UDC 621. 391

MANAGEMENT OF CRITICAL IT-INFRASTRUCTURES

Yaroslav Y.Dorogyy

National Technical University of Ukraine "KPI", Kyiv, Ukraine

In the article the terminology and requirements for safe, reliable operation of critical IT infrastructure were defined. The generalized structure of critical IT infrastructure, by its basic level, sub levels and functionality were described. In the paper for the described structure mathematical model of control of resource allocation in the case of inter-independence processes and universal services were proposed.

Introduction

At present, creation of critical IT-infrastructures is an integral part of the key industries that are vital for the safety and functioning of society.

The existence of critical IT-infrastructure is closely linked to the notion of the critical infrastructure – infrastructure that is vital to the state, failure or destruction of which could significantly negatively affect national security.

Critical IT-infrastructure is a collection of information and telecommunication systems of the state and the private sector, providing performance and security of policy institutions, systems and objects of State (central and local government systems, energy management, transportation, communications, banking sector enterprises during activities that use and / or produced hazardous substances, etc.) and public safety (management of law enforcement agencies and defense sector, etc.) unauthorized intervention in work which could threaten the economic, environmental, social and other types of safety or harm international image of the country. [1] Other critical infrastructures include such fields as public finance, the state's energy sector, food industry, medicine, manufacturing, transportation system, water supply, public administration, etc.

Critical IT-infrastructure needs to:

- ensure the functioning of hazardous and socially important industries and processes, staffing regime violations of may result in man-made emergency;
- serve as an information system disorders or stopping of operation which could lead to negative consequences in the political, economic, social, informational, environmental and other areas;
- assure that a significant amount of information society services, partial or total suspension of may result in serious negative consequences for national security in many areas.

At present, Ukraine is only beginning to develop such global systems of management, although some areas already have well-developed IT-infrastructure, such as transport dispatching management, energy facilities.

Therefore, the development of new approaches, methods and algorithms for creating, analyzing, monitoring, quality assurance, reliability and safety of critical IT-infrastructure is a very topical issue.

Analysis of Existing Solutions

The rapid development of IT and telecommunications, their widespread adoption in the management created a situation where the very process of providing information services is a subject to control. Indeed, a large variety of services and resources in the use of information and telecommunication networks, historically, makes supporting of business processes in large organizations in time and space in real-time in a rather difficult problem.

The main suppliers of computer and telecommunications equipment and IT came to market with a solution designed to solve this problem. Methodological bases of its decision contained in ITIL solutions on which was advanced the development of ITSM. The latest development, which is a fairly detailed description of the problems and almost completely covers the previous design is COBIT [2]. All of these developments are a methodological device to be used to create a specific IT-infrastructure. Specificity of living in a particular country also imposes limitations on the creation of a critical IT-infrastructure.

Currently in our country has already started working towards the development of design issues for critical IT-infrastructures. Several groups of authors have begun to consider some aspects of critical IT-infrastructures. For example, in [3] the authors examine the issue of service of critical IT-infrastructures, in [4]

examined the synthesis of parameters for critical IT-infrastructures, in [5] - the problem of monitoring critical IT-infrastructures was considered.

The main problem of considered works is a lack of generalized patterns of critical IT-infrastructure, its requirements for reliability, quality and safety of their operation.

Purpose of Research

The aim of this work is to develop the basic requirements for the operation of critical IT-infrastructure, development of a generalized structure of the critical IT-infrastructure of enterprise and management model of the distribution of resources.

The problem analysis of management of critical IT-infrastructure in Ukraine

Analysis of critical IT-infrastructure management in Ukraine indicates the presence of these problems:

- lack of consolidated set of terminology on critical IT infrastructures – at this time there is no any terminological base adopted appropriate legislative acts;
- lack list of objects with critical infrastructure – there is no concept, criterion assignment to critical infrastructures;
- weak development of the information component most critical infrastructures (i.e., objects that can intuitively include to critical infrastructures, as you know, in Ukraine such term is not defined);
- lack of consistency priorities of business and IT. Very often, these levels define critical very different things;
- lack of integration of management processes of critical IT infrastructure;
- lack of specific mathematical models, algorithms that could have been used for managing critical IT infrastructure;
- orientation of research on methods of creation, organization and management of IT departments on the whole.

