I. J. Computer Network and Information Security, 2013, 2, 21-28
Published Online February 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.02.03

Integrated Safety Mechanisms Based on Security Risks Minimization for the Distributed Computer Systems

Vadym Mukhin
Department of Computer Systems of National Technical University of Ukraine "KPI",
Kiev, Ukraine
v_mukhin@mail.ru

Artem Volokyta
Department of Computer Systems of National Technical University of Ukraine "KPI",
Kiev, Ukraine
artem_volokyta@kpi.ua

Abstract — Today, there are known the basic principles of decision-making on the safety control of distributed computer systems in the face of uncertainty and risk. However, in this area there are no practical methods for the quantitative risk analysis and assessment, taking into account the dynamic changes of security threats, which is typical for distributed computer systems.

In this paper is suggested an approach to assesment and minimization of the security risks, which allows to reduce the potential losses due to the realization of threats, to analyze the dynamics of intrusions into computer systems and to select the effective security tools.

As a result, there is designed the structure of the tools for risk minimization in the distributed computer systems and are formalized the main functions of this structure. Also, in the paper is suggested the assessment of risk factors of the security threats and the probability of the threats realization, which are based on their division into appropriate groups. The proposed tools for security risk minimization allow effectively identify, classify and analyze threats to the security of the distributed computing systems.

Index Terms — distributed computer systems; safety model; security risks minimization

I. INTRODUCTION. THE SAFETY PROBLEMS IN DISTRIBUTED COMPUTER SYSTEMS

In the modern society, the information technologies have wide implementation and now became the essential development factor. The distributed computer systems (DCS) considerably raise the efficiency of an information component in the organizations activities, but, at the same time they are one of the most vulnerable components, which attract the intruders [1].

The importance of safety providing in the computer systems is increasing due to a number of the objective factors. In particular, the DCS should provide the high level of trust to them since there the valuable and confidential information with the real value for its owner is stored and processed [2,3]. The unauthorized access to this information, such as, the destroying or modification, can lead to a serious damage.

The safety problems in DCS are subdivided into three categories [1, 4]:

1. Integration problems;
2. Interaction problems;
3. Problems of trusted relations

Decisions in one of categories of problems will be often based on decisions in other categories. The dependence between these 3 categories is shown on Fig. 1.

A. Integration problem

The architecture of DCS safety should solve the problem of integration with existing architecture and safety models, irrespective of a platform and an environment hosting. It implies that the architecture implementation should be independent and allows to make changes to existing safety mechanisms (for example, Kerberos, PKI); it should be enable to add the new services of safety when they need; also it should be integrated with existing safety services [4].

