I.J. Intelligent Systems and Applications, **2016, 12, 57-64**
Published Online December 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2016.12.07

Analytical Assessment of Security Level of Distributed and Scalable Computer Systems

Zhengbing Hu
School of Educational Information Technology, Central China Normal University,
No. 152 Louyu Road, 430079, Wuhan, China
E-mail: hzb@mail.ccnu.edu.cn

Vadym Mukhin, Yaroslav Kornaga and Yaroslav Lavrenko
National Technical University of Ukraine "Kiev Polytechnic Institute", Kiev, 03057, Ukraine
E-mail: {v.mukhin, y.kornaga, y.lavrenko}@kpi.ua

Oleg Barabash and Oksana Herasymenko
Taras Shevchenko National University of Kiev, Volodymyrska Street, 64/13, 01601, Kiev, Ukraine
E-mail: oksgerasymenko@gmail.com

***Abstract*—**The article deals with the issues of the security of distributed and scalable computer systems based on the risk-based approach. The main existing methods for predicting the consequences of the dangerous actions of the intrusion agents are described. There is shown a generalized structural scheme of job manager in the context of a risk-based approach. Suggested analytical assessments for the security risk level in the distributed computer systems allow performing the critical time values forecast for the situation analysis and decision-making for the current configuration of a distributed computer system. These assessments are based on the number of used nodes and data links channels, the number of active security and monitoring mechanisms at the current period, as well as on the intensity of the security threats realization and on the activation intensity of the intrusion prevention mechanisms. The proposed comprehensive analytical risks assessments allow analyzing the dynamics of intrusions processes, the dynamics of the security level recovery and the corresponding dynamics of the risks level in the distributed computer system.

***Index Terms*—**Distributed computer systems, Security analysis, Risk-based approach.

NOMENCLATURE

α – the average intensity of the security threats for the distributed computer systems resources x1 and x2;
β – the average intensity of the security mechanisms from the group x3 and x4 activation;
R_0 – the initial security risk;
$R(t)$ – security risks in the distributed computer systems, changing at time t;
x_1 – the number of nodes in the distributed computer system;
x_2 – the number of data link channels;
x_3 – the number of the active security mechanisms;
x_4 – the number of the security monitoring tools in the distributed computer systems;
x_{1max} – the maximum nodes number in a distributed computer system;
x_{2max} – the maximum number of data link channels;
x_{3max} – the maximum number of the active security mechanisms;
x_{4max} – the maximum number of the security monitoring tools in the distributed computer systems.

I. INTRODUCTION

There are a significant number of vulnerabilities in the Distributed Computer Systems (DCS), which can be used by the intrusions agents for the attacks launching to get the unauthorized access to the information. In turn, there are known a number of methods and mechanisms for the intrusion detection and the appropriate host- and network-based systems for the monitoring and intrusion prevention [1]. ISO-15408 [2], [3] defines the requirements to the security mechanism and for the risk analysis at various stages of the security mechanisms design, development, implementation and maintenance. Also, this standard defines the function of the DCS owners and the information that should be implemented for the protection against possible threats and intrusions. The security risk analysis for the DCS is one of the most important trends in the field of modern effective mechanisms for the information protection [4], [5].

The security of the DCS resources is based on their protection from the threats that are classified in view of the possible level of safety violation [6]-[9]. We consider all kinds of threats, and the most dangerous are those that are performed by the subjects. Fig. 1 shows the main components of the DCS security and their interconnection [1]-[3].

