Development of advanced mathematical predictive models for assessing damage avoided accidents on potentially-dangerous sea-based energy facility

Aleksandr Tumanov¹, Vasily Gumenyuk¹ and Vladimir Tumanov¹

¹ Peter the Great St.Petersburg Polytechnic University, Polytechnicheskaya, 29, St. Petersburg, 195251, Russia

E-mail: toumanov@mail.ru

Abstract. The article is devoted to the development of mathematical model for assessing the harm accidents on potentially-dangerous sea-based energy object. Made choice of regression mathematical model that best represents the relationship of the integral indicator with a set of risk factors of emergency situations their probabilities. Shows the main parameters of the model and result indicators. A mathematical model in which risk assessment in addition to the probability of the adverse events, risk factors and possible consequences taken into account the vulnerability of the object.

1. Introduction

Issues of theory of safety in emergency situations and quantitative risk assessment research devoted to the study of many leading Russian and foreign scientists, however, as shown by the analysis of the research and practice in the field security, the scientific basis of risk assessment are not sufficiently developed. So, remain little developed models of risk assessment of emergency situations on potentially hazardous installations energy.

In the case of potentially dangerous sea-based energy projects (hereinafter referred to as the SBEP) is available at the same time complicated system of risk factors (RF) emergency situations (ES), because security concerns SBEP overlap set of security problems in maritime transport and the problems of nuclear and radiation safety, for example in the case of floating nuclear thermal power stations (hereinafter referred to as the FNTPS) and floating energy blocks (FEB).

Thus, the object of research are floating nuclear power plants as potentially dangerous objects sea-based energy. The purpose of the study is to develop a mathematical model to assess damage in emergency situations of natural and technogenic character on potentially dangerous sea-based energy object.

Objectives of research:
1. analysis of the existing views on the damage in emergency situations of natural and technogenic character on SBEP and mathematical models of the effects.
2. Development of a conceptual and verbal models of damage at SBEP.
3. Development of a mathematical model of damage on SBEP vulnerability of sensitive object to affecting factors.

Tasks required: thorough research in order to identify the main RF and their manifestation probabilities affecting the result indicator; determination of model parameters evaluation of damage;
selection of the type of regression (mathematical models) that best reflects the relationship of integral indicator with a set of factors and their probabilities [1-5].

Our era according to several authors has acquired a special quality, which may be awarded with such disastrous thing about epithet. Emergencies became commonplace. It appears that you must correct inaccurate beliefs about how to define and evaluate the incurred as a result of natural phenomena and technogenic accidents and losses and loss fill the gap in knowledge of the part of the various professionals, students and graduate students who are interested in the technical and economic assessment of the impacts of disasters. In preventing and mitigating the effects of emergencies in natural and man-made area of focus should be done on forecasting and prevention of disasters and catastrophes, as forecast and warning, from an economic point of view, cost tens, and sometimes hundreds of times cheaper than cure has already occurred. But the scale of these works in the country, in our view, is not yet commensurate with their value. Here a broad interdisciplinary approach and much more active involvement of the Academy of Sciences [11]. Therefore, in [6], special attention is paid to the methodology of techno-economic evaluation of the direct and indirect consequences of emergency situations that previously, either purposefully ignored or taken into account. The transition of the technical system in emergency operation in accordance with federal law No. 116 commonly referred to as incident. The consequences of these incidents with the technical systems can be of varying severity, defined by the amount of material damage, the number of dead, injured and sick people, the area surrounding Wednesday's defeat.

While the scale of the potential damage is closely related to the type of technological system [20]: technical systems serial, series and mass production with a single value $10^4$-$10^6$ rub. (automobiles, agricultural machines, machines, installations, etc.);

unique technical system unit and small batch production with a single value of order $10^7$—$10^{10}$ rub. (powerful power plants, nuclear reactors, chemical and metallurgical installations, aircraft, mining complexes, oil and gas pipelines, ships, floating drilling rigs and units, etc.)