Requirements for the operation of critical IT infrastructure

Securing critical IT infrastructure is realized by meeting the requirements for its development and operation, including as a set of measures establishing a system of security critical IT infrastructure of legal, organizational and technical. As part of a security system is being developed and implemented by a monitoring system of information security of critical IT infrastructure. This system is designed to provide choice, control and actualization measures and means for information security management of critical IT infrastructure at all stages of its life cycle and in continuous occurrence of security threats. Reliability of critical IT infrastructure provides a choice of methods and ways of planning, design, development, commissioning, direct operation, modernization, decommissioning, allowing to exclude or reduce an acceptable level of losses to critical IT infrastructure as a result of a breach of its staff operation in normal conditions and conditions of implementation of security risks.

Measures to ensure the reliability of critical IT infrastructure shall be provided on all stages of its life cycle. To ensure reliable functioning of critical IT infrastructure is essential to observe the following requirements:

- reservations hardware and software of critical infrastructure at the level of hardware and software means, communications channels and data transfer and means of protection;
- providing allowable downtime of critical IT infrastructure while switching on reserve assets;
- avoid the possibility of launching and functioning critical IT infrastructure, bypassing the security system.

Generalized structure of the critical IT infrastructure of enterprise

IT infrastructure of any company or organization is a set of interrelated structures, systems, objects, etc., which ensures the proper functioning of the IT system. The specific scheme of IT infrastructure is determined by the size of the organization, the nature of business problems being solved, the list of IT used, etc. [6].

Businesses that limited to the use of several LAN installed on the server business applications, allowing slightly improve employee productivity by automating a number of business of processes can carry significant losses due to, for example, loss of data due to the lack of backup. IT infrastructure, which lacks only some of the important components, will be cheaper, but not necessarily effective. The maximum result from the functioning of the IT infrastructure can be achieved only with the complete comprehensive IT infrastructure that allows perform rationally and effective of activity processes decide business challenges. Same time such an organization's IT infrastructure – is a complex and lengthy process which requires serious capital investment company to create IT infrastructure and significant current cost in its support.

When considering questions related to the management of IT infrastructure different numbers of hierarchical levels are allocated, depending on the specifics nature of the business and infrastructure of solvable the control system (MIS) problems. For example, in [7] when considering of metrics operators of telecommunication services (OTS) released five hierarchical levels: telecommunications technology; network; services;

subscriber; the telecommunications business. According to the model OSI [8], the concept of network management (TMN) examines the logical network architecture that includes five levels of management [9] – a level of network elements, management level elements, networks, and the level of business management. In [10] the concept management of IT infrastructure is regarded in relation to the hierarchical structure, which contains three layers: the bottom – management of networks, middle – management systems, top – IT management of service.

It is reasonable to consider IT infrastructure enterprises (which is part of ITS) as a generalized hierarchical scheme, which is shown in Fig. 1.

In the IT infrastructure – organizational and technical totality of IT systems and TCR [11] – it is proposed to allocate four-level hierarchy with two or three sublevels in each: the level of business applications (the sub-critical and other business applications), the level of universal services (sub of protection services, and other critical services), the level of computing resources (the sub-critical and other resources) and the level of network interaction (the sub-objects protection of IT infrastructure, and other objects of critical of IT infrastructure).

On IV-th level are performed distributed applications that are directly related to business process automation or process activity. At this level, are working such systems as: enterprise resource planning (ERP), human resource management (HRM), customer relationship management (CRM), product lifecycle management (PLM), workflow management (Work Flow), document (SEDO), BSM and many other IT that are essential for a successful business venture. Some of those processes are critical (ERP, Work Flow, etc.). Their stoppage can result in serious financial loss or accident. Also on this level there are software tools that determine the importance of business processes in the enterprise, their criticality and MIS components that are responsible for the distribution of computing and communication resources.

On III-th level there are services that do not depend on the specifics of business venture. These services include: email, DBMS, videoconferencing, and various web services, file transfer services, IP telephony, a means of ensuring access to the Internet and so on. Among of these services is also critical. Breaking their work will lead to loss of efficiency critical applications business level. Security level of services is responsible for the security and access to universal services and ensure the provision of protection for business-level applications. The level of computing resources includes a user terminal and the resources data processing center (DPC).