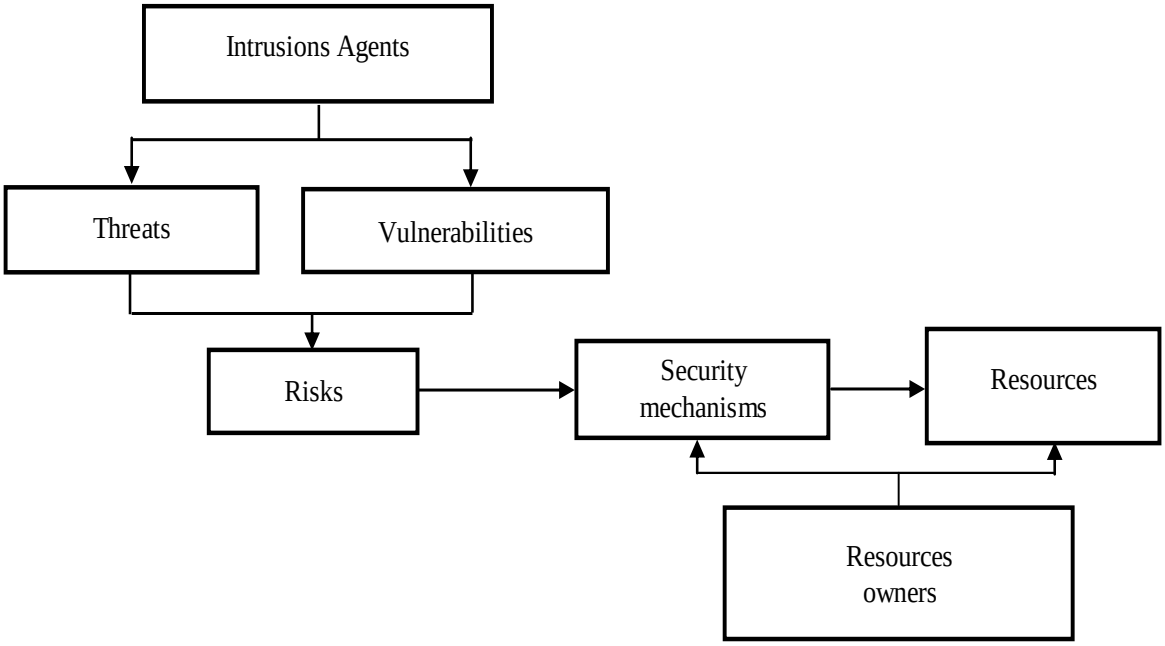

Fig.1. The components of the DCS security and their interconnection.

The effective protection of the modern computer systems requires support the safety of the operations with their resources, so there is a necessity for the timely identification of the potential threats to their security. It is necessary to analyze the full range of the possible threats. [1], [10]-[12].

The typical violations of the DCS security are [1]-[3]:

• disclosure of the resources confidentiality that leads to the certain damage;
• violation of the resources integrity as a result of unauthorized modification;
• blocking of the access to the resources, in particular due to incorrect ban for the legal subjects.

The resources of the computer systems have a certain value, in particular, for their owners and for the intrusion agents as well. So, the security threats have potentially adverse effects on DCS resources, resulting in, inter alia, reducing the resources value [1].

An analysis of existing threats allows us to define the risks to the security of the information systems, in addition, this analysis allows us to determine the countermeasures to neutralize potential threats and reduce security risks to an acceptable level. Standard ISO-15408 defines the requirements to the risk analysis procedure at the various stages of design, development, implementation and maintenance of the security mechanisms, as well as the actions of the owners of information and information systems administrators, to protect them from possible threats and intrusions [2], [3].

Countermeasures can reduce the number of potential vulnerabilities in the information system with the protection mechanisms applying in accordance with established security policy. At the same time in case when the countermeasures are already implemented there may remain the residual vulnerabilities, which can be used by intrusions agents. These vulnerabilities form a residual risk, which is mitigated by the use of additional security mechanisms.

The owners need to make sure that the countermeasures employed by them provide an adequate reaction to the potential threats before to grant the access to their resources. In general, resource owners may not always objectively evaluate the effectiveness of the security mechanisms that are used and in this case there is required an independent assessment. The result of this assessment is the trust level to the security mechanisms in terms of reducing the risk of resources security. The trust level is characteristics of protection, which confirms the correctness and efficiency of their use, as this rating is used by the resource owner in the decision making process how to set an acceptable level of security risk to its resources [13].

The results of evaluation of security mechanisms parameters must be verified in terms of their correctness, which will allow use the received assessment data to substantiate an acceptable level of security risk for a certain information system [14].

II. Methods for the Effects Predicting of the Dangerous Actions of the Intrusion Agents

The methods for the evaluation and prediction of consequences of the dangerous actions of intrusion agents by the time are divided into two groups [15]-[18]:

• methods, that are based on a priori estimates obtained on the basis of theoretical models and analogies;
• methods, that are based on a posteriori assessments - the effects assessments for the already realized intrusion into computer systems.

According to the initial information, the methods for predicting of the dangerous actions consequences are divided into [17]-[19]:

• experimental: based on the processing of the parameters of the realized intrusion;
• combined: computational and experimental, based on the statistical data processing with the special mathematical models;
• mathematical: based on the mathematical models exclusively.

The estimated models, that are used to get a priori estimates, perform the tests on the really realized attacks and intrusions into computer systems.

A priori estimates of the effects of the hazardous actions differ by the time and goal [17]-[19]:

• preliminary assessment of the various scenarios of the dangerous actions initiating, performed by the preventive mechanisms planning to protect the computer systems: it provides a basic security level, security monitoring, operative security control;
• operational parameter estimates of the realized intrusions performed to get an adequate reaction to security incidents.

The evaluation and prediction of the user actions involve the collection and processing of the data on the hazardous activities of the intrusion agents, the definition the perimeter of the computer systems components, that are under attack potentially, determination of the impact of the negative factors on the computer system functioning [20], [21]. This assessment allows select the most effective ways for the computer system protection, minimizes losses due to the attacks realization. [20], [21].

The risk assessment of the dangerous actions realization, i.e., the analysis of the dangerous actions repeatability and the alleged damage to a certain computer system is performed periodically, in particular, when there is performing an audit of the computer security for the risks control [22]. During the assessment of the dangerous actions realization, all the main risk factors are uncertain and there are used their estimates.

