Original article
DOI: 10.21683/1729-2646-2017-17-3-32-40

Method of increasing fault tolerance of satellite communication networks under information technology interference

Sergey M. Klimov, *4-th Central Research and Design Institute of the Ministry of Defence of Russia, Russia, Korolyov*
Sergey V. Polikarpov, *4-th Central Research and Design Institute of the Ministry of Defence of Russia, Russia, Korolyov*
Andrey V. Fedchenko, *4-th Central Research and Design Institute of the Ministry of Defence of Russia, Russia, Korolyov*

Abstract. Aim. *The aim of the paper is to develop a method that would allow for integrated experimental, computational, analytical and expert assessment of the vulnerabilities of satellite communication networks, feasibility of information technology interference by intruders against such vulnerabilities and probability of fault tolerance under the chosen information protection solutions, trusted information technologies and fault tolerance sensors. The paper shows the relevance and importance of the method of increasing fault tolerance of satellite communication networks under information technology interference in service control channels and satellite equipment data. The authors examine targeted information technology interference that causes malfunction of satellite modems, control stations and connected user computer networks. The paper shows the unique nature of satellite communication networks operation due to the global operating range, availability of broadband radio signals from communication and retransmission spacecraft for technical analysis and processing within the operating range, potential possibility of unauthorized connection to communication services. The primary direction of development of procedural and process engineering guidelines on protection and fault tolerance of satellite communication networks are defined.* **Methods.** *A method has been developed that is based on three components: model of experimental identification of satellite communication network vulnerabilities; simulation, computational and analytical model of detection and identification of threats of information technology interference; decision-making algorithm for improvement of the fault tolerance of a satellite communication network under information technology interference. The model of experimental detection of satellite communication network vulnerability allows, as part of bench tests, establishing connections between existing vulnerabilities of the hardware and software of satellite modems, control stations, user networks and the potential information technology interferences by intruders. As part of the vulnerability model the authors describe the certificates of vulnerable radio technical and information technology parameters of the satellite communication network signals, as well as suggest an analytic expression for calculating the probability of detection of such network vulnerabilities. The paper presents a computational and analytical model of detection and identification of information technology interference threats as a structure of advanced means of detection, prevention and elimination of the consequences of information technology interference in satellite communication networks and the mathematical expression for identification of conditional probability of materialization of the threat of information technology interference in satellite communication networks. An algorithm is considered for improvement of fault tolerance of satellite communication networks under information technology interference, including preparation of parameters and evaluation of the fault tolerance of a satellite communication network, adjustment of the parameters of satellite communication network, information security facilities and fault tolerance sensors, situational adjustment of satellite communication network fault tolerance solutions.* **Conclusions.** *It is noted that the developed method enables improved fault tolerance of satellite communication networks under information technology interference based on a set of interconnected procedures of the model of experimental detection of satellite communication network vulnerabilities on testbed; simulation, computational and analytical models of detection and identification of information technology interference threats; application of the decision-making algorithm of improvement of satellite communication network fault tolerance.*

Keywords: *satellite communication networks, vulnerabilities, information technology interference, fault tolerance improvement, information protection facilities, trusted information technologies and sensors of fault tolerance.*

For citation: Klimov SM, Polikarpov SV, Fedchenko AV. Method of increasing fault tolerance of satellite communication networks under information technology interference. Dependability 2017;3: p. 32-40. DOI: 10.21683/1729-2646-2017-17-3-32-40.

Introduction

According to the Doctrine of Information Security of the Russian Federation dated December 5, 2016, one of the primary tasks of information security in terms of state and public security is the improvement of the protection of critical information infrastructure and its operational stability, development of the mechanisms of detection and prevention of information threats and elimination of their consequences.

The satellite communication networks are one of the most complex and still-developing facilities of critical information infrastructure with stricter requirements for security and resilience to information technology interference (ITI). For instance, information and telecommunication systems based on DVB-RCS services of interactive satellite communication of large amounts of data are actively developing [1].

In the process of development of advanced models and methods of ensuring resilience (survivability) of information communication networks under destructive information technology interference [2] the characteristics of interrelated evaluation of actual security and fault tolerance of SCN can be taken into consideration by means of the proposed method of improving SCN fault tolerance under ITI.

Targeted and massive ITI against data communication protocols are a threat to the security and functional stability of SCN, which determines the requirement for the development of methods and facilities for detection, prevention and elimination of the consequences of such information technology threats based on improved fault tolerance of such networks [3, 5].

Currently, the most dangerous are those ITI that secretly penetrate, propagate, cause faults (failures) and damage to information technology resources of SCN.

