Mathematical Model of Threats Resistance in the Critical Information Resources Protection System

© Bogdan Korniyenko[1], © Liliya Galata[2], © Lesya Ladieva[1]

[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[2] National Aviation University, Kyiv, Ukraine

bogdanko@gmx.net, galataliliya@gmail.com, lrynus@yahoo.com

Abstract. The main problems of information security of critical information resources and causes of their occurrence are considered. The main threats to security systems of critical information resources are analyzed. Mathematical model of counteraction of internal and external threats to the system of protection of critical information resources of mineral fertilizers production is developed. The process of building a mathematical model of countering the threats in the system of protection of critical information resources with the help of Markov chain. The methodology of finding current threats to data security during their processing is offered. The software module is developed in the Piton programming language. These examples calculate the probability of mathematical model of information system in one of four states (the threat did not come; the threat came but was not implemented; the threat has been implemented; the threat came, but it was reflected protection system). Examples of numerical results analysis using proposed techniques clearly show that their use helps to define threats that are relevant to the system being investigated and can be used in practice. The disadvantage of proposed methodology is the need to consider the system behaviour when it comes to each type of threat, individually and inability to define behaviour on the simultaneous action of several threats. Studying the influence of each threat separately allows to study each of its types in more detail and to determine the probability of which is the greatest occurrence. As a result of exploitation of critical information resources protection systems and substantial changes in composition and quality of modern threats, it is necessary to project and implement information security of the systems taking into account tendencies of cyber threats development.

Keywords: Mathematical Model; Threat; System of Protection; Critical Information Resources.

1 Introduction

In today's world, automated control systems are used more and more often. The need for information security in automated control systems is increasing every year by increasing the number of attacks by intruders and leakage of confidential information. But the most susceptible to security is the most automated control systems of technological processes, as when attackers attack, it can happen not only leakage of secret information, but also interference into the technological process itself, which, when malfunctions, can lead to environmental catastrophe.

Control of technological processes in enterprises of small, medium and large size is impossible without computer equipment and modern means of automation, without highly effective of automated control systems of technological processes (ACS TP).

ACS is a comprehensive system of hardware and software, which is designed for remote centralized monitoring of processes and system as a whole, as well as for automated control of engineering and technical subsystems.

Information Security (IS) is becoming more and more topical issue with the development of computing equipment and the increasing penetration of such systems into the daily lives of people. This is discussed in almost every event on the security of the IS, and the analysis of reliability and safety of the systems already commissioned is one of the mandatory conditions of State and international certification. One of the biggest problems of the security is that the majority of ACS of small and medium complexity are projected by small organizations under conditions of strict financial limitation, which eliminates or complicates the security issue.

Experts believe that the provision of IS is different from the provision of corporate information systems. Even the term "information security" is very rarely used in relation to ACS TP. The reason for this is that it is necessary to pay attention not so much the confidentiality of information, but ensuring the continuity and integrity of the technological process. Although at the same time a significant amount of attention is given to the problems of ensuring confidentiality of information, because, according to many experts, the solution of this problem leads to the automatic solution of the problem of integrity and availability of information.

Modern ACS in many cases manage difficult and dangerous technological processes, failure of which could potentially lead to accidents in production or, in the worst case, to technogenic disasters. This significantly increases the price of risk due to violations of the IS, because threats can theoretically cause damage to people, the environment, and also leads to the financial and reputational losses.

In modern times, the priority in providing the IS ACS TP is to ensure the availability and integrity of the management and configuration information on the parameters of the technological process. Particular attention should be paid to preventing unauthorized access to the system to preserve the stable functioning of ACS TP [1-5]. Despite the large number of accidents with catastrophic consequences, the problem of critical information resources protection at industrial enterprises in the chemical and energy industries has never been so acute as in recent years.

The general interest to the security of industrial systems occurred only after the incidents with the computer viruses Stuxnet, Duqu, Flame, which attacked Iranian nuclear facilities, government agencies and industrial facilities in India, China and other countries. Separately, attacks to enterprises in the Ukraine’s energy sector and the banking sector should be highlighted. Before these incidents advent, it was considered that the protection system of critical information resources was been very difficult to compromise. Such representations were based on the following postulates: the software of each protection system for critical information resources is unique and closed; penetration into the system is associated with high costs of intellectual resources, and the monetary reward for the attacker is not obvious; the local network of the critical information resources protection system solves access restriction problems.