The forecast of the consequences of the dangerous actions of intrusions agents is a preliminary forecast for the certain computer system and for the certain type of the dangerous actions. The preliminary assessment of the impact of the hazardous activities is a particular problem of the risk assessment in a case when the initiating event has already occurred, i.e. the dangerous action was realized [21], [22]. The forecast is performed on the uncertain factors parameters, and the results of the prediction are used in the planning of the preventive mechanisms to protect the computer systems [22], [23].

The mathematical models for the consequences prediction of the dangerous actions of intrusion agents are based on a probabilistic approach assuming that the intrusion event is occurred already [24]. This takes into account both the probabilistic nature of the negative factors impact on the computer system, and the vulnerabilities of the computer system to these influences [24]. The levels of impact factors on the computer system security are the random variables and are specified by the relevant distribution. The vulnerabilities of the computer system components and resources are also described as random factors, due to the specifics of the development and support of the hardware and software. The random factors affecting the dangerous actions consequences are related to the danger degree, to the space-time threats and to the vulnerabilities of the computer system [24], [25].

The emergency evaluation of the situation in the case of the dangerous actions is performed by the time parameters of intrusions attempts, by the type of the computer system component that is under the attacks, and by the danger degree of the intrusion actions, that is received from the security monitoring and control subsystems [24], [25]. The emergency assessment is a special case of the above-described problem in case if the hazards and threats have already been realized. The results of this assessment are used in decisions making for the security control of the computer systems, to perform an effective reaction to security incidents [18].

The assessment of the real situation that has arisen as a result of dangerous actions is performed by the data, that are obtained from safety monitoring subsystem, and this assessment allow eliminate the uncertainty by the only one remaining uncertain risk-factor - the losses [18], [19]. The results of this assessment are used to clarify the earlier decisions on the implementation of the protective mechanisms and to minimize the consequences of the intrusions.

The effective risk control implies the risks factors prediction, i.e. there are estimated the possible risks indicators for the some future time interval, for example, based on the methods of the time series extrapolation, auto-regression, and the others [25], [26]. In order to perform the risk prediction, the special models are used, which describe the prospective state of DCS based on an analysis of its behavior during operations in the previous time intervals [26].

Let us present the specifics of the risk prediction task in apply to the security risk forecast for the distributed computer systems, which is solved to control of the DCS security. The following methods can be used in the risk prediction process [1], [2], [17]-[19]:

• the prediction of the possible safety violation, i.e. the realization of the corresponding triggering dangerous events;
• the forecasting of the effects of hazardous events, i.e., the safety violation.

For a timely forecasting of hazardous events during the operation of the computer system or to identify them at the initial stage there is required a special system for the subjects actions monitoring in the computer systems. Based on the information, that is received on the monitored data, the security administrator makes the operative decisions on the security mechanisms activation

to prevent and/or to reduce the loss due to a security violations (attacks) on computer systems [17]-[19]. The methods for the forecast of the dangerous events by the projected parameters, in turn, are subdivided into methods of forecasting their location, level, the onset time and the repetition rate [27]-[30].

This problem can be solved in different ways depending on the specifics of the computer systems. The most effective approach is to proactively predict the dangerous events (attacks) and to apply the adequate measures in the stage of their preparation [17]-[19]. In the case when the time is limited for an adequate reaction to a hazardous event, it is expedient to activate the preventive security mechanism, based on the statistical evaluation of the recurrence frequency of dangerous events [1].

In fact, the task of the security risks analysis is associated with the assessment of the risk of exceeding of a predetermined maximum time interval for the reaction to possible intrusions in the DCS Job Manager (JM) functions [34]. This risk depends on two factors: the probability and the consequences of the exceeding of the time for the situation analysis and decision making in the DCS JM. The probability of the time exceeding is functionally linked to the values of the upper and lower bounds of the allowable time period for the situation analysis and decision-making [32].

In general, the following factors have impact on the security risks: the number of nodes and link channels of DCS, the intensity of the security threats to DCS resources realization, the intensity of security mechanisms activation, i.e., the rate of reaction to the hazardous events [1], [17]-[19], [31], [32]. In the case, when the rate of the security threats realization is exceeded the reaction rate, the attack is launched on the DCS resources [33].

