Journal of KONBiN 4(24)2012
ISSN 1895-8281

THE USE OF THE EVALUATION METHOD OF SOFTWARE SYSTEM ARCHITECTURE TO ASSESS THE IMPACTS ON INFORMATION SECURITY IN INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS

WYKORZYSTANIE METODY OCENY ARCHITEKTURY SYSTEMU INFORMATYCZNEGO DO OCENY SKUTKÓW INCYDENTÓW NA BEZPIECZEŃSTWO INFORMACJI W SYSTEMACH TELEINFORMATYCZNYCH

Ireneusz J. Jóźwiak[1], Artur Szleszyński[2]

(1) Wrocław University of Technology,
(2) The general Tadeusz Kościuszko Land Forces Military Academy,
e-mails: (1) ireneusz.jozwiak@pwr.wroc.pl (2) a.szleszynski@wso.wroc.pl

Abstract: *In a paper an application of the architecture evaluation method used for prediction the effects of incidents for information security which is inside of Information and Communication Technology (ICT) system is described. As a base, the ATAM method is taken. During the analysis there is shown, that direct use of the ATAM technique is impossible, because it use only one set of data. Use just one view of ICT system is not adequate for measure the influence of incident on information security, which is inside ICT system. A tool which is useful for assessment effects of incidents, is an incidence matrix that presents logical connections between elements of ICT system. Knowledge of logical connections and structures of the messages being exchanged enables an assessment of operation the elements which receive modified messages.*

Key words: *information security, architecture evaluation, ATAM method.*

Streszczenie*: W artykule opisano adaptację metody oceny architektury systemu informatycznego do oceny wpływu incydentów na bezpieczeństwo informacji znajdującej się wewnątrz elementów infrastruktury technicznej STI. Za metodę bazową przyjęto technikę ATAM. W trakcie analizy stwierdzono, że nie jest możliwe bezpośrednia aplikacja metody ATAM, gdyż bazuje ona na jednym przekroju danych. Korzystanie tylko z jednego przekroju jest nie wystarczające do oceny wpływu incydentów na bezpieczeństwo informacji znajdującej się wewnątrz STI. Użytecznym narzędziem oceny skutków incydentów jest macierz incydencji przedstawiającej połączenia logiczne pomiędzy elementami STI. Znajomość połączeń logicznych oraz struktur wymienianych komunikatów umożliwia ocenę działania elementów odbierających zmodyfikowane komunikaty.*

Słowa kluczowe*: bezpieczeństwo informacji, ocena architektury, metoda ATAM.*

1. Introduction

A process of the development, implementation or modification of information technology (IT) systems is connected with fulfilling of requirements of a stakeholder. Stakeholder needs describes a document called specification of system requirements. In the document, a stakeholder puts requirements that can be divided into two groups: functional and non-functional [8]. The secure operation of Information and Communication Technology (ICT) system is an example of non-functional requirement.

Difficulty with implementation non-functional requirements, in ICT, is with appropriate understanding a stakeholder needs. Because non-functional requirements are expressed in natural language, it is difficult to determine how to settle those requirements. There is more difficulties with determining the measures which can help to verify if a final result is adequate for stakeholder needs. A next question is said if non-functional requirement is necessary for proper operation of ICT system.

During a process of exploring the priorities which are assigned for each of non-functional requirements[1], into created or modified solution, the methods of architecture evaluation are used. One of those methods is the ATAM[2] method, established at Software Engineering Institute of Carnegie Mellon [2,6]. The aim of it is to identify those quality requirements that are important to achieve information system fulfilling a stakeholder needs [2,6]. The architecture of ICT system is a vital factor for achievement assumed goals.

The tool supports a process of evaluation are the scenarios which show events connected with quality attributes. On the beginning of evaluation the scenarios are general. During a process of their analysis they become more detailed [6]. The final result of the process are measures that allow a verification of reached results.

