Monte Carlo method for predicting the stability of the functioning of the informatization object in the conditions of massive computer attacks

V A Voevodin
Department of "Information Security", National Research University of Electronic Technology, Shokin sq., 1, Zelenograd, 124498, Russia

E-mail: vva541@mail.ru

Abstract. The application of the Monte Carlo method for solving the problem of predicting the functioning stability of the object of informatization in the conditions of massive computer attacks (MCA) is considered. The field of research represents practical and theoretical interests, since the methods developed by the theory of reliability are focused on simple, stationary, failure flows, which cannot be applied to the MCA conditions. In the conditions of the MCA, the period of normal functioning is commensurate with the recovery time, therefore, the application of the Poisson flow model leads to a significant error. To ensure the reliability of modeling, it is necessary to use an alternating process model, where the recovery time is commensurate with the period of operation and has a finite value, while analytical models of the real functioning processes are cumbersome, difficult to interpret and have no practical application.

1. Introduction
The development of digital technologies and the complexity of the information infrastructure is accompanied by the growth of cybercrimes [1, 2]. Issues related to the risks of information distortion, business process downtime, and successful computer attacks are becoming relevant [1, 2]. Issues of testing and monitoring of information systems are discussed in [3, 4, 5]. Insurance of the listed risks looks like a reasonable way to ensure the protection of information, which is based on the economic factor [6, 7]. For the purposes of this article, a computer attack is understood as an attempt to destroy, disclose, modify, block, steal, obtain unauthorized access to an information asset or its unauthorized use [8]. By itself, the procedure for insuring information security risks involves the participation of an information security auditor, in addition to the policyholder and the insurer. The auditor's task is to assess the risk of information security and prepare initial data to substantiate the subject of the contract and its value. At the same time, the auditor must have reliable, scientifically based methods that would allow assessing the functioning stability of the insured object of informatization (OI) in the conditions of massive computer attacks (MCA). At the same time, an important condition is that the reliability and completeness of the audit report should be trusted by the audit customers – the policyholder and the insurer. General issues of the organization and conduct of an information security audit are considered in the works [9, 10, 11, 12, 13, 14].

2. Statement of the research problem
The task of predicting the functioning stability of the OI, in the conditions of the MCA, is formulated as follows. The initial data is determined:
• the characteristic of a massive computer attack (MCA) is \( \lambda = \{ F(t), n \} \), including the distribution function \( F(t) \) of random time intervals \( \eta_i \), between \( i \)-th attacks, \( F(t) = \{ F(t) \}, i = 1, 2, \ldots, n \); \( n \) is the number of attacks;

• the characteristic of the stability of OI to computer attacks \( u = \{ T_p, P \} \), including the time between failures of operability in normal operating conditions – \( T_p \) and the values of the probabilities of OI damage as a result of CA, \( P = \{ P_i \} \) in \( i \)-th attacks, it is proposed to determine the probability values \( P_i \) in accordance with the approach given in [11, 12] and the methods published in [9, 10] and software tools [15, 16, 17];

• variable characteristics of recoverability of the OI \( r = \{ T_R, G(t) \} \), where \( T_R = \{ \tau_{01}^i, \tau_{0n}^i \} \) is the predicted recovery time interval \( \tau_{0i} \) of OI and distribution function \( G(t) \) of random recovery time intervals of OI \( \tau \) after the \( i \)-th attack, \( G(t) = \{ G(t) \}, i = 1, 2, \ldots, n \), \( n \) is the number of attacks, \( \tau_{0i}^l \) is the evaluation of the lower bound of the recovery time of the OI after the \( i \)-th attack \( \tau_{0i}^u \) in the estimation of upper bound of the recovery time of the OI after the \( i \)-th attack. It is proposed to determine the values of the parameters using the methodology published in [18] and software tools [15, 16].

It is necessary to develop a general procedure and investigate special cases of determining the smallest value of the \( v_m \) stability function of the OI at a given waiting time interval of MCA \((0, T)\).

\[ v_m = \inf_{t \in (0, T]} v(t, \lambda, r, u). \]

Then the stability function \( v \) of the OI in accordance with [19] will have the form:

\[ v(t, \lambda, r, u) = K_r(u, r) \varphi(t, \lambda, r, u), \]

where \( K_r \) is the readiness coefficient of the OI; \( \varphi(t, \lambda, r, u) \) is the survivability function of the OI, where \( t \) is the current time of the evaluation of the survivability function.

