Original article
DOI: 10.21683/1729-2646-2017-17-1-32-39
Dependability, vol. 17 no.1 2017 УДК: 004.056.53

Method for risk evaluation of functional instability of hardware and software systems under external information technology interference

Sergey G. Antonov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Russia, Korolyov, e-mail: sergey_antonov_1960@mail.ru.*
Sergey M. Klimov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Russia, Korolyov, e-mail: klimov.serg2012@yandex.ru*


Sergey G. Antonov


Sergey M. Klimov

Abstract. *The aim of the article is to develop a method that would allow for a quantitative evaluation of stability risks of hardware and software systems under simulated information technology interference and simulation of real management process cycle. The article shows the relevance and importance of the methods for risk evaluation of hardware and software systems stability in the context of targeted and coordinated information technology interference. Information technology interference is understood as targeted and coordinated hardware and software, as well as software actions aimed at temporary disruption of operation or logical defeat of hardware and software systems. Successful information technology interference is conditioned by the presence of vulnerabilities in the hardware and software systems that include IP and MAC addresses and communication equipment ports available to the intruder. The method presented in the article is based on the following: risk evaluation is performed using a test bed or active facilities with the involvement of respectively a fixed and portable information technology measures simulation system. The risk of destabilization of hardware and software systems is evaluated experimentally as the combination of frequency and consequences of successful information technology interference. The preliminary risk evaluation allows choosing the solution for information protection in order to eliminate potential vulnerabilities. The residual risk is evaluated based on the ability of hardware and software systems to eliminate the consequences of information technology interference through various inbuilt resilience features. The research resulted in the proposed method of evaluation hardware and software system security risks under information technology interference as a logical sequence of steps: risk analysis of information technology interference; identification of vulnerabilities, simulation of system operation processes under information technology interference at the trial facility; selection of the best information protection and system fault tolerance facilities; preliminary an final evaluation of system stability risks. As part of the method, probability and temporal indicators of hardware and software systems stability risk evaluation were developed that enable analysis of recovery from threats of combined information technology interference, selection of rational information protection and fault tolerance measures. As part of the method, it is proposed to use a cubic analysis scheme of elimination of vulnerabilities of critical elements of hardware and software systems that allows identifying the levels of tolerable risk and levels of reference model of interaction of open systems required for elimination of vulnerability subject to the frequency of information technology interference. Additionally, a certificate of evaluation of stability risks of hardware and software systems subject to the frequency of successful interferences was developed. In the conclusion it is noted that the developed method allows using the knowledge regarding potential vulnerabilities and experimental studies to identify the probabilistic values of security risks in order to determine the most hazardous threats and adoption of respective information protection measures.*

Keywords: *hardware and software systems, information technology interference, stability risks, information protection and fault tolerance facilities.*

For citation: *Antonov S.G., Klimov S.M. Method for evaluation of risks of functional instability of hardware and software systems under external information technology interference. Dependability, 2017, vol. 17, no. 1, pp. 32-39. (in Russian). DOI: 10.21683/1729-2646-2017-17-1-32-39*

Introduction

A number of nations, as well as the hacker community are actively involved in the development of software designed for preparation, delivery and secret introduction of information technology interference (ITI) code (computer attacks) against automated process control systems in transportation, energy, telecommunications and other industries [4]. The basic elements of the above automated systems are hardware and software systems (HSSs) interconnected by communications equipment and distributed computer networks.

Currently, HSSs represent sets of information management facilities designed for real-time collection, processing, output of control information and information interaction

