Method of instrumental estimation of critical information infrastructure under information technology interference

*Sergey G. Antonov[1], Ivan I. Antsiferov[1], Sergey M. Klimov[1]**
[1]4-th Central Research and Design Institute of the Ministry of Defense of Russia, Russian Federation, Korolyov
**klimov.serg2012@yandex.ru*

Sergey G. Antonov

Ivan I. Antsiferov

Sergey M. Klimov

Abstract. *The* **Aim** *of the paper is to develop a method enabling quantitative estimation of stability indicators of critical information infrastructure (CII) facilities under information technology interference (ITI) using testbed experimental research data. CII facilities include information and telecommunication networks (ITCN), information systems (IS), automated systems (AS) and telecommunication systems that are used as part of computer-based systems in transportation, energy, communications, navigation, manufacturing and other domains. For the purpose of this paper, the stability of CII operation shall be understood as the ability of CII facility elements to maintain operating parameter values within the specified limits within the specified time period when affected by intruders' ITI. Intruders' ITI is understood as intentional hardware and software interference that cause disruptions (blocking, distortion) of information computation processes in CII facilities within a specified period of time. The developed method is based on experimental research, accelerated testing methods and computational methods of estimation of CII facilities operational stability that were applied subject to the specificity of system analysis of the process of ITCN, IS and ACS operation under simulated intruder ITI. The method uses two primary types of indicators, i.e. the probability of faults and additional (artificial) faults in the course of data communication between CII facility elements caused by ITI, and the probability of faults and additional faults as the result of ITI in the course of information processing in CII facilities. The inclusion in the method of indicators for estimating additional faults due to ITI enables a priori analysis of rare and sudden events of CII facility operational stability disruptions. Subject to the obtained estimates, technical and organizational measures are substantiated for the purpose of neutralizing ITI against CII facilities. Applying the method requires the availability of trial sites for the purpose of estimating the stability and actual security of CII facilities that host the functional equivalents of CII facilities, ITI simulators, information security tools (IST) and computer incident recovery tools. The developed method enables estimating the values of stability indicators, i.e. probability of successful transmission of data between CII facility elements and probability of successful processing of information in CII facility elements affected by faults based on instrumental estimation of system elements' operation processes assessment under simulated ITI.*

Keywords: *information technology interference, critical information infrastructure facilities, faults, stability.*

For citation: *Antonov S.G., Antsiferov I.I., Klimov S.M. Method of instrumental estimation of critical information infrastructure under information technology interference. Dependability 2020;4: 35-41. https://doi.org/10.21683/1729-2646-2020-20-4-35-41*

Received on: *05.08.2020* / **Revised on:** *21.08.2020* / **For printing:** *18.12.2020*

Introduction

The development of critical information infrastructure (CII) facilities is characterized by fast deployment of new information technology of distributed collection, processing, storage and communication of significant amounts of heterogeneous data for the purpose of efficient management of industrial and manufacturing processes in various domains of human activities [13, 14].

A significant share of network protocols and data in CII facilities, standard settings of information security tools (IST) objectively cause a lot of vulnerabilities. The potential vulnerabilities in CII facility elements include the parameters of software vulnerability, dataware, telecommunication equipment, as well as the parameters of functional and network vulnerabilities.

The vulnerabilities in CII facility elements enable potential internal and external information technology interference (ITI) that reduces the operational stability of CII facilities [1, 2, 6, 12].

The paper examines ITI threats that are intentional hardware and software interferences that cause the disruption of the operational stability of CII facilities. An ITI is implemented by an intruder in the form of interrelated and multi-stage actions by means of fuzzing, Denial-of-Service attacks (DDoS attacks) and traffic load [7].

The consequences of a successful ITI against CII facilities are characterized by the following:

- unauthorized access to protected information in CII facilities;
- disruption of operational stability;
- faults and failures in the performance of information processing tasks;
- reduced rate of transfer of process-related information on the status of CII facility elements;
- blocking (disruption) of CII facilities networking;
- possible distortion of information critical for CII facilities application;
- initiation of undocumented features for the purpose of launching mass ITI against SMF CII facilities that are comparable to technological catastrophes in terms of their consequences.

In accordance with the existing requirements for information security, the protection of information in CII facilities is to involve operational stability under an intruder's ITI [10, 11, 13, 14].