Businesses are small, and branches are almost always used in place of a data center or server cluster solution, which hosts the server parts, software levels, business applications and universal services.

All computing resources are proposed to be realized as cloud resources with services as EaaS (all – as a service).

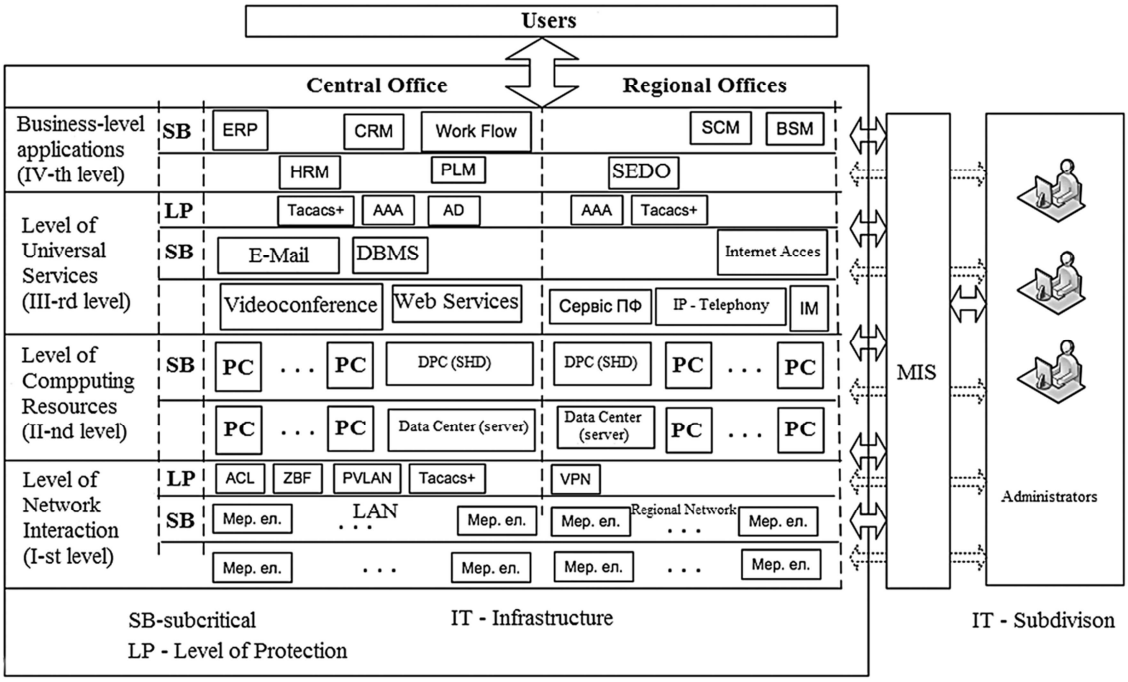

Figure 1. Generalized structure of critical IT infrastructure

When using the external cloud resources IT department must decide organizational matters and it is responsible for monitoring of the services quality. Cloud resources can only be used for the implementation of non-critical services critical IT infrastructure.

User access is carried by means of networking. At this level, the critical elements of a fully reserved, the basic physical topologies which are used to connect elements are Full Mesh or Partial Mesh.

System security of critical IT infrastructure is implemented on all levels. Its main elements are structurally related to the first and third levels (label "C").

As part of the security systems creation of critical IT infrastructure it is necessary to implement the following complex measures:

- classification of assets of critical IT infrastructure, including the categorization of data, information exchange by category access;
- development and correction of information security policy;
- development and correction of requirement for security systems;
- implementation of the requirements while creating security systems;
- development and implementation of information security monitoring system;
- control.

Classification of assets critical IT infrastructure is the defining elements that are important for the execution of business operations. In the classification of assets must be considered: the importance (criticality) to execute key business transactions; security (existing protective measures and their adequacy). The following criteria for classification are proposed (in the absence of any legislation in Ukraine on a given subject):

−criterion of economic significance;
−criterion of environmental significance;
−criterion of significance for defense capability;
−criterion of relevance to national security;
−criterion of social value;
−criterion of significance in the part implementation of management functions.