For the technical systems of the first kind are widely used traditional methods of design and operation, a large amount of repair and reconstruction works, the relatively small losses (1000-100000 rub.) upon refusal of single copies.

For the technical systems of the second kind is characterized by the lack of experience of the earlier operation, a large amount of design development, test bench and great material losses from the failures and accidents, as well as the significant potential environmental damage.

Considered primarily technological hazards and risks associated with the technical systems of the second kind. It is interesting to note that the data available on the actual frequency of major accidents on the technical facilities of the second kind significantly exceeds the calculated values obtained by methods of the theory of security technical systems. For example, the actual probability of severe accidents in nuclear power plant reactor core damage is 0.005, instead of the required values $10^{-6}$—$10^{-7}$. The rocket and spacecraft, the actual probability of accidents involving failed launches, is $(3-7)\cdot10^{-2}$, far exceeds the required amount.

The study authors SBEP — FNTPS, includes FEB «Mikhail Lomonosov» and a complex of hydraulic installations, refers to the complex technical systems of the second kind. FNTPS — super energy-saturated object that is in the sea, costing more than $20\cdot10^9$ rub.

The potential energy of water accumulation leads to transition it into kinetic energy. Tsunami, leading to an increased risk for non-self-propelled ship hydrodynamic, nuclear reactor and waterworks. Generation and transmission processes of thermal and electrical energy leads to increased risks of explosions, fires, electric shock electromagnetic lesions.

2. Methods of determining possible damage potential
At the present time to determine possible damage potential, different methods are used. Among them are the following [12]:

- field experiment;
- methods of mathematical modeling;
The advantage of full-scale experiment is high reliability of the results of the experiment, as well as real-time and real-life systems explore the task. The drawback is the complexity and high cost of the pilot studies, as required to implement several dozen identical experiments. Thus, use of this method for ПАТЭС, as a unique object worth twenty billion rubles, is quite problematic.

Methods of mathematical modeling are among the most common in the modeling and analysis of damage when ЧС. Under the mathematical modeling will understand the process of establishing the conformity of the actual object some together characters, formulae, inequalities, restrictions, logical conditions ratios and algebraic expressions, called mathematical model and study of this model, which allows you to obtain the characteristics under consideration of the real object as dependencies and numerical results. Expert techniques applied in the theory of security in emergency situations, can be divided into two directions [12]:
- the methods of the first directions were intended to create a database through the expert survey specialists in disaster risk assessment SBEP;
- the second track of the methods involve the use of materials databases for the formation of expert system knowledge bases.

As a general rule, expert methods are used as the basis for methods of mathematical modeling.

3. Develop a preliminary model
A necessary step before creating a mathematical model is a description of the properties and characteristics of the original object in a natural language [12]. Build a provisional emergency damage assessment model, which includes:
- General conceptual model, clearly showing the basic processes and concepts of emergency situations on SBEP;
- the model of allocation of costs and avoided damages in the lifecycle of a ES;
- the classification of domestic and foreign causes of emergency situations on SBEP.

The overall conceptual model of emergency situations on SBEP is the basis for the development of advanced mathematical models of risk assessment on SBEP, bearing in mind the vulnerability and life cycles of the object itself, and the life cycle of the emergence and development of emergency situations. As can be seen from the model for reliable assessment of damage from the disaster, as one of the main elements of risk, it is necessary to consider both the deterministic and probabilistic model items, such as:
- sources of danger;
- factors affecting;
- ways and means of protection from damaging factors;
- effects of object and its components;
- damage.

In addition there is a need to clarify the introduction of model and taking into account the life cycle of the object life cycle SBEP ES [15]. Development of model of distribution costs and avoided damages in the life cycle of emergency situations is an important step in creating risk assessment. In Figure 1 presented the concept, showing the balance of costs and effects on crisis prevention in various stages of ES.
Figure 1. Model of allocation of costs and avoided damages in the life cycle of an emergency

It is shown that each step corresponds to the actual damage, the predicted prevented damage (effect), the cost of warning of emergencies. A hypothesis is advanced that there are regularities and interdependencies between the magnitude of the predicted prevented damage and the significant expenditure on the prevention of SBEP ES.