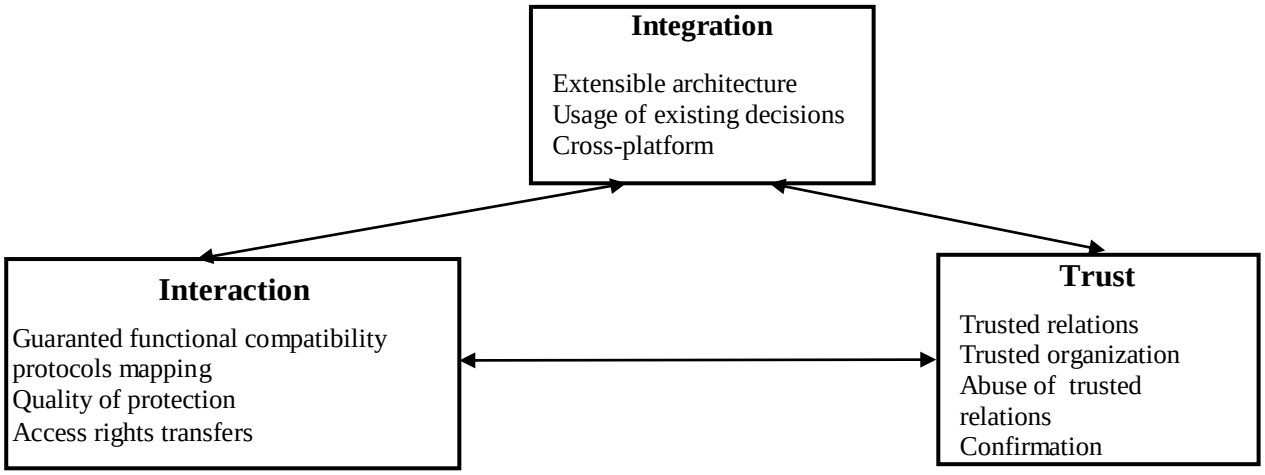

Fig. 1. The categories of safety problems in DCS

B. Interaction problem

Services which are used in set of domains and in the environments hosting, should interact with each other; thus there should be provided the interaction: At the protocol level, At policies level, At users level.

C. Problem of trusted relations

The requests in DCS may be transitted via several safety domains. The trusted relations between these domains are important when point-to-point interactions are performed [5]. There should be the option for users to request corresponding services for the secured access.

The problem of trusted relations in DCS environment is more complicated because there is necessary to support the dynamical scaling of DCS resources and control of temporary services.[6] The node-users create such temporary services to perform the specific requests, which call the other services. The problem of temporary services creation includes Identification and authorization, Introduction of policies, Providing the assurance level, the Composition of policies, Delegation.

The paper contains the next main sections: Model of safety in the distributed computer systems; Approach to security risks minimization in the distributed computer systems; Assessment of risk factors of the security threats and the probability of the threats realization.

II. REQUIREMENTS TO SAFETY IN DCS

The main requirement to the safety mechanisms in DCS is the option to find out and to add the new safety mechanisms. This factor allows to select certain services from a set of the distributed architecture of safety, and to add them in an existing safety infrastructure.

Safety of DCS should be complex from the network level to application and data servers level, and should allow to integrate the safety mechanisms.

The basic model of DCS safety includes following aspects [7, 8, 9]: Authentication; Delegation; the Unified login; Duration of right access actuality and their update. Authorization; Confidentiality; Privacy; Integrity of messages; the policy exchange; the Protected recording; Warranties; Controllability.

These requirements and functions form a basis for interaction, which is based on standards, not only for actions inside the single domain, but also for different domains of DCS. This infrastructure is the basis for trusted relations realization, for corporate applications integration and for B2B-partner cooperation via Internet.

III. MODEL OF SAFETY IN THE DISTRIBUTED COMPUTER SYSTEMS

The model of safety in DCS, which support the complex protection of various DSC segments and resources forming the virtual computing environment, is suggested.

The access to DCS resources is realized with a number of the protocols supporting certain formats of messages; thus security mechanisms should provide the required quality of service, in particular, such safety functions as confidentiality, integrity and authentication. The model as components includes the following [8]:

The protection of data transmission protocols. The DCS use the number of protocols for data transfer, such as SOAP (SOAP on HTTP, SOAP with a queue of messages or SOAP on the other protocol) and IIOP protocol. The suggested model for DCS safety raises the security level of these protocols.

The data transmission. DCS safety mechanisms should support all formats of messages of security tools, implemented on a node, and users should use the same formats. As a result, the users requesting DCS resour-ces and security tools for these resources jointly select an optimal set of protocols for date transmission.

Safe communication channels. The security policy for DCS demands for the protected data transfers to perform the mutual authentication of users and DCS resources and to install a safe data link which further will be used for the protected date transfers.

Authentication and transfer/display of safety certificates. The safe interaction between the various DCS segments requires to coordinate the security mechanisms, for example, Kerberos and PKI, by display or transfers the identifiers and/or certificates via the proxy-server, gateways (routers) or entrusted

intermediate nodes. The uniform structure of the user's registration is formed, which provides their authentication and the access rights to resources delimitation.

Access rights to resources delimitation. Usually, each DCS segment has own tools for access rights delimitation for decision-making on the subjects access to the resources. The users requesting resources, often trust DCS or to the providers, which provide access to them. Otherwise, the authentication of DCS resources, for example, with SSL protocol is performed.

The privacy support of the users. The users anonymity or restriction in access to information about the user are extremely important for some DCS. The model of DCS safety should support specification WS-Privacy, in addition to WS-Policy to support the privacy policy in the DCS environment.