Algorithms of exact analytical models are based on a general estimation procedure, which is based on mathematical models of the distribution functions \( F(t) \) and \( G(t) \) [18].

\[ K_r = T_n(T_n + T_i)^{-1}, \]

where \( T_n, T_i \) – the total time of regular operation of the OI and recovery. They are determined on the basis of the statistics obtained in the conditions of regular operation of the OI. For most cases, \( K_r \geq 0.99 \), and the smallest value of the survivability function is \( \varphi_{\text{min}} \leq K_r \), so \( K_r \) can be neglected, then the mathematical model of the stability function reduces to:

\[ v_m \approx \varphi_{\text{min}} = \varphi(t, \lambda, r, u). \]

The task is solved in two stages:

1) definition of the operator \( A \):

\[ \varphi(t) = A\{ F(t), G(t), P, n \}; \]

2) functional definition:

\[ \varphi_m = \inf_{t \in (0, T]} \varphi(t). \]

The most difficult is the first stage, during which various types of the operator \( A \) are considered and the appropriate one is selected:

• the operator \( A_0 \), defined under arbitrary distribution laws \( F(t) \) and \( G(t) \) and various \( P_i \), (the process of ensuring business continuity). In this case, the recovery process can be characterized as a general semi-Markov process;

• the operator \( A_1 \), defined for the same distribution laws \( F_i(t) = F(t) \) and \( G_i(t) = G(t) \) and equal to \( P_i = P \). In this case, the recovery process can be characterized as a private semi-Markov process;

• the operator \( A_2 \), defined for the exponential distribution laws \( F(t) = 1 - e^{-\lambda t} \) and \( G(t) = 1 - e^{-\mu t} \) and equal to \( P_i = P \). In this case, the process can be characterized as Markov process;

• the operator \( A_3 \), determined by a single computer attack \( n = 1 \).
OI: an exact mathematical model; an approximate analytical model; a statistical model based on the Monte Carlo method.

The derivation of analytic relations for the definition of \( A_2, A_3 \) is given in [19]. It is advisable to use exact analytical methods for a relatively small number of CA, for \( n \leq 2 \), since with an increase in the number of \( n \), rather complex, cumbersome and difficult to interpret analytical expressions are required to calculate the survivability function \( \varphi(t) \).

Algorithms for approximate analytical methods are based on the use of various approximating dependencies that simplify analytical expressions for calculating the functions \( F(t), G_i(t) \), and \( \varphi(t) \), which make it possible to describe the truncated laws of normal distribution of random variables \( \eta \) and \( \tau \) with sufficient accuracy for value judgments. This requires the application of higher order Erlang laws, which greatly complicates the mathematical model.

It is advisable to use the statistical modeling algorithm for large values of \( n \), when the analytical expressions for the mapping \( \varphi(t) \) are cumbersome, the numerical process requires significant resources, the distribution functions of random variables have arbitrary laws, and the probability of being hit in the OI from impact to impact may differ.

For statistical modeling of each \( j \)-th implementation \( z_i(t) \) of a random process \( z(t) \), a sequence of values of the states of the attacked element (OI) is compared, \( z_i(t) = z_i (t_i) \), \( i = 1, 2, ..., m \), determined at discrete time points \( t_i = i * \Delta t \). The values of \( m \) are calculated in accordance with the specified simulation time \( T \) and with the specified unit interval \( \Delta t \) according to the formula \( m = T / \Delta t \). With this in mind, the statistical modeling procedure will include the following enlarged stages:

1. The number \( s \) of required implementations \( z_i(t) \) of a random process \( z (t) \), \( i = 1, 2, ..., s \) is given.
2. A sequence of time points \( t_i, i = 1, 2, ..., m \) is formed.
3. The sequence of possible time points of attacks and recoveries of the modeled element is determined:
   - \( T_{wiy} = \{0, T_{uij}, T_{vij}, T_{uij}, T_{uij}, ..., T_{win}, T_{vin}\} \), where \( T_{wij} = T_{v(i-1)j} + \eta_i^* \);
   - \( T_{vij} = T_{wij} + \tau_i^* \); \( i = 1, 2, ..., n \), \( T_{v0j} = 0 \);
   - \( n \) is the number of computer attacks;
   - \( \eta_i^* \) - \( i \)-th realization of a random variable \( \eta \), formed using a random number sensor in accordance with the selected distribution law \( F(t) \);
   - \( \tau_i^* \) - \( i \)-th realization of a random variable \( \tau \), formed using a random number sensor in accordance with the selected distribution law \( G(t) \).
4. For each implementation of \( j \), the success event of the computer attacks is determined in accordance with the condition: if \( Rnd() > P \), then the attack is considered unsuccessful, where \( Rnd() \) is the value of the random number generator in the interval \( (0, 1) \) distributed according to a given random variable distribution law.
5. Implementations of \( z_i(t) = \{z_{ij}\} \) are formed sequentially due to the following conditions:
   - \( z_{ij} = 1 \), if \( Rnd() > P \);
   - \( z_{ij} = 1 \), if \( Rnd() < P \) and \( T_{v(i-1)j} \leq t_i \leq T_{wij} \);
   - \( z_{ij} = 0 \), if \( Rnd() < P \) and \( T_{wij} \leq t_i \leq T_{vij} \);
   - \( i = 1, 2, ..., m \).
6. The obtained values of the corresponding states \( z_{ij} \) are summed for all implementations and an estimate of \( \varphi^*(t_i) \) values of the survivability function at time points \( t_i \) is determined by the formula:
   \[
   \varphi^*(t_i) = \frac{1}{m} \sum_{j=1}^{m} z_{ij}, \text{where } i = 1, 2, ..., m.
   \]

The algorithm is implemented using a computer program [20], which allows us to obtain the survival function of the OI for MCA condition with an arbitrary number of impacts and arbitrary distribution laws of random variables \( \eta \) and \( \tau \).

As a result of modeling, it is possible to predict:
- the lower and upper limits of the recovery time of the object in conditions of MCA, which provides a given value of the survivability index;
- changing the survivability function of the object of a computer attack in the process of MCA;
- unfavorable time intervals during which the survivability function is minimal or may be lower than the required one.

The simulation results, depending on the number of implementations of the random process of changing the survivability function in the MCA process, are shown in figure 1.

![Figure 1. The type of survivability function depending on the number of implementations.](image)

With an increase in the number of implementations, the survivability function becomes more smoothed, and local minimums can be observed already on 500 implementations, look at the average graph in figure 1.

3. Example. For example, let’s take the following legend. Let’s assume that the insurance company has established lowering coefficients of the insurance tariff for information risk insurance, depending on the security of the OI in relation to the MCA (from the minimum value of the survivability function \( \varphi_m \): (\( \varphi_m < 0.79; \) is risk insurance is unprofitable for the insurer); (\( 0.79 \leq \varphi_m < 0.8; \) \( k = 1 \)); (\( 0.8 \leq \varphi_m < 0.9; \) \( k = 0.7 \)); (\( 0.9 \leq \varphi_m < 0.95; \) \( k = 0.5 \)); (\( \varphi_m > 0.95; \) \( k = 0.45 \), and to provide \( \varphi_m > 0.95 \) requires a significant resource that is unprofitable for the insured), where \( k \) is the coefficient of reduction of the insurance premium depending on the values of the functions of vitality \( \varphi_m \).

The person managing the risks of OI has decided that option 2 is rational - (\( 0.8 \leq \varphi_m < 0.9; \) \( k = 0.7 \)). The management of the OI and the insurer (hereinafter the Parties to the contract) decided to apply for an audit opinion from an independent audit company to assess the protection of the OI from MCA. Based on the results of the audit (audit report), make a decision on the expediency of the financial risks insurance associated with a possible violation of business continuity as a result of MCA.

To assess the level of protection from MCA, the audit company planned an experiment with a statistical model, for which: a) MCA scenario was formed and agreed with the Audit Customers; b) the OI business continuity plan (Plan) was studied and the initial data for modeling was obtained.