It is assumed that at each stage it is necessary to invest the minimum necessary funds in preventive measures to protect facilities, equipment and personnel, so that the risk of ES does not exceed the threshold values of acceptable risk.

The presence of a qualitative pre-model is an initial prerequisite for the development of an adequate mathematical model. Below is the progress of the study on the formation of the main parameters of the mathematical model of ES risk assessment, taking into account the analysis of existing models of risk assessment.

4. Accounting for vulnerability in the mathematical model of risk assessment

A formula was proposed in [13] in which, in order to assess the risk, in addition to the probability of implementing a negative event and possible consequences, the vulnerability of the object was taken into account. According to F. Ragozin, the risk model for risky processes is based on the assumption that over a certain period of time the average risk caused by negative event A can be determined from the expression

\[ R(A) = P(A)W(A) \]  \hspace{1cm} (1)

where \( R(A) \) – is the risk caused by the negative event \( A \); \( P(A) \) – is the probability (frequency) of event \( A \); \( W(A) \) – possible one-time damage caused by an event \( A \).

The size of the damage, or cost, in each case depends, on the one hand, on the intensity of the negative event (the volume and speed of movement of masses of rocks, snow, water, areas of the affected area, etc.), and on the other hand, from the vulnerability of the object.
The vulnerability of an object is understood as the level of possible losses of an object or its individual elements (people, buildings, roads, lands, etc.), caused by the impact of certain factors of intensity on it. As an indicator of this property of the object, it is proposed to apply the degree of vulnerability, is the ratio of the affected (destroyed) objects (elements) to their total number in the affected area, which is fixed for an event of a certain intensity. The degree of vulnerability of one and the same object can differ significantly in the events of different energy class.

Analyzing the structure of SBEP ES, objects that are subject to protection, as well as classified sources of threats, vulnerability of the system and the threat itself, it is possible to identify potential threats for a particular facility. In general, on the basis of analysis, the following types of vulnerabilities of complex socio-technical systems can be identified [17]:

I. Objective – depending on the features of the construction and technical characteristics of the equipment used. Complete elimination of these vulnerabilities is impossible, they can be significantly weakened by technical and engineering methods (for example, building the structure of systems, increasing the durability of components). These include:

1. Defined by the features of the protected technical system:
   - location of system elements (presence of remote and mobile elements of the system);
   - organization of channels for the transfer of control (diagnostic) information (wired or radio channels, information networks).

2. Determined by the characteristics of the elements of the systems, or sensitivity to the effects:
   - electromagnetic field;
   - radiation;
   - aggressive environments;
   - shock waves and debris;
   - high temperature.

3. Radiation related to technical facilities:
   - electromagnetic (spurious emissions of elements of technical means, cable lines of technical equipment, amplifiers);
   - electric (focusing of electromagnetic emissions on the line and wiring, leakage of signals in the power supply network, in the ground circuit, uneven consumption of the power supply).

II. Subjective – depending on the actions of personnel, can be eliminated by organizational and software-hardware methods:

1. Errors:
   - when preparing and using the software (when developing the algorithm, installing and downloading software, operating the software, entering data);
   - at management of systems (the organization of management by streams of an exchange of the information);
   - when using technical means (when switching on / off the technical means, using the means of information exchange).

2. Violations:
   - mode of access to technical facilities;
   - mode of operation of technical facilities (energy supply, life support);
   - mode of use of information (processing and exchange of information, storage destruction of media).

III. Random - depending on the characteristics of the environment and unforeseen circumstances.

1. Failures and failures:
   - aging, failures and malfunctions of technical means;
   - aging and demagnetization of storage media (floppy disks and removable media, hard disks), microcircuits, cables and trunks;
   - software failures (operating systems, application, service, antivirus programs);
   - power failure.