Trust in DCS. The safe handling of requests, which are generated by DCS users, requires to establish the confidential channel between all users. The trust model in DCS is based on specification WS-Trust. Due to the dynamic character of DCS, the confidential relations in also may be dynamically changed with usage the entrusted proxy-servers.

Security control of DCS. The model of DCS safety includes all functions of security control: data transfers protocols, security policy and integration tools for security mechanisms. These functions, in turn, include the keys control for messages crypto-protection, the user's registration control in DCS, the access control to resources, control of policy of trust and control of tools for DCS resources integration.

Security tools of DCS and modern standards in the field of DCS safety. The virtual environment of DCS supports the full integration of all resources into the united complex.

The DCS security is based on the existing technologies, for example, certificate X.509 with public keys, secret Kerberos tickets, etc. Thus, the suggested model for DCS safety supports and expands the existing standards in the field of computer systems safety.

Due to the fact, that the open DCS has the server-oriented architecture, the DCS safety model should be compatible to the safety model for the single nodes of DCS. The safety tools of nodes are based on the multi-level approach. Fig. 2 shows the levels of the safety technologies and standards [8].

Security mechanisms of DCS are developed either during DCS creation, or existing security mechamisms (for example, tools of access delimitation, built in an operating system, authentication etc.) are used. The elements of DCS, which implement the security mechanisms are the platforms (for example, Kerberos in z/OS-environment on platform AIX), the base environments (for example, the application-oriented server on J2EE uses the embeddable mechanism for the access rights delimitation), or applications (for example, the financially-oriented program applications may support the payment mechanism on the digital signature).

IV. SECURITY RISKS MINIMIZATION IN THE DISTRIBUTED COMPUTER SYSTEMS

To reduce the vulnerability level in DCS and to avoid the losses of the critical information, the additional security mechanisms should be applied [10].

One of such mechanisms is a security risk analysis in DCS. This analysis allows to research the object, to estimate the current level of the security, to reveal weak spots in safety system, to create models of possible threats for DCS, to check up the correctness of the security tools selection and adjustment.

The risk is the probability of the undesirable event realisation, which leads to the information losses, and also the volume of damage in result of unauthorized access. The security risk analysis implies to perform the estimation of the risk level and damage volume due to the unauthorized access, performed with a special methods and tools [11].

Also, the process of the risk analysis implies the analysis of DCS components, which can undergo to threats, the reveling of the weak spots in the system, the estimation of the probability of the each specific threat realization and of the possible volume of losses, the selection of the possible security methods and the estimation of their cost. At the final stage, the efficiency of the suggested mechanisms implementation is estimated.

