requirements for information protection during year will be about 0,222 for the entire complex of knowledge centers, see Figure 1, amounting to 0,080 for the 1st element ("bottleneck"), not exceeding 0,041 for the 2nd-4th elements, and 0,072 for the 5th element ("bottleneck"). If the duration of the

prognostic period changes from one to four months, the risk increases from 0.020 to 0.080. For an acceptable risk level of 0,050, a period of up to 2.5 months is justified, in which guarantees are maintained that the acceptable risk will not be exceeded for the entire complex of KnC, characterized by the conditions of the example from Table 1-see Figure 2.

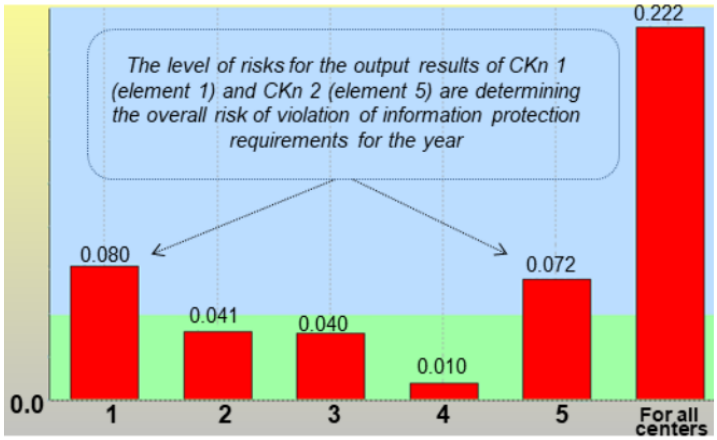

Figure 1: *Assessment of the risk of violation of information protection requirements*

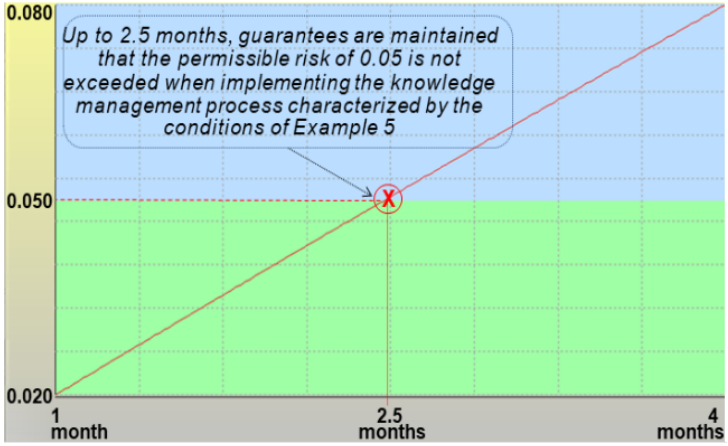

Figure 2: *Dependence of the risk for all knowledge centers on the prognostic period of one to four months*

The risk levels for threats to the output results of the KnC 1 (related to subjective factors and errors of intermediate-qualified IT specialists in solving problems of ensuring environmentally safe offshore exploration, production and transportation of various types of minerals in extreme natural and climatic conditions - element 1) and threats to the output results of the KnC 2 (related to the use of undeclared software capabilities in Earth remote sensing technologies, including environmental monitoring, resource estimation and forecasting of the state of the Arctic environment-element 5) are determining the overall risk of violating information protection requirements for the year. Moreover, the reason that element 1 is a kind of" bottleneck " in the KnC complex is the relatively high frequency of occurrence of sources of threats to commit human errors (4 times a year). And for element 5, the reason is the relatively long average time between the end of the previous one and the beginning of the next diagnostics of the system's capabilities in terms of meeting information protection requirements (after 8 hours) – see Table 1.

7.5. Example 5

The example demonstrates the prediction of the risk of violation of information protection requirements with the addition of a single KnC that integrates the capabilities of all autonomous KnC and performs the functions of a backup center for various types of failures in specialized KnC (option 2) – see Figure 5.

Figure 3: *The Dependence of risk for all KnC from the prognostic period lasting from 6 to 24 months (for case 1)*

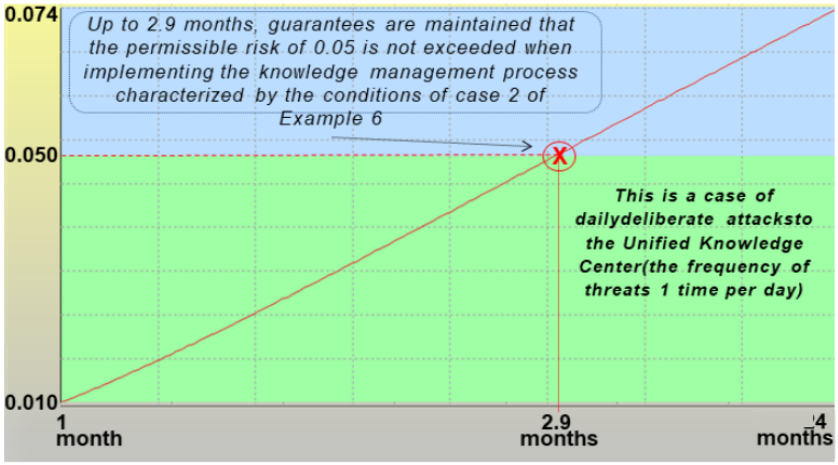

Figure 4: *Dependence of the risk for all KnC on the prognostic period lasting from 1 to 4 months (for case 2 – deliberate attacks)*

Two cases are considered:

- case 1: the frequency of occurrence of threat sources increases to 1 time per month, which is not much higher than the total frequency of occurrence of various threat sources for KnC 1 – KnC 5 according to Table 1;
- case 2: the frequency of occurrence of threat sources increases to 1 time per day, which is 30 times higher than the frequency compared to case 1 and is comparable to deliberate computer attacks on a single KnC.