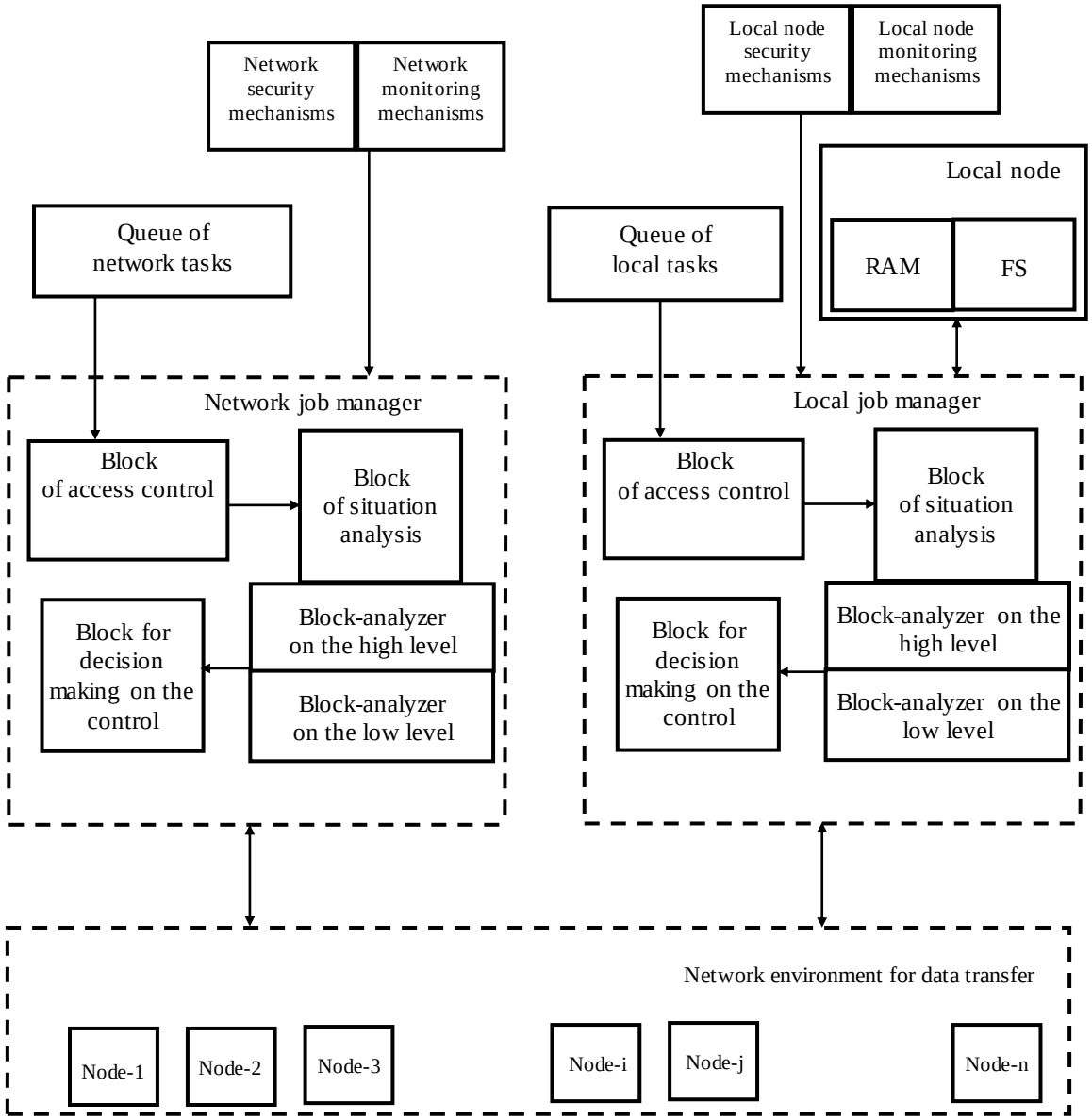

Fig.2. The generalized structural scheme of Job Manager in the context of risk-based approach to security analysis (RAM – Random Access Memory, FS – File system)

III. The DCS Job Manager in the Context of Risk-based Approach for Security Analysis

The analysis of the existing security threats allow determine the risks of safety violations for the computer systems resources and determine the countermeasures to neutralize the potential threats, by reducing the security risks to an acceptable level [31]. Taken countermeasures allow reduce the number of potential vulnerabilities in the computer system, and for this purpose, in accordance with the current safety policy in DCS, are implemented the protection mechanisms. However, even if the countermeasures are already implemented there may remain so-called residual vulnerabilities that form the residual security risk, which can be reduced by the additional protective mechanisms [31].

One of the most important components of modern distributed computer systems is the Job Manager, which, inter alia, performs the distribution of solving tasks between the DCS resources, including the tasks related to the DCS security. The malfunctions of JM, particularly the time delays during the analysis of critical situations and decisions making, especially in the case when the DCS process the confidential information can disrupt or even a completely stop the DCS functioning [31], [32]. Thus, the parameters analysis and the reducing of security risk for Job Manager operations is a very important task.

Fig. 2 shows a generalized structural scheme of Job Manager [35]-[37] in the context of a risk-based approach.