The distinctive features of SCN, particularly those based on spacecraft (SC) in geostationary orbits, are:

- global operating range (e.g., the Yamal 401 SC serves the territory of the Russian Federation and cross-border regions)
- availability of broadband radio signals from communication and retransmission SC for technical analysis and processing within the operating range
- potential possibility of unauthorized connection to communication services within the distance up to 10 ths km between the users both from the territory of the Russian Federation and neighboring countries
- the hierarchical network infrastructure of SCN with geographically distributed users that interact through heterogeneous communication and retransmission SCs and landline networks using standardized data communication protocols.

This paper uses the following key terms:

- SCN vulnerability, software, architectural or logical deficiency of SCN that can be exploited to gain unauthorized access to protected information, compromise its integrity and availability, as well as cause SCN malfunction
- information technology interference (computer attack), targeted interference in automated and information and telecommunication systems by means of hardware and software facilities carried out for the purpose of causing malfunction and compromising information security in SCN
- SCN fault tolerance improvement method, a set of models and algorithms of analysis, detection of SCN vulnerabilities, detection of ITI threats, experimental, computational, analytical and expert evaluation of actual fault tolerance of SCN under ITI.

The primary future directions of development of procedural and process engineering guidelines of SCN protection and fault tolerance include the development of:

- simulators of targeted and massive ITI for SCN testing
- methods, algorithms and facilities for detection, prevention and elimination of consequences of ITI against SCN
- testbeds for testing SCN under ITI
- training facilities based on virtualization, cloud computing and multiplayer computer games involving ITI counteraction
- computer-assisted SCN operators training in preparation to actions under emergency threats of targeted and massive ITI.

Problem definition

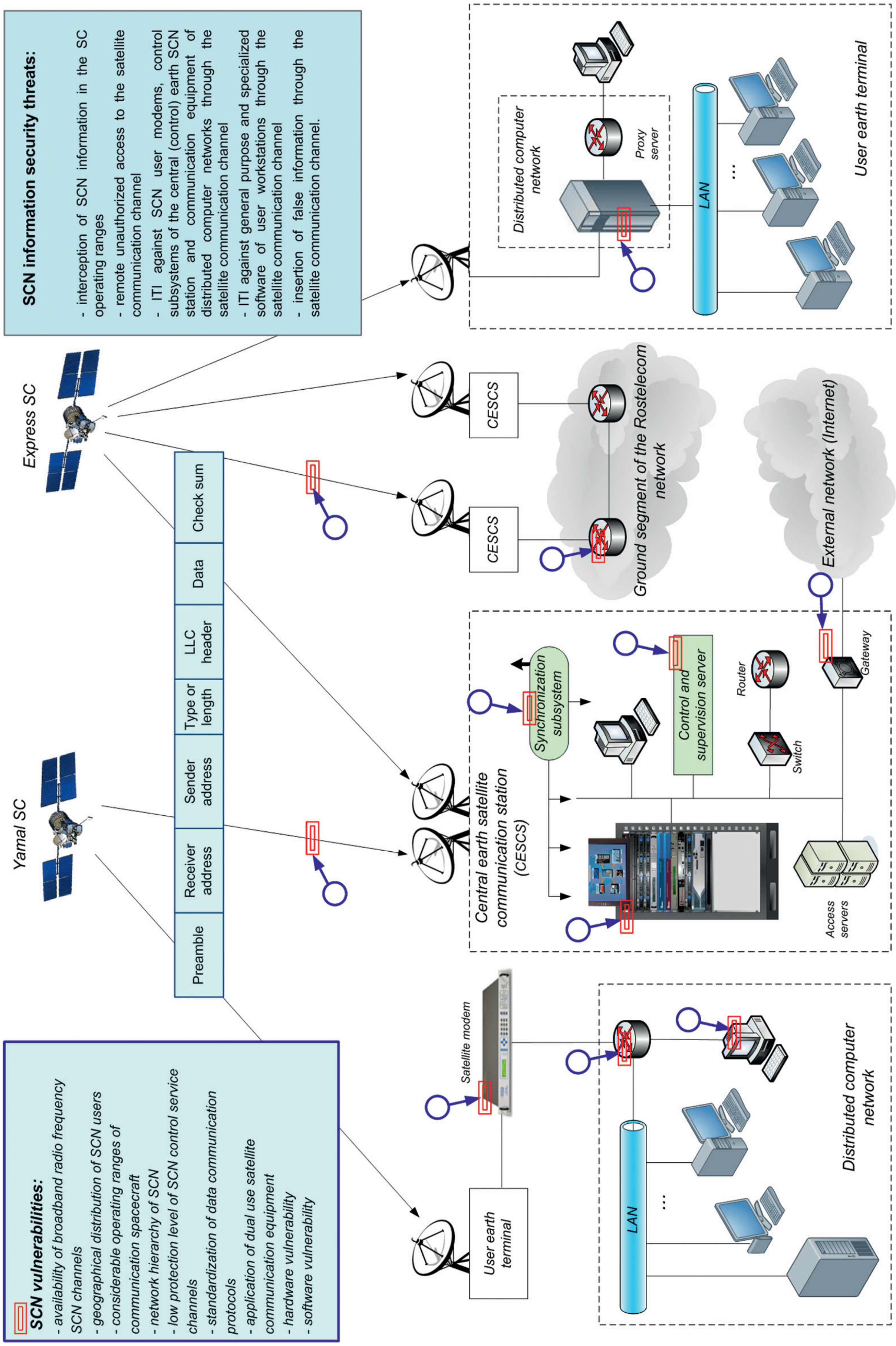
The method proposed in this paper is based on an interconnected set of experimental evaluations of actual SCN fault tolerance under simulated ITI, computational, analytical and expert evaluations of the achieved SCN fault tolerance under the chosen solutions, trusted information technologies (TIT), information security facilities (ISF) and fault tolerance sensors (detection, prevention and elimination of the consequences of ITI).