2. Damage:
   - elements of the object and its components;
life-supporting communications (electricity, heat, ventilation and air conditioning); encircling structures (external fences of territories, walls and ceilings of buildings, buildings with technological equipment).

5. Accounting for security in a mathematical model of risk assessment

It is proposed in [1, 2] that in the problems of ensuring the safety of technical systems $S(\tau)$ and security $Z(\tau)$, the basic parameters of risk $R(\tau)$ are defined as a function $F[(P(\tau), U(\tau))]$, reflecting the behavior of the elements of systems (first of all, materials and subsystems), should be analyzed for such components of complex safety, as a mechanical $S_M$, chemical $S_X$, fire explosive $S_p$, electromagnetic $S_e$, radiation $S_r$. These types of security are identified through the risks of $R$ and their constituents: $R_M$, $R_e$, $R_p$. In all cases of assessing safety $S$ and risks $R$, it is essential to determine the likelihood of occurrence $P(\tau)$ and development of dangerous situations in time $\tau$.

Solving the problems of security and risk should be based on solving the problems of survivability, reliability, resource and strength (resistance to impacts). At the same time risk indicators can be considered as integral indicators of security determined by indicators of survivability, reliability, resource and strength (durability) of the system under consideration.

Formal approaches to solving the problem of assessing security due to the difficulties associated with formalization have not received wide practical dissemination. Significantly more effective is the use of informal classification approaches. Instead of valuation, categorization is used: threats; objects of protection; means of protection (in terms of functionality and guaranteed capabilities), etc. This approach does not give exact values of the security indicators, but it can allow to classify the ITS in terms of the level of security and compare them among themselves.

The greatest threat to SBEP in the case of man-made and natural disasters is the impact of damaging factors. When determining the parameters of the damaging factors, one should take into account the possibility of a joint effect of the damaging factors from various sources on the elements of the object. Realization of threats leads to damage or destruction (partial or complete) SBEP.

6. Degree of vulnerability in assessment

The degree of vulnerability that can be decomposed in before the lesions from total losses in the affected area. The damage in formulas is related to the degree of vulnerability

$$W(A) = C_y(A)W_p(A)$$

where $C_y(A)$ – the degree of vulnerability as a result of the implementation of event A; $W_p(A)$ – conditional full damage as a result of the realization of event A, equal to the number of people or the value of all objects (elements) in the affected area. The degree of vulnerability is determined separately for each dangerous natural process or anthropogenic object by means of empirical dependencies of losses in the social, economic or environmental spheres from the intensity of these processes obtained from the statistical processing of actual data or from mathematical modeling of negative events.

For potentially dangerous objects, a simplified, deterministic analysis of the risk of natural and man-made emergencies is performed with the introduction of the following basic assumption [18]: the exhaustion of the design allowable resource of an $\tau_p$ object, determining the degree of accumulated damage $D$ or vulnerability $C_y$, with the passage of time $\tau$ occurs according to a linear law:

$$D = K_D \tau_p$$

gде $K_D$ – coefficient of gravity of a given degree of damage.

At the same time, the permissible design resource $\tau_p$ is determined through the time $\tau_{op}$ to reach the dangerous (limiting) state and the resource margin $n_r$.
The reserve size $n_t$ is taken within 2 ... 10, the minimum values $n_t = 2 ... 3$ are chosen for potentially dangerous objects for which the reduction in their weight (rocket and aircraft facilities) is of great importance, and the maximum values of $n_t$ are for high-risk objects for example, nuclear power facilities, defense facilities, unique hydraulic structures.