Improving the operational stability of CII facilities under ITI requires prior experimental assessment of their actual security and stability using testbeds or trial sites [3, 4, 9].

Bed testing and actual security and stability assessment of CII facilities under ITI will ensure the preparation, selection of substantiated organizational and technical information security measures aimed at eliminating any vulnerabilities reducing the probability of ITI, which will allow improving the operational stability of CII facilities through the implementation of such measures.

Thus, the development of the method enabling improved operational stability of CII facilities under ITI by means of a priori assessment and multiple selection of organizational and technical information security measures, vulnerability elimination is relevant and of practical interest.

Problem definition

For the purpose of substantiating the instrumental estimation of CII stability under ITI and when affected by faults, the following assumptions were made:

- increased structural complexity, list, number of active tasks, simultaneous operation of subsystems of various generations, organization of information interaction between remote elements of CII facilities under ITI en able possible faults and require estimation for the purpose of maintaining the required level of stability of CII facilities;
- the random nature of detection of vulnerabilities by an intruder and ITI penetration of CII facilities causes the requirement for multivariate simulation of ITI threats;
- assessing CII facilities resilience against faults caused by ITI through analytical means only is complicated; a full-scale simulation of significant CII elements is required under conditions similar to actual processes of operation;
- instrumental estimation of CII facilities stability under simulated ITI is, in its nature, a verification, subject to the results of which it is established that the values of the probabilistic stability indicators in the presence of faults are not below the targets;
- in the course of instrumental estimation, accelerated testing of CII facilities is conducted at the trial site with the simulation of information loading modes that precipitate faults;
- given the CII facility information security measures taken, the values of the probability indicators of stable operation in the presence of low-intensity faults may be so low as to require significant system testing time, which underlines the importance of calculated prediction based on the instrumental estimation [8, 11, 13];
- the duration of instrumental prediction equals to the time required for an accurate estimation of the probabilistic indicators of CII facility stability under allowable values of time to fault [14];
- the use of an ITI simulator enables accelerated testing of CII facilities as part of instrumental estimation, as the testbed imitates factors of increased intensity of artificial faults (their increased probability) under CII facility overloading.

In a general way, the problem of CII facility stability estimation under ITI is defined as follows:

It is given:

w_{ac}, the number of actual faults in data transfer between CII facilities;

h_{ac}, the number of actual faults in information processing systems in CII facilities;

Δt_{DCM}, is the mean time of data transfer between CII facilities;

Δt_{HSS}, the mean time of information processing in CII facilities.

It is required:

to find such values of actual fault parameters in CII facilities: number w^*_{ad} of additional faults in the data communication network (DCN) , number h^*_{ad} of additional faults in the data processing system (DPS), time t^{FT*}_{DCN} of fault in the DCN and time t^{FT*}_{HSS} of fault in the DPS whereas the required values of the probability of stable operation are preserved

$$P^*_{SHSS} \geq P^{REQ}_{UHSS}\left[\left(w^*_{ac}, w^*_{ad}, t^{FT*}_{DCN}\right), \left(h^*_{ac}, h^*_{ad}, t^{FT*}_{HSS}\right), \left(\Delta t^*_{DCN}, \Delta t^*_{HSS}\right)\right]$$

subject to limited characteristic of data transmission and processing features in CII facilities:

$$\Delta t_{DCN} \in T_{DCN}, \Delta t_{HSS} \in T_{HSS}.$$

The problem was defined on the assumption that the CII operation is represented by Markovian processes, while the ITI processes that cause additional faults are described by a Poisson distribution.

Figure 1 shows the diagram of the instrumental estimation of CII facility stability under ITI. A fault in CII facilities will be understood as a short (from several seconds to 60 minutes accounting for the restoration time) disruption of the parameters of operation [1, 8, 14]. Due to the fact that the categorized CII facilities are of hazard to life and their disruption causes significant damage, the research assumes that in CII facilities failure is unacceptable. In other words, in case of ITI, events of disrupted CII facility operability of more than 60 minutes are neutralized by means of organizational and technical information security measures, operability restoration facilities and redundant elements.

Essentially, the presented method ensures confirmation of the compliance of the stability indicators of planned or upgraded CII facilities affected by faults caused by ITI with the customer's technical requirements.