The method of improving SCN fault tolerance consists of the following models and algorithms:

1. Model of experimental identification of SCN vulnerabilities.
2. Simulation, analytical models of detection and identification of ITI threats.
3. Algorithm of decision making regarding the improvement of SCN fault tolerance under ITI.

Figure 1 shows the diagram of the model of experimental identification of SCN vulnerabilities. It is a generic SCN critical information technology infrastructure with typical vulnerabilities of geographically distributed facilities that interact through communication and retransmission SC and landline backbone networks. Vulnerabilities are associated with potential ITIs.

The primary vulnerability is the standard and open SCN data communication protocols that are not sufficiently secure in the service control and synchronization channels. High connectivity of heterogeneous segments of several SCNs enables unauthorized access to targeted objects that are not elements of individuals SCNs.



SCN vulnerabilities:

- availability of broadband radio frequency SCN channels
- geographical distribution of SCN users
- considerable operating ranges of communication spacecraft
- network hierarchy of SCN
- low protection level of SCN control service channels
- standardization of data communication protocols
- application of dual use satellite communication equipment
- hardware vulnerability
- software vulnerability

SCN information security threats:

- interception of SCN information in the SC operating ranges
- remote unauthorized access to the satellite communication channel
- ITI against SCN user modems, control subsystems of the central (control) earth SCN station and communication equipment of distributed computer networks through the satellite communication channel
- ITI against general purpose and specialized software of user workstations through the satellite communication channel
- insertion of false information through the satellite communication channel.

Yamal SC
Express SC
Preamble
Receiver address
Sender address
Type or length
LLC header
Data
Check sum
User earth terminal
Satellite modem
LAN
...
Distributed computer network
Central earth satellite communication station (CESCS)
Synchronization subsystem
Control and supervision server
Router
Switch
Gateway
Access servers
CESCS
CESCS
Ground segment of the Rostelecom network
External network (Internet)
Distributed computer network
Proxy server
LAN
...
User earth terminal

Figure 1. Model of experimental detection of SCN vulnerabilities

Experimental detection of SCN vulnerabilities is carried out by means of practical verification (testing) of the availability of control and information exchange protocols for technical analysis of radio technical parameters and revealing of information parameters of broadband signals of data communication channels through passive and active scanning.

The double red rectangle indicates the vulnerability, while the blue line with a circle indicates the ITI. The considered model of experimental detection of SCN vulnerabilities enables a preliminary evaluation of the exposure of an SCN with the employed information technologies and ISF to potential ITI. The experimental research is performed on actual SCN data communication channels with the use of communication and retransmission SC frequency resource, equipment for simulation of satellite communication channels between the control station and users taking into consideration the special features of the control cycle and with the use of a testbed system.

As part of the modelling process, the testbed hardware and software system enables technical analysis of the SCN radio technical and information technology parameters, simulation of ITI, interference environment according to the designed scenarios and input data. The testbed for experimental evaluation of SCN security under ITI must include antenna systems of various bandwidths, transceivers, demodulators, software that implement the actual operating process of SCN under ITI.

Table 1. An example of the certificate of vulnerable radio technical parameters of SCN signals

Description elements of vulnerable radio technical parameters	Description of vulnerable SCN radio technical parameters
Signal identifier	alphanumeric sequence that identifies a radio-frequency signal in the database
Name of communication and retransmission spacecraft	Yamal-401
Orbit location	90 e.l.
Transition frequency	3050 MHz
Signal level	-30 dBm
Carrier frequency	11245 MHz
Frequency band	20 MHz
Polarization type	horizontal (linear)
Modulation type	QPSK
Multiple access type	MF-TDMA
Type of interference immune coder	5/6
Type of turbo coder	Reed-Solomon
Scrambling	not used
Multiplexing	Yes

As the result, the model ensures the generation of the list of detected SCN vulnerabilities.