On the base of the proposed criteria of critical IT infrastructure it makes sense to divide them into three classes of hazard: high, medium and low.

Management of critical IT infrastructure is carried out by means MIS. The objectives of the MIS is to conduct the inventory database on Enterprise Resource monitoring and management support for the state of these resources at the right level, access control and distribution of computing and telecommunication resources, supervision, behavior analysis and user support, planning and acquisition management of IT assets and activities automation of reporting IT department, appropriate functioning of critical infrastructure. MIS can not only reduce the cost of the IT department maintaining, but also can automatize the work of IT department.

Mandatory constituent of the critical IT infrastructure of the critical infrastructure is the IT department. Businesses with critical infrastructure through its specifics cannot use the services of outsourcing companies. The main task of the IT department – service requests of business processes in strict time limits. Requirements for the provision of IT services are governed by Service Level Agreements service (SLA). In the SLA it is determined by key performance indicators (KPI) and quality (KQI) – limited set of objectively measurable parameters that allows us to estimate the effectiveness of the work of critical IT infrastructure. ISO 20000 standard [11] defines a role for MIS which supports IT service management, such as control metrics that characterize the behavior of IT processes.

For IT service management in the critical IT infrastructure it is necessary to have at least three IT departments: support critical services and infrastructure elements, non-critical support services, managing critical IT infrastructure that is responsible for the functioning of ITS in general.

Mathematical model of management resource allocation CIT & for the case interdependencies business processes and universal services

According to ITSM [13] the following main groups of IT can be identified:

- IT support services and resource management;
- management of IT services and processes;
- performance and the delivery of IT services.

Consider one of the primary goals of the first groups – task of managing resource allocation for critical IT infrastructure. For this task, you can build many different models with different initial conditions and restrictions. Consider the model the case of interdependence business processes and universal services.

Enter the model for the formation of CIT & notation: $Z_1,...,Z_n$ – a set of business processes, which ensures efficient operation of the facility management;

$S_1,...,S_m$ – a set of universal services, which provides support for the effective functioning of the control object;

$w_i^z,...,w_n^z$ –critical business processes factors respectively for fuzzy scale:

- critical - $\alpha_1 \le w_i^z \le 1$;
- very important - $\alpha_2 \le w_i^z < \alpha_1$;
- important - $\alpha_3 \le w_i^z < \alpha_2$;
- not important - $w_i^z < \alpha_3$.

$w_i^S,...,w_m^S$ –critical factors for universal services $S_1,...,S_m$ in accordance with fuzzy scale:

- critical - $\gamma_1 \le w_i^S \le 1$;
- very important - $\gamma_2 \le w_i^S < \gamma_1$;
- important- $\gamma_3 \le w_i^S < \gamma_2$;
- not important - $w_i^S < \gamma_3$.

$R_1,...,R_m$ – resources of critical IT infrastructure needed to support of business processes;

$p = \left\| \tilde{p}_{ij} \right\|$ – matrix needs of business process of resource critical IT infrastructure, where $\tilde{p}_{ij}$ equal to the amount required for the business process Z_i resource R_j in the form of the triangular fuzzy numbers $\tilde{p}_{ij} = (p_{ij}^{\text{п}}, p_{ij}^{\text{с}}, p_{ij}^{\text{к}})$ or 0 if the resource is not required where $p_{ij}^{\text{п}}$ - worst (maximum) version resource needs $p_{ij}^{\text{с}}$ - average resource requirements, $p_{ij}^{\text{к}}$ - the best (minimum) variant resource requirements. $s = \left\| \tilde{s}_{ij} \right\|$ – matrix needs universal service resource critical IT infrastructure, where $\tilde{s}_{ij}$ equal to the number required for universal service S_i resource R_j in the form of the triangular fuzzy numbers $\tilde{s}_{ij} = (s_{ij}^{\text{п}}, s_{ij}^{\text{с}}, s_{ij}^{\text{к}})$ or 0 if the resource is not required where $s_{ij}^{\text{п}}$ - worst (maximum) variant resource requirements, $s_{ij}^{\text{с}}$ - average resource needs $s_{ij}^{\text{к}}$ - the best (minimum) variant resource requirements. High demand for resources is determined by (1):

$$p_{ij}^{\text{с}} = \frac{p_{ij}^{\text{п}} + \beta p_{ij}^{\text{нв}} + p_{ij}^{\text{к}}}{2+\beta}, \qquad s_{ij}^{\text{с}} = \frac{s_{ij}^{\text{п}} + \chi s_{ij}^{\text{нв}} + s_{ij}^{\text{к}}}{2+\chi}, \quad (1)$$

where $p_{ij}^{\text{нв}}$, $s_{ij}^{\text{нв}}$ - the most likely options for resource requirements for business process and universal service β, χ - weighted averaging parameter that determined experimentally.