For the purpose of collecting evidence of the compliance of the actual indicators of CII facility stability when

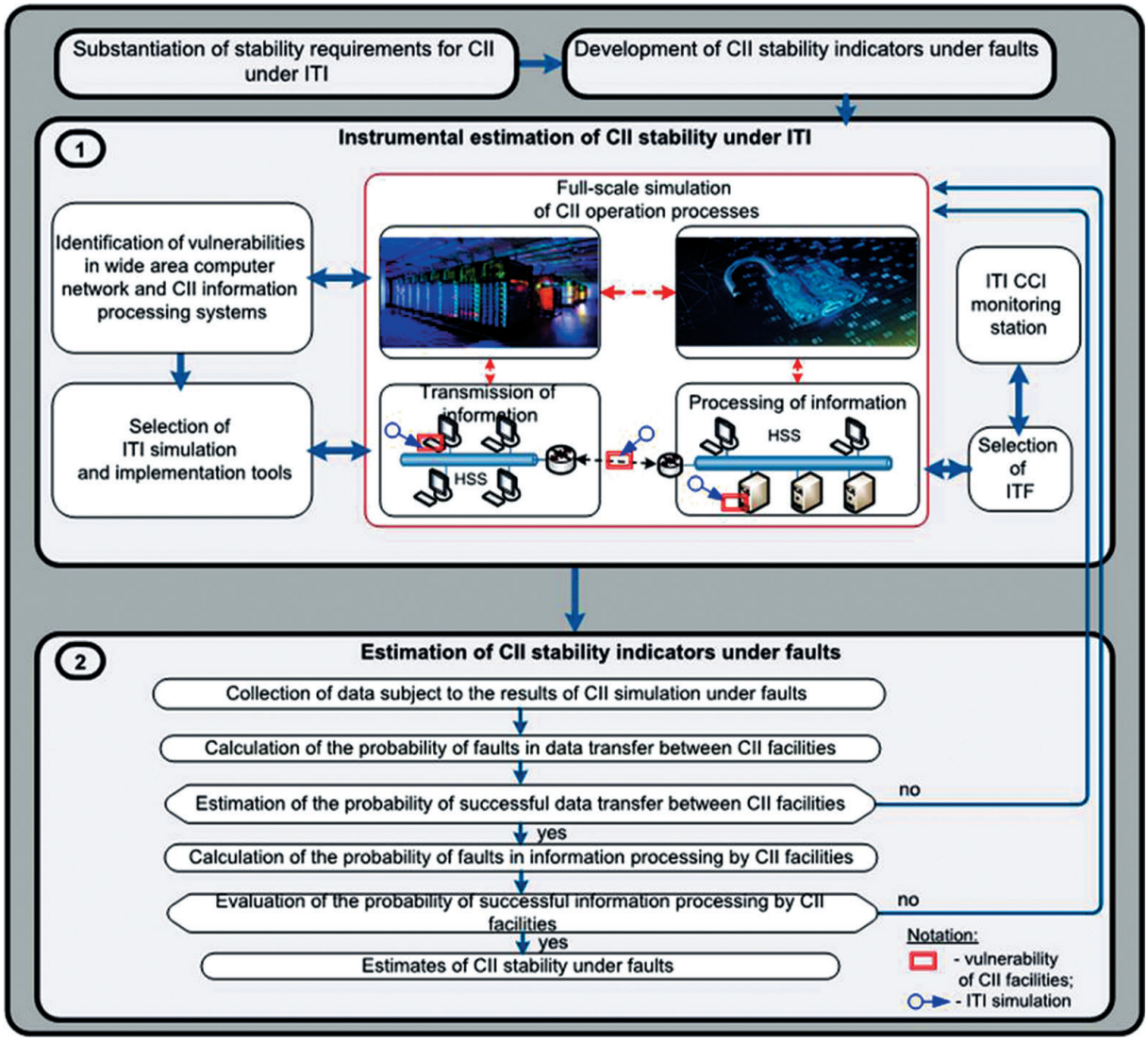

Fig. 1. Diagram of instrumental estimation of CII stability under simulated ITI

Table 1. Initial data for the estimation of the probability of successful transmission of data between elements of standard TCP/IP data communication features of CII facilities

Name of the characteristic of the processes of data transfer between elements of standard CII facility data communication assets affected by faults	Value of characteristic
Mean time of data transfer between elements of standard CII facility data communication assets	$\Delta t_{DCN} = 2, \ldots, 16$ sec
Number of additional faults in CII facility data communication assets under within 24 hours	$w_{ad} = 1, \ldots, 10$
Mean fault time in standard CII facility data communication assets	$t_{DCN}^{FT} = 2, 4, \ldots, 24$ hours

affected by faults with the obtained estimates, the method verifies the concordance between the results of full-scale modeling and trial site simulation and the estimates of the selected indicators.