The certificate of vulnerable radio technical parameters of SCN signals available for technical review by an intruder is given in Table 1.

The analytic expression for calculation of the probability of detection of SCN vulnerabilities based on the experimental findings using [3-5] is as follows:

$$P_{\text{vuln}}^{\text{SCN}}\left(t_{\text{sc}}\right)=P_{\text{NAA}}^{\text{SCN}}\left(t_{\text{sc}}\right)+\left(1+P_{\text{NAA}}\left(t_{\text{sc}}\right)\right)\cdot P_{\text{PSC}}\left(t_{\text{sc}}\right)+ \\ +\left(1-P_{\text{NAA}}\left(t_{\text{sc}}\right)\right)\cdot P_{\text{ASC}}\left(t_{\text{sc}}\right), \quad (1)$$

where $P_{\text{NAA}}\left(t_{\text{sc}}\right)$ is the probability of points of unauthorized access in data communication channels between SCN users in the directions SC-to-Earth (back link with available broadband signals) and Earth-to-SC;

$P_{\text{PSC}}\left(t_{\text{sc}}\right)$ is the probability of passive scanning of data communication channels between SCN users within the time t_{sc};

$P_{\text{ASC}}(t_{\text{sc}})$ is the probability of active scanning of data communication channels between SCN users within the time t_{sc};

Let us represent the certificate of vulnerable information technology parameters of the SCN data communication channels using GOST R 56546-2015 (Table 2).

The simulation, computational, analytical models of detection and identification of threats of ITI in SCN define the list of threats to SCN information security that corresponds with the structure of the protocol of data communication between the control station and user segment, as well as SCN elements. The simulation model of ITI threats helps reveal the vulnerabilities of protocols, possible ways of implementing ITI threats against them and the consequences of SCN information security violations.

The presence of potential vulnerabilities and threats of ITI in SCN conditions the possibility of unauthorized connection to the network and interception of information.

The diagram of the model of detection and identification of SCN ITI threats is generated in the form of a structure of prompt response to ITI and improvement of fault tolerance is composed of three loops (Figure 2):

- first, SCN ITI
- second, control of information security and improvement of fault tolerance using the information from sensors of the ITI detection and identification facilities
- third, notification of information security violation using a generic form of computer incident description.

SCN TIT elements are secure hardware and software platforms that include operating systems (OS), database management systems (DBMS), translators from high-level programming languages and other general software. The hardware component of SCN TIT includes secure processors, memory modules, interface buses, satellite modems, control stations, trusted communication equipment of distributed landline networks that together must allow creating satellite and communication equipment immune to ITI.

Table 2. An example of the certificate of vulnerable information technology parameters of SCN

Elements of the description of vulnerable information technology parameters of SCN	Description of vulnerable information technology parameters of SCN
1. Name of vulnerability	Satellite modem control protocol vulnerability
2. Vulnerability identifier	USM-2017-00002
3. Brief description of vulnerability	Vulnerability allows interception of satellite modem software control channel
4. Vulnerability class	Satellite modem software vulnerability
5. Name of vulnerable element and its version	Satellite modem software ver. 7.34
6. Data communication protocol	Telnet control protocol, direct access to the satellite modem controls
7. Hardware and software design details	Hardware and software platform is based on the client/server and data communication protocol TCP/IP v.4.0 technology
8. Type of deficiency	Deficiencies related to operator authentication
9. Location of occurrence (manifestation) of vulnerability	Vulnerability exists due to the absence of legitimacy test of the source of satellite modem control
10. Deficiency type identifier	No data
11. Date of vulnerability detection	1.03.2017
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 satellite modem control protocols
17. Additional information	The network used satellite modems that allow remote software reboot via SCN

In the model of detection and identification of ITI the information security facilities (ISF) include on the one hand well-known ISFs such as automated trusted loading modules (ATLM), firewalls (FW), false network information entities (FNIE), and on the other had the set of sensors that implement the detection, prevention and elimination of consequences of ITI. In order to improve SCU fault tolerance under ITI the set of sensors records and identifies the facts of interference and generate the input data for SCN recovery.

SCN ISF elements should be implemented based on hardware and software facilities of the ITI monitoring and information security control station.

As part of SCN fault tolerance improvement the potential threats of SCN security and fault tolerance violations, potential target facilities, SCN TIT, ISF system and required testbed system for testing SCN under ITI are analyzed.

The distinction of improving the fault tolerance of SCN under ITI is that its required level must be ensured over a long period of operation in the context of ever-improving threats and control system paths with different data communication protocols.