2. State of art and problem's genesis

The aim of the method of architecture evaluation, information technology system, is to discover the consequences architectural decisions in connection with chosen quality attributes [2,6]. According to work, written by R. Kazman, M. Klein and P. Clements, information technology system is a result of implementation a set of requirements prepared by stakeholder. The architecture of ITC system can enable or disable to reach goals specified by stakeholder [6]. Evaluation of ICT system architecture allows an identification:

- threats, that can occur,
- the elements of ICT system where identified threats can occur [6].

Evaluation of ICT system architecture, according to C. Larman, is a kind of

1 Non-functional requirements used during a process of the analysis are call by terms: quality attributes or quality requirements.

2 Architecture Trade-off Analysis Method.

requirements analysis where we focus on those of requirements which have an influence on created solution [8]. The author says that main goal is to identify factors that have an influence on ICT system operation. Then to discover their priorities and degree of their variability, we also have to show a method of their implementation [8]. The evaluation of ICT system architecture brings advantages such as:

- reduction of risk linked to a neglect of important factor which has influence on ICT system,
- minimize work consumption on requirements which have low priorities,
- better suits of developed software product for business goals.

The question of safety and reliability of ICT system are described into technical standards and law regulations. Both of those documents recommend providing activities which can keep or increase a level of overall ICT system security. As a consequence of that we can keep an appropriate level of information security [7,9,13]. The standards include more precise recommendation related to analysis of the level of information security. They suggest to make activities such as:

- preparation of security policy,
- make a risk analysis,
- monitoring of vulnerabilities which can occur into ICT system elements,
- incidents reactions,
- recovery of ICT system after failure occur or disaster.

In both documents we cannot find a recommendation to provide an incidents analysis and their influence on secure work of ICT system. Because there are no recommendation to do this work we may ask a question why we should do this? The document Security Policy describes the goals of protection for organization's informative assets. It presents regulations associated with a grant and revocation a necessary privileges to the access to organisation's informative assets [5,9,11,13]. Risk analysis focuses on selected ICT system elements, which is a result of rules and ease of doing risk analysis [1,9,13]. In the available literature, the authors found no methods to assess the impact of information security incidents. The lack of this may be due to the specific characteristics of ICT systems. Each solution is individual and depends on the administrator's knowledge, skills.

In the literature there can be found two definitions of term information security incident. The first one comes from the standard ISO/IEC-17799 where information security incident is defined as: *"... a single event or series of events or unexpected adverse events related to information security, which pose a significant likelihood of disruption of business activities and threaten the security of information"* [9]. Otherwise, the concept of information security incident is defined by A. Białas, he states that: *"the incident is a security-related adverse event data communication system, which under current rules or guidelines may be considered a failure, actual or alleged infringement of the principles of protection of information, or the rights of property"* [3]. Considerations will be taken to the second definition.

At the beginning of elaboration of incidents' evaluation the aim that action must be specified. The aim of evaluation of influence incidents on information security is to enable:

- show relations between elements of evaluated ICT system in domain of information flow;
- determining the influence of information security attributes changes on proper operation of ICT system as a whole.

The subject of the evaluation is information transmitted and proceeded by technology elements of ICT system. While making an assessment of the influence of incident on information security which is inside the element, we can discover the paths of threat propagation. Next reliability of operation of the solution will be assessed. Knowledge of the connection between elements of ICT system during a process of messages exchange enables to plan safeguards solution that should to protect organization's informative assets. This method is better than simple risk analysis because it focuses on a group of connected elements not only one selected solution's element. That gives a possibility to protect a group of ICT system elements rather than one chosen system element.

3. Problem identification

The problem that is going to solved is to verify a possibility of use IT systems architecture evaluation method in process of incidents influence prediction. The ATAM method should minimize risk neglecting a crucial factor that has an influence on the project. Architectural solutions can enable an achievement of business goals by developed IT solution. The aim of safeguards implementation into ICT system is to keep a business operation of ICT system and rise or keep of the level its safety and reliability. Raising the level of security of the system will affect the level of information security[3] which is gathered and processed in it. Ensuring secure and reliable exchange of messages and processing has an impact on the activities of the organization. It is important to have tools that allow to predict the impact of information security incidents inside the communication system operated by the organization [4,5,13].