IV. Risk-based Security Analysis of the Distributed and Scalable Computer Systems

Let us introduce the next parameters: x_1 - the number of nodes in a distributed computer system; x_2 - the number of data link channels; x_3 - the number of the active security mechanisms; x_4 - the number of the security monitoring tools in the DCS. Next, let α - the average intensity of the security threats for the DCS resources x_1 and x_2; β – the average intensity of the security mechanisms from the group x_3 and x_4 activation, and the parameter R_0 – the initial security risk.

To assess the security risks in the DCS, we introduce a function:

$$R(t) = \frac{R_0}{1 + e^{(\beta \frac{x_3 x_4}{x_{3\max} x_{4\max}} - \alpha \frac{x_1 x_2}{x_{1\max} x_{2\max}})t}} \quad (1)$$

Function R(t) is a risk of the DCS security threats realization, in depending on the time t.

There are some various ways for the risks changing, which depend on the relationship between the expressions:

$$\alpha \frac{x_1 x_2}{x_{1\max} x_{2\max}} \text{ and } \beta \frac{x_3 x_4}{x_{3\max} x_{4\max}}. \quad (2)$$

If $\alpha \frac{x_1 x_2}{x_{1\max} x_{2\max}} > \beta \frac{x_3 x_4}{x_{3\max} x_{4\max}}$, then where the security risks are growing and threats can be transformed into a real attack.

Conversely:

if $\alpha \frac{x_1 x_2}{x_{1\max} x_{2\max}} < \beta \frac{x_3 x_4}{x_{3\max} x_{4\max}}$, then there is a reduction of the security risks and the possibility of the attacks realization is low.

According to the statistical data, in the modern distributed computer systems, an average 25 intrusion attempts are launched per workstation in the daytime period [18]. Then in the DCS, consisting of 1000 nodes workstations, there are performed about 25,000 intrusion attempts per daytime period, and thus the expected value of the intensity of the security threat realization is α_i=0.3, i.e., on average, the 1 intrusion attempt is launched every 3.33 seconds.

The evaluations of the security risks R in DCS allow performing the simulation for different configurations of distributed computer systems considering the resources scaling. Let us consider the configuration of a distributed DCS, which after the scaling has the following parameters: the maximum nodes number $x_{1\max}$=1000; the maximum number of data links channels $x_{2\max}$ = 5500; the maximum number of active security mechanisms $x_{3\max}$ = 100; the maximum number of active security monitoring tools $x_{4\max}$ = 50.

Let us consider the various configurations of the DCS:

1. The DCS is scaled to the largest possible number of nodes and data links channels ($x_{1\max}$ = 1000, $x_{2\max}$ = 5500), and there are the maximum possible number of active security mechanism and active security monitoring tools ($x_{3\max}$ = 100, $x_{4\max}$=50).
2. The DCS is used x_3 = 50 active security mechanisms; x_4 = 20 active security monitoring tools for the maximum possible number of nodes and data links channels ($x_{1\max}$ = 1000, $x_{2\max}$ = 5500);
3. The DCS is used the maximum possible number of active security mechanisms and active security monitoring tools ($x_{3\max}$ = 100, $x_{4\max}$ = 50), and the DCS have x_1 = 700 nodes and x_2 = 3700 data link channels;
4. The DCS is used x_3 = 50 active security mechanisms; x_4 = 20 active security monitoring tools, and the DCS have x_1 = 700 nodes and x_2 = 3700 data link channels.

Let us fix an average intensity of activation of the security mechanisms from the group x_3 and x_4 at the level β = 0.4, the average intensity of realization of the security threats to DCS resources x_1 and x_2 at the level α = 0.3. Next, we draw a set of the curves that are reflecting the functional dependence between the risk value R and the time t for the four above mentioned DCS configurations with the initial risk R_0 = 0.2. The results are shown in Table 1.

Table 1. The values of the security risks R in DCS

t,c	0	1	2	3	4	5	6	7	8	9	10
X_{1max} = 1000, x_{2max} = 5500, x_{3max} = 100, x_{4max} = 50	0.2	0.190	0.180	0.170	0.161	0.151	0.142	0.133	0.124	0.116	0.108
X_{1max} = 1000, x_{2max} = 5500, x_3 = 50, x_4 = 20	0.2	0.222	0.243	0.264	0.283	0.300	0.316	0.329	0.341	0.351	0.360
X_1 = 700, x_2 = 3700, x_{3max} = 100, x_{4max} = 50	0.2	0.174	0.149	0.126	0.105	0.086	0.07	0.056	0.045	0.036	0.028
X_1 = 700, x_2 = 3700, x_3 = 50, x_4 = 20	0.2	0.206	0.212	0.218	0.224	0.230	0.236	0.242	0.248	0.254	0.259

In accordance with the data from the table 1, the Fig. 3 shows the dynamics of security risk R in time t. Fig. 3 shows that in the DCS configurations 2 and 4 there are the increasing of the security risk, that is caused by the fact that the number of active security and monitoring mechanisms is insufficient for a given amount of the DCS resources and for a given intensities of intrusion realization and the security mechanisms activation. On the other hand, the for the DCS configurations 1 and 3, the number of active security and monitoring mechanisms is quite sufficient for preventive and protective measures, accordingly, the security risk is reduced. In the DCS configuration 3 the security risk is reducing in a sufficiently fast way and the risk level 0.15 is achieved after 3 seconds after the activation of the security mechanisms. For the DCS configuration 1, the same reduction of the security risk level takes about 6 seconds.

