Synthesis of Models for Ensuring Information Security of Subjects of Critical Information Infrastructure under Destructive Influences

Elena Maksimova [1], Maria Lapina [2] and Vitalii Lapin [3]

[1] *MIREA - Russian Technological University, Vernadsky ave, 78, Moscow, 119454, Russia*
[2] *North Caucasus Federal University, Pushkin St., 1, Stavropol, 355017, Russia*
[3] *Stavropol Regional Clinical Advisory and Diagnostic Center, Stavropol, 355000, Russia*

Abstract

The transition to the digital economy is not possible without considering the issues of creating a modern information infrastructure, which is confirmed by a number of documents adopted at the level of the President and the Government of the Russian Federation. One of the main problems in the implementation of these documents is associated with the creation of an effective system for managing the information infrastructure of state bodies, state institutions, Russian legal entities and (or) individual entrepreneurs who are subjects of critical information infrastructure (hereinafter – SCII). At the same time, the task facing the heads of the SCII, who in this case bear criminal responsibility for the low level of reliability of the subject, is associated with the creation of an effective management system for the operation of facilities of the CII.

The existing regulations of the regulators on the safety of the SCII fix the composition of the factors influencing the facilities of the SCII. Strict regulation in this matter increases the level of error in the complex assessment of information security (hereinafter – SCII) of the subject, therefore, leads to a decrease in the level of requirements already at the stage of categorizing objects.

The proposed solution is a synthesis of cognitive and logical-probabilistic approaches, taking into account destructive influences on the infrastructure in dynamics at all stages of the life cycle of a critical information infrastructure (hereinafter – SCII) objects.

Keywords

Information security, subject of critical information infrastructure, anthropomorphism, destructive influences, inter-object relationships, static model

1. Introduction

The legislation of the Russian Federation [1-5] defines the areas of functioning 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 the CII, are responsible for maintaining the stability of the area to which they belong.

One of the guarantors of stability and information security of society and the state as a whole is the reliability and security of SCII. Currently existing methods and models for assessing IS, as applied to SCII, are considered without taking into account the factors of destructive impact on SCII. This leads to significant errors in the analysis of the information security of the SCII, therefore, reduces the effectiveness of the information protection means declared for the facilities of the CII.

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia

EMAIL: maksimova@mirea.ru (Elena Maksimova), norra7@yandex.ru (Maria Lapina), vitlx@yandex.ru (Vitalii Lapin)
ORCID: 0000-0001-8788-4256 (Elena Maksimova), 0000-0001-8117-9142 (Maria Lapina), 0000-0002-0611-7002 (Vitalii Lapin)

2. Formulation of the problem

In the process of modeling the actions of an attacker, as a basis, for example, descriptive models of networks and attackers [6], structured description based on trees [7], object-oriented discrete event modeling [8], regulatory modeling [9], etc. are considered.

However, when building the SCII protection system, the algorithm of actions prescribed in [1] is used and does not take into account the "strength" of destructive influences as one of the significant indicators of a potential violator. In addition, the assessment of information security is often considered without considering infrastructure changes over time. Thus, the purpose of the study is to build a model for assessing the information security of the SCII through integrative components - models for assessing the reliability and security of the SCII, taking into account the destructive effects on the facilities of the SCII. At the same time, the subject of CII is considered within the framework of this study as a set of objects of CII, which are its structural components.

3. Models and Methods

The "input" research was carried out in the following directions: analysis of models and methods for assessing the reliability of the subject of CII, analysis of ways to increase the reliability of the subject of CII, analysis of existing software systems for assessing the reliability of technical systems, analysis of approaches to model development and assessment of destructive malicious influences.

The considered approaches to the development of a model and the assessment of destructive malicious influences (DMI) [10-15], despite their certain significance, do not fully describe the model of behavior and actions of the offender with any simple and understandable indicator convenient for further use in the assessment or the development of a set of protective measures. The methodology proposed below takes advantage of the strengths of existing algorithms, fills in the gaps and removes a number of assumptions that limit functionality during development, and introduces a reasonable quantitative value that characterizes the level of destructive impact of an intruder on the system.