The purpose of this article is to present the application methods for assessing trade-offs for information systems architecture (ATAM) to analyze the impact of security incidents in the operation of the communication system. Based on the data, it will be performed to assess the level of protection of information assets stored and processed in a IT system analysis.

4. The proposed solution

Security of ICT system, which combines hardware, software, telecommunications equipment, and users are non-functional requirement. Precise definition of what is

3 The term „level of security" is understand as keeping unchanged information security attributes according to recommendation at International standard ISO/IEC-17799.

to be done, as the implementation requirements of the safety of the solution is difficult and depends on the knowledge and experience possessed by the stakeholder [4,7].

Because in the structure of the ICT is telecommunications equipment, which allows remote access to information assets, it should take into account the risks associated with the described functionality. The subject of study will estimate the level of information security inside the technical infrastructure communication system in conjunction with the risks. To do this, you need to identify compounds that occur between:

- assessed elements of the technical infrastructure solutions and common vulnerabilities in them;
- incidents that exploit vulnerabilities in the elements of the technical infrastructure solutions;
- impact of the incident on the attributes of information security from the inside of the item at the time of its occurrence;
- impact of changes of information security attributes to the elements of the technical infrastructure, to whom it is given.

The security level determines the expected, by the user solution, state of information security attributes distributed in different parts of the technical infrastructure. This means that information will hold unchanged value of information security attributes[4]. If the value of information security attributes, as a result of the incident, would change, the differences should be in the accepted range. Variability range of information security attribute value creates an acceptable level of safety area information assets.

To determine an expectant level of security, we should describe an expectant level of protection for information assets, then the acceptable range of changes information security attributes. These data will be used to verify the accuracy of the results of assessment of the expected impact of the incident on the value of information security attributes.

To carry out the analysis will be prepared the following sets of data:

- a set of elements of the technical infrastructure ICT system;
- a set of logical connections that exist between the technical infrastructure ICT, along with a set of messages exchanged between the connected elements of the technical infrastructure ICT system;
- a set of known vulnerabilities present in the elements of the technical infrastructure and communication system with a set of events that use vulnerabilities in elements of the technical infrastructure of ICT system;
- a set of expected values and acceptable differences in values of information security attributes inside the ICT system.

4 The names of information security attributes are taken from International standard ISO/IEC-17799.

A sample set of elements of ICT system are shown in the table 1. In the table 1 users of ICT system are omitted. The action is intentional, as the subject of discussion will assess the risks for elements of technology infrastructure of the solution. Personal safety is the subject of an action in the domain of selection and training of members ICT. These actions constitute a separate area of providing security and reliability of IT systems.

Table 1. A sample set of the elements of ICT system (source: author's own work)

No	Group	Element
1.	Computer Hardware	Server or servers use by the organization
2.	Computer Hardware	Users workstations
3.	Computer Hardware	Printers
4.	Computer Hardware	Data storage devices
5.	Software	Server's operating system
6.	Software	Workstation operating system
7.	Software	Web site access database server
8.	Software	Depot's database server
9.	Software	Orders database server
10.	Telecommunication network	Gateways
11.	Telecommunication network	Wireless access points
12.	Telecommunication network	Switches
13.	Telecommunication network	Users network interface cards

A set of logical links is related to identification data flows between elements of technology infrastructure of ICT system. Relations between them can be shown as graphs or activity diagrams. Choice of the presentation method of logical links between the elements of ICT system depends on analysis team preferences. A sample activity diagram, that shows data flows between elements of ICT system, is shown in figure 1.