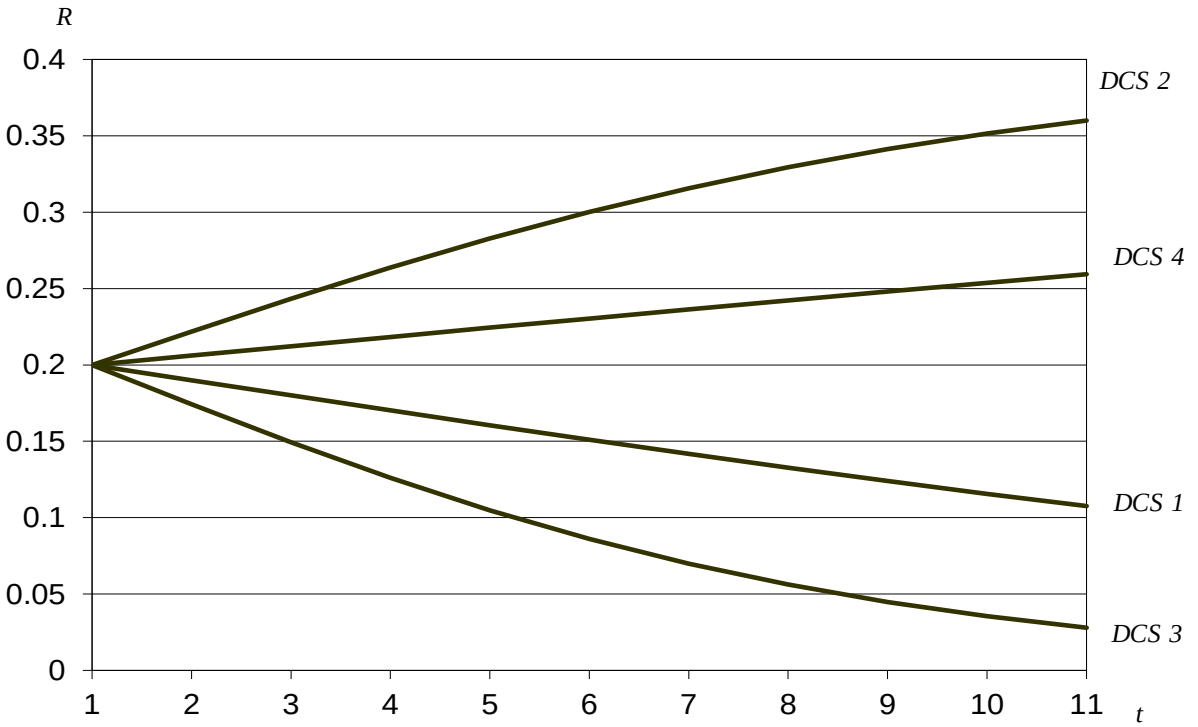

Fig.3. The dynamics of security risk R in time *t*.

This case is explained by the fact, that there is the excessive number of the active security and monitoring tools for DCS configuration 3. However, such redundancy allows in a more fast way provide the secure state of the computer system, thereby to minimize the time interval when the DCS is in a potentially dangerous state, that reduces the probability of the successful attacks from the intrusion agents.

V. Conclusion

Thus, the proposed analytical assessment for security risk level in the DCS allows forecast the values of the critical time for the situation analysis and decision-making for the current configuration of a distributed computing system. This forecast takes into account the number of used nodes and data links channels, the number of active security and monitoring mechanisms at the current period, as well as on the intensity of the events related to the security threats and the activation intensity of the intrusion prevention mechanisms. Also, the proposed comprehensive analytical assessments of the risk allow analyzing the dynamics of intrusion processes, the dynamics of the security level recovery and the corresponding dynamics of the risks level in the DCS. The analysis of the probability of a critical time exceeding for the decision-making, i.e. the reaction time of the security mechanisms to the threats in case of dynamic change of DCS security parameters, requires to perform a formal description of the processes in the DCS job manager, in particular, with dedicated networking mechanisms and models that will allow dynamically evaluate the interval boundaries of critical response time for the actions of the intrusions agents.

References

[1] E. Maiwald, "Fundamentals of network security," *Technology Education*, 2004.

[2] ISO / IEC 15408-1-2002 Information technology. Methods and security features. Criteria for Information Technology Security Evaluation.

