The logical-probabilistic model for assessing the information security assessing of the critical information infrastructure subject under destructive influences

E A Maksimova¹, M A Lapina², V V Baranov³, O S Lauta⁴

¹ Russian Technological University MIREA (RTU MIREA) Moscow, Russia
² North-Caucasus Federal University, Stavropol, Russia
³ South Russian State Polytechnic University (NPI) named after M.I. Platov, Novocherkassk, Russia
⁴ Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, Saint-Petersburg, Russia

E-mail maksimova@mirea.ru

Abstract. Security of the subject of critical information infrastructure (SCI) is one of the key issues of our time at the international level. One of the guarantors of stability and information security of society and the state as a whole is the reliability of the SCI functioning. The currently existing methods and models for assessing reliability, as applied to CII, are considered without taking into account the factor of influence of the offender, which can have a destructive effect on the subject of CII. This leads to significant errors in the analysis of the information security of the subject of CII, therefore, reduces the effectiveness of the information protection means declared for CII objects.

The proposed logical-probabilistic model is associated with the use of the specifics of the regulatory and legal framework in the field of SCI safety; structured detailing of the CII subject, taking into account the specifics of the subject; stages of the life cycle of the SCI information protection system; highlighted destructive malicious influences of an infrastructural nature; interrelationships of the selected destructs with a number of vulnerabilities on CII objects. The model takes into account physical, physicochemical, chemical, biological, operational factors of threat realization as factors affecting the decrease in the reliability of the functioning of the CII subject. The assessment of reliability indicators is carried out taking into account the characteristics of recoverable and non-recoverable objects, backup methods. The model allows you to assess the reliability of the subject of CII as an integrative characteristic, which is an indicator of the assessment of information security.

Keywords: Critical Information Infrastructure, International Level, Security of Society, Destructive Effect, Significant Errors, Logical-Probabilistic Model, Legal Framework, Recoverable and Non-Recoverable Objects, the Assessment of Information Security.

1. Introduction
The legislation of the Russian Federation [1-5] defines the areas of operation of enterprises and organizations that affect the quality of life and health of society, in order to ensure their safety. State bodies, government agencies, Russian legal entities and individual entrepreneurs operating in the selected areas, which are subjects of critical information infrastructure (SCII), are responsible for maintaining the stability of the area to which they belong.

Necessity Assessment of the reliability of the functioning of CII subjects is characterized by the possibility of assessing the probability of failure-free operation of CII facilities and preventing failures in the functioning of CII spheres, which guarantees stability and information security of society and the state as a whole. Thus, the problem of assessing the reliability becomes key in the comprehensive assessment of IS SCII.

2. Models and methods
The "input" research was carried out in three directions: analysis of models and methods for assessing the reliability of the subject of CII, analysis of ways to improve the reliability of the subject of CII, analysis of existing software systems for assessing the reliability of technical systems.

In the course of analyzing the models and methods for assessing the reliability of the subject of CII, the following were considered: the probabilistic method (the model "block-diagram"), the logical-probabilistic method, the model "fault tree", Markov model [6-13]. The following criteria are defined for the analysis: reliability assessment based on the interdependence and interrelation of CII objects; calculation of indicators in a time interval; calculation of indicators at time t; sufficiency for the research of complex systems; relative ease of calculation; reliability assessment when implementing various methods of redundancy; reliability assessment when applying various recovery strategies; high estimation accuracy; simplicity of circuit construction. According to the selected criteria, the probabilistic method was determined as the most effective (the model "block-diagram").

To analyze the ways to improve the reliability of the functioning of the CII subject, the following criteria are highlighted: the accuracy of calculations, the convenience in reserving sub-objects, the relative simplicity of calculations, the involvement of reserve sub-objects in the work, the inclusion of reserve sub-objects as needed, the guarantee of replacing a failed sub-object with a reserve one. The following methods of redundancy are analyzed: loaded redundancy, unloaded redundancy, light redundancy, sliding redundancy. Based on the analysis results, the most effective and appropriate backup methods are loaded and loaded redundancy.