The advantage of activity diagrams is to show, in single figure, actors and the messages exchanged between them (see Fig. 1). The disadvantage of a sequence diagram is not present, a place where the class is installed. Therefore it is difficult to determine how the incident may affect the elements of the technical

infrastructure of ICT system. Therefore, we can use deployment diagrams that show the physical location of the class. In addition, we can use a graph that will show the logical links[5] between the elements ICT system, which participate in data flow between the elements (see Fig. 2). The use of three types of diagrams, in one document, expand the process of analysis.

Make an analysis of graph's (see Fig. 2) incidence matrix (1) we can identify three crucial elements that are: Web Site Server, Telecommunication Network and Database Server. All those elements have the highest vertex degree (2), all of them are responsible for data exchange with other ICT system elements (see Fig. 2) [12].

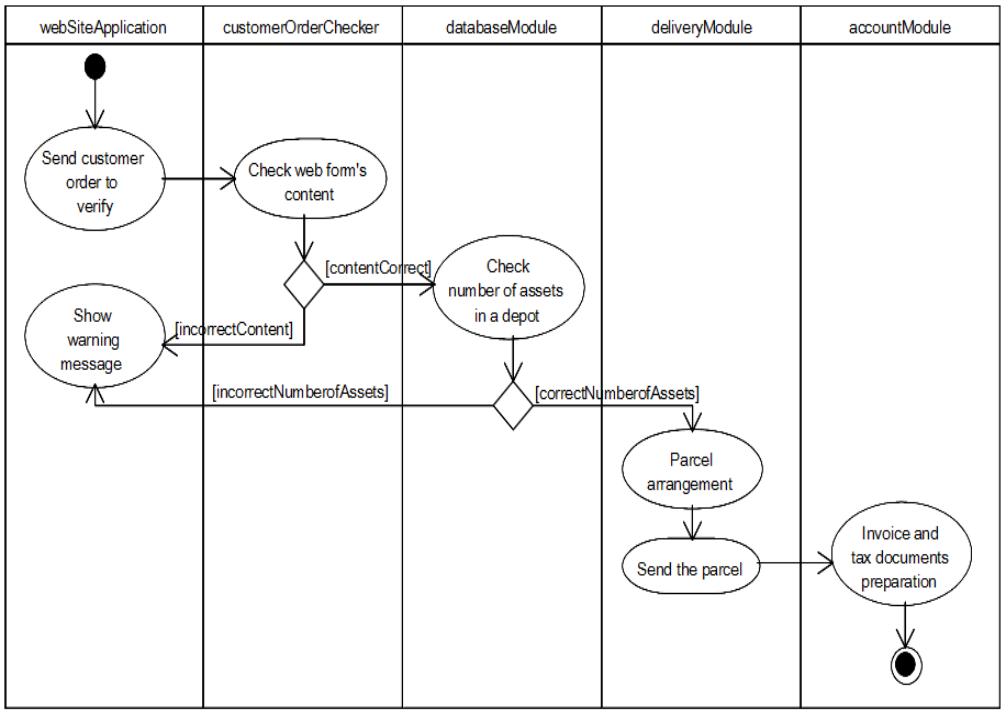

Fig. 1. A sample activity diagram (source: author's own work)

5 The term of logical link is understood as possibility to access informative assets without having a direct (physical) connection to the element that stores the informative asset. See ISO/IEC-17799.