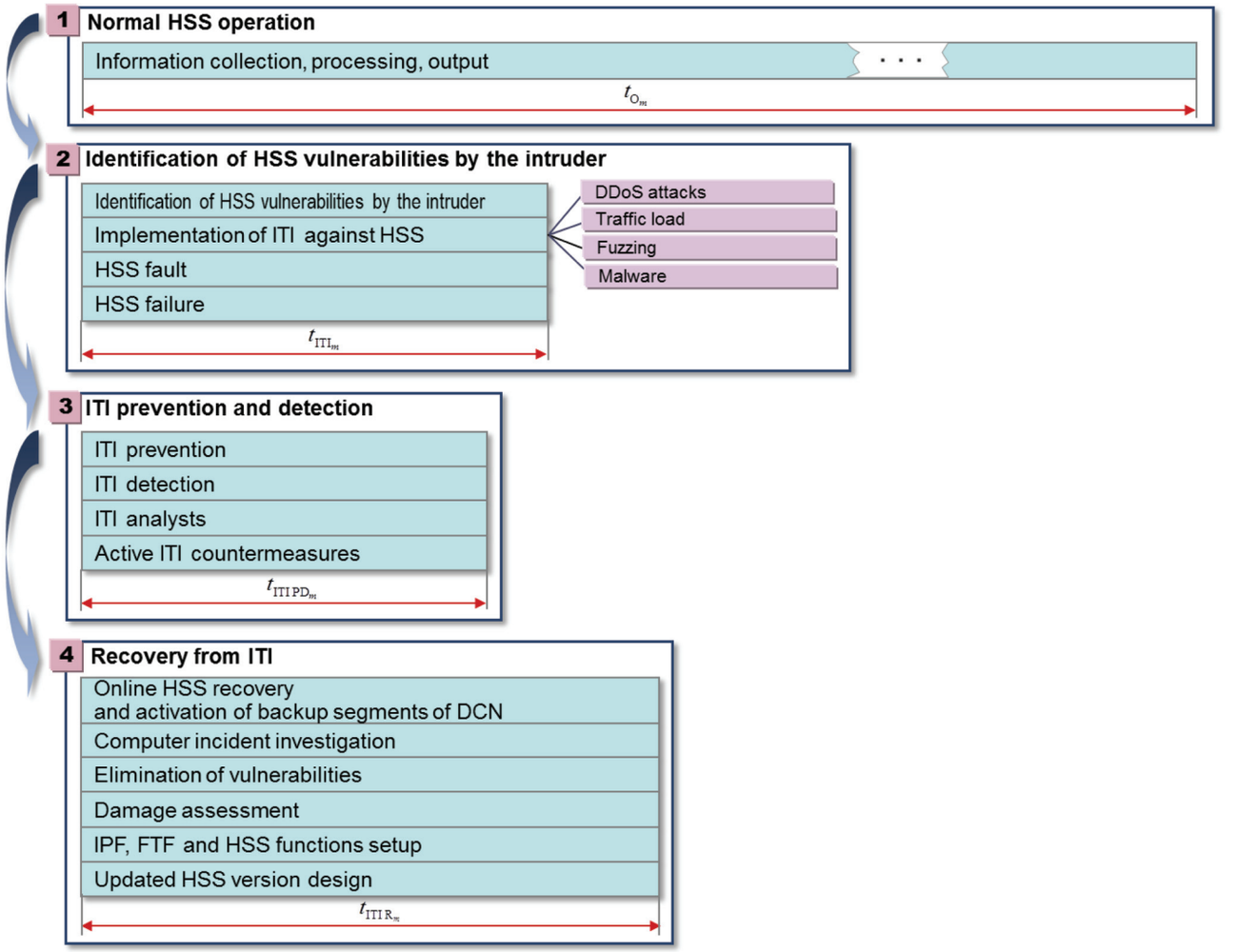


Figure 1. Time picture of HSS-based DCN operation processes under ITI

between control elements and data management centers. In this article H SSs are primarily regarded as complex and multifunctional sets of programs, while the technical equipment is regarded as the processing resource required for the execution of such programs.

HSS-based distributed computer networks (DCNs) are essentially critical distributed information management systems that can be targeted by intruders' ITIs.

ITIs are understood as targeted and coordinated hardware and software, as well as software actions aimed at temporary disruption of operation or logical defeat of HSSs. The above interferences can be considered a variety of malicious remote computer attacks against software, control processes, computer and telecommunications equipment of a HSS network [1].

The HSS components vulnerable to ITIs are accessible IP, MAC addresses and port numbers of communication equipment. The potential vulnerabilities of the considered HSSs are due to the following:

a) use of public TCP/IP data communication protocols; foreign-made backbone link equipment with potential undocumented capabilities and remote programmed control; untrusted hardware and software platforms (imported servers, e-mail software, self-updating operating systems or kernels);

b) possible unauthorized actions of internal intruders aimed at intentional or unintentional ITI;

c) uncoordinated and inadequate operation of diverse elements of information protection facilities (IPF).