At each time interval $\tau$, measured in years, the conditional probability of reaching the limit state will be

$$P_y = \frac{\tau}{\tau_p n_\tau},$$

where the denominator determines the increment of the conditions for the probability of reaching a dangerous state in a year. Damage $U$ for the most severe accidents and disasters can also be considered linearly dependent on the degree of depletion of the resource. Then for time $\tau$

$$U = \frac{\tau \cdot K_U \cdot Z_i}{\tau_p n_\tau},$$

where $Z_i$ – total costs for the creation of the analyzed object (initial investment); $K_U$ – coefficient taking into account the severity of the consequences of an accident or a catastrophe ($1 \leq K_U \leq 20$), the more its value, the heavier the consequences. The value of $K_U$ in the first approximation can be chosen proceeding from the potential danger of objects. For infrastructure objects, $K_U = 2 ... 6$.

Given the degree of vulnerability of the object, formula (2) for risk assessment becomes

$$R(A) = P(A)C_y(A)W_p(A)$$

where $R(A)$ is the risk caused by the negative event $A$; $P(A)$ is the probability of the event $A$; $C_y(A)$ - the degree of vulnerability as a result of the implementation of event $A$; $W_p(A)$ - conditional full damage as a result of the realization of the event $A$.

Formula (3) is common to all types of risk. However, for its practical use in each specific case, it may be necessary to introduce appropriate refinements. Thus, we replace $W_p(A)$ by $U$ and write formula (3) in a modified form:

$$R(A) = P(A) \cdot C_y(A) \cdot \frac{\tau \cdot K_U \cdot Z}{\tau_p n_\tau}$$

or

$$R(A) = P(A) \cdot C_y(A) \cdot P_y \cdot K_U \cdot Z$$

where $R(A)$ – риск, вызванный негативным событием $A$; $P(A)$ – is the probability of the event $A$; $C_y(A)$ – the degree of vulnerability as a result of the implementation of event $A$; $P_y$ – conditional probability of reaching the limiting state of the system; $Z$ – total costs for the creation of the analyzed object; $K_U$ – is a coefficient that takes into account the severity of the consequences of an accident or disaster ($1 \leq K_U \leq 20$).

Linking the probability of an unfavorable event with the initial total costs of creating the analyzed object and the time when it reached the dangerous (limiting) state and the reserve for the resource $n_\tau$, an analytical formula for risk assessment was obtained.

7. Vulnerability Matrix

Parameters for substitution in the formula (4) are entered in the vulnerability matrix, the components of which are the probabilities of realizing the possible damaged states of the object, subject to rendering to the object, various extreme effects.

In modern practice, a model is widely used to formalize the risk $R$, which connects the probability of occurrence of negative events $P_i$ (accidents, catastrophes), the likelihood of possible losses $W_i$, the magnitude of the losses $W_i$ as a result of these events:
\[ R = \sum_{i}^{n} P_i \cdot P(W_i) \cdot W_i \]  

(5)

Risk assessment should include the development of adverse events in different scenarios, which requires a generalization of the formula (5):

\[ R = \sum_{ij}^{n} P_{ij} \cdot P(W_{ij}) \cdot W_{ij} \]  

(6)

where the index \( i \) refers to the event, the index \( j \) to the corresponding scenario.

Table 1 shows the elements of the vulnerability matrix.

| Final state | \( C_1 \) | \( C_2 \) | \( C_i \) |
|-------------|-----------|-----------|-----------|
| 1           | \( P_{11} \) | \( P_{12} \) | \( P_{1i} \) |
| 2           | \( P_{21} \) | \( P_{22} \) | \( P_{2i} \) |
| \( j \)     | \( P_{ji} \) | \( P_{j2} \) | \( P_{ji} \) |

8. The method of arbitration pricing

A well-known researcher of financial risk, Stephen Ross, proposed a method called the theory of arbitration pricing (TAP). The method of arbitration pricing assumes that the relationship between risk and damage is multifactorial and this is the main theoretical advantage of this method. Also in the TAP method, a mathematical model is used, which is based on the equation of multiple linear regression.