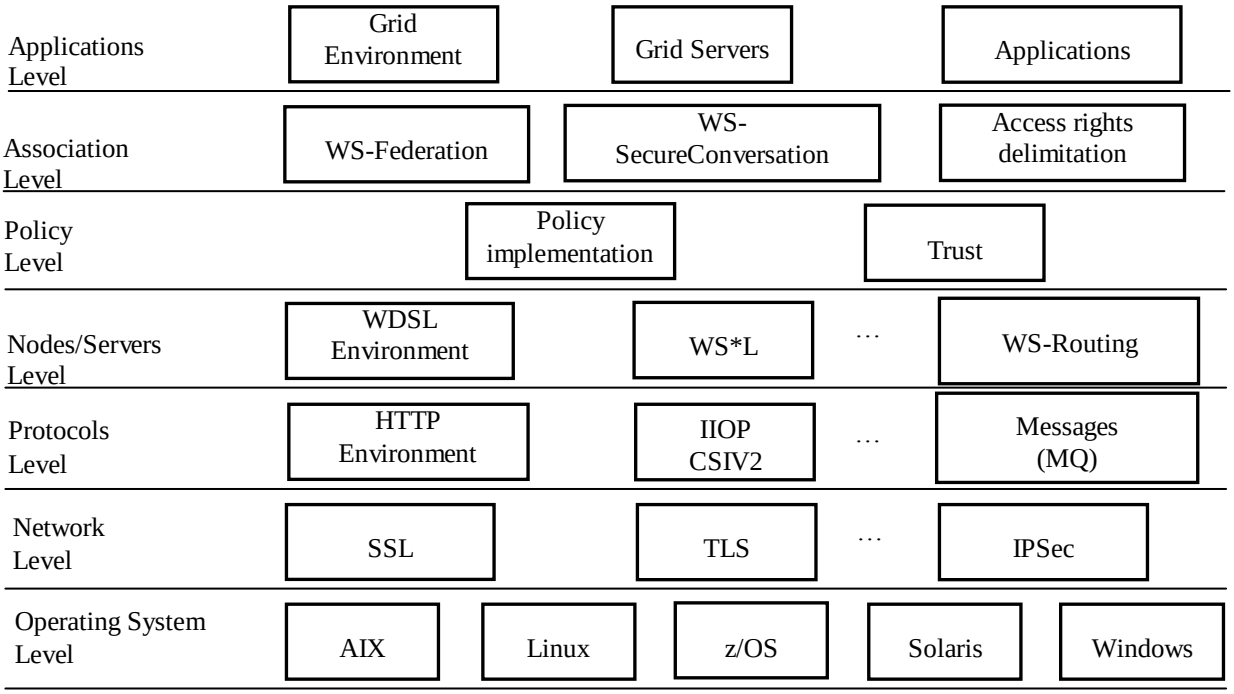

Fig. 2. The levels of architecture of DCS safety system

As a result, the security risk analysis is the base for the decision making how to use the certain security methods and tools, which are represented in the special document on the security policy in DCS.

A. Mechanisms for the security risks minimization

Let's consider the general structure of the mechanisms for the security risks minimization. (Fig. 3) The structure includes 8 blocks: set of the goals, the safety threats estimations, the vulnerabilities estimations, the security risks analysis, the choice of reaction (on potential attacks) variants, the decision-making, the reaction, the DCS parameters monitoring.

The blocks of the set of the goals, the security risks estimations and the vulnerabilities estimations perform the preliminary gathering of information about the DCS security status and provide the data for the following stages of security risks estimation. The block of the security risk analysis is the main block because it defines a current risk level, its criticality, and also the factors, allowing to lower the security risks. The following 4 blocks define the possible variants of reaction to the potential intrusions, make the decision and react to the attacks, and also perform the modification and monitoring of the parameters of the DCS security tools.

Let's consider the specifics of these blocks realization in more detail.

B. The block of the set of the goals

This block defines the parameters, which are in use for the analysis and minimization of the security risk in DCS. Usually, these parameters are set by the safety administrator, who should reveal permanently the potential threats, vulnerability and to estimate risks.

The block of the set of the goals is represented by criterion function *f*:

$$f = f(s_i, a_i, g_i) \quad (1)$$

where s_i – the subject -initiator of the event, a_i – the parameters of the subjects actions, g_i – the possible goals.

In turn, the parameters of subjects actions a_i are represented in the data tuples form:

$$a_i = f'(\{t_1,...t_c\}, \{l_1,...l_d\}, \{r_1,...r_e\}, \{\gamma_1,..., \gamma_f\}) \quad (2)$$

where t_i – the time of event appears, l_i – the event place, r_i – used tools, γ_i – the danger level of the event.

The parameters, defined in this block, are used in other blocks of the security risks minimization system.

C. The block of the safety threats estimations

Security risk is the possibility (probability) of the fact that the intruder can get unauthorized access to DCS resources. In general, all the security risks are subdivided into the threats of modification or stealing