The procedure of detection and identification of SCN ITI threats is as follows:

1. Installation of ITI detection server in the central control (Earth) station, installation of fault tolerance sensors at connected user control stations (terminals) and monitoring of SCN security.

2. Initial notification of the appearance of an unregistered user in case of unauthorized connection of an intruder to the SCN with active use of an unauthorized satellite modem.

3. Notification of a computer incident in case of ITI against the SCN users and control station by the fault tolerance sensors with the use of embedded signature-based and heuristic methods.

4. Analysis of targeted and massive ITIs, identification of their type and updating of ITI signatures database.

5. Decision-making regarding elimination of ITI consequences by means of blocking of the intruder's satellite modem based on the supervision of the parameters of the forward and reverse satellite channels, information from the fault tolerance sensors.

The monitoring of SCN security for ITI detection and identification is implemented by means of the following tests:

- supervision of radio technical parameters
- supervision of SCN control service channels
- supervision of SCN users connection and operation parameters
- supervision of SCN information traffic
- detection of insecure control and data communication channels

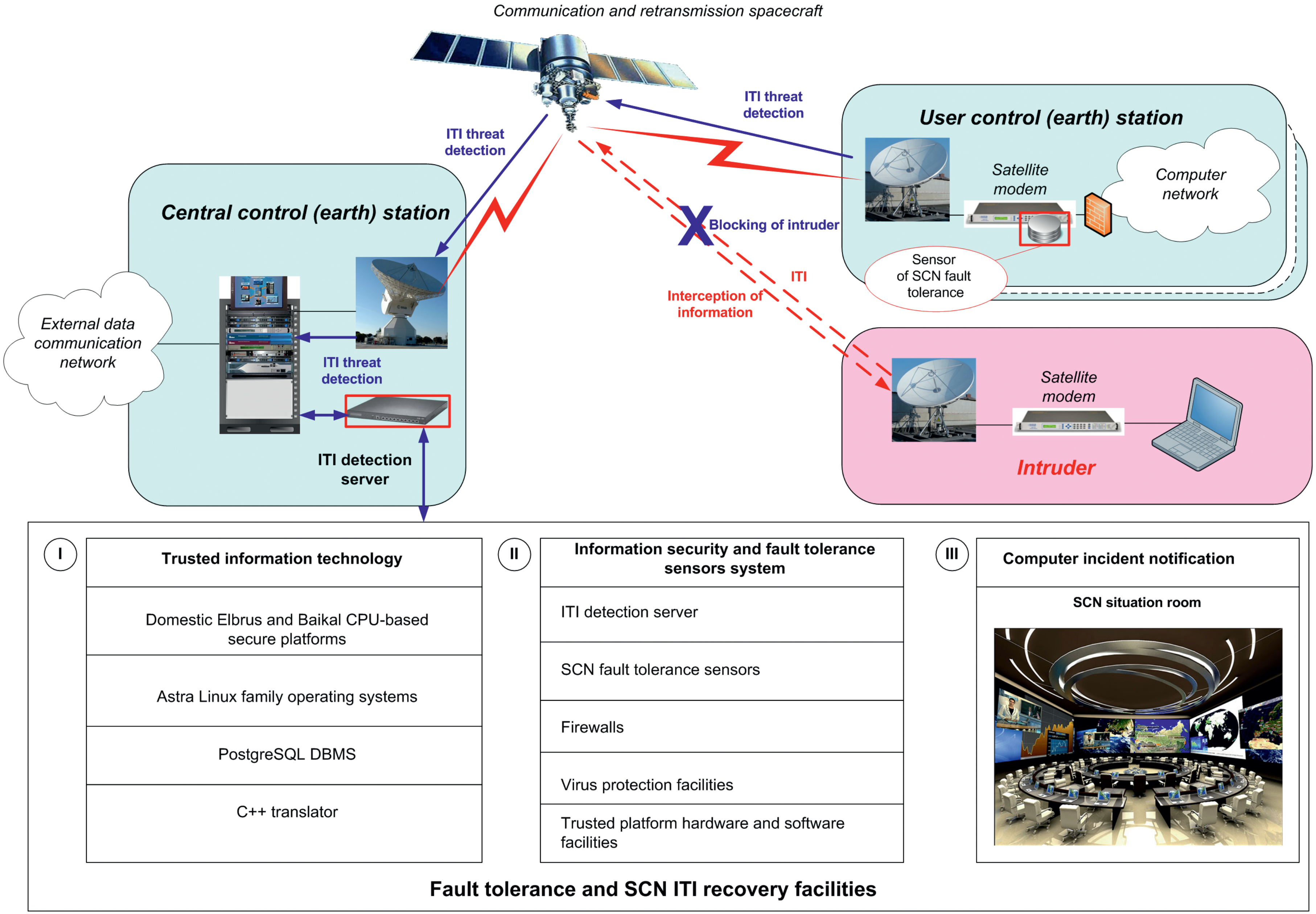

Communication and retransmission spacecraft
ITI threat detection
ITI threat detection
Central control (earth) station
External data communication network
ITI threat detection
ITI detection server
User control (earth) station
Satellite modem
Computer network
Sensor of SCN fault tolerance
Blocking of intruder
ITI
Interception of information
Satellite modem
Intruder
I
Trusted information technology
Domestic Elbrus and Baikal CPU-based secure platforms
Astra Linux family operating systems
PostgreSQL DBMS
C++ translator
II
Information security and fault tolerance sensors system
ITI detection server
SCN fault tolerance sensors
Firewalls
Virus protection facilities
Trusted platform hardware and software facilities
III
Computer incident notification
SCN situation room
Fault tolerance and SCN ITI recovery facilities

Figure 2. Diagram of the model of detection and identification of ITI threats

- detection of ITI in the forward and reverse SCN channels