A study of software and hardware structure, that used in the protection systems of critical information resources, has shown that there have been big changes in recent years. Almost everywhere, widely known software is used, such as Windows OS, TCP/IP protocols, etc., which, together with their advantages in standardization, simplicity, and quality of use, have also brought disadvantages - vulnerabilities. Computers connected to the Internet appear in the local network, and they also present a large number of potential threats to the system [6-10].

2 Formulation of the problem

In industrial systems of critical infrastructure there are the same vulnerabilities as in most conventional IT systems. In addition, the peculiarity of industrial systems is the existence of unique vulnerabilities, which include:

Human factor. Operation Industrial and corporate systems are usually involved in various divisions and specialists. In turn, the personnel of industrial systems, as a rule, are not far from the issues of providing information security, in its composition there are no security specialists, and the recommendations of the IT staff are not distributed. The solution of technological problems arising during the operation of the system, ensuring its reliability and availability, efficiency and minimization of overhead should be one of the main tasks of specialists.

OS vulnerabilities. The vulnerabilities of OS (operating systems) are inherent for both industrial and enterprise systems, but software installations are not normally implemented in industrial systems. Uninterrupted operation of such system is the responsibility of the administrator. The establishment of pre-approved software corrections can contribute to serious problems, and there is no time or money on full testing.

Authentication. Common passwords are usually used for industrial systems. The two-factor authentication system is rarely used, and sensitive information is often transmitted in an open form.

Remote access. To control the industrial systems often used remote access by dial-up channels or by VPN channels via the Internet. If not controlled use, this may cause serious security problems.

External network connections. Lack of appropriate regulatory framework and usage is aimed more at convenience rather than security, sometimes lead to the fact that network connections are created between industrial and corporate networks. There are even recommendations for using "composite" networks that allow you to simplify administration. This can adversely affect the security of both industrial and corporate systems.

Means of protection and monitoring. Unlike enterprise systems, use IDS. Systems, etc. In the industrial system is not a common practice, the analysis of security audit logs is also not rarely bypassed.

Wireless networks. In industrial systems, various types of wireless communication are often used, including 802.11 protocols, which are known to not provide sufficient capabilities to protect the information.

Remote processors. Some remote processor classes have known vulnerabilities. Performance of these processors does not always allow to implement security functions. In addition, after installation, they try not to touch for years, during which they remain vulnerable.

Software. The software of the industrial systems usually does not have enough security functions. In addition, in most cases, it is not devoid of architectural weaknesses.

Disclosures. The owners of industrial systems are often deliberately publish information about their architecture. Consultants and developers often share experiences and reveal useful information about employees.

Physical security. Remote processors and industrial systems equipment can be outside the controlled area. In such conditions they physically cannot be controlled by the personnel, and the only mechanism of their physical protection is the use of metal doors and locks. Such measures are not a serious obstacle to intruders.

In this way, we can conclude that there is a significant number of vulnerabilities that are both common to any information systems and specific to industrial systems. These vulnerabilities cause specific security requirements and special operating regimes for such systems [11-15].

Also, the new term “cyberwarfare” has recently appeared, which is often mentioned in the media, because there is a problem in critical information resource system protection at infrastructure facilities and hazardous industries. Thus, the widespread use of computer equipment in the management of industrial enterprises creates the need to pay more and more attention to the problems of information security of such systems.

The main problems of information security of critical information resources, according to experts, appear because there are:

- low protection against unauthorized access (passwords);
- undeclared SCADA capabilities;
- lack of control in management actions;
- using of wireless communications (crypto persistent Wi-Fi encryption);
- lack of clear boundaries between different network segments;
- untimely or incorrect software updates;
- rejection from even minimal security tools (often for convenience or performance, companies refuse to install not only, for example, anti-virus protection, but also password protection for critical assets);
- the distribution of Windows as an operating system for workstations and even

servers;

- development for trusted environment of closed industrial networks;
- creating systems without taking into account the best practices in safe code development;
- human factor, poor staff discipline.