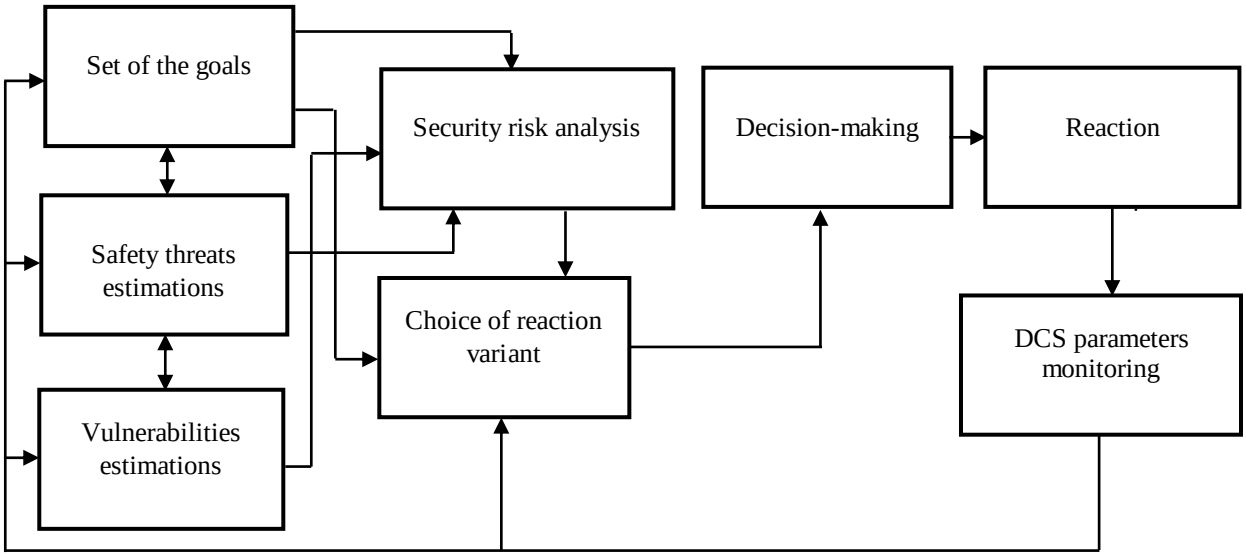

Fig. 3. The structure of the mechanisms for the risk of security risks minimization in DCS

of the critical data; the threats of violation of the DCS system software functioning; the threats, which leads indirectly to the unauthorized access. This block performs the general analysis of the possible threats for the DCS, grouped into the classes.

The safety threats estimation includes 2 components: the situational analysis and the threats detection.

The situational analysis is the detailed analysis of DCS hardware/software parameters, including the parameters of security tools. This analysis implies that the same data will be grouped, and they are estimated separately on each group.

The threats detection provides the complex and detailed analysis of all factors which can be influent on the DCS safety. Threats are divided into 3 basic groups: "potential" threats – actions, which can be theoretically dangerous; "real" threats – the intruders actions; "direct" threats – actions, directed on the certain vulnerabilities in DCS hardware/software.

The effective level TL_j of the safety threat from j intruder is suggested to calculate as:

$$TL_j = \omega_1 * LP_j + \omega_2 * \frac{1}{n} \sum_{i=1}^{n} F_{ij} \quad (3)$$

where LP_j – the potential threat level of the intruders actions, F_{ij} – the adjusting factors from the intruders model, n – the number of the analysed factors, ω_1, ω_2 - the weight factors, which regulate the relative weight of both components in TL_j, and $\omega_1 + \omega_2 = 1$. In case if the some factor of the intruders actions has several values, the average value of this factor is used. The potential threat level of intruder LP_j actions is his general possibilities, unlike the certain possibilities TL_j for the certain DCS.

The data of the block of set of goals are used to calculate and adjust the parameters ω_1, ω_2, F_{ij}, LP_j.

D. The block of the vulnerabilities estimations

This block allows to reveal the vulnerabilities, i.e. the potential possibilities for the intruder to receive the unauthorized access to the DCS resources, which lead to damage to the DCS hardware/software and to the processed data.

The vulnerabilities estimations include 2 components: the vulnerabilities detection and the determination of the factors, which allow to reduce the risk of the vulnerabilities realization

The vulnerabilities detection. The vulnerability is the potential way of the threat realization, i.e. this is a weak point ("hole") in the existing DCS safety mechanisms. The factors, which may generate the new vulnerabilities in particular, are the unsafe resources or resources with the low security level, the ineffective security mechanisms, the incorrect actions on the threats preventing, the lack of the qualification of safety administrators, the potential errors in the software etc.

Determination of the factors, which allow to reduce the risk of the vulnerabilities realization.

There are 6 main factors, which make influence on the DCS vulnerability: the point of vulnerability appearance, the level of DCS security, the value of the processed information, the influence of DCS specifics, the adequateness of security tools applying, the qualification of safety administrator.