The method involves a step-by-step sequence of indicator identification as part of instrumental estimation of the operational stability of CII facilities affected by faults that includes two primary stages:

I. Instrumental estimation of CII stability under simulated ITI.

II. Estimation of CII stability indicators under faults.

First, the requirements for stable operation of CII facilities affected by ITI are to be substantiated. Such requirements are to be included in the performance specifications for research and development activities regarding the CII facility (prototype, trial site of the CII facility) or taken into consideration while upgrading the CII facility's elements.

Then, in accordance with the method, the indicators are calculated for the instrumental estimation of CII facilities stability when affected by ITI.

Due to the fact that the operation of a CII facility is characterized by two primary processes: data communication between elements of a CII facility and information processing, it is proposed to use two indicators as part of the method:

1. Probability of successful data transfer between CII facilities.

2. Probability of successful information processing by a CII facility.

The instrumental estimation of the operational stability of a CII facility under simulated ITI is conducted using a test bed and consists in the following:

1. Full-scale simulation of the CII facility elements' operation processes on the test bed or at the trial site, including data communication between elements, as well as data processing in local area networks with hardware and software systems (HSS) in CII facilities.

2. Selection of information security tools in accordance with the requirements for the security class of automated systems (AS), computer technology, data security tools, intrusion detection tools, virus protection tools, firewalls, cryptographic tools, as well as the trust level of AS software [5].

3. Identification of vulnerabilities in a wide area computer network and HSS for model-based CII facility information processing [8].

4. Selection of ITI simulation and implementation tools using the method [9].

Output statistical data of the stage of instrumental estimation of CII facilities' stability under simulated ITI are the input parameters for the estimation of their stability in the presence of faults.

At the stage of estimation of the operation process stability of CII facilities under simulated ITI using the method of accelerated testing [14] the following assumptions were made:

a) CII facilities include two primary types of elements:

1) *j*-th data communication features of a CII facility, in which over time t_{DCFj} with the probability P_{DCN}^{FTAC} actual faults w_{acj} occur, and with the probability P_{DCN}^{FTAD} additional (artificially created) faults w_{adj} occur in case of ITI;

2) *i*-th data processing features of a CII facility, in which over time t_{HSSi} with the probability P_{HSS}^{FTAC} actual faults h_{aci} occur, and with the probability P_{HSS}^{FTAD} additional (artificially created) faults h_{adi} occur in case of ITI;

b) in the course of data communication and processing in a CII facility, each element performs a process-related operation in the course of which a fault may occur;

c) the probability of a fault in elements of a CII facility in the course of process-related operations is normally geometrically distributed that is approximated by the exponential distribution law [14];

d) the flow of fault events in data communication and processing elements of a CII facility is interpreted as a continuous Poisson flow.

The estimation of a CII facility's stability when affected by faults caused by ITI using the method of acceleration testing consists of the following steps:

Step 1. Collection of data subject to the results of CII facility ITI simulation, required and sufficient parameters for the estimation of CII facility stability when affected by faults.

Step 2. Calculation of the probability of faults in data transfer between CII facilities:

a) calculation of the probability w_{acj} of actual faults in the course of data transmission between CII facilities during time t_{DCNj} in the *j*-th data transmission facility:

$$P_{\text{DCN}}^{\text{FTAC}}\left(w_{acj}\right)=\prod_{j=1}^{k}e^{-t_{\text{DCN}j}^{\text{FT}}\,P_{\text{DCN}j}^{\text{FT}}/\Delta_{\text{DCN}}}\left(P_{\text{DCN}j}^{\text{FT}}\right)^{w_{acj}},\qquad(1)$$

where w_{acj} is the number of actual faults in the j-th data transmission facilities;

$t_{\text{DCN}j}^{\text{FT}}$ is the duration of a fault in the j-th data transmission facility;

$P_{\text{DCN}j}^{\text{FT}}$ is the probability of actual fault in the j-th data transmission facility;

Δt_{DCN} is the mean time of data transfer between CII facilities;

k is the number data transmission facilities.