- localization of the intruder (identification of ITI source and the supposed location)

- blocking of the intruder (disconnection from SCN)

- technical analysis and identification of SCN vulnerabilities

- supervision of the performance parameters of satellite equipment of the central and user stations, communication equipment, hardware and software, information security and fault tolerance improvement facilities.

The computational and analytical model is based on the mathematical expression for identification of the conditional probability of materialization of SCN ITI threats (with the use of [3-5]):

$$P\left(S_{\mathrm{O}}/Y_{\mathrm{ITI}}\right)=\frac{P\left(S_{\mathrm{O}i}\right)\cdot P\left(Y_{\mathrm{ITI}i}/S_{\mathrm{O}j}\right)}{P\left(S_{\mathrm{O}j}\right)\cdot P\left(Y_{\mathrm{ITI}i}/S_{\mathrm{O}j}\right)+P\left(S_{\mathrm{NO}k}\right)\cdot P\left(Y_{\mathrm{ITI}i}/S_{\mathrm{NO}k}\right)},\quad(2)$$

where $P(S_{\mathrm{O}})$ is the probability of SCN being operable under ITI,

$P(Y_{\mathrm{ITI}i}/S_{\mathrm{O}j})$ is the conditional probability of materialization of the *i*-th ITI threat against the *j*-th operable SCN element,

$P(S_{\mathrm{NO}k})$ is the probability of the *k*-th SCN element being non-operable under ITI,

$P(Y_{\mathrm{ITI}i}/S_{\mathrm{NO}k})$ is the conditional probability of materialization of the *i*-th ITI threat against the *k*-th SCN element that causes violation of its fault tolerance.

Figure 3 shows the algorithm of improvement of SCN fault tolerance under ITI.

The algorithm of SCN fault tolerance is based on a set of experimental, computational and analytical and expert evaluations of SCN parameters under ITI for the purpose of selecting SCN fault tolerance solutions by means of their situational adjustment.

The essence of the algorithm of SCN fault tolerance under ITI consists in the implementation five stages:

1. Preparation of parameters (input data) for evaluation of SCN fault tolerance under ITI
2. SCN actual security evaluation.
3. SCN parameters adjustment.
4. ISF and fault tolerance facilities parameters adjustment.
5. Situational adjustment of SCN fault tolerance solutions.

The algorithm of SCN fault tolerance under ITI essentially defines the logic of stage-by-stage management of network fault tolerance, selection of the least vulnerable