Let's enter the concept of the vulnerability of types I and II. The type I are such vulnerabilities, which are potentially prevented by the security tools implemented in DCS and the type II are those, which are not prevented even potentially. We generate an integral estimation C, determined the potential damage due to the attacks on DCS vulnerability:

$$C = \sum_{i=1}^{N} \frac{UI_i}{U} + \sum_{j=1}^{M} K_j * \frac{UII_j}{U} \quad (4)$$

where UI – the number of users, who are compromated as a result of attack to the vulnerability of the type I; N – the number of vulnerabilities of type I; UII– the number of users, who are compromated as a result of attack to the vulnerability of the type II; M - the number of

vulnerabilities of type II; U – the total number of users in system; K_j - the coefficient, characterizing the vulnerability of type II.

To obtain this estimation it is necessary for the each revealed vulnerability:

1. To define the vulnerability type: I or II;
2. If there is the vulnerability type II with the experts estimations to define the possible consequences of this vulnerability realization and to calculate coefficient K_i;
3. To estimate the number of users, who may suffer the attacks, realized with using vulnerabilites types I and II, in relation to the total number of users in DCS.

E. The block of the security risks analysis

The security risk analysis is based on the probability estimation of the unauthorized actions realization which performed using the vulnerabilities in safety mechanisms. This analysis requires the complex registration of all factors on the security risks in DCS. Thus in the case when the existing security risk is serious, but the probability of its realization is low, i.e. its influence on DCS safety is estimated as insignificant then the security risk level also is considered low.

The security risk analysis uses 2 parameters: the probability of the security risks realization and the estimation of damage level due to the security threats realization.

The estimation of a damage level due to the security threats realization requires to divide the factors into the groups, which are reflecting their danger level to DCS resources. Thus, factors with low danger level are considered as harmless, and factors with a high danger level should be neutralized.

Groups of the safety threats on their danger level are the next: critical, high, medium, low, insignificant.

The reference of the safety threats to the certain group of the risk level is based on expert estimations and on the previous statistical information on DCS parameters.

The probability of the security risks realization also is in one of the groups, which reflect the level of the possibility of the security threats realization.

The possibilities of the safety threats realization are grouped on the basis of the preliminary gathered statistical information about the DCS safety mechanism parameters. The levels of the possibility of the safety threats realization are next: practically impossible, improbable, possible, highly probable, almost inevitably.

We suggest using the function *TR*, reflecting the possibility of threat realisation, for the estimation of the risk of the threats realization by intruders:

$$TR = \frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PE_j = \frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PB_j TL_j, m \le n \qquad (5)$$

where K_{ij} =0, if the i-th position in the threat list is not related to the j-th intruder (non-dangerous factor), K_{ij} =1, if the i-th position in the threat list is related to the j-th intruder (dangerous factor), m – the number of potentially dangerous subjects, n – the total number of the subjects, PE_j – the effective probability of threat realization, PB_j – the basic probability of threat realization, i.e. the well-known or standard probability of certain threat.

The volume of the possible damage due to the threat realization is defined as:

$$PL_i = c_i \sum_{k=1}^{3} K_{ki} A_k \qquad (6)$$

where A_k - the priory-formed requirements to support 3 main features of the secured information: confidentiality, integrity and availability. These requirements can be formalized with the relative scale, and K_{ki} = 0 if the certain threat does not influence on k-feature of the information, K_{ki} = 1 if the certain threat influences on k-features of the information, c_i – the normalizing coefficient.

Thus, the risk of the safety threat realization R in DCS is next:

$$R = \left(\frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PB_j TL_j \right) x \left(c_i \sum_{k=1}^{3} K_{ki} A_k \right) \qquad (7)$$

The suggested approach allows to estimate the influence of the various factors on the quantitative values of the effective risk level and to formulate the requirements to the security methods and mechanisms.