As the above vulnerabilities condition the potential possibility of implementation of ITIs that could cause disruptions in HSS operation, the development of a method that would allow for a quantitative evaluation of HSS stability risks under simulated ITIs is of relevance.

Problem definition

The research is based on the following premises:

- risk assessment can be done on a test bed or active facilities using respectively fixed and portable ITI simulation systems;
- risk is evaluated experimentally based on the frequency of successful ITIs;
- preliminary risk assessment allows choosing an IPF solution to address potential vulnerabilities;

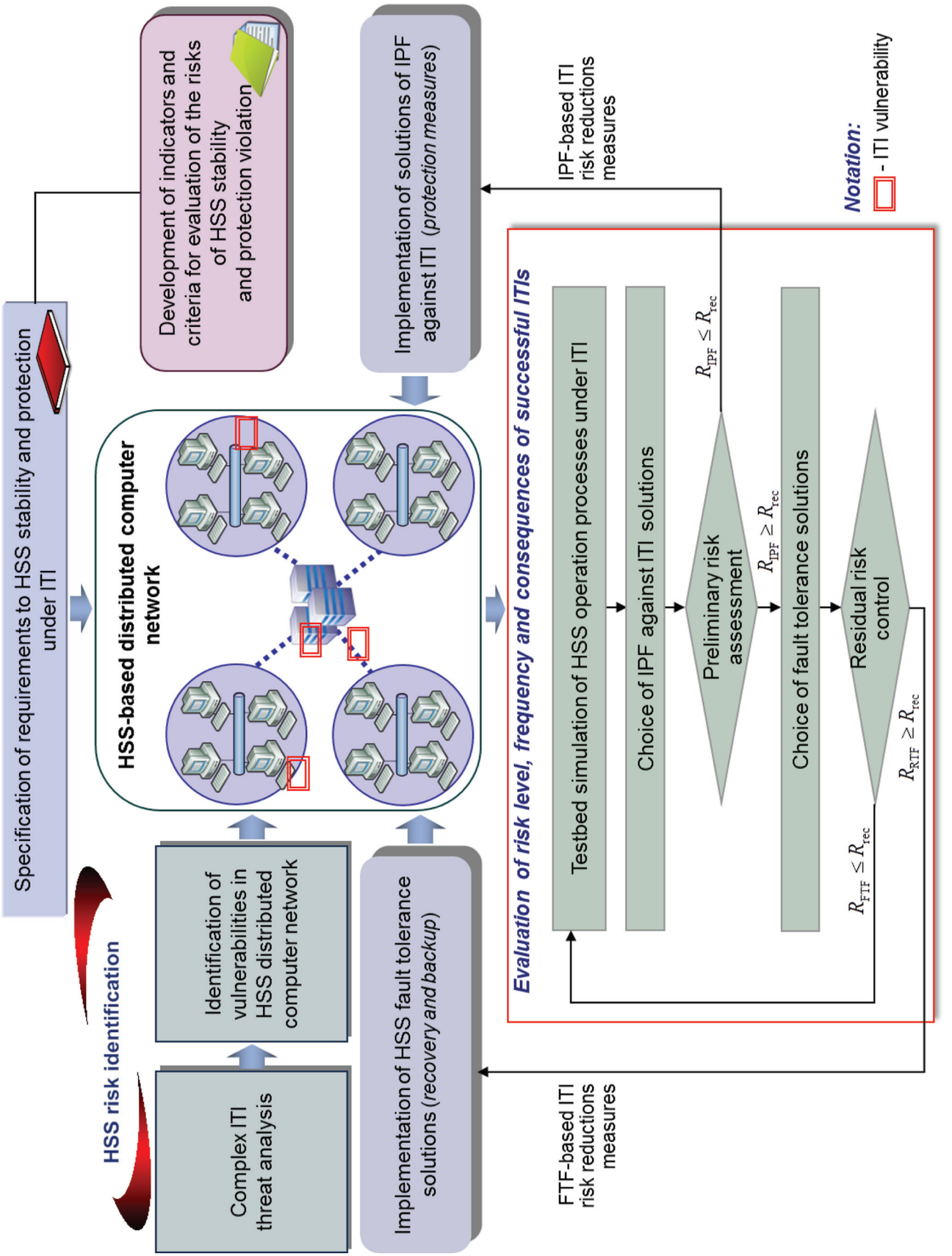


Figure 2. Evaluation scheme of HSS security risks under ITI

- the residual risk is evaluated by the ability of HSS to eliminate the consequences of ITI by means of fault tolerance facilities (FTF), i.e. HSS functions and elements recovery and backup facilities.