Characteristics of the massive CA on the OI (fixed variables):
- The predicted number of computer attack in the MCA – 4.
- The forecast of the computer attack intensity is one computer attack for 12 hours. The predicted period of implementation of the MCA is 2 days.

The moments of application of the computer attack are characterized by random numbers \( \eta_i \), \( i = 1, 2, 3, 4 \), distributed according to a uniform law. The first and subsequent computer attack are carried out at random times: \( \eta_1 \in [\eta_1=0, \eta_1=12 \text{ h.}] \); \( \eta_2 \in [\eta_2=12 \text{ h.}, \eta_2=24 \text{ h.}] \); \( \eta_3 \in [\eta_3=24 \text{ h.}, \eta_3=36 \text{ h.}] \); \( \eta_4 \in [\eta_4=36 \text{ h.}, \eta_4=48 \text{ h.}] \), where \( \eta_{\text{lo}}, \eta_{\text{up}} \), the lower and upper bounds of the uniform distribution law of the time the \( i \)-th computer attack.

Characteristics of the OI business continuity plan (managed variables):
Assessment of the probability of the OI damage $P = 0.4$.
The plan for restoring the continuity of the OI business has established that $n$ – the minimum possible time for restoring the OI's operability after the computer attack is 6 hours (0.25 days), and the maximum permissible time is $n = 12$ hours (0.5 days). The random variable $\tau$ is distributed according to a uniform law within the lower - $\tau_l$ and upper - $\tau_u$ boundaries of the specified range (variable variables).

**Limitations:** the recovery is carried out by scanning the server equipment and workstations with the help of an antivirus, deleting the malicious files and restoring the affected files; the business continuity plan provides that the lowest value of the OI survivability function should not fall below 0.8, i.e. $\varphi_m \geq 0.8$.

It is required to determine whether the specified characteristics of the business continuity restoration plan meet the established requirement for the specified characteristics of the MCA - ($\varphi_m \geq 0.8$, in order to obtain a discount coefficient $k = 0.7$).

If the requirements are not met, then by correcting the values of the changeable variables, find their values at which the requirements are met and at the same time the minimum resource is required - $R_c$, such problem statements are given in [21, 22]. $R_c$ is the required resource for the implementation of the $\pi$ - th plan for maintaining the continuity of the OI business, $\pi$-th, is the set of plans for maintaining the continuity of the OI business satisfying the condition $0.8 \leq \varphi_m \leq 0.81$. The upper limit of the OI survivability function, $0.81$, is motivated by the fact that it is necessary: a) reduce the dimension of the task of finding a rational Plan; b) eliminate the excessive resource intensity of the Plan.

If the value of the survivability function for a given Plan meets the requirements ($0.8 \leq \varphi_m \leq 0.81$: $k = 0.7$), then an audit report is formed on the compliance of the Plan with the requirements. Otherwise, the task becomes more complicated and the search for a rational version of the Plan is carried out. If the survivability function significantly exceeds the requirements, then an audit report is formed on the excessive resource intensity of the Plan. If the survivability function is less than the requirements, then an audit opinion is formed on the insufficient level of protection of the OI.

To solve the problem, an experiment was planned and conducted with a statistical model of the Plan. The model was built using Excel tools. The final result is represented by OI survivability functions graph, Figure 2. The search problem is solved graphically. So, if the survivability function is below the permissible limit ($\varphi_m \leq 0.8$; $k = 0.7$), then either $P$ is fixed, and the lower- $\tau_l$ and $\tau_u$ decrease within the limits of the recovery time of operability. Or, with fixed $\tau_l$ and $\tau_u$, measures are taken to reduce the probability of the OI damage. The required resource is estimated and compared with the benefit from the resulting reduction coefficient of the insurance premium.