Unlike the valuation model of U. Sharpe's capital assets, where only one factor is used (fluctuations in the yield of the market portfolio) to determine the future yield of a security, the Ross model uses a variety of factors. The general formula of the arbitrage pricing model is the following [14]:

\[ r = r_0 + \beta_1 r_1 + \beta_2 r_2 + \beta_n r_n + \xi \]  

where:

\( r \) – expected yield of securities;

\( r_0 \) – profitability of a risk-free asset;

\( r_1 \ldots r_n \) – premium (loss) for risk;

\( \beta_1 \ldots \beta_n \) is the sensitivity of the expected stock return on the risk factor change.

A common risk equation linking risk factors to their expected return [14]:

\[ r = \sum_{i=1}^{n} \beta_i FP_i + \sum_{j=1}^{m} \gamma_j MA_j + \sum_{p=1}^{k} \tau_p MFI_p + \sum_{l=1}^{r} \alpha_l V_l + \xi \]  

where:

\( FP \) – the head of financial indicators of the company;

\( MA \) – a vector of macroeconomic indicators of the country;

\( MFI \) – a vector of currency quotations;

\( V \) – vector of currency quotations;

\( \alpha, \beta, \gamma, \tau \) – vectors of sensitivity coefficients;

\( \xi \) – the error vector.

It is assumed that for this method, it is most often possible to use factors such as inflation, changes in output, changes in the structure of interest rates, etc.

In the appendix to assessing the risk of emergencies, the concept of the TAP method nevertheless has a number of shortcoming{s, the most serious of which is that the list of risk factors is not justified within the TAP.
9. Risk factors for emergencies
To fill this gap, we will use the classification and list of risk factors proposed in SBEP - floating nuclear thermal power plants (hereinafter - FNTPP) in [15].

Internal hazards for FNTPP facilities are triggered by hazardous processes, the impact of which is determined by the following:
- mass and composition of chemical and radiation hazardous substances on the site (stored or transported);
- the amount of energy used at the facility;
- the level of personnel training for the implementation of tasks to prevent and eliminate emergencies.

To understand and further develop the parameters of the mathematical model for assessing the risk of emergencies on the SBEP, we present the main risk factors used in the creation of the pre-model.

10. Theoretical linear equation of multiple regression
It is known that the multiple regression equation can be represented as:

$$ Y = f(\beta, X) + \varepsilon $$

where
- $X = (X_1, X_2, ..., X_m)$ – vector of independent (explanatory) variables;
- $\beta$ – vector of parameters (to be determined);
- $\varepsilon$ – random error (deviation);
- $Y$ is a dependent (explained) variable.

The theoretical linear multiple regression equation has the form:

$$ Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + ... + \beta_m X_m + \varepsilon $$

$\beta_0$ – a free term that determines the value of $Y$, in the case when all the explanatory variables $X_j$ are 0.

11. Description of the proposed model
Using the theoretical equation of linear regression, for potentially dangerous objects it is possible to convert the Ross formula to the following form:

$$ R(A) = \beta_0 r_0 + \beta_1 r_1 + \beta_2 r_2 + \varepsilon \quad (7) $$

where:
- $r_1$ – risk adjustment taking into account internal risk factors;
- $r_2$ – correction for risk taking into account external risk factors;
- $\varepsilon$ – random measurement error.

Considering the formulas (4,5,6), we write $r_1$ and $r_2$ in the form:

$$ r_1 = \sum_{f}^N P(A) P(F_f) P(W_f) C_y(A) W_p(F_f) $$

$$ r_2 = \sum_{l}^K P(A) P(F_l) P(W_l) C_y(A) W_p(F_l) $$

Substituting $r_1$ and $r_2$ in (7), we obtain the following expression

$$ R(A) = r_0 + \sum_{f}^N P(A) \cdot P(F_f) \cdot P(W_f) \cdot C_y(A) \cdot W_p(F_f) + \sum_{l}^K P(A) \cdot P(F_l) \cdot P(W_l) \cdot C_y(A) \cdot W_p(F_l) + \varepsilon \quad (8) $$

where:
- $R(A)$ – the integral indicator of the generalized risk of emergencies caused by a negative event A, taking into account internal and external causes, total damage and vulnerability of the object;
- $C_y(A)$ – the degree of vulnerability of the object or its components as a result of the implementation of event A;
- $r_0$ – the expected initial risk of SBEP, even if all security measures are carried out.
- $P(A)$ – the a priori probability of occurrence of an adverse event A (for example, an accident at an SBEP);
\( P(F_f) \) – the probability that an adverse event (failure, incident, accident) will occur due to a specific cause (internal factor) \( F_f \), where \( f \) is the number of factors from 1 to \( N \). Further, the probability of an internal risk factor;