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 "block - diagram" model), the logical - probabilistic method, the logical - probabilistic method. Failure tree model, Markov model. According to the criteria highlighted in the study, the probabilistic method (the “Block-diagram” model) was determined as the most effective.

Based on the results of the analysis of ways to improve the reliability of the functioning of the CII subject, the most effective and appropriate methods of redundancy are loaded and loaded redundancy.

In the study of software systems for assessing the reliability of technical systems, (Automated Calculation of Safety and Technical Risk) (PC ASM SZMA), ASONIKA-K, ASRN (2000, 2002), Isograph (England, USA), RAM Commander (Israel), Windchill Quality Solutions (Relex) (USA) were considered. In the course of the study, 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.

4. Description of the simulation system

To implement the modeling process, sub-objects are identified - inventory units of the CII subject. The reliability of the CII objects and the CII subject as a whole depends on their reliability of functioning.

In order to reduce the error in the assessment of information security, the life cycle of the subject of CII was determined and analyzed in accordance with GOST 34.601-90 [16]. On the basis of the "Life Cycle of the information security information system of the CII subject", the types of destructive influences leading 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 cybercriminals 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 of the subject of the CII; 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 at SBCII and PSBCII; Destr 7 - Errors in the technical design; Destr 8 - Errors entering SBCII and PSBCII; Destr 9 - Errors while accompanying the CII subject [17].

Vulnerabilities of typical APCS, GIS, ISPDN, KIS are analyzed by the method of constructing vulnerability trees. The relationship between the selected destructs and a number of vulnerabilities has been revealed [14-15]. Destructions Destr 0, Destr 1, Destr 2, Destr 3, Destr 4, Destr 5, Destr 6, Destr 7 are associated with the vulnerability of lack of compliance with information security requirements in the design of information security system 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 possibility of affecting the rest of the system, as well as the cancellation of such access at the end of work; lack or insufficient level of knowledge in the field of information security among the maintenance personnel; long service life of vulnerable components caused by the complexity of upgrading equipment and systems.

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

When assessing the reliability of SCII, the indicators of the reliability of recoverable and non-recoverable objects are assessed. For recoverable ones - mean time between failures, mean time between failures, probability of recovery, mean time to recover, availability factor, coefficient of technical utilization. For non-recoverable ones - the probability of failure, the probability of failure-free operation, the time of failure-free operation, the intensity of failure.

5. Discussion

The subject of CII is a complex, multicomponent system [16-30]. It can be viewed from the point of view of different approaches. For example, when conducting a comprehensive assessment of the IS of a CII subject, the assessment of the security of the IS - CII objects, which, in turn, can be considered as economic systems, is taken into account.

Another indicator when analyzing the functioning of a CII subject is reliability. In [21], mathematical support for the analysis of the reliability of network ICs is proposed. This apparatus can also be used in the study of CII objects. As a model of a network IS, a graph representation is used, based on the formalization of the description of the graph by bracketed projections. Based on the resulting combination of projections, obtained as a result of the cutting algorithm implementation, a probabilistic reliability function is constructed.

Comprehensive information security of a CII subject is also an example of a socio-technical system [22] operating under conditions of uncertainty. Thus, taking into account the peculiarities of poorly formalized processes occurring in socio-technical systems, in particular, in the system for assessing the information security of a CII subject, it was decided to use the methods of cognitive and logical-probabilistic modeling.

To assess the IS SCII, it is proposed to consider the cognitive model for assessing the security of the SCII as a base one, where one of the influencing factors - the reliability of the SCII is the result of the work of the logical-probabilistic model.