Figure 1 shows the time picture of the HSS-based DCN operation processes under ITI that are represented in seven standard periods.

The particular feature of ensuring operational stability of HSS under ITI consists in the fact that, in theory, a multitude of ITIs is supposed to be countered by the IPF. At the same time, in practice the IPF only record ITIs against HSS at best, while the task of ensuring the operability and restorability of the disrupted system remain unsolved. It should be noted that state-of-the-art ITIs, the so-called targeted computer attacks, are primarily intended for incapacitating HSSs by disrupting the probabilistic and temporal characteristics of their information processing policy. The consequences of a successful ITI against an HSS consist in short-time faults (from several seconds to 30 minutes) and failures (up to several hours) of HSSs.

The time taken to execute the information management functions of the HSS' special software (SSW) under ITI is the primary parameter of its operational stability.

The notations for Figure 1 are as follows:

t_{O_m} is the operation time of DCN with HSS; t_{ITI_m} is the duration of the intruder's ITI; $t_{PD\ ITI_m}$ is the time taken to prevent and detect the intruder's ITI; $t_{R\ ITI_m}$ is the time of ITI recovery.

Therefore, the total time of the control process cycle (CPC) of DCN with HSS under ITI can be defined with the formula:

$$t_{CPC} = \sum_{m=1}^{N} [t_{O_m} - (t_{ITI_m} + t_{PD\ ITI_m} + t_{R\ ITI_m})], \quad (1)$$

where $m=\{1, 2, \ldots, N\}$ is the natural integers.

An assessment of HSS risks under ITI involves the following:

1. Choice of assessed HSSs and definition of the detail of their characteristics evaluation within the CPC.
2. Simulation of a set of ITIs against HSS.
3. Identification of known and unknown ITIs in the context of the dynamic HSS operation process.
4. ITI analysis (parametric identification, cataloguing of signatures and updating of ITI database).
5. Choice of solutions for protection of information against ITI (ITI countermeasures) and HSS fault tolerance (recovery and backup).

While using state-of-the-art ITI counter-strategies and critical information systems risk management methods [1–3, 5–7], let us represent the method for evaluation of HSS security risks under ITI as the following sequence of steps (Figure 2):

1. Complex ITI threat analysis.
2. Identification of vulnerabilities of DCN with HSS.
3. Testbed simulation of HSS operation processes under ITI.
4. Choice of solutions for protection of information against ITI.
5. Preliminary assessment of the risk to HSS stability with the chosen IPFs (under the optimal solution for protection of information against ITI).
6. Choice of HSS fault tolerance solutions.
7. Residual risk control (final assessment) subject to the chosen HSS fault tolerance solution.

Table 1. Standard HSS vulnerabilities certificate

HSS vulnerability description elements	HSS vulnerability description
1. Name of vulnerability	Operator HSS vulnerability
2. Vulnerability identifier	HSS-2016-00007
3. Brief description of vulnerability	Vulnerability allows malicious HSS takeover
4. Vulnerability class	Windows OS vulnerability
5. Name of vulnerable element and its version	Version 10 e-mail modules
6. HSS data communication protocol	Data communication protocol, direct access to HSS controls
7. HSS hardware and software design details	Hardware and software platform is based on the client/server, hypervisor and software virtualization technologies, data communication protocol TCP/IP v.6, special software version 1.1
8. Type of defect	Operator authentication defects
9. Location of occurrence (manifestation) of vulnerability	Vulnerability exists due to the absence of legitimacy test of the source of HSS control
10. Defect type identifier	No data
11. Date of vulnerability detection	1.11.2016
12. Author of information on detected vulnerability	Information security unit
13. Means (rule) of vulnerability detection	Execution of step-by-step instructions
14. Vulnerability hazard criteria	Exceeding of specified risk probability value
15. Hazard level of vulnerability	High
16. Possible vulnerability elimination measures	Improvements to information protection facilities and HSS information interaction protocols
17. Additional information	A Juniper router is used in the network