[3] ISO / IEC 15408-2009 Information technology - Security techniques - Evaluation criteria for IT security. http://ebookbrowse.com/i/iso-15408-1-pdf

[4] Risk Management Guide for Information Technology Systems: SP 800-30. – Recommendations of the National Institute of Standards and Technology, 2002.

[5] ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements, 2005.

[6] E. Alsous, A. Alsous, and A Botnet, "Detection System Using Multiple Classifiers Strategy," *International Review on Computers and Software*, Vol. 7. n. 5, 2012, pp. 2022-2028.

[7] K. Suresh Kumar, and T. Sasikala, "A Technique for Web Security Using Mutual Authentication and Clicking-Cropping Based Image Captcha Technology," *International Review on Computers and Software*, Vol. 9, n. 1, 2014, pp. 110-118.

[8] R. Pal, and P. Hui, "Cyber-insurance for cyber-security: A topological take on modulating insurance premiums. Performance Evaluation Review," 2012.

[9] K. Rama Abirami, M. G. Sumithra, and J. Rajasekaran, "An Efficient Secure Enhanced Routing Protocol for DDoS Attacks in MANET," *International Review on Computers and Software*, Vol. 9, n. 1, 2014, pp. 119 – 127.

[10] S. I. Sabasti Prabu, and V. J. Senthil Kumar, "Entropy Based Approach to Prevent the DDoS Attacks for Secured Web Services," *International Review on Computers and Software*, Vol. 8. n. 4, 2013, pp. 888-891.

[11] "Practical Threat Analysis for Information Security Experts," TA Technologies, 2010. http://www.ptatechnologies.com/default.htm

[12] Y. Senhaji, H. Medromi, and S. Tallal, "Network Security: Android Intrusion Attack on an Arduino Network IDS," *International Review on Computers and Software*, Vol 10, n. 9, 2015, pp. 950-958.

[13] V.Mukhin. Adaptive Approach to Safety Control and Security System Modification in Computer Systems and Networks, *Proceedings of the 5-th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2009),* Rende (Cosenza), Italy, 21 - 23 September 2009. – pp. 212 - 217.

[14] V. Mukhin, A Bidkov, Vu Duc Thinh. The Forming of Trust Level to the Nodes in the Distributed Computer Systems, *Proc. of XIth International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science TCSET'2012"*, Lvov – Slavsko, 21 - 24 February 2012. – p. 362.

[15] IEC/ISO 31010 Risk management – Risk assessment techniques, 2009.

[16] ISO 31000:2009 Risk management - Principles and guidelines, 2009.

[17] P. Hopkin, "Fundamentals of Risk Management: Understanding, Evaluating and Implementing – The Institute of Risk Management," 2010.

[18] R. Sohizadeh, M. Hassanzadeh, H. Raddum, and K. Hole, "Quantitative risk assessment," 2011.

[19] "Risk Management Fundamentals Homeland Security Risk Management Doctrine," 2011. https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

[20] "Security risk analysis and management". https://www.nr.no/~abie/RA_by_Jenkins.pdf

[21] "Risk management, concept and methods," CLUSIF, White paper. https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-risk-management.pdf

[22] "Managing Information Security Risk Organization, Mission, and Information System View," *NIST Special Publication 800-39*, March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[23] "Basics of Risk Analysis and Risk Management". http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

[24] "NHS Information Risk Management Digital Information Policy NHS Connecting for Health," 2009. http://systems.hscic.gov.uk/infogov/security/risk/inforiskmgtgpg.pdf

[25] M. Ketel, "It security risk management," *Proceedings of the 4 6th Annual Southeast Regional Conference*, 2008.

[26] L. P. Rees, J. K. Deane, T. R. Rakes, and W. H. Baker, "Decision support for cybersecurity risk planning," *Decision Support Systems*, vol. 51. no. 3. 2011, pp. 493-505.

[27] P. Saripalh, and B. Walters, "Quire: A quantitative impact and risk assessment framework for cloud security," *IEEE 3rd International Conference on Cloud Computing*, 2010.

[28] Mohamed Hamdi, and Noureddine Boudriga, "Computer and network security risk management: theory, challenges, and countermeasures," *International Journal of Communication Systems*, Volume 18, Issue 8, 2005, pp. 763–793. DOI: 10.1002/dac.729

[29] Yang Liu, Zhikui Chen, and Xiaoning Lv, "Risk computing based on capacity of risk-absorbing in virtual community environment," *International Journal of Communication Systems*, 2014.