b) calculation of the probability of w_{adj} additional (artificially created) faults in the course of data transmission between CII facilities during time $t_{\text{DCN}j}$ in the j-th data transmission facility:

$$P_{\text{DCN}}^{\text{FTAD}}\left(w_{adj}\right)=\prod_{j=1}^{k}e^{-t_{\text{DCN}j}^{\text{FT}}\,P_{\text{DCN}j}^{\text{FTAD}}/\Delta t_{\text{DCN}}}\left(P_{\text{DCN}j}^{\text{FTAD}}\right)^{w_{adj}},\qquad(2)$$

where w_{adj} is the number of additional faults in the j-th data transmission facility;

$P_{\text{DCN}j}^{\text{FTAD}}$ is the probability of additional fault in the j-th data transmission facility.

Step 3. Estimation of the probability of successful data transfer between CII facilities.

$$P_{\text{SDCN}}=\frac{1}{N_w}\sum_{j=1}^{N_w}U_{P_{\text{UDCN}}}\left(w_{acj},w_{adj}\right)\frac{\prod_{j=1}^{k}e^{-t_{\text{DCN}j}^{\text{FT}}\,P_{\text{DCN}j}^{\text{FT}}/\Delta t_{\text{DCN}}}\left(P_{\text{DCN}j}^{\text{FT}}\right)^{w_{acj}}}{\prod_{j=1}^{k}e^{-t_{\text{DCN}j}^{\text{FT}}\,P_{\text{DCN}j}^{\text{FTAS}}/\Delta t_{\text{DCN}}}\left(P_{DCNj}^{FT}\right)^{w_{adj}}},\qquad(3)$$

where N_w is the number of instrumental assessments done at the trial site with realization of fault vectors w_{acj} and w_{adj};

$U_{P_{\text{SDCN}}}\left(w_{acj},w_{adj}\right)$ is the indicator function that takes on the value of 1 if the event corresponds to indicator P_{SDCN}, and 0 if otherwise.

Step 4. Calculation of the probability of faults in information processing in a CII facility:

a) calculation of the probability of h_{aci} actual faults in the course of information processing in a CII facility over time $t_{\text{HSS}i}$ in the i-th HSS:

$$P_{\text{HSS}}^{\text{FTAC}}\left(h_{pi}\right)=\prod_{i=1}^{l}e^{-t_{\text{HSS}i}^{\text{FT}}\,P_{\text{HSS}}^{\text{FT}}/\Delta t_{\text{HSS}}}\left(P_{\text{HSS}i}^{\text{FT}}\right)^{h_{aci}},\qquad(4)$$

where h_{aci} is the number of actual faults in the information processing facilities;

$t_{\text{HSS}i}^{\text{FT}}$ is the duration of a fault in the i-th data processing facility;

$P_{\text{HSS}i}^{\text{FT}}$ is the probability of actual fault in the i-th data processing facility;

Δt_{HSS} is the mean time of information processing in CII facilities;

l is the number of the information processing facilities.

b) calculation of the probability of h_{adi} additional (artificially created) faults in the course of information processing in a CII facility over time $t_{\text{HSS}i}$ in the i-th HSS:

$$P_{\text{HSS}}^{\text{FTAD}}\left(h_{adi}\right)=\prod_{i=1}^{l}e^{-t_{\text{HSS}i}^{\text{FT}}\,P_{\text{HSS}i}^{\text{FTAD}}/\Delta t_{\text{HSS}}}\left(P_{\text{HSS}i}^{\text{FTAD}}\right)^{h_{adi}},\qquad(5)$$

where h_{adi} is the number of additional faults in the information processing facilities;

$P_{\text{HSS}i}^{\text{FTAD}}$ is the probability of additional fault in the i-th data processing facility;