For both cases, the average time between the end of the previous and the beginning of the next diagnosis of the system's capabilities to meet the requirements for information protection is 1 hour, which is typical for most specialized KnC.

The analysis of the simulation results for the complex structure shown in Figure 5 showed the following.

For case 1, in probabilistic terms, the total risk of violating information protection requirements during year will be about 0,051 for the entire complex of knowledge centers, i.e. it will decrease by more than 4 times compared to Example 4. This is achieved by reserving the operation of specialized knowledge centers with the capabilities of a single KnC. If the duration of the prognostic period changes from 6 to 24 months, the risk increases from 0,015 to 0,161. And for an acceptable risk at the level of 0,050, a period of up to 11,7 months is justified, in which guarantees are maintained that the acceptable risk is not exceeded for the entire complex of KnC characterized by the conditions of case 1 of Example 4 (see Figure 3).

For case 2, associated with daily deliberate attacks on a single KnC, the total risk of violating information protection requirements during year will be about 0,222 for the entire complex of knowledge centers, i.e. the same as for example 5 with a frequency of threat sources 30 times less. If the duration of the prognostic period changes from 1 to 4 months, the risk increases from 0,010 to 0,074. And for acceptable risk level 0,050 justified period to 2,9 months, which retain guarantee not to exceed acceptable risk to the whole complex of knowledge, characterized by the conditions of case 2 of example 4 (see Figure 4).

7.6. Example 6

Given that the prognostic period $\boldsymbol{T_{spec}}$ = 1 year, year, according to the results of calculations of examples 1–3 takes place $\boldsymbol{R_{gen}}$ ($\boldsymbol{T_{spec}}$)= 0,030, and according to the results of calculations of the 5th example (case 2-deliberate attacks on a single KnC) $\boldsymbol{R_{sec}}$ ($\boldsymbol{T_{spec}}$) = 0,051, then

$$\boldsymbol{R_{int}}\ (\boldsymbol{T_{spec}}) = 1 - (1-0{,}030)\cdot(1-0{,}051) \approx 0{,}080.$$

As a result, the integral risk of the violation of the knowledge management process performance during year, taking into account the requirements for information protection, will be 0,080. At the same time, the risk of violating the requirements for information protection (0,051) is 1,57 times less than the generalized risk of unreliability of the knowledge management process performance without taking into account the requirements for information protection.

CONCLUSION

Within the framework of the proposed methodical approach, the knowledge management process is formalized taking into account the requirements for information protection. The approach allows to estimate the impact of various threats (including threats to the violation of information protection requirements) on the effectiveness of process implementation. The measures of integral risk of the violation of knowledge management process performance, taking into account requirements for information protection, particular risks (covering knowledge acquisition, creating useful knowledge, distribution of acquired or created useful knowledge), and generalized risk taking into account all particular risks are proposed. Recommendations on methods of risk prediction are interpreted, taking into account the complexity of the modelled system and measures to counter threats in each element. The examples illustrate the proposed methodical rationale of system solutions to reduce risks and retain them within acceptable limits with a practical interpretation of the results obtained. This methodical approach is implemented on the level of national standard GOST R 59333-2021.

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] L. Grigoriev , A. Kostogryzov , V. Krylov , A. Nistratov , G. Nistratov Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V.1. P. 217–244. http://www.scirp.org/journal/ajor/

[3] A. Kostogryzov, P. Stepanov, A. Nistratov, G. Nistratov, O. Atakishchev and V. Kiselev Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling // Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186-192. www.dropbox.com/s/a4zw1yds8f4ecc5/AMSM2016%20Full%20Proceedings.pdf?dl=0

[4] 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

[5] V. Artemyev, A. Kostogryzov, J. Rudenko, O. Kurpatov, G. Nistratov, A. Nistratov Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373

[6] 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.

[7] 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

[8] A. Kostogryzov, A. Nistratov, G. Nistratov (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364. https://www.springer.com/gp/book/9783030468941

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] A. Kostogryzov, P. Kanygin, A. Nistratov. Probabilistic comparisons of systems operation quality for uncertainty conditions. RTA&A No1(56), 2020, 15:63-73 http://www.gnedenko.net/RTA/

[15] 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

[16] 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

[17] D. Neganov., N. Makhutov. Combined calculated, experimental and determinated and probable rationale 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

[18] 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

[19] 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

[20] V. Borcovskaya and D. Passmore Risk Reduction Strategy and Risk Management on The Basis of Quality Assessments, 2020 IOP Conf. Ser.: Mater. Sci. Eng. 869 062051

[21] E. P. Voronina Comprehensive socio-economic development of Arctic territories of the Russian Federation: case of risks in the coordinate plane. 2021 IOP Conf. Ser.: Earth Environ. Sci. 625 012012

[22] M. Ulfah, F. Arina and C. Lutfiah Analysis and strategy of supply chain risk mitigation using fuzzy failure mode and effect analysis (fuzzy fmea) and fuzzy analytical hierarchy process (fuzzy ahp) Dyah Lintang Trenggonowati, 2020 IOP Conf. Ser.: Mater. Sci. Eng. 909 012085.