\( P(F_l) \) – the probability that an adverse event (failure, incident, accident) will occur due to a specific cause (external risk factor) \( F_l \), where \( l \) is the number of factors from 1 to \( K \). Further, the probability of an external risk factor;

\( P(W_f) \) – the probability of damage from \( f \) of that internal risk factor;

\( P(W_l) \) – the probability of damage from \( l \) of that external risk factor;

\( \varepsilon \) - random error of risk assessment;

\( W_p(F_f) \) – damage from \( f \) of that internal risk factor;

\( W_p(F_l) \) – the damage from \( l \) of that external risk factor.

Denote \( W_p(A) \) - conditional total damage as a result of the implementation of event \( A \), rub. Using the risk classification of SBEP it can be seen that it is equal to the sum of total conditional losses from internal and external causes:

\[
W_p(A) = \sum_{f}^{N} W_p(F_f) + \sum_{l}^{K} W_p(F_l)
\]

The damage that we assess can be actual and predictable. Actual damage is determined when event \( A \) has already occurred. It is more interesting from the standpoint of prevention of emergencies to be able to assess the projected damage, which as a result of the activities carried out can be presented as prevented damage. As an assumption, we assume that the effect of pre-existing emergency risk reduction activities is equal to the amount of damage prevented by these activities. We write \( E_u = W_p(A) = U_p \). The creation of an object, its operation takes place over a certain time, which can be calculated over the years. Without certain transformations, it is impossible to compare investments in an object, the costs of ensuring safety and damage from accidents. To correctly compare the elements of investment and current costs with the effects of measures to prevent accidents, mathematical methods of discounting cash flows within the framework of the theory of the time value of money are used. To estimate the net prevented damage \( (NPU) \) can be in the form of the difference between the costs of preventing accidents and the amount of effects from the actual measures taken to prevent accidents by formulas, taking into account the discounting of cash flows, presented in [19]. The authors of the work put forward a hypothesis about the existence of a relationship between the capital (investment) \( Z_k \) and the current costs \( Z_t \) to ensure the safety of the SBEP and prevented damage.

\[
NPU = -Z_t + \sum_{t}^{T} \frac{(U_p - Z_t)}{(1 + k)^t}
\]

12. Model verification
In order to confirm the correctness of the proposed hypotheses, the proposed mathematical model of ES risk assessment for SBEP for adequacy is checked according to existing regularities. The audit was carried out in a retrospective way by the example of a comparative assessment of the actual and forecasted prevented damage to the accident at the Sayano-Shushenskaya SBEP.

13. Conclusion
Thus, in the course of the study, a multifactorial stochastic regression mathematical model for estimating the generalized risk of ES SBEP, \( R(A) \), caused by negative event \( A \), taking into account the probabilities, internal and external causes of emergencies, predicted total damage and vulnerability of the risk object, initial costs to create an object. The proposed model serves as a basis for the development of a methodology for assessing the risk of emergencies at the SBEP. The next step to improve the ES risk assessment will be the computational experiment and the run of the proposed mathematical model of the ES emergency risk assessment using a computer and the definition of thresholds for acceptable damage to emergencies, and the development
of proposals for methodological recommendations on SBEP ES risk reduction activities that are based on the management of the baseline the vulnerability parameter in order to minimize the risk. If, after undertaking risk reduction activities by eliminating a number of causes and sources, the generalized risk indicators become below the established empirically acceptable risk thresholds \( R_{op} \) or the risk values before they occur, then it is considered that the measures taken are effective.