For graphics $\tau_l = 0.25$ day and $\tau_u = 0.5$ days, the value $\varphi_m \approx 0.62$ does not meet the requirements to receive a reducing factor ($0.9 \geq \varphi_m \geq 0.8$; $k = 0.7$). By sequentially reducing $\tau_l$ and $\tau_u$ and performing statistical modeling and displaying the results graphically, the search for a variant when $\varphi_m \approx 0.81$, i.e. slightly exceeds the required value, is carried out. The desired solution is $\tau_l = 0.1$ days (2.4 hours) and $\tau_u = 0.2$ days (4.8 hours). To achieve this result, it will be necessary to increase the resource allocated to maintain the readiness of the OI, to increase the capabilities of the recovery system.

The results of statistical modeling by the Monte Carlo method are shown in figure 2. According to the figure, the security of the informatization object $P_A=0.25$ is required ($\varphi_m \approx 0.81$) - this is a very high level of security. To ensure this level of security, a significant resource is required for the construction of protection lines and for annual operating costs.
Figure 2. A family of graphs of the survivability function depending on the probability of a successful computer attack.

With the help of the constructed statistical model, variable parameters of the business continuity maintenance plan were selected, at which the minimum value of the survivability function meets the requirements. The simulation results are shown in figure 3. At the same time, it is clear that the burden of ensuring the security of the informatization object from computer attacks is assigned to the recovery system. New parameters have been set for the recovery system - \( n = 2,4 \) hour and \( \tau_u = 4,8 \) hour. With such a business continuity plan, the information security system becomes more maneuverable and less resource-intensive.

Figure 3. The survivability function of the object of informatization with the recommended parameters of the business continuity plan.
4. Modeling scenarios of massive computer attacks
The application of the Monte Carlo method for modeling the processes of OI functioning in the conditions of the MCA, taking into account the importance of the CA object as part of the computational network (CN) is of practical interest. For this purpose, a block for setting various attack implementation scenarios was introduced into the model. The variants of process control schemes considered in [21, 22] are shown in figure 4.

Verbal problem statement:
Given:
a) structure $S=\{M, L\}$, $N$ - the set of nodes (0 - N) - pole CN of an automated process control system, 0 - the index of the CN control element-the network bus; from 1 to N-the elements of the CN - the final vertices; $L$ - the set of connections between the nodes of the CN;
b) requirements for the minimum value of the OI survivability function;
c) a subset of controlled elements that are included in the technological chain (characteristic of the attack period) and are elements of the CN.
It is required: to ensure the exchange of technological information between the decision-maker (DM) and the management objects – MO) - to ensure the controllability of the automated process control system. The attacker's goal is to cause maximum damage to the controllability of the OI (to minimize the number of MO).

Formal statement of the problem:
Initial data:
- $n$ - is the number of computer attacks;
- the structure of the (1-N) automated control system, $I$ is the pole of the automated control system, $N$ are the poles of the controlled objects (CO); the threshold number of controlled objects $N_R$, that have at least one connection with the automated control system, which ensures the controllability of the automated control system;
- $V=\{v_i\}$ – the set of node elements of the CN, $v_i = 1$, if the element is in a working state, $v_i = 0$, otherwise, $i = 0, 1, 2,..., K$, $K$ is the number of node elements of the CN, $i = 0$ is the index of the poles of the DM, $i = 1$ to $K$ are the indices of node elements of the CN;
- $E = \{e_{ij}\}$ – the set of connection lines between the node elements of the set $V$, $e_{ij}=1$, if the connection between the i-th and j-th nodes is provided, $e_{ij}=0$, if the connection between the nodes is not provided, $i = 1,2,..., K-1$, $j=2,3,...K$, $K$ is the number of elements of the set $V$, including the control element and $N$-controlled elements;
- $V^* = \{v^*\} \in V$ is a subset of MO that are under the control of the DM.

Figure 4. Variants of the process control scheme.
Scenarios of massive computer attacks:
1. The attacker does not know whether the elements of the computer network belong to the OI.
2. The attacker does not know the structure of the OI – $S_{ds}$ computer network, but there is information about belonging to the OI.
3. The attacker knows $S_{ds}$: he is able to assess the structural importance of the $S_{ds}$ elements, and is able to plan the first and subsequent computer attacks taking into account the structural importance of the $S_{ds}$ elements. Computer attacks is planned according to the criterion of decreasing $w_i$, where $w_i$ is the coefficient of structural importance of the element, it is calculated according to a special method of the author.
4. The attacker knows the result of the previous attack, which allows it to correct the initial attack scenario. For example, if the attack was unsuccessful, as a result, the target of the attack turned out to be operational, this object can be included in the attack plan again.