In the research of software systems for assessing the reliability of technical systems, ARBITR (PC ASM SZMA), ASONIKA-K, ASRN (2000, 2002), Isograph (England, USA), RAM Commander (Israel), Windchill Quality Solutions (Relex) (USA) were considered. By criteria: the ability to take into account the specifics of CII; taking into account the likelihood of the implementation of threats leading to a malfunction of the CII; the possibility of an integral assessment for the system; analysis of the interaction scheme of elements in the form of a block diagram (sub-objects, CII objects); system lifecycle accounting; the ability to assess the reliability of systems other than industrial. As a result of the analysis, the WQS software package was determined as satisfying the largest number of selected criteria. However, to solve the problem, it is necessary to fulfill all the criteria, which leads to the need to develop an appropriate model.

3. Description of the simulation system
To implement the modeling process, sub-objects are selected inventory units of the CII subject: InvU1 – PC, InvU2 – servers, InvU3 – ACO, InvU4 – system software, InvU5 – application software, InvU6 – SRZI, InvU7 – communication channels, InvU8 – peripheral devices; InvU9 – CII sub-object specific for each individual CII subject, InvU10 – processed and stored information, including configuration information. The reliability of the CII objects and the CII subject as a whole depends on their reliability.

In order to reduce the error in the assessment of information security, the life cycle of the subject of CII has been determined and analyzed in accordance with GOST 34.601-90 [17]. On the basis of the "Life Cycle of SIS of the CII subject", the types of destructive influences that lead to the emergence of
vulnerabilities in the protection system of CII objects at different stages of the life cycle of the CII subject are identified. Vulnerabilities can be used to implement threats, attacks by malefactors on the subject of CII as a whole. Selected types of destructive influences (destructions): Destr 0 – Errors associated with the primary development of the plant's AS; Destr 1 – errors at the categorization stage; Destr 2 – Infrastructure Analysis Errors; Destr 3 – Errors in the formation of requirements for the information security system of the CII subject; Destr 4 – Errors in the development of the concept of information security for a CII subject; Destr 5 – Errors in the development of technical specifications; Destr 7 – Errors in the technical design; Destr 8 – Errors entering; Destr 9 – Errors while accompanying the subject of CII [18-20].

Vulnerabilities of typical systems are analyzed by the method of constructing vulnerability trees. The relationship between the selected destructs and a number of vulnerabilities has been revealed. Destructions Destr 0, Destr 1, Destr 2, Destr 3, Destr 4, Destr 5, Destr 6, Destr 7 are associated with the vulnerability of the lack of compliance with information security requirements in the design of information security solutions. Destruction Destr 8 is associated with a vulnerability in the absence or insufficient level of knowledge in the field of information security among the maintenance personnel. Destr 9 destruct identifies a number of vulnerabilities, such as the problems of delimiting and controlling access for contractors associated with the need to provide temporary access to a limited amount of equipment without the ability to affect the rest of the system, as well as cancellation of such access at the end of work; lack or insufficient level of knowledge in the field of information security among service personnel; long service life of vulnerable components due to the complexity of upgrading equipment and systems.

Physical, physicochemical, chemical, biological, operational, implementation of threats by intruders have been identified as factors affecting the decrease in the reliability of the functioning of the CII subject.

When assessing the reliability of SCI, the indicators of the reliability of restored and non-renewable objects are evaluated. For recoverable ones - mean time between failures, mean time between failures, probability of recovery, mean time to recover, availability factor, technical utilization factor. For non-recoverable – probability of failure, probability of failure-free operation, time of failure-free operation, failure rate.

4. Discussion
The proposed mathematical model for assessing the reliability of the subject of critical information infrastructure is represented by the function of the model for assessing the reliability of the subject of CII:

\[ F = F(P_{thr}, P_{rel}), \]

where \( P_{rel} \) – probability of failure-free operation of CII facilities;
\( P_{thr} \) – the likelihood of an IS threat.
\( P_{thr} \) can take the following values:

\[ P_{thr} = P_{Destr, i} \]
\[ P_{thr} = P_{exp} \]

where \( P_{Destr, i} \) – the likelihood of the implementation of threats generated by destructions at different stages of the CII life cycle;
\( P_{exp} \) – expert assessment of the likelihood of threats.