Table 2. Certificate of evaluation of HSS stability risks under ITI

ITM frequency	ITM risk evaluation			ITM hazard rate
	I variant ***CADPF functions minimal***	**II variant** ***CADPF functions medium***	**III variant** ***CADPF functions maximal***	
Incredible event $P_{ITI} \leq 10^{-8}$ 1/h	Low	Low	Low	Minor
	Score: 3	Score: 3	Score: 3	Total score: 9
Possible event $P_{ITI} \leq 10^{-7}$ 1/h	Low	Medium	High	Tolerable
	Score: 3	Score: 5	Score: 7	Total score: 15
Probable event $P_{ITI} \leq 10^{-6}$ 1/h	Medium	High	High	Undesirable
	Score: 5	Score: 7	Score: 7	Total score: 19
Probability of event is high $P_{ITI} \leq 10^{-5}$ 1/h	Medium	High	Very high	Significant
	Score: 5	Score: 7	Score: 10	Total score: 22
Probability of event is very high $P_{ITI} \leq 10^{-4}$ 1/h	High	High	Very high	Intolerable
	Score: 7	Score: 7	Score: 10	Total score: 24
The event will certainly happen $P_{ITI} \leq 10^{-3}$ 1/h	High	Very high	Very high	Critical
	Score: 7	Score: 10	Score: 10	Total score: 27

The complex ITI threats to HSS include the following simulated effects:

- distributed denial of service (DDoS attacks);
- traffic load with data batches (multiple streams with standard data batches);
- fuzzing, i.e. exposure to non-standard (with distorted fields) data batches;
- secretly inserted and self-propagating malware.

Step 1. It is suggested to analyze complex ITI threats using a classification similar to the one suggested in [1], i.e. in terms of classification criterion of ITI effect on HSS. According to the above classification criterion let us identify ITIs of five types:

- functional disruption (fault or failure) of HSS;
- link disconnections in data communication channels;
- insertion of false information (distortion of information);
- information overloading of HSS;
- identification of zero day ITI vulnerabilities by means of fuzzing (multiple streams of semantically distorted data batches).

Step 2. Let us identify the vulnerabilities of DCN with HSS for the purpose of developing the ITI simulation model by using GOST R 56546-2015 "Information security. Vulnerabilities of information systems. Classification of vulnerabilities of information systems" and designing a standard HSS vulnerabilities certificate (Table 1).

The method assumes the presence of potential zero day vulnerabilities in the software design of data communication protocols, communications equipment, operating systems, device drivers and other HSS-based DCS components within 3-5% of all possible IP, MAC addresses and port numbers.

Step 3. Simulation of HSS operation processes under ITI involves using the specially equipped test bed to experimentally reproduce interrelated processes:

- normal operation of a segment of a distributed computer network with HSS;
- simulation of an intruder's ITI system;
- ITI counteractions based on various applications of IPF and FTF.

Modelling the above processes should allow experimental research and analysis of HSS network security under ITI. HSS network security is analyzed per seven levels of the reference model of interaction of open systems (RM IOS) by verifying the implementation of DCN security functions at each level. The most important aspect of evaluation of HSS security under ITI is to verify the access control to network services at the transport, session and network levels of RM IOS.

The level of detail of the HSS, ITI, IPF and FTF simulation models is to ensure reproduction of the main functions of risk objects, performance of a sufficient number of tests and generation of statistical data for risk assessment.

Step 4. To an array of chosen IPFs against ITI we'll ascribe the following:

- computer attack detection and prevention facilities (CADPF);
- firewalls (FW);
- false network information objects (FNIO);
- virus protection facilities (VPF);

- automated trusted loading modules (ATLM), identification and authentication of operators.

Let us assume that a DCN with HSS carries restricted access information. Then let us define that the proposed method considers IPF classes that ensure protection of restricted access information in DCN.

Step 5. Preliminary evaluation of risks of HSS stability with chosen IPFs.

The choice of measures and means of information protection against ITI must involve vulnerability diagnostics of network configuration and software, each of the IPFs for compliance with regulatory documents, as well as a general assessment. The input data for preliminary assessment of the risk to HSS stability with the chosen IPFs under ITI are as follows:

1. The probability of detection and identification of complex ITIs can take minimum (0,2–0,4), medium (0,5) and maximum values (0,7–0,9).