Limitations:
1. The probability of damage to the elements of the $S_{ds}$ is a subjective probability, set by expert assessments [16, 17] or is found using the statistical model given above.
2. The elements of the $S_{ds}$ change the state at time $t_i$, where $i = 0 + \Delta t$, $\Delta t$ is the step of sampling the events of the statistical model.
3. The costs of a successful attack on a vertex element (DM) are disproportionately large compared to successful attacks on the elements of the $S_{ds}$;
4. Management objects of equal value.

Using the laboratory stand [20]:
1. The initial data is entered: a) about the security of the object of attack; b) about the capabilities of the attacker.
2. The results of the simulation implementation are summarized.
3. The coefficient of operational readiness of the OI is estimated.
4. The interpretation of the obtained result is carried out in the conditions of decision-making under many criteria [23] and in terms understandable to the DM.

The simulation result for 10,000 implementations is shown in figure 5.

![The effect of a massive computer attack scenario](image)

Figure 5. Changing the effect of a massive computer attack depending on its scenario.
5. Conclusion
The developed statistical model, based on the Monte Carlo method, allows the decision-maker to solve practically significant managerial tasks on information protection:
1. With the given initial data allows to estimate the minimum value of the survivability function of the informatization object.
2. To carry out a purposeful search for an effective plan for maintaining business continuity.
3. Evaluate the effectiveness of random attacks on the computer network, which are the least effective.
4. Knowing the structure of the computer network, the enemy can strike at important elements without adjusting the attack plan. This method of implementing an attack is more effective than random attacks.
5. Knowing the network structure and having an attack plan, the enemy can cause serious damage to the computer network at a lower cost.
6. Knowing the results of a computer attack, an attacker can quickly correct a computer attack and cause maximum damage to the computer network.

Thus, it is possible to assess the effect of protecting the confidentiality of information.

The proposed approach is implemented as an integral part of the educational and methodological complex for the preparation of the audit group [24].

Acknowledgements
The work was carried out with the support of the Vladimir Potanin Charitable Foundation for Master's Degree teachers.

References
[1] Report on Network security and Availability in 2020 Available at: https://qrator.net/presentations/2021/QratorLabs_Network_Security_Availability_in_2020_RU.pdf [In Russian. Visited June 5, 2021]
[2] Data Breach Investigations Report Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf [Visited June 5, 2021] Business Impact Analysis https://bit.ly/37Lb1zP
[3] Cardwell K 2014 Building Virtual Pentesting Labs for Advanced Penetration Testing (Packt Publishing) p 518
[4] Tipton H F and Krause M 2006 Information Security Management Handbook (Auerbach Publications) p 3279
[5] Moeller R 2010 IT Audit, Control, and Security (Hoboken, John Wile & Sons Inc.) p 696
[6] State Standard GOST R 59516-2021. Information technology. Information security management. Guidelines for cyber-insurance. (Moscow: Standartinform Publ.) 2021 p 20 (in Russian).
[7] Voevodin V, Kovalev I and Folomeev L 2020 Implementation of Cyber-Insurance as a Data Protection Tool Norwegian Journal of development of the International Science 2(41) pp 14-17 (in Russian)
[8] State Standard ISO/MEK 27000-2012. Information technology. Security techniques. Information security management systems — Overview and vocabulary (Moscow: Standartinform Publ.) 2019 p 29 (in Russian)
[9] Makarenko S I 2018 Audit of Information Security – the Main Stages, Conceptual Framework, Classification of Types Systems of Control, Communication and Security (1) pp 1-29 (in Russian)
[10] Makarenko S I 2018 Audit bezopasnosti kriticheskoy infrastruktury specialnymi informacionnymi vozdeystviyami. Monografiya [Security Audit of Critical Infrastructure by Special Informational Actions. Monograph] (Saint Petersburg: Naukoemkie tehnologii Publ.) p 122 (in Russian)
[11] Markov A S, Cirlov V L and Barabanov A V 2012 *Metody ocenki nesootvetstviya sredstv zashechity informacii* [Methods for Assessing the Inconsistency of Information Protection Means] (Moscow: Radio i svyz' Publ.) p 192 (in Russian)