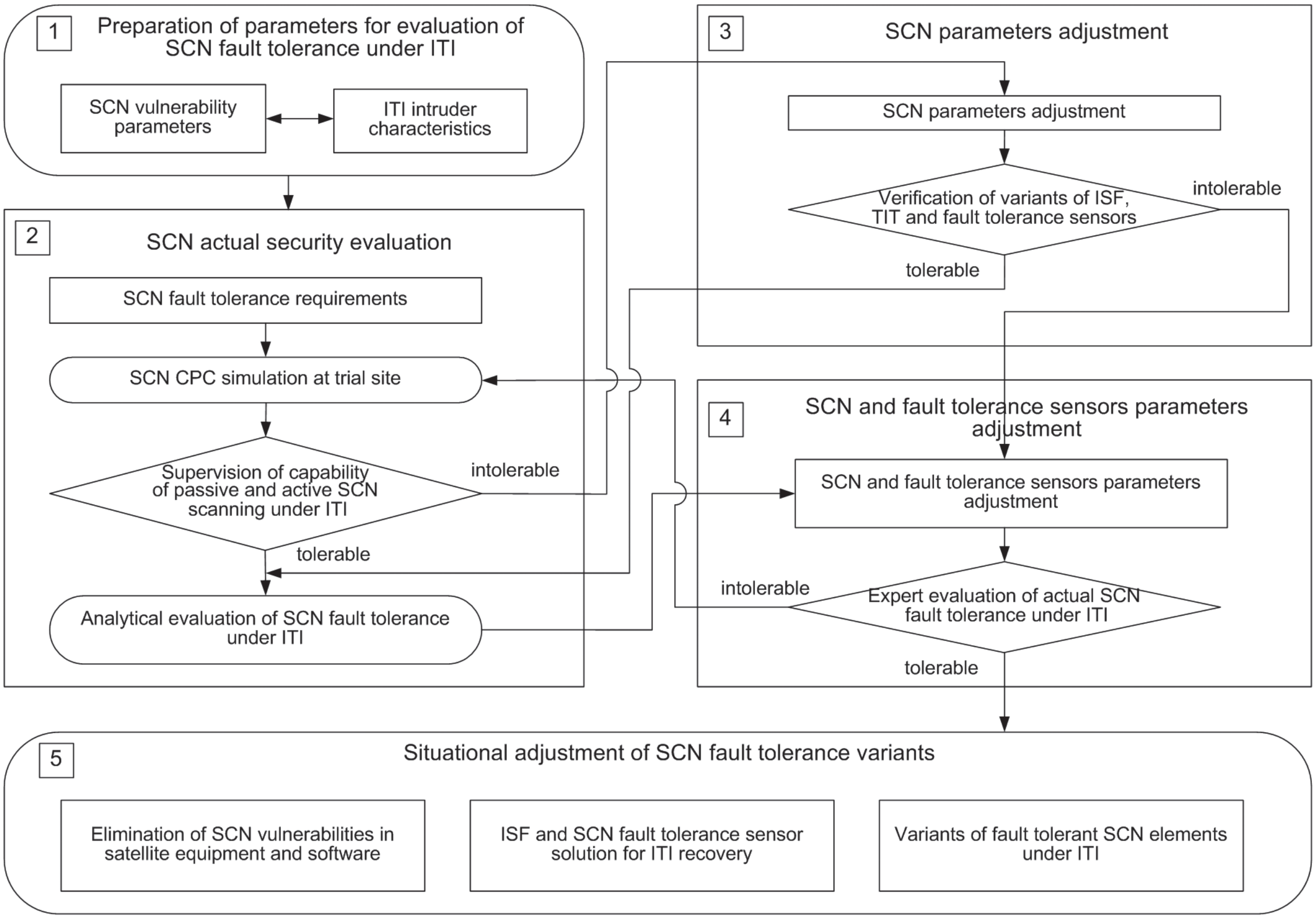

1
Preparation of parameters for evaluation of SCN fault tolerance under ITI
SCN vulnerability parameters
ITI intruder characteristics
2
SCN actual security evaluation
SCN fault tolerance requirements
SCN CPC simulation at trial site
Supervision of capability of passive and active SCN scanning under ITI
intolerable
tolerable
Analytical evaluation of SCN fault tolerance under ITI
3
SCN parameters adjustment
SCN parameters adjustment
Verification of variants of ISF, TIT and fault tolerance sensors
intolerable
tolerable
4
SCN and fault tolerance sensors parameters adjustment
SCN and fault tolerance sensors parameters adjustment
Expert evaluation of actual SCN fault tolerance under ITI
intolerable
tolerable
5
Situational adjustment of SCN fault tolerance variants
Elimination of SCN vulnerabilities in satellite equipment and software
ISF and SCN fault tolerance sensor solution for ITI recovery
Variants of fault tolerant SCN elements under ITI

Figure 3. Algorithm of SCN fault tolerance under ITI

and most secure SCN configuration with the capability to eliminate ITI consequences.

The SCN control cycle is characterized by the real-time operation, dynamic ITI environment, large numbers of TIT, which requires situational adjustment of the SCN fault tolerance parameters according to the current situation.

It is assumed that the initial stage of algorithm operation, the input ITI data, SCN vulnerabilities, TIT, ISF and fault tolerance sensors are undefined, which causes the requirement for experimental and analytical research to ensure ITI fault tolerance under ITI.

The algorithm is to be used both at the stage of secure SCN design and development and the stage of SCN parameters and fault tolerance facilities adjustments in operation.