2. The probability of implementation of ITI against HSS can take minimum (0,2–0,4), medium (0,5) and maximum values (0,7–0,9).

3. The options of measures and means of information protection against ITI are finite (3 – 5 solutions) and are defined by the certified IPFs that can be used as part of HSS (subject to the nature of its hardware and software platform).

The control of the required level of HSS information protection under ITI is ensured by maintaining the value of probability of CPC performance over a given time (for near-rel-time systems) under ITI not lower than required (for instance, R_{rec}=0,95).

Complex ITIs disrupt HSS protection and primarily jeopardize the availability and integrity of information, data batch routing logic. An intruder carries out interference only if an HSS has vulnerabilities.

A preliminary assessment of the risk of HSS security violation involves experimental verification of the capability to ensure HSS and IPF elements functional stability against faults and failures under ITI.

It is assumed that ITI processes are independent and exponentially distributed. The probability of successful ITI conditions the risk of HSS faults and failures.

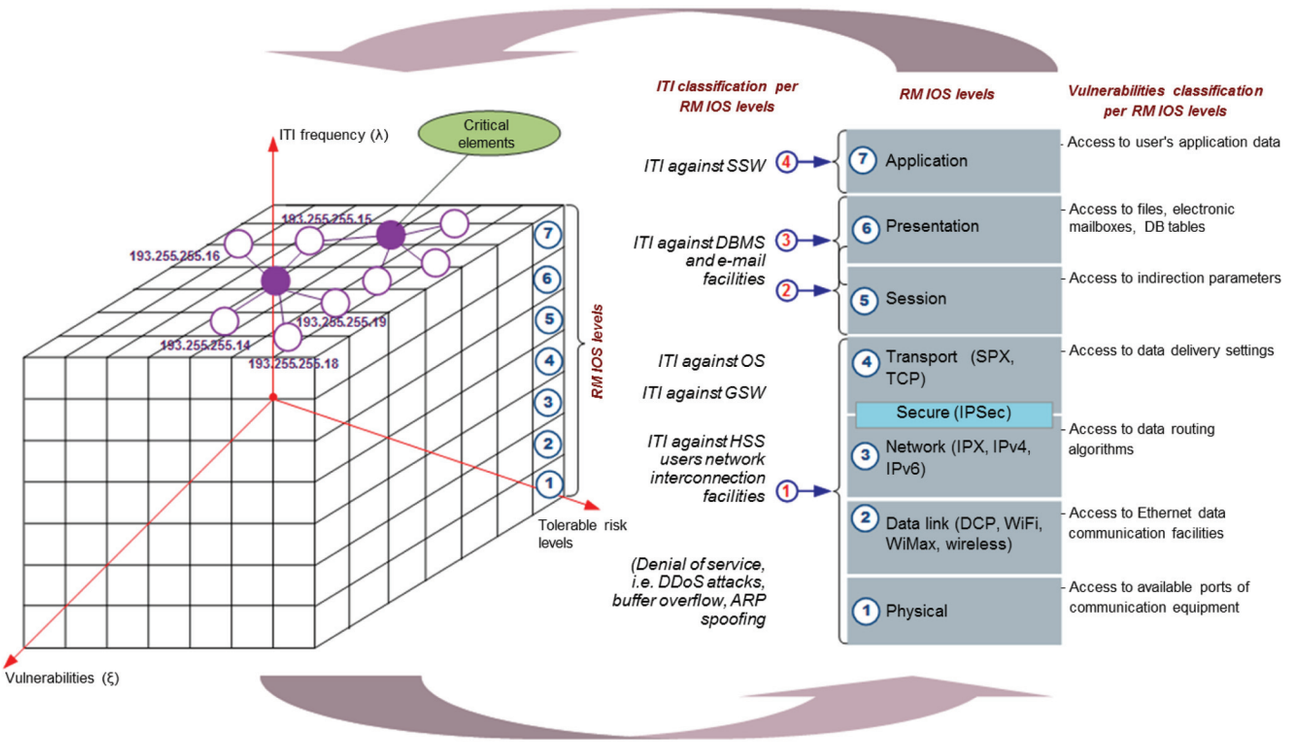
A preliminary assessment of HSS risks under ITI includes the following:

a) development of indicators for risk evaluation:

- probability (frequency) of successful ITI (according to Table 2), P_{ITI};
- probability of successful ITI countermeasures, P_{SCM};
- expected damage (levels of ITI consequences, Table 2) – Υ_i;
- the value of risk of HSS security violation due to ITI equals to the product of the probability of successful ITI ant the expected damage, R_{ITI_j};

b) choice of confidence interval (tolerability limits) of successful HSS-based ITI [5]:

- identification of confident probability:



Notations: *special software (SSW), database management system (DBMS), operating system (OS), general software (GSW), data communication protocol (DCP).*

Figure 3. Cubic analysis scheme of elimination of vulnerabilities of critical elements of HSS

$P_{ITI}(\varepsilon)=\beta=0{,}95$ is the maximum achievable value for HSSs of complex systems [2], where ε is a half of the length of the confidence interval;

- identification of HSS failure rate as a result of successful ITI:

$$\lambda_{ITI_i}=\sum_{i=1}^{m}\frac{n_{D\ HSS_i}}{N_{HSS_i}t_{ITI_i}}, \quad (2)$$

where λ_{ITI_i} is the average number of successful ITIs per time unit; $n_{D\ HSS_i}$ is the number of disrupted HSSs in DCN; N_{HSS_i} is the total number of HSSs in DCN; t_{HSS_i} is the duration of ITI; m is the number of tests;

c) identification of a potential risk value for HSS solution per correlation (of fault and failure rate as a result of successful ITI):

$$R_{HTB_i}^{ITTP}\left(t_{HTB_i}\right)=\left[\prod_{i=1}^{k}\left(1-e^{-\lambda_{HTB_i}t_{HTB_i}}\right)\right]\gamma_i, \quad (3)$$

where i is the HSS solution; γ_i is the magnitude of damage caused by ITI (identified from the total score in Table 2).

Calculating R_{ITI_j} follows the principle of the risk being as low as practically possible.

Step 6. Choice of HSS fault tolerance solutions based on redundancy (structural and functional redundancy) and recovery (time redundancy of process control cycles of DCN with HSS) using [1–3]:

a) the HSS fault tolerance based on recovery facilities (assuming that FTF ensures elimination of ITI consequences by recovering HSS) will be defined with the formula for probability of recovery:

$$P_{rec}^{FTF}\left(t_{rec}\right)=\frac{\mu_{R_i}}{\lambda_{ITI_i}+\mu_{R_i}}+\frac{\lambda_{ITI_i}}{\lambda_{ITI_i}+\mu_{R_i}}e^{-(\lambda_{ITI}+\mu_R)t_{rec}}, \quad (4)$$

where under condition of exponential law of distribution of ITI frequency and HSS elements recovery, μ_{R_i} is the HSS recovery rate based on the i^{th} HSS;

b) the HSS fault tolerance based on redundancy will be defined with the formula for availability factor:

$$K_{A_i}^{HSS}=\frac{1}{1+m\dfrac{\lambda_{ITI_i}}{\mu_{R_i}}}P_{adap}, \quad (5)$$

where m is the number of backup HSS elements in DCN; $P_{\text{adap}}>0{,}85$-$0{,}90$ is the probability of successful HSS adaptation to faults and failures after occurrence of ITI.

Step 7. Residual risk control (final evaluation) subject to the chosen HSS fault tolerance solution consist in the fact that for the chosen solutions and IPF against ITI, additional risk evaluations are performed that allow confirming that said measures and IPF allow reducing the risk to the tolerable level (as practically achievable).

The condition of minimization of residual risk of the chosen solution for HSS fault tolerance under ITI is considered the elimination of vulnerabilities that can be exploited for accomplishing the interference or the neutralization of ITI by means of coordinated application of IPF and FTF.

Figure 3 shows the proposed cubic analysis scheme of elimination of vulnerabilities of critical elements of HSS that allows identifying the levels of tolerable risk and levels of RM IOS required for elimination of vulnerability subject to the frequency of ITI.