[12] Kulp'ba V V, Shelkov A B, Gladkov Y M and Pavel'ev S V 2009 *Monitoring i audit informacionnoj bezopasnosti avtomatizirovannyh sistem* [Monitoring and Audit of Information Security of Automated Systems] (Moscow: Institute of Control Sciences RAS) p 94 (in Russian)

[13] Gordon L A and Loeb M P 2005 *Managing Cybersecurity Resources: A Cost-Benefit Analysis* (The Mcgraw-Hill Homeland Security Series) p 224

[14] Skabkov N 2018 *Audit bezopasnosti informacionnyh sistem* [Information Systems Security Audit] (Saint Petersburg: Piter Publ.) p 272 (in Russian)

[15] Voevodin V A, Markin P V, Markina M S and Burenok D S 2021 Technique for developing an information security audit program taking into account the weight coefficients of certificates based on the hierarchy analysis method. Systems of Control *Communication and Security* (2) pp 96-129 (in Russian). DOI: 10.24412/2410-9916-2021-2-96-129

[16] Burenok D S, Voevodin V A, Markin P V and Markina M S 2020 *Komp'yuternaya programma metoda analiza ierarhij. Svidetel'stvo ob ofitsial'noi registratsii programm dlya EVM* [Program For The Analytic Hierarchy Process. The Certificate on Official Registration of the Computer Program] No. 2020667542

[17] Burenok D S and Voevodin V A 2020 *Programma metoda ekspertnyh oценок. Svidetel'stvo ob ofitsial'noi registratsii programm dlya EVM* [Program For The Expert assessment method. The Certificate on Official Registration of the Computer Program] No. 2020616093

[18] Voevodin V A, Markina M S and Markin P V 2020 Determination of the Weight of Audit Evidence by the Method of Point Ratings in the Information Security Audit. *Computational nanotechnology* (1) pp 57-62. doi: 10.33693/2313-223X-2020-7-1-57-62 (in Russian)

[19] Hohlachev E N 2012 *Organizatsiya i tekhnologiya vyrabotki reshenij pri upravlenii sistemoj i vojskami svyazi. Chast' 1. Metodicheskie osnovy vyrabotki voenno-upravlencheskih reshenij* [Organization and Technology of Decision-Making in the Control of the System and Signal Troops. Part 1. Methodological Foundations for the Development of Military Management Decisions] (Moscow: Military Academy of Strategic Rocket Forces) p 234 (in Russian)

[20] Ganenkov D S, Kuchin N V and Voevodin V A 2020 *Komp'yuternaya programma ocenki gotovnosti avtomatizirovannoj sistemy upravleniya technologicheskim processom v uslovijah komp'yuternyh atak. Svidetel'stvo ob ofitsial'noi registratsii programm dlya EVM* [Computer program for assessing the readiness of an automated process control system in conditions of computer attacks. The Certificate on Official Registration of the Computer Program] No. 2020616191

[21] Voevodin V A 2019 Conceptual Model of Information Security Auditobject *Computational nanotechnology* (3) pp 92-95. doi: 10.33693/2313-223X-2019-6-3-92-95 (in Russian)

[22] Voevodin V A 2019 Etalonnaya model' ob"ekta audita informacionnoj bezopasnosti [Reference Model of an Information Security Audit Object] *Modern Science: actual problems of theory and practice. Series of "Natural and Technical Sciences"* (9) pp 56 - 60 (in Russian)

[23] Keeney R L and Raiffa H 1976 *Decisions with Multiple Objectives: Preferences and Value Trade-Offs* (New York: Wiley) p 569

[24] Voevodin V A 2019 Uchebo-metodicheskij kompleks dlya podgotovki k prakticheskому auditu informacionnoj bezopasnosti [Educational-methodical complex for preparation for practical audit of information security] *Modern Science: actual problems of theory and practice. Series of "Natural and Technical Sciences"* (10) pp 56-61 (in Russian)