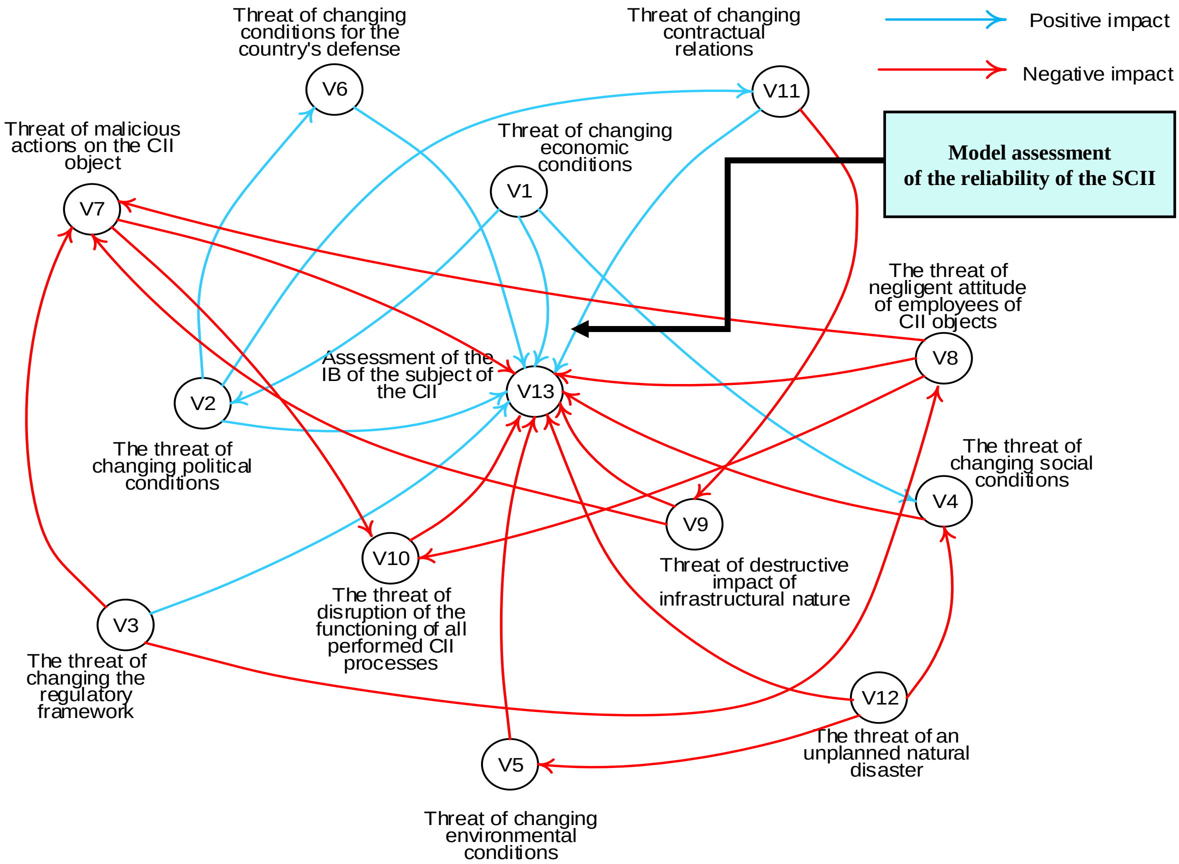
Positive impact
Negative impact
Model assessment of the reliability of the SCII
Threat of changing conditions for the country's defense
V6
Threat of changing contractual relations
V11
Threat of malicious actions on the CII object
V7
Threat of changing economic conditions
V1
The threat of negligent attitude of employees of CII objects
V8
Assessment of the IB of the subject of the CII
V13
V2
The threat of changing political conditions
The threat of changing social conditions
V4
V9
Threat of destructive impact of infrastructural nature
V10
The threat of disruption of the functioning of all performed CII processes
V3
The threat of changing the regulatory framework
V12
The threat of an unplanned natural disaster
V5
Threat of changing environmental conditions

Figure 1: Synthesis of a cognitive map for assessing the IS of the subject of CII under destructive influences with a logical-probabilistic model for assessing the reliability of the CII

The main sources of risk factors in the activities of CII subjects for building a cognitive model are presented in accordance with the Decree of the Government of the Russian Federation of February 8, 2018 No. 127 "On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of critical information infrastructure of the Russian Federation. Federation and their meanings (as amended on 13.04.2019). In addition, the target vertex V13 "Information security of the CII subject" has been introduced into the cognitive model, according to the results of the work in which the impact of DMI on the information security of the CII subject will be assessed.

In the course of modeling, a cognitive map is built for assessing the IS of the subject of CII under destructive influences (Figure 1). For a deeper analysis of the model in the form of a weighted digraph, an algorithm is built for the influence of changes in the values of one vertex on the values of other vertices.

