Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):39-47
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

THE PURPOSE AND TASK OF BUILDING COMPLEX DISTRIBUTED SYSTEMS, THE PARAMETERS OF STABILITY AND SECURITY IN THE FORMATION OF THE SYSTEM DEVELOPMENT GOALS OF ITCS

Y. Shestak, V. Vialkova, S. Mahula L.Mirutenko
Taras Shevchenko National University of Kyiv

ABSTRACT:
The main purpose of the establishment and operation of distributed information and telecommunication systems is the organization of effective user access to information and software resources, and effective interaction as users with the resources and various kinds of resources between themselves. There is also the importance of considering the stability parameter distributed ITCS in the context of its functional stability. Admittedly, distributed systems can potentially have a higher resistance to failure, compared to centralized structures. There also several objectives of sustainability and security of distributed ITCS The network's security settings, sustainability and security of the system against internal and external effects are significant. That is because of ensuring the implementation of the key requirements of availability, confidentiality and integrity of data, processes and procedures inside the system.

KEYWORDS: distributed information and telecommunication systems, information security, stability

Distributed systems are created in order to help users to access remote resources. The notion of resource here must be understood in a broad sense: from devices (printers, scanners) and ending with files, web pages and the like. Sharing of resources is justified in the first place economically. The use of shared resources also enables the rapid exchange of information between users. At the same time, easy access to resources should not be a resignation for the deterioration of stability and security distributed ITCS, reducing security operations performed in the system. It concerns issues of both privacy and integrity of transmitted data, a reliability of

the system.

As complex systems, distributed ITCS represent a set of interrelated technical and technological elements, functioning under the action of random factors, in an active interaction with the external environment, in the presence of negative influences of different nature and high cost of the consequences of possible violations or errors in the system [1].

Describing the basic concepts concerning security issues of distributed ITCS should define "fails" – the state when the system does not perform its functions; is not acting under a specific protocol [2,3].

Eror – the part of the system state, which can reach up to the accident (eg. error data broadcasts).

A vulnerability is the cause of the error.

Vulnerabilities control is performed through prevention, removal and expectations.

Failure – the visible inability to perform the function of the system, which is a consequence of errors due to vulnerabilities.

Fault tolerance– the ability to provide services despite the existence of vulnerabilities..

In the formation of development goals distributed ITCS significant place should be occupied by the parameters of the stability and security of complex distributed ITCS, which will allow using certain methods, information technologies and tools to ensure the stable operation and development (using the properties of scaling) distributed ITCS under the influence of these threats [4;5] (table 1.2):

Table 1.2 The main threats types to the sustainability and security of distributed ITCS

Threat types	Essesance	The motives and methods of cyber criminals
Passive attacks	Provide motion analysis, monitoring unsecured communications, decoding network traffic that is encrypted with weak cryptographic algorithms and intercepting information	Passive reception of information on the network can serve as a source of information for cybercriminals, providing certain data and possibilities of interference with the system without the need for user consent.
Active attack	Involve attempts to bypass or hacking, using, for example, special software, or theft or	These attacks may be to use the transmitted information, the attacks on the authenticated user

	modification of information	when you attempt remote login to the system. Active attacks can serve as identification or dissemination of data, blocking delivery of services
Convergence	One is obtaining physical access to network, access or block access to information	Convergence can be accomplished through covert or overt actions can also be the result of a combination of these two methods of action
Attack from within:		It should be remembered that more than 80% of attacks on systems is carried out from the internal environment of information and telecommunication networks [6]. Given this, users on the network should not have more opportunities than they need and all their actions should be recorded for the possibility of establishing the source of danger
- M*alicious attacks*	One is obtaining physical access to network, access or block access to information	
- *Not malicious attacks*	As a rule, impose a frivolity, a lack of competence	
Distribution	It is the adaptation of equipment and software at the time of manufacture or distribution	Attacks of this type are the inclusion in the product, which is used in distributed ITCS code, the so-called back door, thanks to which cyber criminals will continue to have access to systems that use these products

The growing complexity of the structure and functioning of complex distributed ITCS leads to the emergence of such properties as a natural redundancy, adaptability, reliability, fault tolerance, resilience, survivability [6].