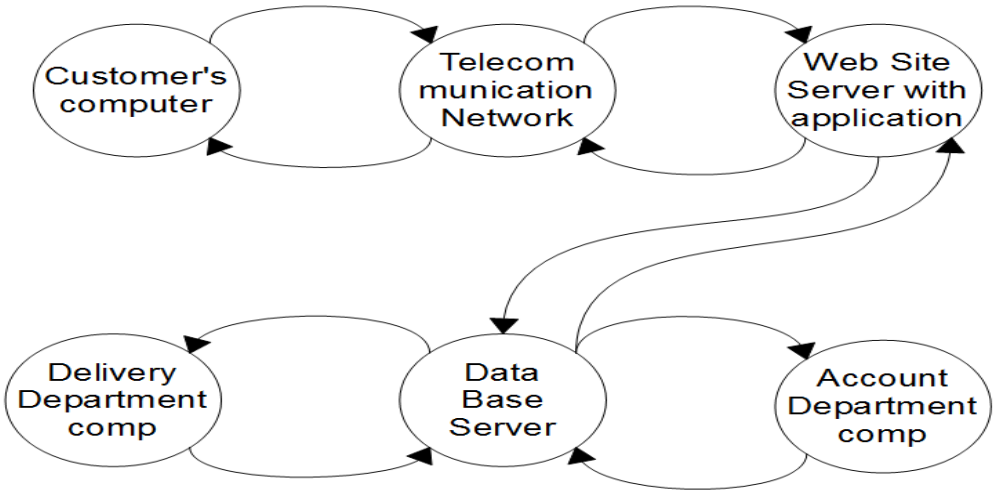

Fig. 2. A sample graph presents logical links between the elements of the ICT system (source: author's own work)

$$M = \begin{bmatrix} 1 & 1 & 0\,0 & 0 & 00 & 0 & 0\,0 \\ 1 & 1 & 1\,1 & 0 & 00 & 0 & 0\,0 \\ 0 & 0 & 1\,1 & 1 & 10 & 0 & 0\,0 \\ 0 & 0 & 0\,0 & 0 & 01 & 1 & 0\,0 \\ 0 & 0 & 0\,0 & 1 & 11 & 1 & 1\,1 \\ 0 & 0 & 0\,0 & 0 & 00 & 0 & 1\,1 \end{bmatrix} \tag{1}$$

$$\begin{cases} \deg(v_5) = 6 \\ \deg(v_2) = \deg(v_3) = 4 \\ \deg(v_1) = \deg(v_4) = \deg(v_6) = 2 \end{cases} \tag{2}$$

Where:
M – graph's incidence matrix,
deg(v_i) – the i-th vertex of graph degree – element of infrastructure of the ICT system,
v_1 – Customer computer,
v_2 – means the Telecommunication Network,
v_3 – means the Web Site Server,
v_4 – Delivery Department Computer,
v_5 – Database Server,
v_6 – Account Department Computer.

The elements, that have the highest vertex degree, will be taken as first in process of threats analysis. The assumption is a result of those elements which are responsible for data transmission to other elements or they can be a source of data. Exploitation of the vulnerabilities inside them can be cause for severe loss.

5. Utility tree as a tool for evaluation of incidents influence on information security

A tool use for evaluation of IT system architecture by ATAM method is utility tree [2,6]. The root of it is called utility, the branches contain names of quality attributes with connected scenarios [2,6,7]. Each scenario contain information about its importance, for proper ICT system operation, and risk, that is linked with its implementation. In references we can find the modification of the utility tree adopted for information security risk assessment purposes [5,11,13].
During the process of analysis the incidents effect on information security there is necessary to prepare a set of possible vulnerabilities in each of the elements of ICT system. Then we have to predict their influence on information security attributes [7]. A set of sample vulnerabilities are shown in Table 2.

Table 2. A sample list of vulnerabilities inside the elements of ICT system (source: author's own work)

No	Element's name	Vulnerability	Affected information security attribute
1	Web Site Server	Web application form has an SQL injection vulnerability	C
2	Web Site Server	Intruder can stop the server	A
3	Web Site Server	Intruder gains an administrator privileges and can control the server	C, A
4	Database Server	Incorrect data type input from Web application form	I
5	Database Server	Lost of index file for data into the tables	I, A
6	Database Server	Intruder gain an unauthorized access to data	C
7	Database Server	Intruder can change or erase data from database tables	I, A
8	Customer computer	Malicious software can catch customer log on name and password to get an access to company's Web Site	C
9	Customer computer	Order's data can be changed	I

where: C – confidentiality, I – integrity, A – availability.

The set of vulnerabilities is a basis for first, draft, version of utility tree that allows for evaluation incident influence (Fig. 3).