$\tilde{r}_1,...,\tilde{r}_m$ – triangular fuzzy numbers look $(r_i^{\text{п}}, r_i^{\text{с}}, r_i^{\text{к}})$, determining the amount of resources $R_1,...,R_m$ in accordance.

Critical process or service is always maintained. Other processes or services served by critical ratios.

We introduce the coefficients of the triangular fuzzy variables as follows:

$$x_i = \begin{cases} 1, \text{ if business process } Z_i \text{ is critical and maintained primarily} \\ \alpha_2, \text{ process is very important and is served} \\ \alpha_3, \text{ process is important and is served} \\ 0, \text{ process is not important and is not served} \end{cases}$$

$$y_i = \begin{cases} 1, \text{ service } S_i \text{ is critical and maintained primarily} \\ \gamma_2, \text{ service is very important and is serviced} \\ \gamma_3, \text{ service is very important and is serviced} \\ 0, \text{ service is very important and is serviced} \end{cases}$$

Thus, control of resource allocation CIT & A is to find the maximum following objective function (2):

$$\tilde{U} = \sum_i \tilde{x}_i \tilde{w}_i^Z + \sum_k \tilde{y}_k \tilde{w}_k^S \to \max, \quad (2)$$

in the presence of constraints (3) and (4):

$$\sum_{i=1}^{n} \tilde{x}_i \cdot \tilde{p}_{ij} + \sum_{i=1}^{m} \tilde{y}_i \cdot \tilde{s}_{ij} \le \tilde{r}_j, \quad (3)$$

$$N_{кр} \to \max, \quad (4)$$

for $j = 1,..., m$.

Condition (4) defines the fact that the number of critical processes and universal services that are required to serve a maximum, that all critical processes and services need to be resourced. Otherwise, the control of the resources distribution is not possible to enter the additional resources.

Odds $\tilde{w}_i^Z, \tilde{w}_k^S$ objective function represent a fuzzy number - $\tilde{w}_i^Z \in \left[w_i^{zL}; w_i^{zR} \right]$, $\tilde{w}_k^S \in \left[w_k^{sL}; w_k^{sR} \right]$, L і R - left and right borders of the carrier fuzzy numbers.

Problem (2) - (4) is a fuzzy linear programming problem which can be solved using the methods described in [14].

Example of using the proposed model

Consider a distributed and multi-cluster. Typically, this cluster has hundreds of servers located in different racks. The connection between the two machines on different racks can pass through one or more switches. Multi-distribution is a very difficult task for reliable, scalable, accessible dissemination. For a cluster need to develop policies placement of replicas that must satisfy the following properties:

- maximize reliability;
- Maximizing the availability of data;
- maximize the use of network bandwidth.

Replicas should be placed not only on different disks or different machines, but in different racks. This ensures that the process or service will be available, even if the whole rack is damaged or disconnected from the network. With this arrangement, reading takes time, which is approximately equal to the bandwidth, while the flow of data when writing to go through the different racks.

At the same time, when creating a new critical process or service is determined where to place the replica. It should consider the following:

1. Discover the replica of critical process or universal service hosted on the server with the lowest Average discs. In this way, the workload is aligned disks on different servers.

2. Created number of new critical processes or universal services on each server is limited. Despite the fact that the creation of a new process is fast transaction, it provides further writes data to the server that is already a difficult operation, and that can lead to imbalance of traffic data in different parts of the system.

3. As stated above, it is necessary to distribute servers between racks.

4. Once the number of replicas falls below a user- settable values must again perform a remark critical process or service. This may occur for several reasons:

server became unavailable;

one of the disks has failed;

increased number of replicas.