Functional stability and security of distributed ITCS characterizes its ability to implement fully their roles and perform tasks, for which the organizers distributed ITCS receive income from providing services [7,8].

The stability of the system describes its ability to operate in a continuous mode. Unlike availability, description of sustainability refers to the period of time. It is the quality that allows ITCS distributed smoothly to withstand changes in the parameters of the external environment different from the design and carry out their basic functions. Thus, distributed ITCS can be considered sustainable if it can cope with variations (sometimes unpredictable) in the operating environment with minimal: loss, configuration changes or loss of functionality.

This implies the importance of considering the stability parameter distributed ITCS in the context of its functional stability (ability to ensure the functionality of the system under the influence of environmental parameters and their changes). Among the components of the functional stability of distributed ITCS, following ones should be highlighted:

- ensuring of the availability, characterizing the condition in which is stored the user access to the services of ITCS distributed in full without additional (unspecified agreement) access restrictions in time and space;
- ensuring of the integrity of information that characterizes the state, which retains the ability of users to access services distributed ITCS in full and no additional (unspecified agreement) access restrictions in volume), due to the impact of ITCS on distributed.

Security distributed ITCS is a complex characteristic that is characterized by a complex interaction of means and technological methods, as well as procedural, logical, and physical measures aimed at [9,10]:

– countering threats to information resources and components of the information environment;

– protection components of the information environment;

– minimize risk to the components and resources of the information environment.

Thus, the parameters of sustainability and security of distributed ITCS, although they have some functional commonality, differ primarily the orientation to specific tasks, in particular, to ensure sustainability it is important to ensure the uninterrupted operation of the system, for security – combating external interference and threats, which ultimately determines the possibility of stable (without interruptions caused by external interference) of the system.

Distributed systems work by using separate computers connected to the network. From the programmer's point of view, this is important, because the operation of individual machines in a distributed system affects the way of programming such systems. An important parameter in

determining the nature of ITCS distributed architecture connections between nodes, which can be implemented via a central bus or dial-up technology [11].

These systems have a specific purpose of functioning, a large number of interacting subsystems, a complex hierarchical control system. They are also characterized by complexity and functions that they are, the constant rise in the number of users and connected equipment, a constant modification of the components, which leads to the impossibility of constructing an adequate mathematical model for a comprehensive description of the functioning of the system [12].

Most often, when designing a distributed information-telecommunication system in the first place put a division of its functions between multiple computers [13]. This approach is distributed in any computer system where data processing is divided between two or more computers.

Organization of work with information resources in distributed ITCS provides a solution to the complex task of ensuring convenient and quick access to information for those who are entitled to it and protect information from those who do not have appropriate access rights. This leads to the need to solve additional problems of sustainability and security of distributed ITCS related [14]:

- authentication of remote users and programs;
- protection of communication channels;
- protection of remote nodes of the system;
- protection of the entire distributed system as a whole, its management.

These very requirements for durability and security when building distributed ITCS determine today the biggest r problems of a technical and technological plan, the reason for this is that the creation of systems of information security seriously lagging behind in the development of technologies of transfer and processing of information, it is rather a consequence of the reaction to potential threats, rather than a systematic process of preventing instability and insecurity of the system, carried out constantly, at the stage of design and planning of building systems. Distributed systems can potentially have a higher resistance to failure, compared to centralized structures. Partial failure in a distributed system may cause damage to one component of the system that can be replaced by another, and does not require stopping the functioning of the entire distributed ITCS to recover her health. In centralized systems, the failure usually causes partial immobilization of the entire system.

Most fault tolerance of distributed systems describes only its potential, but not necessarily the fact of its stability and security, and requires the use of various supplementary methods of

protection, the implementation of corrective actions in case of failure or unauthorized interference in its activities.