[30] Shi, C. Beard, and K. Mitchell, "Analytical Models for Understanding Misbehavior and MAC Friendliness in CSMA Networks," *Performance Evaluation*, Vol. 66 (9–10), 2009, pp. 469. DOI:10.1016/j.peva.2009.02.002.
[31] N. Mohammadi, and M. Zangeneh, "Customer Credit Risk Assessment using Artificial Neural Networks," *I.J. Information Technology and Computer Science*, Vol.8, N3, 2016, pp. 58-66. DOI: 10.5815/ijitcs.2016.03.07
[32] P. R. Vamsi, and K. Kan, "Self Adaptive Trust Model for Secure Geographic Routing in Wireless Sensor Networks," *International Journal of Intelligent Systems and Applications*, Vol. 7, N3, 2015, pp. 21-28. DOI: 10.5815/ijisa.2015.03.03
[33] A. Koul, and M. Sharma, "Cumulative Techniques for Overcoming Security Threats in Manets," *International Journal of Computer Network and Information Security*, Vol. 7, N. 5, 2015, pp.61-73. DOI: 10.5815/ijcnis.2015.05.08
[34] S. G. Ponnambalam, P. Aravindan, and P Sreenivasa Rao, "Comparative equation of genet IC algorithms for job-shop scheduling," *Production Planning Control*, vol. 12, 2001, pp. 560-574.
[35] S. Dimassi, A. B. Abdelali, A. Mrabet, M. N. Krifa, and A. Mtibaa, "A Modeling Tool for Dynamically Reconfigurable Systems," *International Review on Computers and Software*, Vol. 9, n. 4, 2014, pp. 600-608.
[36] H. Shan, W. Smith, L. Oliker, and R. Biswas, "Job scheduling in a heterogeneous GRID environment". http://www.osti.gov/bridge/servlets/purl/860301-UfJBKm/860301.pdf
[37] I. Bowman, "Conceptual Architecture of the Linux Kernel". www.grad.math.uwaterloo.ca/~itbowman/CS746G/a1/

Authors' Profiles

Zhengbing Hu: Associated Professor of School of Educational Information Technology, Huazhong Normal University, PhD.

M. Sc (2002), PhD (2006) from the National Technical University of Ukraine Kiev Polytechnic Institute".

Postdoctor (2008), Huazhong University of Science and Technology, China.

Honorary Associate Researcher (2012),Hong Kong University, Hong Kong, Major interest: computer science and technology applications, artificial intelligence, network security, communications, data processing, cloud computing, education technology.

Vadym Mukhin: Professor of computer systems department of National Technical University of Ukraine "Kiev Polytechnic Institute", Doct. of Sc.

Born on November 1, 1971. M. Sc. (1994), PhD (1997), Doct. of Sc. (2015) from the National Technical University of Ukraine "Kiev Polytechnic Institute"; Assoc. Prof. (2000), Professor (2015) of computer systems department.

Major interest: the security of distributed computer systems and risk analysis; design of the information security systems; mechanisms for the adaptive security control in distributed computing systems; the security policy development for the computer systems and networks.

Oleg Barabash: Professor of networking and Internet technologies department, Taras Shevchenko National University of Kiev, Ukraine, Kiev, Doct. of Sc.

Born on July 28, 1964. M. Sc. (1986), PhD (1992), Doct. of Sc. (2006) from the National Academy of Defence of Ukraine; Assoc. Prof. (1996), Professor (2007) of computer systems department.

Major interest: the functional stability of information systems and diagnostic systems for digital objects; security of distributed computer systems; design of the information security systems computer systems; design of the information security systems.

Yaroslav Kornaga: Assoc. professor of computer systems department of National Technical University of Ukraine "Kiev Polytechnic Institute", PhD.

Born on January 1, 1982. M. Sc. (2005), PhD (2015), from State University of Telecommunications; Assoc. Prof. (2015) of techical cybernetics department.

Major interest: the security of distributed database and risk analysis; design of the distributed database; mechanisms for the adaptive security control in distributed database; the security policy development for distributed database.

Oksana Herasymenko Assist. professor of networking and Internet technologies department, Taras Shevchenko National University of Kiev.

Born at 1983 in Borzna town, Chernihiv region, Ukraine. M. Sc. in computer system and networks (2006) from Chernihiv State Technological University, Ukraine.

Major interests: resource control in distributed computing system and data mining. Now she is preparing her Ph.D. thesis in information technologies.

Yaroslav Lavrenko: Assoc. professor of dynamics and strength of machines and strength of materials department of National Technical University of Ukraine "Kiev Polytechnic Institute", PhD.

Born on March 15, 1983. M. Sc. (2006), PhD (2014), from National Technical University of Ukraine "Kiev Polytechnic Institute"; Assoc. Prof. (2015) of dynamics and strength of machines and strength of materials department.

Major interest: Dynamics and durability of high rotation system, vibrations.

How to cite this paper: Zhengbing Hu, Vadym Mukhin, Yaroslav Kornaga, Yaroslav Lavrenko, Oleg Barabash, Oksana Herasymenko, "Analytical Assessment of Security Level of Distributed and Scalable Computer Systems", International Journal of Intelligent Systems and Applications (IJISA), Vol.8, No.12, pp.57-64, 2016. DOI: 10.5815/ijisa.2016.12.07