F. The matrix of the security risks

The final stage of the security risk analysis is the generation of the matrix of security risks. This matrix is formed with two main parameters, describing the security risks: the danger level of the safety threats and the probability of safety threats realization. (Fig. 4)

The existing security risks are allocated in this matrix and for them are assigned the priorities, i.e. danger levels as probabilities of safety threats realization, and also the expert estimations are in use. There are 4 categories of security risks: Low, Medium, High and Ultrahigh. So, those risks, which are allocated in the right upper quadrant of a matrix (Fig. 2), are considered as the most dangerous risks. It is important to note that the assignment of the category to the risks depends on certain DCS specifics. The goal is to relocate all possible security risks in the left lower corner of a security risks matrix.

The regular updating of the security risks matrix allows to reveal the tendencies in the secured environment and also allows to estimate the fact of the lowering or increase of security risk in DCS. The security risks matrix can be used as a basis for the development of the strategy of security risks minimization and for the planning of the possible ways to lower the probability of the security risks realization.

G. The block of the choice of reaction (on potential attacks) variants

At this stage, the safety administrator should define a complex of mechanisms for DCS safety. The choice of securing mechanisms should be based on the analysis in a real-time mode of the critical parameters of safety and

the security risks. The possible variants of reaction to the attacks are the usage of the existing security mechanisms in an invariable way; the readjust of the parameters of the existing security mechanisms; the adding and the change of the configuration of the existing security mechanisms; the suspension or switch-off those security mechanisms, which are not necessary at the certain period.

H. The block of the decision-making

This block realizes 2 main functions.

First, here is making a decision about the priority directions of the security risks and the vulnerabilities detection. Often it appears that the spectrum of security risks is rather wide, and it is very difficult to provide the operative reaction to all actual threats. First of all, it is necessary to reveal the most dangerous threats and to neutralize them in a minimum time interval. Besides that, in case if the critical threats cannot be neutralized operatively, probably, there is a necessity to make the decision on the temporary halt of the entire DCS or of the some domains.

Second, at this stage it is necessary to define the required hardware/software resources and to estimate the corresponding expenses for the security risks mechanism implementation for the choice of the most effective security tools, in particular, by criterion the price/quality. The effectiveness of the security mechanisms is defined, first of all, by such parameters as the provided security level and expenses for the hardware/software for their implementation.

I. The block of the reaction to the threats

This block generates the reaction of the security mechanisms to the safety risks and prevents the unauthorized access to DCS resources.

J. The block of the DCS parameters monitoring

The effective prevention of the safety threat in DCS requires the permanent monitoring of the existing threats and vulnerabilities. This block is the final component in the suggested structure of the security risk minimization mechanism, and it coordinates the other blocks.

The suggested mechanism for the security risk minimization consider the requirements to the modern methods to the risk minimization and allow effectively to reveal, classify and analyze the security risks in DCS that provides the efficiency increasing of security mechanisms.