An important feature of many applications is their indivisibility. This applies, for example, to Checkout, where the individual steps must be completed in full. Implementation integrity of a distributed system requires a distributed statement, which is equivalent to consensus.

Ensuring of sustainability and security of distributed ITCS requires the use of a certain number of specific means of information protection. These tools combine hardware and software components into a coherent, complex system of protection. However, there is a certain probability of violation of the stability and security of distributed ITCS, which can be described using the following model:

$$p_i = \frac{NA_{refl.i}}{NA_{tot.\ i}},$$

where – p_i – the probability of loss of stability and security distributed ITCS as a result of the threats of *i*-type;

- $NA_{refl.i}$ – the number of reflection attacks (threats) sustainability and security of distributed ITCS of *i*-type;
- $NA_{tot.\ i}$ – the total number of attacks (threats) sustainability and security of distributed ITCS of *i*-type

The probability of cracking (system security breach which leads to the impossibility of performance of its functions) distributed ITCS as a whole can be modelled in the following way:

$$p_{prot} = 1 - p_1 * p_2 * p_3 * p_4 * p_5 * \ldots * p_n,$$

where p_{prot} — probability of breaking (system security breach which leads to the impossibility of performance of its functions) distributed ITCS as a whole;

$p_{1\ldots}p_n$ – the probability of security breach distributed ITCS as a result of the threats of the *i*-type (i=1…n).

In this model, however, does not take into account the activity of the organizers distributed ITCS in the protection from threats to the sustainability and security of distributed ITCS. Based on the foregoing, a violation of resource availability can be described as:

$$p_{avail} = 1 - (1 - p_1) * (1 - p_2) * (1 - p_3) * (1 - p_4) * (1 - p_5) * \ldots * (1 - p_n),$$

where p_{avail} — the probability of violation of availability (the system loss of stability and

security, which leads to the impossibility of the availability of users to distributed services ITCS) in general.

Violation of the integrity of the information can be presented in the form of the model:

$$p_{int.} = p_j * [1 - (1 - p_{conf}) * (1 - p_{net}) * (1 - p_{other}),$$

where $p_{int.}$– the probability of violation of integrity of information;

p_j – the probability of violation of control and you need to recover information;

p_{conf} – probability of breach of confidentiality;

p_{net} – the probability of a negative impact on information from the vulnerability exploits a telecommunications network;

p_{other} – the probability of a negative impact on information from exploit out of a telecommunication network.

Based on previous dependencies, complex value of the probability of loss of stability and security distributed ITCS can be shown by the following equation:

$$p_{\text{ст.та зах.}} = 1 - (1 - p_{\text{зах}}) * (1 - p_{avail}) * (1 - p_{int.}),$$

where p_{avail} — the probability of system loss of stability and security, which leads to the impossibility of the availability of users to distributed services ITCS;

p_{prot} — the probability of cracking (system security breach which leads to the impossibility of performance of its functions) distributed ITCS as a whole;

p_{avail} — the probability of violation of availability (the system loss of stability and security, which leads to the impossibility of the availability of users to distributed services ITCS) in general.

$p_{int.}$– the probability of violation of the integrity of the information due to the impact of ITCS on distributed.

The security vulnerabilities distributed ITCS and, thus, their causes cause may be very different. Depending on their nature, is necessary to implement relevant activities. Important in this context is the classification of different types of vulnerabilities of security systems.

– Temporary vulnerability – appear and fade, are transient. These types of vulnerabilities may occur through temporary weather conditions, or as a result of transient interference from external devices or animals.

– Fitful of vulnerability also appear and disappear, but their condition is characterized by relapses. An example of this type of vulnerabilities can be, for example, poor contact of

conductors in the network. This type of vulnerability is relatively difficult to detect because they can appear when the monitoring system is not configured to reveal them.

– Permanent vulnerability does not disappear until they are fixed. This is the result of, for example, fault or error in the software.