Here is an example of the main threats to critical information resource systems found after analyzing these incidents:

- attacks to SCADA;
- attacks to PLC, PLC vulnerabilities (standard password, unauthorized access to original software);
- attacks to the infrastructure and the operating system (viruses, trojans, worms, DoS and DDoS attacks, ARP spoofing);
- attacks to protocols, protocol vulnerabilities (unauthorized access, SQL injection);
- attacks such as Buffer Overflow, Information Disclose, Denial of Access, Manipulation of View.

Among all types of vulnerable components of critical information resources protection systems, the next one prevails: SCADA - 87%, systems providing human-machine interfaces - 49%, programmable controllers - 20%, protocols - 1%.

The vulnerabilities by type was divided as follows: buffer overflow - 36%, authentication / key management - 22.86%, Web application vulnerabilities - server - 10.86%, client - 9.14%, remote code execution - 13.14% [16-18].

As a result of the operation of protection systems for critical information resources and a significant change in the composition and quality of modern threats, it is necessary to design and implement information security systems taking into account trends in cyber threats development. On the other hand, it is necessary to carry out regular work to neutralize emerging or potential threats on working systems. At this level, the following information security services are implemented: access control, integrity, secure network connections, antivirus protection, security analysis, intrusion detection, information security system management (continuous state monitoring, incident detection, reaction).

3 Analysis of recent research and publications

The protection system of critical information resources of mineral fertilizers production was chosen as the object of research [19-21]. The basis of information security models are the following theories: formal-heuristic approach; probability theory and random processes; evolutionary modeling; theory of graphs, automata, and Petri nets; game theory and conflict; catastrophe theory; theory of fuzzy sets; entropy approach. The differences between the majority of models are which parameters they use as input and which parameters are given as output after calculations. In addition, recently, modeling methods based on the informal theory of systems are widely used: structuring methods, estimation methods, and methods for finding optimal solutions [22-24].

Structuring methods is the development of a formal description, applies to organizational and technical systems. Using these methods allows us to present the architecture and process of complex system functioning in the form that satisfies the following conditions: completeness of main parts display and their relationships; simplicity of elements organization and their relationships; flexibility - simplicity of making changes to the structure, etc. Evaluation methods allow you to determine the values of system characteristics, that cannot be measured or obtained using analytical expressions, or in the statistical analysis process, such as the probability of threats, the effectiveness of the protection system element, etc. The basis of such methods is expert assessment - an approach of attracting specialists in relevant fields to obtain some characteristics values.

Methods for finding optimal solutions is a generalization of a large number of independent, mostly mathematical, theories, in order to solve optimization problems. In the general case, this group includes methods for informally reducing a complex problem to a formal description, followed by formal approaches. Combining of methods for these three groups allows you to expand the possibilities of applying formal theories to do a complete simulation of protection systems.

The purpose of the article is the development and research of a mathematical model of threats resistance in the critical information resources protection system, obtaining transitional characteristics for system states.

4 Main research material

The mathematical model of influence resistance of internal and external threats on the protection system of critical information resources of the mineral fertilizers production is proposed. The process of constructing a mathematical model for threats resistance in the critical information resources protection system by using the Markov chain [25-27] is described in stages. The methodology for finding relevant threats to data security during their processing is proposed. The examples of calculating the probabilities of finding a mathematical model of an information system in one of four states is shown (the threat has not occurred; the threat occurred, but has not been implemented; the threat occurred, and has been implemented; the threat occurred, but has been reflected by the security system).

The system can be interpreted as a queuing system, which receives threats. First, consider the situation when threats of the same type come to the system input, assuming that the threat cannot be realized and come several times in the same time period. If these conditions are met, then the system can be in one of four states (see Fig. 1):

1. the threat has not been occurred and, accordingly, was not implemented;
2. the threat occurred, but has not been implemented;
3. the threat occurred, but has been implemented;
4. the threat occurred, but has been reflected by the security system.