In the model for assessing the reliability of the subject of CII \( P_{Destr, i} \) is predicted by the least squares extrapolation method based on the existing statistics on the implementation of threats at enterprises and organizations operating in the areas of CII.
If it is necessary to assess the reliability of the CII subject, based on the probability of the implementation of threats received by the expert, the software provides the ability to enter the value \( P_{\text{exp}} \), different from the predicted value \( P_{\text{Dest}_1} \) based on existing statistics.

\( P_{\text{Dest}_1} \) for destructs related to infrastructure errors, can take on the values:

\[
P_{\text{Dest}_1} = P_{\text{Dest2}}, P_{\text{Dest10}}.
\]

\( P_{\text{Dest}_1} \) for destructs associated with the remaining stages of the life cycle of the CII subject, it can take on the values:

\[
P_{\text{Dest}_1} = P_{\text{Dest1}}, P_{\text{Dest3}}, P_{\text{Dest4}}, P_{\text{Dest5}}, P_{\text{Dest6}}, P_{\text{Dest7}}, P_{\text{Dest8}}, P_{\text{Dest9}}.
\]

The occurrence of errors, destructions, at different stages of the life cycle of the information security system of the CII subject generates vulnerabilities in the CII protection system, which attackers can exploit to implement threats to the CII subject.

To rate \( P_{\text{exp}} \) an expert can use the value of the frequency probability of the implementation of threats [16]:

\[
P_{\text{exp}} = \lim_{N \to \infty} \frac{n}{N},
\]

where \( N \) is the total number of incidents that occurred during the year; \( n \) - the number of specific incidents per year.

To get the value \( P_{\text{Dest}_1} \) - the likelihood of threats being realized is extrapolation by the least squares method [16]:

\[
P_{\text{Dest}_1} = a \times X + b,
\]

where \( X \) is a symbol of time;

\( a \) – coefficient calculated by the formula:

\[
a = \frac{\sum_{i=1}^{n} (act \times X) - (\sum_{i=1}^{n} act) \times (\sum_{i=1}^{n} X)}{\sum_{i=1}^{n} X^2 - (\sum_{i=1}^{n} X)^2}
\]

\( b \) – coefficient calculated by the formula:

\[
b = \frac{\sum_{i=1}^{n} act}{n} - \frac{a \times \sum_{i=1}^{n} X}{n}
\]

where \( act \) is the actual values of a number of dynamics (in this case, the values from the threat statistics in the CII spheres);

\( n \) – the number of levels in the time series (the number of years (months) for which the statistics of threats in the areas of CII were taken).

Probability of failure-free operation of CII facilities \( P_{\text{rel}_1} \) depends on the probabilities of failure-free operation of CII subobjects and their interconnections:

\[
P_{\text{rel}_1} = P(\text{InvU}_1, \text{InvU}_2, \text{InvU}_3, \text{InvU}_7, \text{InvU}_9)
\]

where \( \text{InvU}_1 \) – PC; \( \text{InvU}_2 \) – server; \( \text{InvU}_3 \) – ACO; \( \text{InvU}_7 \) – channels of connection; \( \text{InvU}_9 \) – CII sub-object specific for each individual CII subject.

When calculating the probabilities of failure-free operation of CII objects, we do not take into account such CII sub-objects as system and application software, information security tools, peripheral devices, processed and stored information, since these CII sub-objects in case of failure will not critically affect the CII object in comparison with the output out of order, for example, ASO, a server for collecting technological information or a dispatcher’s workstation.
In the course of the research, all indicators of the reliability of recoverable and non-recoverable CII sub-objects were considered. The analysis showed that to assess the reliability of the subject of CII, the indicator "probability of failure-free operation".

To calculate the assessment of the reliability of CII facilities $P_{rel_i}$, three cases are considered, where $p_i$ is the probability of failure-free operation of CII sub-objects:

1. Scheme with a series connection of $n$ dependent sub-objects of the CII:
   
   $$P_{rel_i} = \prod_{i=1}^{n} p_i(t).$$

2. Scheme with parallel connection of $n$ dependent KII sub-objects:
   
   $$P_{rel_i} = 1 - \prod_{i=1}^{n}(1 - p_i(t)).$$

3. Serial-parallel circuit. To assess the reliability of CII facilities, a phased simplification of the circuit and the use of formulas to assess the reliability of circuits with serial and parallel connection are used.