To describe the maximum effect of neutralizing the threats to the sustainability and security of distributed ITCS i-type (i=1…n) using the tools on your system (d) using the following equation:

$$\sum_{j=1}^{m}\sum_{i=1}^{n} d(i,j)p(i,j) \Rightarrow \max$$

Subject to the restrictions on the costs (C) to ensure the stability and security of the system equations will have the following form:

$$\sum_{i=1}^{n} c(i) * sign \sum_{uj \in U}^{n} p(i,j) \le C$$

$$p(i,j) \in (1,0), \quad j = 1, \ldots m; \quad i = 1,\ldots n.$$

The objectives of sustainability and security of distributed ITCS are:

– the elimination of these vulnerabilities even before the negative impact of events related to vulnerabilities in the system, on the functioning of the system;

– prevention of negative influence of events related to vulnerabilities in the system;

– fixing effect on distributed ITCS of events related to vulnerabilities in the system;

– elimination of consequences of the negative influence of events related to vulnerabilities in the system;

– stabilization of the system operation after system failures caused by events related to vulnerabilities in this system.

The implementation of these tasks is in the process of management and administration of complex distributed ITCS as one of the key elements of the integrated functions and ensure the realization of the main goal of the functioning of modern complex distributed ITCS is the efficient user access to information and software resources as well as the effective interaction of users with resources and different types of resources between them. In fulfilling of this objective, the network's security settings, sustainability and security of the system against internal and external effects are important, because in this way ensure the implementation of the key

requirements of availability, confidentiality and integrity of data, processes and procedures within the system.

REFERENCES:

1. Dodonov A. G., Kuznetsova M. G., E. S. garbacik Survivability and reliability of complex systems. Methodical manual. — International scientific-training center of UNESCO/IIP of information technologies and systems. — 2001. — 163 c.
2. Tsymbal, A. A. the Technology of creation of distributed systems. For professionals /A. A. Tsymbal, M. L. Ensina - SPb.: Peter, 2003. - 576
3. Pleskach, V. A. Informatin technology the system /V. A. Pleskach, V. Rogushina, N. P. Kustova; Kiski NAT. torgovelnye-Econom. UN-t. - K:. “The book”, 2004 - 519.
4. The usage of mechanisms to improve survivability to ensure the security of the information resource in distributed systems / N.G. Kuznetsova // Registration, storage and processing. data. — 2006. — Vol. 8, No. 3. — S. 40-47.
5. Schneier. Network control and security // Protection of information. Konfident. — 2004. — No. 4. — S. 75-81Radchenko G. I., a Distributed computing system / G. I. Radchenko. – Chelyabinsk: Photographer, 2012. – 184
6. Radchenko G. I., a Distributed computing system / G. I. Radchenko. – Chelyabinsk: Photographer, 2012. – 184
7. Domarev V.V. Protection of information and security of computer systems. — K.: Publishing house "Diasoft", 1999. 480 p.
8. Kuznetsova M. G. the Security of information resources in distributed systems: Sat. scientific. Tr. "Information technologies and security". Vol. 7. — K. AND NASU, 2004. — Pp. 38-40.
9. Domarev V.V. Protection of information and security of computer systems. — K.: Publishing house "Diasoft", 1999. 480 c .
10. Kuznetsova M. G. the Security of information resources in distributed systems: Sat. scientific. Tr. "Information technologies and security". Vol. 7. — K. AND NASU, 2004. — Pp. 38-40.
11. Papazoglou M.P. Web Services: Principles and Technology / M.P. Papazoglou // Prentice Hall. – 2007. – Vol. 21. – P. 139-145

12. The usage of mechanisms to improve survivability to ensure the security of the information resource in distributed systems / N.G. Kuznetsova // Registration, storage and processing. data. — 2006. — Vol. 8, No. 3. — S. 40-47.
13. The usage of mechanisms to improve survivability to ensure the security of the information resource in distributed systems / N.G. Kuznetsova // Registration, storage and processing. data. — 2006. — Vol. 8, No. 3. — S. 40-47.
14. Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead. Survivability: Protecting Your Critical Systems. http://www.cert.org/archive/html/ protect-critical-systems.html