This algorithm is based on the idea of an impulse process proposed by F.S. Roberts. Its essence lies in the fact that an external disturbance is introduced into some vertex of the analyzed graph.

The algorithm for the development of the impulse process can be represented by the following matrix formula:

$$V\_((t)) = V\_((initial)) + P_0*(I+A+A^2+\cdots+A^t),$$

where V_((initial)) – initial state vector; P_0 – initial impulse; A – adjacency matrix; I –identity matrix of size n×n.

Evaluation of DMI is implemented in the module for categorizing the attacker in the model of cognitive assessment of information security of the subject of CII under destructive influences (Figure 2). A methodology is proposed to implement this assessment.

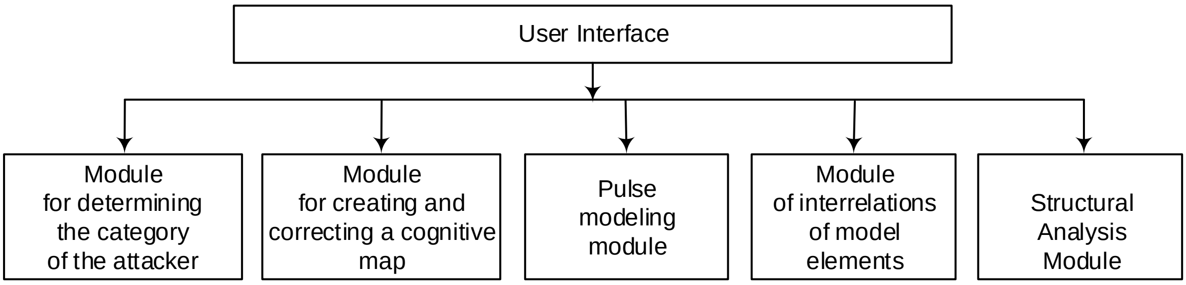
User Interface
Module for determining the category of the attacker
Module for creating and correcting a cognitive map
Pulse modeling module
Module of interrelations of model elements
Structural Analysis Module

Figure 2: The architecture of the model for assessing the information security of the subject of CII under destructive influences

Thus, when modeling the actions of an IS intruder, a formalized model is built that takes into account the parameters (potential) of the intruder in the space of his destructive effects on CII objects. The result of modeling here is a five-level model of an IS intruder's access to information and (or) to the components of CII objects at the level of physical access (PhL), logical access (LogL), competencies (C) of the intruder, equipment (A) of the intruder, motivation (M) of the intruder ... The access levels are determined according to the RF Resolution No. 127 (as amended on 13.04.2019).

The capabilities of the intruder at the designated levels of access to information and (or) to the components of CII objects determine the basic potential (Pt〗 _BASE), which the IS violator possesses on the CII subject. The basic potential is used to build a model of IS threats in terms of assessing the likelihood of their implementation. The preliminary basic potential of the offender is assessed on the basis of the numerical values of the levels of competence and equipment.

Based on the above, we will present a five-level model of an IS intruder's access to information and (or) to the components of CII objects as:

P_{hL}: [x]/Log_L: [x]/C: [x]/A: [x]/ /M: [x],

where [x] – the value of the corresponding parameter.

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:

$$F = F(P_{thr}, P_{rel_i})$$

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

$$P_{thr} = P_{Destr_i} \vee P_{exp}$$

where P_{Destri} – 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 the implementation of threats.

In the model for assessing, the reliability of the subject of CII P_{Destri} 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. Wherein

$$P_{Destr_i} = \{P_{Destr2}\ PDestr10\ if\ the\ destruct\ is\ related\ to\ infrastructure\ errors\ \ P_{Destr_i},\ if\ i \neq \{2, 10\}$$

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.

Probability of failure-free operation of CII facilities P_{reli} depends on the probabilities of failure-free operation of CII subobjects and their interconnections:

$$P_{rel_i} = P(InvU_1, InvU_2, InvU_3, InvU_7, InvU_9)$$

where InvU1 – APM; InvU2 – server; InvU3 – ACO; InvU7 – channels of connection; InvU9 – CII sub-object, specific for each individual CII subject.