Assessment of the reliability of the subject of CII $P_{subj}$ is calculated similarly to the schemes for assessing the reliability of CII objects: using calculations for parallel and serial connection of CII objects. After assessing the reliability of the CII objects, to assess the reliability of the CII subject, the formation of a structural diagram of the interconnection of the CII objects is carried out and, based on the probabilities of the failure-free operation of the CII objects and the probability of the implementation of threats, the reliability assessment of the CII subject is calculated.

$$P_{subj} = P_{rel_i} \ast (1 - P_{thr}).$$

In the event that the reliability of the CII subject is insufficient ($P_{subj} \leq 0.5$), it is necessary to apply redundancy methods to improve reliability.

To increase the reliability of the CII subject, the following methods and calculations are used to reserve CII sub objects, where $p_i$ is the probability of failure-free operation of the CII sub objects:

1. When using loaded redundancy (for a system with a serial connection of $n$ sub objects with general redundancy with a multiplicity of $k$), the reliability of the CII subject is calculated as follows:
   
   $$P_{subj} = 1 - (1 - P)^{k+1} = 1 - (1 - \prod_{i=1}^{n} P_i(t))^{k+1}.$$

2. When using loaded redundancy (for a system with a serial connection of $n$ objects with separate redundancy with a multiplicity of $k$), the reliability of the CII subject is calculated as follows:
   
   $$P_{subj} = \prod_{i=1}^{n}(1 - (1 - P_i(t))^{k+1}).$$

3. When using unloaded redundancy (systems with unloaded redundancy of multiplicity $k$ (total sub objects $k + I$)), the reliability of the CII subject is calculated as follows:
   
   $$P_{subj} = 1 - \frac{1}{(k+1)} \prod_{i=1}^{k+1}(1 - P_i(t)).$$

Based on the results of the assessment of the reliability of the CII subject before and after the reservation, the reliability gain coefficient is calculated:

$$G_p = \frac{P_{before}}{P_{after}},$$

where $P_{before}$ – assessment of the reliability of the subject of CII before reservation;

$P_{after}$ – assessment of the reliability of the subject of CII after reservation.

To assess the level of reliability of the subject of CII, the value 0.5 was chosen as the threshold value. In the case of assessing the reliability of the subject of the CII below 0.5, recommendations are proposed to improve the reliability of the CII subject, which include the methods of loaded and unloaded redundancy.
To implement the proposed model, a functional model for assessing the reliability of the subject of critical information infrastructure has been developed in the form of a context diagram in the IDF0 notation (figure 1).

![Context Diagram](image)

Figure 1. Context diagram for assessing the reliability of the subject of critical information infrastructures in the IDF0 notation

The architecture of the software package for the implementation of this model is shown in figure 2.

![Architecture Diagram](image)

Figure 2. Architecture of the software package for the implementation of the reliability assessment model for the subject of critical information infrastructure

5. Experimental research

In the course of the work, experimental studies were carried out to assess the reliability of CII subjects operating in various industries, which include various types of CII objects. The problem to be solved is to increase the reliability of the subject of the CII if the initial assessment of the reliability of the CII subject is less than 0.5.

Experimental studies involved not only assessing the reliability of the CII subject, based on the presented schemes of CII objects, but also, if necessary, the subsequent application of backup methods to the CII sub objects in order to increase the reliability of the CII subject.
So, for example, the assessment of the reliability of the subject of the CII of the hospital, which includes the object of the CII, which is the personal data information system (PDIS), a structural diagram was taken for the experiment (figure 3).