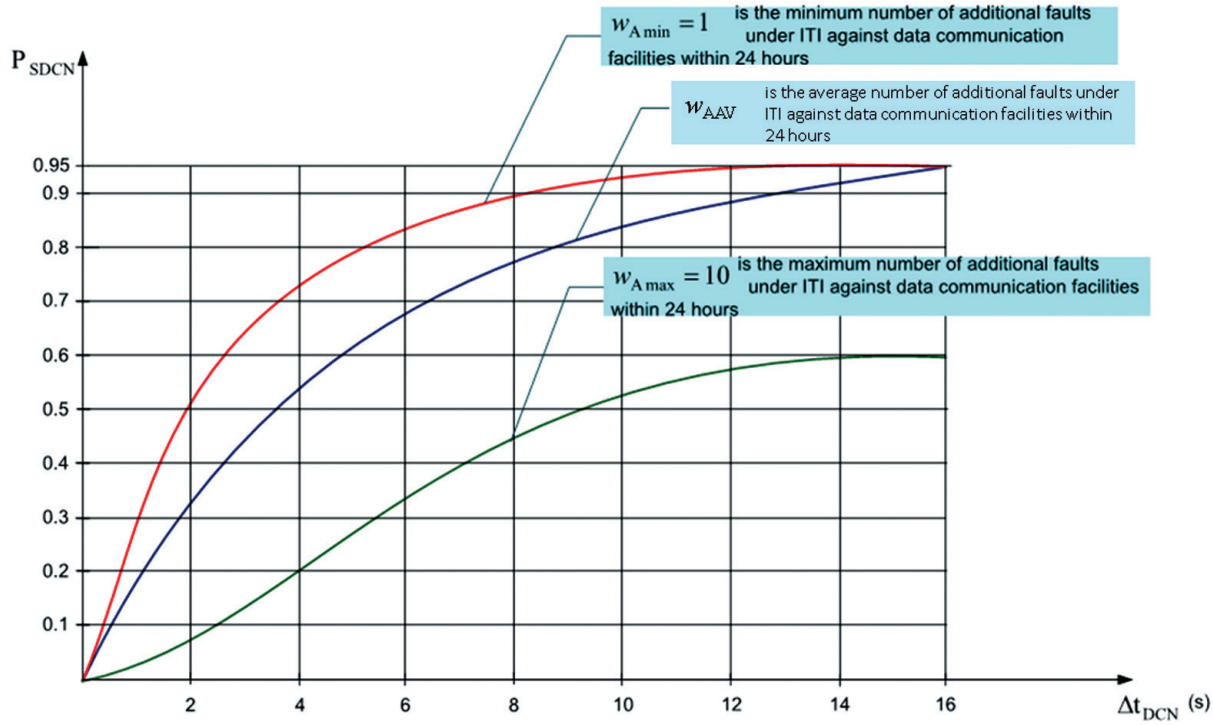

Fig. 2. Values of the probability of successful data communication between elements of data communication features of CII facilities under varying mean time of data communication and number of additional faults

Step 5. Evaluation of the probability of successful information processing by a CII facility:

$$P_{\text{SHSS}}=\frac{1}{N_h}\sum_{i=1}^{N_h}U_{P_{\text{SHSS}}}\left(h_{aci},h_{adi}\right)\frac{\prod_{i=1}^{l}e^{-t_{\text{HSS}i}^{\text{FT}}P_{\text{HSS}i}^{\text{FT}}/\Delta t_{\text{HSS}}}\left(P_{\text{HSS}i}^{\text{FT}}\right)^{h_{aci}}}{\prod_{i=1}^{l}e^{-t_{\text{HSS}i}^{\text{FT}}P_{\text{HSS}i}^{\text{FTAD}}/\Delta t_{\text{HSS}}}\left(P_{\text{HSS}i}^{\text{FTAD}}\right)^{h_{adi}}}, \quad (6)$$

where N_h is the number of instrumental assessments done at the trial site with realization of fault vectors h_{aci} and h_{adi};

$U_{P_{\text{SHSS}}}\left(h_{aci},h_{adi}\right)$ is the indicator function that takes on the value of 1 if the event corresponds to indicator P_{SHSS}, and 0 if otherwise.

Upon completion of steps 1 to 5 of the method, the set of estimates is prepared of indicators of CII facility stability when affected by faults.

As part of the research, a preliminary estimation was conducted of the probability of successful transmission of data between elements of standard TCP/IP data communication features of CII facilities (initial data shown in Table 1). The estimates of the effect of faults caused by ITI on the stability of elements of standard TCP/IP data communication features of CII facilities are shown in Figure 2.