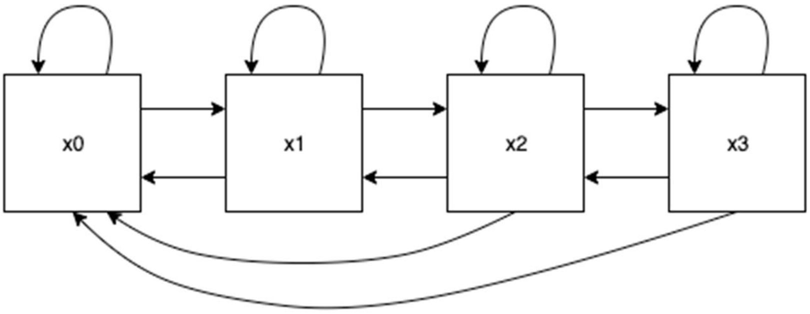

Fig.1. The graph of system states.

The system under consideration is a system with recovery, this system can go from any state to the initial one. We will consider a system with continuous time. The transition from state to state occurs according to a directed graph (see Fig. 1). To describe the transition from state to state, we will construct a transition intensity matrix:

$$p_{ij} = \begin{vmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} & 0 \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & \lambda_{24} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} & \lambda_{34} \\ \lambda_{41} & \lambda_{42} & \lambda_{43} & \lambda_{44} \end{vmatrix} \tag{1}$$

From prior approvals, as a result, the elements of this matrix have the following properties:

$$\begin{aligned} \lambda_{11} &= -\lambda_{12} - \lambda_{13} \\ \lambda_{22} &= -\lambda_{21} - \lambda_{23} - \lambda_{24} \\ \lambda_{33} &= -\lambda_{31} - \lambda_{32} - \lambda_{34} \\ \lambda_{44} &= -\lambda_{41} - \lambda_{42} - \lambda_{43} \end{aligned} \tag{2}$$

To determine the probabilities of being the system in the states x_0, x_1, x_2, x_3, we construct a system of differential equations:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = p_0(t)\lambda_{11} + p_1(t)\lambda_{21} + p_2(t)\lambda_{31} + p_3(t)\lambda_{41} \\ \dfrac{dp_1(t)}{dt} = p_0(t)\lambda_{12} + p_1(t)\lambda_{22} + p_2(t)\lambda_{32} + p_3(t)\lambda_{42} \\ \dfrac{dp_2(t)}{dt} = p_0(t)\lambda_{13} + p_1(t)\lambda_{23} + p_2(t)\lambda_{33} + p_3(t)\lambda_{43} \\ \dfrac{dp_3(t)}{dt} = p_1(t)\lambda_{24} + p_2(t)\lambda_{34} + p_3(t)\lambda_{44} \end{cases} \tag{3}$$

As

$$p(0) = (1,0,0,0) \tag{4}$$

is set, so vector of absolute probabilities

$$p(n) = (p_0(n), p_1(n), p_2(n), p_3(n)) \tag{5}$$

defines by the ratio:

$$p(n) = p(0)\|p_{ij}(n)\| \tag{6}$$

After research on the simulation model, two results of finding the coefficients λ_{ij} were determined, which will be given below [28-30].

Option 1. Let the transition intensity matrix λ_{ij} be as follows:

$$\begin{vmatrix} -0.040 & 0.015 & 0.010 & 0.015 \\ 0.225 & -0.250 & -0.025 & 0.050 \\ 0.625 & -0.160 & -0.855 & 0.390 \\ -0.000 & 0.075 & 0.200 & -0.275 \end{vmatrix} \tag{7}$$

We get the solution of the equations system by the fourth-order Runge-Kutta method for the time t = 50 s. To implement the solution, a software module has been developed by Python. As a result of the calculations, the probability values of being the system in each of the states were found (see Fig. 2).

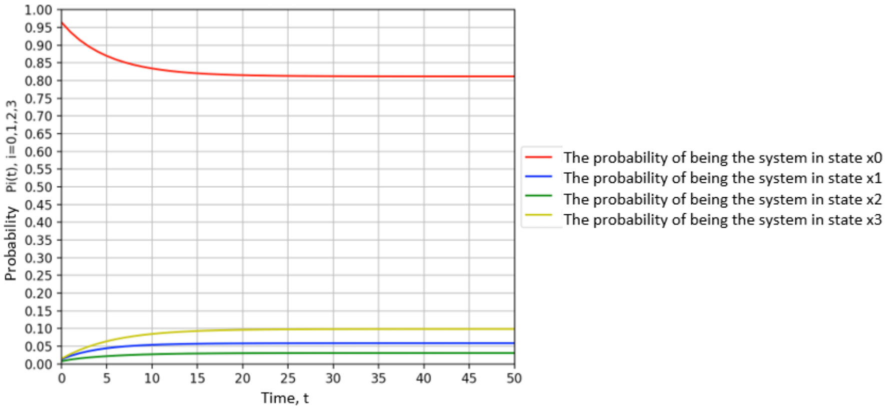

Fig.2. The probability of being the system in each state.