Each critical process or universal service for which you want to make an appropriate priority replica set, which also depends on several factors. First priority is higher in the critical process or universal service that has the least number of replicas. Second, to increase the reliability of applications increased priority processes or services that are blocking progress in the client. First, serviced critical processes.

5. Selects process or service with the highest priority and is copied from one of the replica server, which is the most affordable. The new replica is located, based on the same reasons as in the creation.

6. Creating replicas is balanced constantly. Depending on the distribution of the replicas in the system, replicas are moved to align the load drive and load balancing. You also need to constantly decide which of the replicas are wise to be removed at this time. Typically, deleted replica that is on a server with the smallest available hard drives.

The resource management model (respectively, the number of required resources are servers and hard disks, the number of free resources to create new processes and services replicas to accommodate each of our critical processes and universal services for their reliable operation) within the existing constraints (availability of servers and place to place replicas on separate servers, the number of available resources to create new processes and services) can allocate the maximum number of critical business processes and universal service in a way that is not considered breached the principles of operation of the cluster.

By a similar principle MapReduce technology from Google works. The main difference is that the technology does not work with critical processes, and works with a variety of data in a file.

Conclusion

During the research the terminology and requirements for safe, reliable functioning of critical IT-infrastructure was identified. The generalized structure of critical IT - infrastructure, identified its main level, the sub levels and functionality. Also in work for the proposed structure is described a mathematical model of resource allocation control in case of interdependent processes and universal services.

References

1. On Amendments to some laws of Ukraine to ensure the cybernetic security of Ukraine: Draft Law / Verkhovna Rada of Ukraine [electronic resource]. – Available: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=44208.
2. COBIT 5.0. The Russian edition. ISACA. – Moscow: – 2012. – 94 p..
3. E.N. Mashchenko Investigation of the processes of critical IT infrastructures service maintenance based on semi-Markov model / E.N. Maschenko, V.I. Shevchenko // Radio-electronic and computer systems, № 5. – SevNTU, 2013. – P.57-63.
4. A.V. Skatkov Mathematical model for solving the problem of parametric synthesis in critical IT-infrastructures / A.V. Skatkov, A.A. Skidan, D.Yu. Voronin, N.I. Kuznetsova // Collected Works of SNUNEandI. – SevNTU, 2013. – P.229-233.
5. E.N. Mashchenko Investigation of critical situations in IT infrastructure by cluster analysis methods / E.N. Maschenko, V.I. Shevchenko // Radio-electronic and computer systems, № 5. – SevNTU, 2013. – P.191-196.
6. A.I. Rolik Trends and perspectives of information technology management development / A.I. Rolik // Visnyk of NTU "KPI": Informatics, Management and Computer Science. – K.: "VEK +", 2012. – № 55. – P.81-109.
7. Boutaba R. CyberPlanner: A Comprehensive toolkit for network service Providers / R. Boutaba, J. Xiao, I. Aib // NOMS 2008 — 11th IEEE/IFIP Network Operations and Management Symposium. — 2008.— Vol. 11, No. 1. — pp. 379—386.
8. Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model: ISO/IEC 7498-1:1994. Second editions, 1994. — 68 p.
9. Principles for a telecommunications management network: ITU-T Rec. M.3010. — Geneva. — 2000. — 36 p.
10. S. Katishev On a concept of distributed resources management // Open Systems. – 1998. – № 3.
11. A.I. Rolik The control system of corporate information and telecommunication infrastructure on the basis of the agency approach / A.I. Rolik, A.V. Voloshin, D.A. Halushko, P.F. Mozharovsky, A.A. Pokotilo // Visnyk of NTU "KPI": Informatics, Management and Computer Science. – K.: "VEK +", 2010. – № 52. – P.39-52.
12. Information technology. Service management. Part 2: Code of practice: ISO/IEC 20000-1:2005. — ISO/IEC, 2005. — 34 p.
13. Mendel T. Holistic View: The IT Management Software Market / T.Mendel, C.Townsend. – Forester Research, Inc. – 2008. – Jun. 19. – 13 p.
14. Liu B. *Theory and Practice of Uncertain Programming* / B.Liu. – UTLAB. – 2009. - http://orsc.edu.cn/liu/up.pdf.

Received in final form March 19, 2014