![Structural diagram of the object of the CII of the hospital]

**Figure 3.** Structural diagram of the object of the critical information infrastructure of the information system of personal data of the subject of the CII – Hospital

To conduct an experiment according to the scheme in Figure 3, a special scheme is built (figure 4), which displays the mutual influence and interaction of CII sub objects. In accordance with the values of the probabilities of no-failure operation of the CII sub objects from the experimental research plan, the reliability of the CII subject – Hospital.
Figure 4. Scheme of interaction between the critical information infrastructure sub objects of the critical information infrastructure object of the personal data information system. Experiment - Hospital (Screen Copy)

To assess the reliability of the subject of CII, the probability of the implementation of threats, predicted on the basis of the existing statistics of threats implemented at enterprises and in organizations operating in the areas of CII, was taken into account.

The assessment of the reliability of the subject of the CII-Hospital showed an insufficient level of reliability. In connection with this, redundancy methods were applied to CII sub-objects. Figure 5 shows a diagram of the CII ISPD object using the methods of loaded and unloaded redundancy.

For the CII ISPD object, loaded and unloaded redundancy was applied for the following KII sub-objects:

- For D-link, acting as routers and firewalls, unloaded redundancy was applied, since it is more efficient for the system so that the backup D-links come into operation after the main.
- For routers Cisco 7206 routers, unloaded redundancy was applied, since it is more efficient for the system so that the standby Cisco 7206 comes into operation after the failure of the main.
- For the Cisco 2960 switches, unloaded redundancy was applied, since it is more efficient for the system so that the redundant Cisco 2960s come into operation after the failure of the main.
- For ISPD servers, a loaded reservation was applied, since it is necessary that the backup servers collect, process and store information on a par with the main.
Figure 5. Scheme of interaction of the critical information infrastructure sub-objects of the critical information infrastructure object of the personal data information system. Application of redundancy. Experiment – Hospital (screen copy)

The analysis of the results of experimental studies of the software complex for the implementation of the reliability assessment model of the CII subject is presented in table 1.

Table 1 – Analysis of the results of the experimental research "Subject of CII – Hospital"

| Subject CII – Hospital | Assessment of object reliability | | Post-backup reliability assessment |
|----------------------|---------------------------------|-----------------|----------------------------------|
| **An object**        | Reliability assessment before redundancy | **PDIS** | 0.69 | 0.89 |
| **Assessment of the reliability of the subject of CII** | | | |
| **A subject**        | Reliability assessment before redundancy | **Hospital** | 0.43 | 0.56 |
| **Reliability win rate** | | | | **0.77** |
6. Analysis of experimental research results
The results of experimental studies show an increase in the level of reliability of the subject of CII using the results of the proposed model. So, as a result of the application of backup methods, the level of reliability of the subject of CII – Hospital increased by 0.13 and the reliability gain was 0.77.

7. Conclusion
The proposed logical-probabilistic model is associated with the use of:
• the specifics of the regulatory framework in the field of CII safety,
• structured detailing of the CII subject, taking into account the specifics of the subject,
• stages of the life cycle of the CII information protection system,
• highlighted destructive malicious influences of an infrastructural nature,
• the relationship of the selected destructs with a number of vulnerabilities on CII objects,
• as factors affecting the decrease in the reliability of the functioning of the CII subject – physical, physicochemical, chemical, biological, operational, implementation of threats by intruders,
• evaluating the reliability indicators of recoverable and non-recoverable objects, backup methods and allows you to assess the reliability of the subject of CII as an integrative characteristic, which is an indicator of the assessment of information security.