The analysis of the values of the probability of successful data communication between elements of standard TCP/IP data communication features of CII facilities affected by faults under varying mean time of data communication and number of additional faults shows the following:

- the probability of successful data communication between elements of standard data communication features of CII facilities reaches 0.9 within 8 seconds under the minimal number of additional faults when affected by an intruder's ITI (1 fault per a 24-hour work period);
- the probability of successful data communication between elements of standard data communication features of CII facilities becomes 0.8 within 10 seconds under the average number of additional faults when affected by an intruder's ITI through the use of redundancy and recovery (5 faults per a 24-hour work period);
- the probability of successful data communication between elements of standard data communication features of CII facilities reaches only 0.6 within 16 seconds under the maximum number of additional faults when affected by an intruder's ITI even if computer incident recovery facilities are used (10 faults per a 24-hour work period).

In cases when an intruder's ITI are identified in a timely manner and neutralized by ISS at a CII facility, the functional stability of data communication facilities affected by additional faults is ensured.

Conclusion

The suggested method of instrumental estimation of CII facilities stability under an intruder's ITI allows estimating the values of stability indicators, i.e. probability of successful transmission of data between CII facilities and probability of successful processing of information in CII facilities affected by faults based on instrumental estimation of system elements' operation processes assessment under simulated ITI.

References

1. Antonov S.G., Klimov S.M. Method for risk evaluation of functional instability of hardware and software systems under external information technology interference. *Dependability* 2017;17(1):32-39.

2. Antonov S.G., Gordeev S.V., Klimov S.M., Ryzhov B.S. Models of threats of joint information-technical and information-psychological impacts in hybrid wars. *Informatsionnye voyny* 2018;2(46):83-87. (in Russ.)

3. Gapanovich V.A., Shubinsky I.B., Zamyshlyaev A.M. Risk assessment of a system with diverse elements. *Dependability* 2016;16(2):49-53.

4. Gapanovich V.A., Rozenberg E.N., Shubinsky I.B. Some concepts of fail-safety and cyber protection of control systems. *Dependability* 2014;2:95-100.

5. GOST R 56939-2016 Information protection. Secure software development. General requirements. (in Russ.)

6. GOST R 56546-2015. Information protection. Vulnerabilities in information systems. The classification of vulnerabilities in information systems. Moscow: Standartinform; 2015. (in Russ.)

7. Klimov S.M., Kupin S.V., Kupin D.S. Models of malicious software and fault tolerance of information communication networks. *Dependability* 2017;4:36-43. DOI: 10.21683/1729-2640-2017-17-4. (in Russ.)

8. Klimov S.M., Astrakhov A.V., Sychiov M.P. [Basic methods of computer attack reaction]. Moscow: Bauman MSTU; 2013. (in Russ.)

9. Klimov S.M., Astrakhov A.V., Sychiov M.P. [Basic processes of computer attack reaction]. Moscow: Bauman MSTU; 2013. (in Russ.)

10. Klimov S.M., Polovnikov A.Yu., Sergeev A.P. A model of function-level fault tolerance of navigation signals provision processes in adverse conditions. Dependability 2017;17(2):41-47.

11. Klimov S.M., Polikarpov S.V., Fedchenko A.V. Method of increasing fault tolerance of satellite communication networks under information technology interference. *Dependability* 2017;17(3):32-40.

12. Klimov S.M., Polikarpov S.V., Ryzhov B.S. et al. Procedure for assuring the continuity of critical information infrastructure under conditions of information influence. *Voprosy kiberbezopasnosti* 2019;6(34):37-48. (in Russ.)

13. Shubinsky I.B. [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016. (in Russ.)

About the authors

Sergey G. Antonov, Head of unit, 4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, e-mail: sergey_antonov_1960@mail.ru

Ivan I. Antsyferov, Researcher, 4-th Central Research and Design Institute of the Ministry of Defense of Russia, Korolyov, e-mail: antsiferov-ivan@mail.ru

Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4-th Central Research and Design Institute of the Ministry of Defense of Russia, Russian Federation, Korolyov, e-mail: klimov.serg2012@yandex.ru

The authors' contribution

Antonov S.G. Development of the diagram and description of the method of instrumental estimation of CII facilities stability under simulated ITI. Performance and analysis of the results of experimental estimation of the probability of successful transmission of data between elements of standard data communication features of CII facilities.

Antsiferov I.I. Mathematical problem description for the development of the method of instrumental estimation of CII facilities stability under ITI.

Klimov S.M. System analysis of the basic assumptions and development of mathematical expressions for calculating the probabilities of faults in the course of data communication between CII facilities and successful processing of information in the CII facility.

Conflict of interests

The authors declare the absence of a conflict of interests.