To calculate the assessment of the reliability of the P_{reli} CII facilities, three cases were considered, where pi – probability of failure-free operation of CII subobjects:

$$P_{rel_i} = \begin{cases} \prod_{i=1}^{n} p_i\,(t), for\ a\ circuit\ with\ a\ series\ connection\ of\ n\ dependent\ CII\ subobjects \\ 1 - \prod_{i=i}^{n} (1 - p_i\,(t)), for\ a\ parallel\ circuit, n\ depends\ of\ number\ of\ CII\ subobjects \\ \bigvee_{i,j} (\prod_{i=1}^{n} p_i\,(t), (1 - \prod_{j=i}^{k} (1 - p_j\,(t)))), for\ serial - parallel\ circuit \end{cases}$$

Assessment of the reliability of the subject of CII Psubj 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, a structural diagram of the interconnection of the CII objects is formed and, based on the probabilities of the failure-free operation of the CII objects and the probability of the implementation of threats, an assessment of the reliability of the CII subject is calculated.

$$P_{subj} = P_{rel_i} * (1 - P_{thr})$$

Assessment of the reliability of the CII, when using the methods of redundancy in order to increase the reliability of the subject of the CII, the following methods and calculations are used to reserve the subobjects of the CII, where pi – probability of failure-free operation of CII subobjects:

$$P_{subj} = \begin{cases} 1 - (1 - P)^{k+1} = 1 - (1 - \prod_{i=1}^{n} P_i(t))^{k+1}, & (1) \\ \prod_{i=1}^{n} (1 - (1 - P_i(t))^{k+1}), & (2) \\ 1 - \frac{1}{(K+1)!} \prod_{i=1}^{k+1} (1 - P_i\,(t)), & (3) \end{cases}$$

Here 1 – when using loaded redundancy - for a system with a serial connection of n subobjects with a general redundancy with a multiplicity of k,

2 – when using a loaded redundancy - for a system with a serial connection of n objects with a separate redundancy with a multiplicity of k,

3 – when using an unloaded redundancy - systems with unloaded redundancy of multiplicity k (all subobjects are k + 1).

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 CII subject after reservation.

6. Experimental research

At the first stage, the assessment of the reliability of the CII subjects operating in various industries, including various types of CII objects, was carried out. The problem being solved is to increase the reliability of the CII subject, if the initial assessment of the reliability of the CII subject is less than the permissible one. 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.

At the second stage, experimental studies were carried out on:

- study of the influence of the destructive influences of an intruder with a low potential on the assessment of the IS of the CII subject, consisting of an object - IS with 1 category of significance;
- study of the influence of destructive influences of an intruder without potential and with high potential on the assessment of IS of a CII subject, consisting of an object - IS with 3 categories of significance and ACS - 2 categories of significance with destructive influences of an infrastructural nature;

- the study of the impact of destructive influences of violators with high, medium and low potentials on the assessment of IS of the subject of CII, consisting of objects: IS of the 2nd category of significance, ITS - 1 category and ACS - 3 categories of significance with destructive influences of an infrastructural nature.

The analysis of the results of the first stage of experimental studies using the example of SCII-Hospital is presented in table 1. The results of stage 2 are in table 2.

Table 1
Analysis of the results of the experimental study "Subject CII - Hospital"

Subject CII - Hospital		
Assessment of the reliability of the object		
Object	Reliability assessment before redundancy	Post-redundancy reliability assessment
personal data information system	0,69	0,89
Assessment of the reliability of the subject of CII		
Subject	Reliability assessment before redundancy	Post-redundancy reliability assessment
Hospital	0,43	0,56
Reliability win rate		
Reliability win rate	0,77	

Table 2
The results of the experimental study (stage 2) of the model for assessing the IS of the subject of CII under destructive influences

№ Exp. (2 step)	Vertex - source	Vertex recipient – V7		Tracked vertex	Experi-ment result	IS assess-ment of the subject of CII	Result repeated experiment taking into account recommen dations	Information security assessment subject after applied recommen-dations
		An object/ object category	Category					
1	HIGH	IS-1	LOW	V13	–0,45	A significant level of reduction in the IS of the subject of the CII relative to the initial	0,55	Average level of IS
2		IS-3	ABSENT		–0,39		0,71	Average level of IS
		ASU-2	AVERAGE					
3		ITS-1	AVERAGE		–0,40		0,8	High level of IS
		IS-2	AVERAGE					
		ASU-3	ABSENT					

7. Analysis of the results of the experimental study

The use of the developed model made it possible to assess the IS of the subject of CII under destructive influences, taking into account the indicator of the infrastructural component - the reliability of the CII. The synthesis of models made it possible to categorize the attacker, build a cognitive map for assessing the IS of the CII subject, simulate the DMI through various vertices-sources, and provide recommendations for increasing the level of the IS of the CII subject.