Option 2. We will make the calculation similar to Option 1 with the values of the transition intensity matrix λ_{ij}:

$$\begin{vmatrix} -0.040 & 0.015 & 0.010 & 0.015 \\ 0.225 & -0.250 & -0.025 & 0.050 \\ 0.575 & -0.200 & -0.875 & 0.500 \\ -0.125 & 0.145 & 0.180 & -0.200 \end{vmatrix} \tag{8}$$

As a result, we will get the following graph (see Fig. 3):

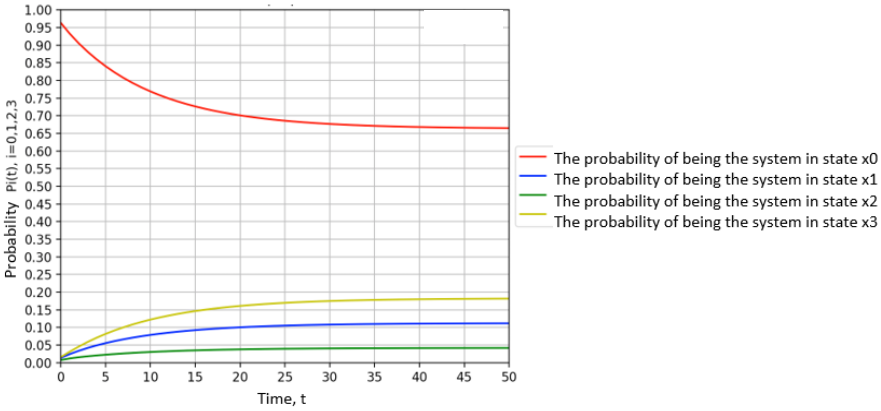

Fig.3. The probability of being the system in each state.

5 Conclusions

Based on the obtained results, it can be said that in Option 2, the system is more probable to be in a threatened state, although there is a high probability that the security system will successfully reflect the threat.

The mathematical model of threats resistance in the protection system of critical information resources of the mineral fertilizers production is proposed. A methodology for identifying actual security threats on the basis of this model has also been developed and displayed.

Examples of the numerical results analysis using the proposed methodology clearly demonstrate that their use helps to identify threats that are relevant to the research system and can be used in practice. The disadvantage of the proposed methodology is the need to consider the behavior of the system when each type of threat is exposed to it separately and the inability to determine the behavior of the system when simultaneous action of several threats is exposed to it. But on the other hand, research of the influence of each threat separately allows you more detailed study each of its types and identify those with the highest probability of occurrence.

References

1. Kurilov F. M. Simulation of information protection systems. Graph Theory App/ Technical Sciences: Theory and Practice: Materials III Internar. Scientific. Conf. - Reading: Young Scientist Publishing House, pp. 6-9. (2016).
2. Rosenko AP. Theoretical basis for analyzing and assessing the impact of internal threats on the security of confidential information: monograph. M.: Helios ARV, 154 p. (2008).
3. Raphael Hertzog, Jim O’Gorman, and Mati Aharoni «Kali Linux Revealed» , Offsec Press, 347 p. (2017).
4. Lei Chen, Hassan Takabi, Nhien-An Le-KhacJohn Wiley & Sons. Security, Privacy, and Digital Forensics in the Cloud, 360 p. (2019).