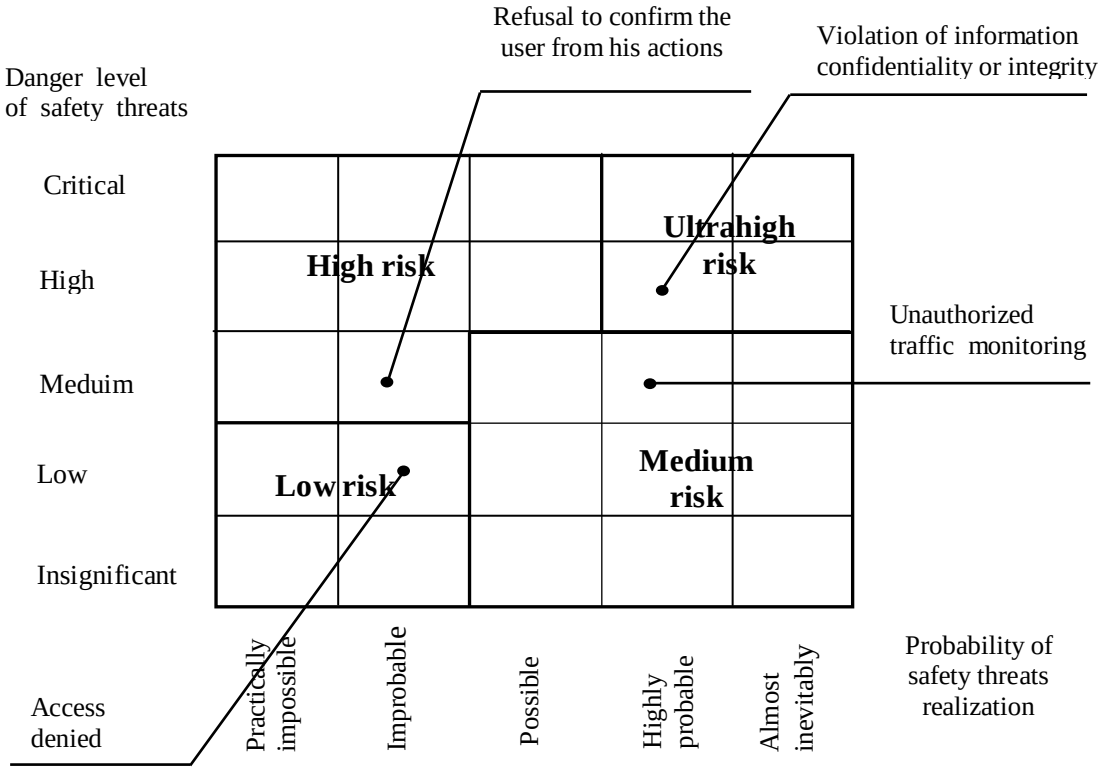

Fig. 4. The security risks matrix

V. CONCLUSION

The safety of DCS is based on the set of mechanisms, such as, in particular, the tools for the hardware/software security and the security administrator actions on their application. It is well known that the absolute safety of DCS to provide, in principle, impossible, but we may significantly reduce the security threats and security risks in the DCS. Due to the scaling of the DCS with the virtual computing environment and due to the implementation in the DCS such elements as firewalls, load balancers, routers, and due to the need to ensure the safe handling of data, the creation of the architecture and the special securing methods and mechanisms for the highly secured DCS is very actual.

This paper describes the requirements to the security of the modern virtual environment, and there is suggested the safety architecture for open DCS.

REFERENCES

[1] N.Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist, V. Welch, I. Foster, S. Tuecke, The Security Architecture for Open Grid Services: IBM Corporation, 2003.

[2] Risk Taxonomy, Open Group Publication, January 2009 www.opengroup.org/onlinepubs/9699919899/toc.pdf

[3] Information technology – Security techniques – Information security risk management, ISO/IEC27005:2007, Geneva, Switzerland, 2007

[4] P. Mell and T. Grance, Effectively and Securely Using the Cloud Computing Paradigm (v0.25), NIST Publication, 2009, http://csrc.nist.gov/ groups/SNS/ cloud-computing/index.html.

[5] M. Hentea, "Enhancing information security risk management with a fuzzy model", Proc. of 19th International Conference on Computer Application in Industry and Engineering. Las Vegas, USA, 2006. – pp. 132 – 139.

[6] R.Tassabehji, Information security threats. Encyclopedia of multimedia technology and networking. IDEA Group Reference. Hershey, Pennsylvania, 2005. – pp. 404 – 410.

[7] I. Foster, C.Kesselman, G. Tsudik, S. Tuecke, "A Security Architecture for Computational Grids", Proc. of 5-th ACM Conference on Computer and Communications Security Conference, 1998.

[8] I. Foster, C. Kesselman, J. Nick, S. Tuecke, "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration", 2002.

[9] A. Chakrabarti, Grid Computing Security: Springer, 2007.

[10] E. Maiwald, Fundamentals of network security. McGraw-Hill. Technology Education, New York, 2004.

[11] M. Hentea, Information security management. Encyclopedia of multimedia technology and networking. IDEA Group Reference. Hershey, Pennsylvania, 2005. – pp. 390 – 395.

Author's Profiles

Vadym Mukhin: Associate professor of computer systems department of National Technical University of Ukraine "Kiev Polytechic Institute", PhD, major interest in the security of distributed computer systems and risk analysis

Artem Volokyta: Post-graduate of computer systems department of National Technical University of Ukraine "Kiev Polytechic Institute", PhD, major interest in the cloud computing systems.