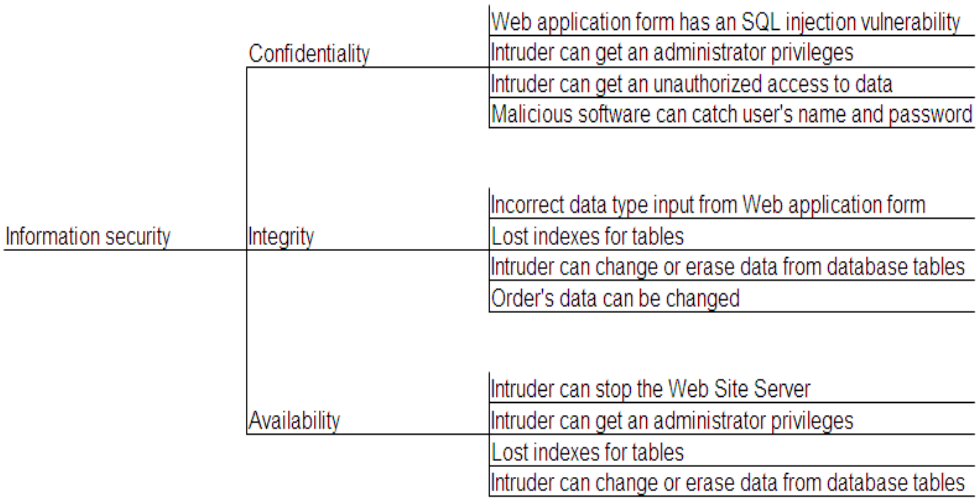

Fig. 3. A draft of utility tree for evaluation incident influence on information security (source: author's own work)

The tree (Fig. 3) presents which of information security attributes can be change in time of incident occur. The tree describes relation between information security attribute and the incident which is the scenario (3). However it does not include information about the element which the vulnerability occur.

$$REL_1 = ISA \times VU \tag{3}$$

where:

REL_1 – relation between information security attribute,
ISA – information security attribute that is stored by the ICT element,
VU – vulnerability exploited during incident.

The lack of the elements in relation force us to analyse data's views described the same elements of ICT system and connected with them incidents. There is a possibility to create a relation that contains all of elements, what is shown in formula (4).

$$REL_2 = ISA \times VU \times ETI \times RI \times IMP \tag{4}$$

where:

REL_2 – aggregated relation between information security attribute, vulnerability, system's technology element, risk and importance of the incident,
ISA – information security attribute that is stored by the ICT element,
VU – vulnerability exploited during incident,
ETI – ITC system's technology element,
RI – risk connected with the incident,
IMP – importance of incident for information security.

However making analyses by using that relation can be difficult. The research will need a dedicated software to support a creation of necessary data's views. The relation shows in (4) does not inform the analysts about incident effects on another connected element of ICT system. That piece of information can be found in incidence matrix (1).
There is a necessity to know a structure of messages exchanged between the elements, then we can verify a level of changes for each of information security attribute and their effects on work connected elements. There will be also a possibility of verification of connected element in case of failure previous element which is a source of input message.
Number of analyses, which should to be done is more than one, but ATAM method suggests do only one analysis base on one data view. That contradicts the main idea of method, which assumes a simplicity for better communication between the analysts and the stakeholders teams [2,6]. However simplicity of ATAM method do not allow to make a full analysis of incidents influence on information security which is inside the elements of ICT system.