8. Acknowledgments
This work was supported by the Russian Ministry of Science (Information security, project №3)

References
[1] On the security of the critical information infrastructure of the Russian Federation: Federal Law of July 26 2017 N187-FZ (as amended and supplemented) [Electronic source]. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/
[2] On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation: Order of the FSTEC of December 25 2017 N239 (as amended and supplemented) [Electronic source] – URL: https://fstec.ru/document/53
[3] On the approval of requirements for the creation of security systems for significant objects of the critical information infrastructure of the Russian Federation and ensuring their functioning: Order of the FSTEC of December 21 2017 N235 [Electronic source]. – URL: https://fstec.ru/document/53
[4] On approval of the Procedure for informing the FSB of Russia about computer incidents, responding to them, taking measures to eliminate the consequences of computer attacks carried out against significant objects of the critical information infrastructure of the Russian Federation: Order of the FSB of Russia dated June 19 2019 N282 [Electronic source] – URL: https://www.garant.ru/document/72198410/
[5] On approval of the List of information submitted to the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation and the Procedure for submitting information to the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation: Order of the FSB of Russia from July 24 2018 No367 [Electronic source] - URL: https://www.garant.ru/document/71941504/
[6] Shubin R A 2012 Reliability of technical systems and technogenic risk / R.A. Shubin Tambov Publishing and Printing Center FGBOU VPO TSTU P 24-51
[7] Mozhayev A S 1999 General logical-probabilistic method for analyzing the reliability of complex systems Uch allowance L VMA 68 p
[8] Mozhayev A S, Gromov V N 2000 Theoretical foundations of the general logical-probabilistic method of automated system modeling SPb VITU 144 p
[9] Remenyte R, Andrews J D 2006 A simple component connection approach for fault tree conversion to binary decision diagram Availability Reliability and Security ARES 2006 / The First International Conference 20-22 April P 8

[10] Woo Sik Jung Sang Hoon Han and Jaejoo Ha 2015 A fast BDD algorithm for large coherent fault trees analysis Reliability Engineering & System Safety Vol 83 Issue 3 pp 369-374

[11] GOST R IEC 61165-2019 Application of Markov methods 2019 M Standartinform [Electronic source] – URL: https://files.stroyinf.ru/Data2/1/4293727/4293727169.pdf

[12] GOST R 51901.15-2005 (IEC 61165: 1995) Risk management. Application of Markov methods 2005 M Standartinform [Electronic source] – URL: http://docs.cntd.ru/document/1200041677

[13] Zhuk A, Orel D 2019 Improved Method for Estimating Noise Immunity of Global Navigation Satellite Systems Proceedings of the 2nd international conference on modelling, simulation and applied mathematics (MSAM2017) https://doi.org/10.2991/ITIDS-19.2019.54

[14] Kalmykov I, Lapina M, Kalmykov M, Voloshin E, Provornov I 2019 Development of Imitation-resistant Authentication Protocol for Low-orbitall Space Satellite Communication System: CEUR Workshop Proceedings YSIP3 – Proceedings of the Young Scientist's Third International Workshop on Trends in Information Processing

[15] Kalmykov I, Lapina M, Kononova N, Kalmikov M 2018 Development of the protocol "electronic cash" with inspection correction rules of the electronic e-cash number for e-commerce systems: CEUR Workshop Proceedings REMS 2018 – Proceedings of the 2018 Multidisciplinary Symposium on Computer Science and ICT Pp 147-153

[16] Linets G I, Melnikov S V, Govorova S V, Medenee V V, Lapina M A 2018 Decrease energy consumption of transport telecommunication networks due to the usage of stage-by-stage controlling procedure: CEUR Workshop Proceedings REMS 2018 – Proceedings of the 2018 Multidisciplinary Symposium on Computer Science and ICT Pp 181-190

[17] GOST 34.601-90 2009 Interstate Standard Information Technology. Set of standards for automated systems. Automated Systems. Stages of Creation. M Standartinform [Electronic source] – URL: http://docs.cntd.ru/document/gost-34-601

[18] Maksimova E.A. 2020 Evaluation of information security of the subject of critical information infrastructure under destructive influences [Text] monograph / E. A. Maksimova; Feder. state ed. educated. institution of higher. education "Volgogr. state university" Volgograd: VolGU Publishing House 95 p

[19] Maksimova E A Research of algorithms for secure data transfer between objects of critical information infrastructure // Collection of reports of the XXIII plenum of FUMO VO IS and the All-Russian scientific conference "Fundamental problems of information security in the context of digital transformation" (INFOSE-2019) reports of the XXIII plenum of FUMO VO IB and the All-Russian scientific conference. Resp. editor: V.I. Petrenko 2019 pp 157-163

[20] Maksimova E A, Shikherdiyeva A Sh 2019 Management of the operation of critical information infrastructure facilities // Materials of the XVI All-Russian School-Conference of Young Scientists "Management of Large Systems" Tambov Publishing Center of the Federal State Budgetary Educational Institution of Higher Education "TSTU" 2019 pp 392-397