The proposed model can become an active assistant for the owners of CII facilities in the process of solving practical problems at all stages of the SCII life cycle. For regulators, the proposed approach to assessing the IS SCII will increase the reliability of the data provided by the owners of the objects of CII facilities at the categorization stage.

8. Conclusions

The proposed model is related to the use of:

- specifics of the regulatory and legal framework in the field of SCII safety,
- structured detailing of the CII subject, taking into account the specifics of the subject,
- stages of the life cycle of the SCII information protection system,
- highlighted destructive malicious influences of an infrastructural nature,
- the relationships between the selected destructs and a number of vulnerabilities on CII objects,
- factors affecting the decrease in the reliability of the functioning of the CII subject,
- evaluating the reliability indicators of recoverable and non-recoverable objects, backup methods and allows you to perform a comprehensive assessment of the information security of the subject of CII.

9. Acknowledgments

The reported study was funded by Russian Ministry of Science (information security, project №3)

10. References

[1] On the security of the critical information infrastructure of the Russian Federation: Federal Law of July 26, 2017. N 187-FZ (as amended and supplemented) [Electronic source]. - URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

[2] On the 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 N 239 (as amended and supplemented) [Electronic source]. - URL: https://fstec.ru/en/53-normotvo.

[3] On the approval of requirements for the creation of security systems for significant objects of critical information infrastructure of the Russian Federation and ensuring their functioning: Order of the FSTEC of December 21, 2017 N 235 [Electronic source]. - URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-.

[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 critical information infrastructure of the Russian Federation: Order of the FSB of Russia dated June 19, 2019 No. 282 [Electronic source]. - URL: https://www.garant.ru/products/ipo/prime/doc/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 No. 367 [Electronic source]. - URL: https://www.garant.ru/products/ipo/prime/doc/71941504/.

[6] Yuill J., Wu F., Settle J., Gong F., Huang M. Intrusion-detection for incident-response, using a military battlefield-intelligence process. Computer Networks. 2000; 34 (4): 671-697. DOI: 10.1016 / S1389-1286 (00) 00142-0

[7] Jha S., Sheyner O., Wing J.M. Minimization and Reliability Analyses of Attack Graphs. CMU-CS-02-109. Pittsburgh: School of Computer Science Carnegie Mellon University, 2002.

[8] Chi S.-D., Park J.S., Jung K.-C., Lee J.-S. Network Security Modeling and Cyber Attack Simulation Methodology. Proceedings of the 6th Australasian Conference on Information Security and Privacy on Information Security and Privacy, 11-13 July 2001, Sydney, Australia. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer; 2001.vol.2119. DOI: 10.1007 / 3-540-47719-5_26

[9] The basic model of threats to personal data during their processing in personal data information systems. Moscow, 2008. URL: https://fstec.ru/component/attachments/download/289 (date of treatment 10/29/2020)

[10] State Technical Commission of Russia. Guidance document. Protection against unauthorized access to information. Terms and Definitions. M: Military publishing house, 1992.

[11] Methodological recommendations for the development of regulatory legal acts that determine threats to the security of personal data, relevant when processing personal data in personal data information systems used in the implementation of relevant activities. No. 149/7/2 / 6-432. from 03/31/2015.

[12] Boyarintsev A.V., Nichikov A.V., Redkin V.B. General approach to the development of models of intruders // Security Systems. 2007. No. 4. P. 50-53.

[13] Spivak A.I. Evaluating the effectiveness of an attacker's attacks in the process of constructing his model // Scientific and technical bulletin of the St. 2010. No. 2 (66). P. 108-112.

[14] Zhukov V.G., Zhukova M.N., Stefarov A.P. Model of the violator of access rights in an automated system // Software products and systems. 2012. No. 2 (98). P. 75-78.