5. Glen D. Singh, Rishi Latchmepersad. CompTIA Network+ Certification Guide, 422 p. (2018).
6. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody. Software-Defined Networking and Security: From Theory to Practice, 328 p. (2018).
7. Robert M. Lee. Active Cyber Defense Cycle, 651 p. (2016).
8. Jason C. Neumann, The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More 1st Edition, 274 p. (2015).
9. Kwangjo Kim, Muhamad Erza Aminanto, Harry Chandra Tanuwidjaja. Network Intrusion Detection Using Deep Learning: A Feature Learning Approach, 79 p. (2018).
10. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources. CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018) Kyiv, Ukraine, November 27, 2018, Vol-2318, - pp. 176-187, urn:nbn:de:0074-2318-4 (2018).
11. Korniyenko B., Yudin O., Galata L. Research of the Simulation Polygon for the Protection of Critical Information Resources. CEUR Workshop Proceedings, Information Technologies and Security, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017), Kyiv, Ukraine, November 30, 2017, Vol-2067, - pp. 23-31, urn:nbn:de:0074-2067-8 (2017).
12. Zhulynskyi, A. A., Ladieva, L. R., Korniyenko, B. Y. Parametric identification of the process of contact membrane distillation. ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 17, pp. 3108-3112 (2019).
13. Galata, L., Korniyenko, B. Research of the training ground for the protection of critical information resources by iRisk method. Mechanisms and Machine Science, Volume 70, pp. 227-237, (2020). doi:10.1007/978-3-030-13321-4_21
14. Korniyenko, B. Y., Borzenkova, S. V., Ladieva, L. R. Research of three-phase mathematical model of dehydration and granulation process in the fluidized bed. ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 12, pp. 2329-2332, (2019).
15. Kornienko, Y. M., Liubeka, A. M., Sachok, R. V., Korniyenko, B. Y. Modeling of heat exchangement in fluidized bed with mechanical liquid distribution. ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 12, pp. 2203-2210, (2019).
16. Bieliatynskyi, A., Osipa, L., Kornienko, B. Water-saving processes control of an airport. Paper presented at the MATEC Web of Conferences, 239, (2018). doi:10.1051/matecconf/201823905003
17. Korniyenko, B.: Informacijni tehnologii' optymal'nogo upravlinnja vyrobnyctvom mineral'nyh dobryv. K.: Vyd-vo Agrar Media Grup (2014).
18. Korniyenko, B., Osipa, L.: Identification of the granulation process in the fluidized bed. ARPN Journal of Engineering and Applied Sciences Volume 13, Issue 14, pp. 4365-4370 (2018).
19. Babak, V., Shchepetov, V., Nedaiborshch, S.: Wear resistance of nanocomposite coatings with dry lubricant under vacuum. Scientific Bulletin of National Mining University Issue 1, pp. 47-52 (2016).
20. Kravets, P., Shymkovych, V. ; Hardware Implementation Neural Network Controller on FPGA for Stability Ball on the Platform 2nd International Conference on Computer Science, Engineering and Education Applications, ICCSEEA 2019; Kiev; Ukraine; 26 January 2019 - 27 January 2019 (Conference Paper), Volume 938,pp. 247-256 (2019).
21. Arber, B. and Davey, J. The use of the CCTA risk analysis and management methodology CRAMM. Proc. MEDINFO92, North Holland, pp. 1589 –1593. (1992).
22. Ryabko B.Y., Monarev V.A. Using information theory approach to randomness testing. Journal of Statistical Planning and Inference, Vol. 133, № 1, pp. 95-110, (2005).
23. Chris Clymer, Ken Stasiak, Matt Neely, Stephen Marchewitz. IRisk Equatuion Available via https://securestate.en/iRisk-Equation-Whitepaper.pdf
24. Common Vulnerability Scoring System v3.0: User Guide. Available via https://www.first.org/cvss/user-guide

25. Loch K, Carr Houston, Warkentin M. Threats to Information Systems: Today's Reality, Yesterday's Understanding, Management Information Systems Quarterly 16.2; (1992).

26. McCue A. Beware the insider security threat, CIO Jury; http://www.silicon.com/management/cio-insights/2008/04/17/bewaretheinsider-security-threat-39188671/ (2008).

27. Howard MD. LeBlanc, Writing Secure Code 2nd ed., Redmond, Washington: Microsoft Press; (2003).

28. Rasmi M, Jantan A. Attack Intention Analysis Model for Network Forensics. Software Engineering and Computer Systems; 403-411. (2011).

29. Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A. A cybersecurity model in cloud computing environments. Journal of King Saud University – Computer and Information Sciences; 1: 63-75. (2012).

30. Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A.. An economic model of security threats for cloud computing systems. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec); 100-105. (2012).