The implementation of the stages of the algorithm of SCN fault tolerance adjustment under ITI ensures:

- preparation of input data and taking account of the factors for evaluation of SCN fault tolerance under ITI
- simulation of real SCN operation processes using the testbed system
- instrumental verification of the intruder's potential capabilities in terms of passive and active scanning of SCN vulnerabilities
- adjustment of SCN, ISF, TIT and fault tolerance sensors parameters based on the results of experimental, computational and analytical and expert evaluations
- situational adjustment of SCN fault tolerance solutions under dynamic ITI based on elimination of vulnerabilities of hardware and software, selection of SCN elements, ISF and fault tolerance sensors fault tolerance solutions
- selection of the SCN models, ITI, ISF, TIT, fault tolerance sensors for the purpose of identifying the measures of improving (insuring) SCN functional stability
- comprehensive experimental, computational and expert evaluation of SCN fault tolerance under ITI
- preparation of elimination of the consequences of ITI against SCN
- efficient management of SCN fault tolerance under uncertain ITI and various degradations in the control cycle in terms of satellite communication and data transmission services
- evaluation of fulfilment of the requirements for SCN fault tolerance under ITI and associated practical recommendations.

The many various parameters of SCN, ISF, TIT, fault tolerance sensors and ITI factors lead to a multitude of possible current SCN fault tolerance conditions. In practice, the number of adjustment (control) solutions for improving SCN fault tolerance is limited. In this context the considered algorithm based on situational adjustment of SCN fault tolerance solutions enables the fulfilment of the SCN fault tolerance requirements.

The situation is understood as the sum of vulnerabilities and states of SCN, ISF, TIT and fault tolerance sensors at a certain moment of operation for the purpose of identifying the requirement for an intervention in the SCN control process.

The procedures of supervision, verification and expert evaluation of the SCN fault tolerance parameters under ITI implies that based on the data regarding the testbed findings as part of decision-making at the stages of the algorithm implementation the facts are established of allowable and unallowable deviation of the current SCN state from the required values.

The interval of SCN fault tolerance state adjustment is chosen based on the significance of the users and units (control stations) and most probable ITI implementation.

If the state of SCN under ITI requires situational adjustment, its description is classified on the basis of the certificate of the SCN radio technical and information technology parameters, normal behavior profile and results of computer incident investigation. Each current state of the SCN under ITI can be assigned to a certain class that is associated with a certain set of adjustable parameters.

Situational adjustment of SCN fault tolerance is done in the following order: description of SCN state under ITI – preparation of adjustable parameters of SCN, ISF, TIT, fault tolerance sensors – control inputs for ITI counteractions and SCN recovery (initiation of backup segments).

The calculation formula for the probability of fault tolerance of SCN fault tolerance under ITI with the use of [3-5] is as follows:

$$P_{\text{fl}}(t)=\prod_{i=1}^{k}\left[1-\left(1-\prod_{j=1}^{r}P_{\text{PNF}i}\left(S_{\text{O}j}\right)\right)\right], \tag{3}$$

where $P_{\text{PNF}i}\left(S_{\text{O}j}\right)$ is the probability of no-failure of the *j*-th SCN element under the *i*-th ITI threat;

k is the total number of ISF (sensors) within the SCN;

r is the total number of backup SCN elements.

Conclusion

The paper suggests a method of improving SCN fault-tolerance under possible ITI based on system analysis of potential vulnerabilities and unique operational characteristics of SCN. The method is based on a set of interconnected procedures of the model of experimental detection of SCN vulnerabilities on testbed, generation of the simulation, computational, analytical models of detection and identification of ITI threats and application of the decision-making algorithm of improvement of SCN fault tolerance under ITI.

References

1. Voronin AV, Ivanov VN, Sotov AM. Somov AM, Doctor of Engineering, editor. Tsyfrovoe televizionnoe veshchanie [Digital television broadcasting]. Moscow: Goriachaia linia-Telekom; 2017 [in Russian].

2. Velichko VV, Popkov GV, Popkov VK. Modeli i metody povyshenia zhivuchesty sovremennykh sistem sviazi

[Models and methods of improving the resilience of present day communication systems]. Moscow: Goriachaia linia-Telekom; 2016 [in Russian].

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

4. Kapur K, Lamberson L. Ushakov IA, editor. Reliability in engineering design. Moscow: Mir; 1980 [in Russian].

5. Shubinsky I.B. Nadiozhnie otkazoustoychivie informatsionnie sistemy. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016 [in Russian].

About the authors

Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4-th Central Research and Design Institute of the Ministry of Defense of Russia. Russia, Korolyov, phone: + 7 (985) 928 13 55, e-mail: klimov.serg2012@yandex.ru.

Sergey V. Polikarpov, Deputy Head of Unit, 4-th Central Research and Design Institute of the Ministry of Defense of Russia. Russia, Korolyov, phone: +7 (916) 332 60 66, e-mail: polikarpov.s.v@yandex.ru.

Andrey V. Fedchenko, Head of unit, 4-th Central Research and Design Institute of the Ministry of Defense of Russia. Russia, Korolyov, phone: +7 (916) 334 87 89, e-mail: fedchandr@yandex.ru

Received on 15.05.2017