[15] Savchenko S.O., Kapchuk N.V. Algorithm for constructing a model of an intruder in an information security system using game theory // Dynamics of systems, mechanisms and machines. 2017.Vol. 5. No. 4.P. 84–89. DOI: 10.25206 / 2310-9793-2017-5-4-84-89

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

[17] Maksimova E.A. Assessment of information security of a subject of critical information infrastructure under destructive influences [Text]: monograph / E. A. Maksimova; Feder. state ed. educated. institution of higher. education "Volgogr. state un-t ". - Volgograd: VolGU Publishing House, 2020. -- 95 p.

[18] Maksimova E.A. Research of algorithms for secure data transmission 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. P. 157-163.

[19] Maksimova E.A., Shikhverdiyeva A.Sh. 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. P. 392-397.

[20] Baranov V.V., Maksimova E.A., Lauta O.S. Analysis of the model of information support of processes and systems in the implementation of multi-agent intelligent interaction // Pribory i sistemy. Management, control, diagnostics. 2019. No. 4. P. 32–41.

[21] E. Y. Kostyuchenko, L. N. Balatskaya, S. S. Kharchenko and M. A. Lapina Comparison of recognition using Google and Kaldi to solve the problem of assessing intelligibility. 2nd Scientific Conference on Fundamental Information Security Problems in terms of the Digital Transformation (FISP 2020) 30 November 2020, Stavropol, Russian Federation. – IOP Conference Series: Materials Science and Engineering, Vol. 873, 2021, 012032. doi:10.1088/1757-899X/1069/1/012032

[22] Gromov Yu.Yu., Eliseev A.I., Minin Yu.V., Sumin V.I. Reliability analysis in network information systems // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2018. No. 1. P. 33 P .41

[23] Parfenov, D.I., Bolodurina, I.P., Lapina, M.A. Development of a model for detecting security incidents in event flows from various components in a network of telecommunication service providers // IOP Conference Series: Materials Science and Engineering 2020, 873(1), 012020, https://doi.org/10.1088/1757-899X/873/1/012020

[24] Azhmukhamedov I.M. Management of poorly formalized socio-technical systems based on fuzzy cognitive modeling (on the example of integrated information security systems). Dis. ... doct. tech. sciences. Astrakhan: Astrakhan State Technical University, 2014

[25] Privalov, A.N., Bogatyreva, Y.I., Lapina, M.A., Lapin, V.G., Mysina, Y.A. Decision support information system for patient treatment procedures in hospital // CEUR Workshop Proceedings, 2021, 2914, pp. 441-448 http://ceur-ws.org/Vol-2914/

[26] Kostyuchenko, E., Rakhmanenko, I., Lapina, M. Evaluation of a method for measuring speech quality based on an authentication approach using a correlation criterion // 17th International Conference on Intelligent Environments, IE 2021 – Proceedings, 2021, 9486435

[27] Basan, A.S., Basan, E.S., Lapina, M.A., Lapin, V.G. Behavior-Based Assessment of Trust in a Cyber-Physical System. Communications in Computer and Information Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2021, 1395 CCIS, pp. 190-201, https://doi.org/10.1007/978-981-16-1480-4_17

[28] Petrenko V.I., Bereznitsky A.S., Ogur M. G., Nekrasova E.A. Judicial technical expertise methods for investigation of cybercrimes // IOP Conference Series. Materials Science and Engineering; Bristol 1069(1):012042 (March 2021). DOI:10.1088/1757-899X/1069/1/012042.

[29] E. A. Maksimova, M. A. Lapina, V. V. Baranov and O. S. Lauta The logical-probabilistic model for assessing the information security assessing of the critical information infrastructure subject under destructive influences. // IOP Conference Series: Materials Science and Engineering, Vol. 873, 2021, 012035. doi:10.1088/1757-899X/1069/1/012035

[30] Petrenko V.I., Ogur M.G., Zubkov M.V., Solgalova O.E. Using of live response technologies during the blocking of the attacks and investigation of incidents in real time // IOP Conference Series. Materials Science and Engineering; Bristol 1069(1):012042 (March 2021). DOI:10.1088/1757-899X/1069/1/012042