Acknowledgement Work is performed within the framework of the State job (project 13.8874.2017/8.9)

Reference

[1] Gumenyuk V, Karmishin A and Kireev V 2013 *Nauchno-tekhnicheskie vedomosti SPbGPU* 2(171) pp 281-288
[2] Gumenyuk V, Karmishin A, Kireev V, Karmishin A and Reznichak V 2013 *Bezopasnost’ v tekhnosfere* 6 pp 38-45
[3] Gumenyuk V, Tumanov A and Shegeda N 2016 *Nedelya nauki SPbPU: Materialy nauchnogo foruma s mezhdunarodnym uchastiem. Luchshe doklady* (Saint-Peterburg: Izd-vo Politekh. un-ta) pp 389-393
[4] Gumenyuk V, Tumanov A, Tolochko I and Gorshkova E 2016 *Nedelya nauki SPbPU: materialy nauchnoi konferentsii s mezhdunarodnym uchastiem. Institut voenno-tekhnicheskogo obrazovaniya i bezopasnosti* (Saint-Peterburg, Izd-vo Politekh. un-ta) pp 11-14
[5] Tumanov A 2008 *Nauchno-tekhnicheskie vedomosti SPbGPU* 2(123) pp 66-75
[6] Koff G, Gusev A, Vorob’ev Yu and Koz’menko S 1997 *Assessment of the impact of emergencies* (Moscow, Izdatel’eko-poligraficheskii kompleks REFIA) 364 p
[7] Kobzar’ Y and Khlobystov E 2013 *Methodological framework for assessing the damage from emergencies* 342 p
[8] Tumanov A 2013 *Nauchno-tekhnicheskie vedomosti SPbGPU* 2(171) pp 289-299
[9] Vetoshkin A and Tarantseva K 2001 *Tekhnogennyi risk i bezopasnost* (Penza: Izd-vo Penz. gos. un-ta) p: il.,bibliogr. 215 p
[10] Gumenyuk V, Dobroborskii B and Fedosovskii M 2012 *Nauchno-tekhnicheskie vedomosti SPbGPU* 3-2(154) pp 249–253
[11] Malinetskii G 2002 *Matem. Modelirovanie* 8(14) pp 107–112
[12] Voronin Yu and Chudinskii R 2001 *Modelirovanie v tekhnologicheskom obrazovanii* (Voronezh, VGPU) 226 p
[13] Ragozin F 1993 *Problemy bezopasnosti pri chrezvyachainykh situatsiyakh* 5 pp 16-41
[14] http://www.beintrend.ru/2010-09-06-06-39-10. (15.03.2016).
[15] Gumenyuk V and Tumanov A 2017 *Problemy bezopasnosti i chrezvyachainyh situatsii* 1 pp 85-97.
[16] Zhilina I 1998 *Otsenka posledstvii chrezvyachainyh situatsii* (Moscow, izd. -poligraf, kompleks "REFIA") 364p
[17] http://cyberleninka.ru/article/n/98-03-032-otsenka-posledstviy-chrezvyachaynyh-situatsiiy-koff-g-l-gusev-a-a-vorobiev-yu-l-kozmenko-s-n-mezhdunar-akad-informatizatsii-otd-geoekol (data obrashcheniya: 27.03.2017).
[18] http://cyberleninka.ru/article/n/98-03-032-otsenka-posledstviy-chrezvyachaynyh-situatsiiy-koff-g-l-gusev-a-a-vorobiev-yu-l-kozmenko-s-n-mezhdunar-akad-informatizatsii-otd-geoekol#ixzz4cVrfae3q.
[19] Makhutov N 2008 *Problemy bezopasnosti i chrezvyachainyh situatsii* 5 pp 57-73
[20] 1998 *Bezopasnost’ Rossii* (Moscow, MGf «Znanie») 448 p