6. Conclusion

The authors do not know the commercial software tools that support analysts' work and base on principles of ATAM method. Direct implementation of ATAM method for incidents influence on information security assessment is pointless. There is necessary to provide more than one analysis what should be supported by dedicated software. There can be created a team-specific products but they will be strongly connected with analysts team preferences and they will be useless for other teams.
Architecture assessment method associated with the estimation of the impact of incidents allows for repeatable procedures to evaluate the various ICT systems. An important role in process of evaluation will play in the historical data collected during the monitoring of work of ICT system. They will allow a more accurate assessment of parameters describing the importance and risks associated with the incident and its impact on the operating of assessed ICT system.
The lack of tools to support the analysts work can be an obstacle to the method propagation. A proposed method requires from the team conducting the assessment, has knowledge in two areas that are included in the method. The first concerns the architecture of ICT system, the second the relationship between architecture and incidents occurring during the operation of ICT. The second is related to vulnerabilities inside the elements of ICT system. The second area includes the impact of the incident on information security attributes contained in it, and the consequences that stem from the combined elements.

7. References

[1] Aven T., *Foundation of risk analysis. A Knowledge and Decision – Oriented Perspective*, John Wiley & Sons Ltd, Chichester, West Sussex 2003, England.
[2] Bass L., Clements P., Kazman R., *Software architecture, Second edition*, Helion Publishing, Gliwice 2011, (polish translation).
[3] Białas A., Bezpieczeństwo informacji i usług we współczesnej firmie, WNT, Warszawa 2006. (in polish)

[4] Jóźwiak I.J, Szleszyński A., *The specification requirements for information security collected and proceeded in the server's operation system*, Pomiary, Automatyka, Kontrola, PAK Publishing, Warszawa 2011, pp.1075-1078. (in polish).
[5] Jóźwiak I.J, Szleszyński A., *Use of the Utility Tree Technique in Process of Threats Analysis for Information Security in Information and Communication Systems*, Journal of KONBiN No 2,3(14,15)2010, Warszawa 2010, pp. 297-306.
[6] Kazman R., Klein M., Clements P., *ATAM: Method for Architecture Evaluation, Technical report, CMU/SEI-2000-TR004,ESC-TR-2000-004*, Carnegie Mellon Software Engineering Institute, Pitsburgh, PA 15213-3850.
[7] Kuchta D., Szleszyński A., Witkowski M., *Metodyka opracowania scenariuszy przebiegu incydentów w bezpieczeństwie systemu, wykorzystywanych w zarządzaniu bezpieczeństwem informacji w wojskowych systemach teleinformatycznych*, Praca naukowo – badawcza, WSOWL, Wrocław 2012. (in polish)
[8] Larman C., *UML i wzorce projektowe. Analiza i projektowanie obiektowe oraz iteracyjny model wytwarzania aplikacji. Wydanie trzecie*, Helion, Gliwice 2011.
[9] *Polish Standard PN ISO/IEC 17799:2007 Information Technology. Security techniques. The practical guide for information security management*, PKN, Warszawa 2007(in polish).
[10] *Polska norma PN-I-13335-1. Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, PKN, Warszawa 1999.
[11] Liderman K., *Risk analysis and protection of information in computer systems*, PWN, Warszawa 2008. (in polish).
[12] Wilson R. J., *Introduction to Graph Theory. Fourth Edition*, Pearson Education Limited, Essex 1996.
[13] Wolaniuk L., Szleszyński A., *Metodyka szacowania ryzyka bezpieczeństwa informacji wojskowego polowego systemu teleinformatycznego. Etap I: Wykorzystanie drzewa użyteczności do analizy ryzyka dla bezpieczeństwa informacji w wojskowym polowym systemie teleinformatycznym*, WSOWL, Wrocław 2010. (in polish).

Ireneusz J. Jóźwiak Ph.D. *– is a professor at Institute of Informatics, which is a department of the Faculty of Computer Science and Management, Wrocław University of Technology. In his scientific work professor Ireneusz JÓŹWIAK focuses on questions of reliability and security of ICT systems. He is author and co-author many of scientific works connected with computer technology reliability and security. A lot of them were published at International Scientific Journals.*

Artur Szleszyński Msc *– is a lecturer at Chair of Systems Engineering, which is a department of the Faculty of Management, The general Tadeusz Kościuszko Land Forces Military Academy. His works are focus on questions of ICT systems security.*