The cubic scheme is used as follows:

a) one of the seven RM IOS levels is chosen (as an example, in the scheme the seventh level is chosen), at which the critical HSS elements are considered;

b) using Table 1, the facts of elimination or non-elimination of HSS vulnerabilities are established;

c) on the right-hand side of Figure 3 (ITI types corresponding to available network services at RM IOS levels) the possible ITIs for the respective level are chosen;

d) based on experimental data and Table 2, ITI frequencies are identified;

e) the tolerable risk for critical HSS elements is defined based on the mathematics:

$$R_{ITI_j}^{TR}\left(t_{ITI_j}\right)=\gamma_{HSS_j}\prod_{j=1}^{N_E}\left[1-P_{vul_j}\left(t_{ITI_j}\right)P_{ITI_j}\left(t_{ITI_j}\right)\right], \quad (6)$$

where t_{ITI_j} is the period of time of the j^{th} ITI implementation by the intruder; γ_{HSS_j} is the damage caused by the fault (failure) of a critical HSS element during the j^{th} ITI; N_E is the number of experiments; $P_{vul_j}\left(t_{ITI_j}\right)$ is the probability of vulnerability exploits over time t_{ITI_j}, identified by means of expertise or based on statistical data of HSS-based DCN operation; $P_{ITI}\left(t_{ITI_j}\right)$ is the probability of successful implementation of the j^{th} ITI over time t_{ITI_j} against a critical HSS element.

Let us evaluate the minimal possible risk of HSS destabilization under ITI using the Savage test:

$$R_{HSS}(t_{CPC})=\max_i \min_j R_{ITI_{ij}}(t_{CPC}), \quad (7)$$

where i is the fault tolerant DNS with HSS solution based on IPF and FTF; j is the successful ITI against HSS.

Conclusion

As the result of examination of HSS-based DNSs that can be targeted by ITIs, the article proposes a method to be used to evaluate actual level of protection of HSSs against ITIs that allows using the knowledge regarding potential vulnerabilities and experimental studies to identify the probabilistic values of security risks in order to determine the most hazardous threats and adopt respective information protection measures.

References

1. Klimov SM, Astrakhov AV, Sychiov MP. Tekhnologicheskiye osnovy protivodeystvia kompiuternim atakam. Elektronnoe ouchebnoe izdanie [Basic processes of computer attack reaction. Electronic study guide]. Moscow: Bauman MSTU; 2013. Russian.

2. Klimov SM., Astrakhov AV, Sychiov MP. Metodicheskie osnovy protivodeystvia kompiuternim atakam.

Elektronnoe ouchebnoe izdanie [Basic methods of computer attack reaction. Electronic study guide]. Moscow, Bauman MSTU; 2013. Russian.

3. Klimov SM, Astrakhov AV, Sychiov MP. Eksperimentalnaia otsenka protivodeystvia kompiuternim atakam. Elektronnoe ouchebnoe izdanie [Experimental evaluation of computer attack reaction. Electronic study guide]. Moscow: Bauman MSTU; 2013. Russian.

4. Ovchinsky VS. Novaya strategia kiberbezopasnosti SShA [The new US cyber security strategy]. Mezhdunarodny nauchno-analiticheskiy zhurnal Strategicheskie prioritety [Strategic Priorities International Scientific and Analytical Journal]. 2015; 4 (8): 41 – 48. Russian

5. Shubinsky IB. Strukturnaya nadiozhnost informatsionnykh system. Metody analiza [Structural dependability of information systems. Analysis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2012. Russian.

6. Shubinsky IB. Funktsionalnaia nadiozhnost informatsionnykh system. Metody analiza [Functional reliability of information systems. Analysis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2012. Russian.

7. Shubinsky IB. Nadiozhnie otkazoustoychivie informatsionnie systemi. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016. Russian.

About the authors

Sergey G. Antonov, Head of unit, 4th Central Research and Design Institute of the Ministry of Defence of Russia. 38/2 M.K. Tikhonravova Str., app. 176, 141092 mkr. Yubileyny, Korolyov, Moscow Oblast, Russia, phone: +7 (916) 788-57-92, e-mail: sergey_antonov_1960@mail.ru.

Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4th Central Research and Design Institute of the Ministry of Defence of Russia. 12 B. Komitetskaya Str., app. 105, 141092 mkr. Yubileyny, Korolyov, Moscow Oblast, Russia, phone: +7 (985) 928-13-55, e-mail: klimov.serg2012@yandex.ru.

Received on 22.12.2016