The security system for maintenance of the required information security level

Maciej Kiedrowicz[1,*], and *Jerzy* Stanik[1]

[1]Military University of Technology, Faculty of Cybernetics, Urbanowicza Str. 2, Warsaw, Poland

Abstract. The article outlines the concept of maintaining the required security level of the information system in the organization (SIO) through appropriate control of the security configurations of the security system. The security system (SS) model was proposed and its basic elements characterized to maintain the current security level of the information resources. The desired current security feature of the SIO shall be obtained by generating appropriate security technical and organizational configurations from the set of permissible solutions. The proposed concept, which takes into account the impact of not only basic security elements of the information resources (e.g. types of resources, security attributes, risks, vulnerability), but also changes in the working conditions of the information system and security system as well as the entire security and quality management environment of the organization, constitutes own proposal of the authors.
Key words: security, security system, security configuration, configuration of security measures, loss of efficiency of the security system.

Introduction

The rapid development of security systems for organizations observed over the last few years significantly goes ahead present knowledge of design and construction of efficient security systems. It is also noticeable that there are no formal and commercial models or descriptions of the security systems used to control the current performance characteristics of such systems in terms of efficiency of the applied security mechanisms as well as technical and organizational security measures. What is more, there are not any methods for formulating and solving tasks related to the control of the current performance characteristics of such systems, aimed at maintaining the required security level of the information. The difficulties in devising the formula or rules of controlling the current security level mainly result from the specific properties of the security systems, which currently constitute basic equipment of the Information Security Management System.

In this article, the security system efficiency is understood as a current positive assessment of the possible functioning of the security attributes assigned to each asset of the organization, belonging to the present A(t) set of the information resources of the information system (IS), in a secure manner, regardless of the emergency situations in its environment. The assessment shall be always positive, since the IS must ensure continuity of functions requested by the users of various information systems - services and/or business processes. It means that there should always be a possibility of safe processing of the information collected in the IS of the organization. With such an understanding of the current security, it is further assumed that such security is of basic significance for the IS and, without it, it would not be possible to have an efficient security system. We assume that the purpose of the operations of the security system is to assign the required statuses $\dot{\alpha_p}$ to the IS information resources, within the time limit $\Delta\dot{T_p}$, not only from the point of view of functionality, but also security. The diagram of the organization from the point of view of controlling current performance characteristics is in figure 1 [1-3].

When determining the current security level, two main issues, typical for the structure of the article, must be taken into consideration:

1) currently, it must be possible to process the required set of the information resources with respect to which basic security attributes are required at the tolerable security level,
2) to maintain the security attributes assigned to the information resources, the security system shall involve strictly defined security configurations to ensure the required security level.

In light of the above, the current security level of the SI security system shall be deemed to mean a possibility of activating sets of appropriate security configurations or configurations of security measures in the security system, using the set of the currently operational security measures that remain at the disposal of the team responsible for designing and operating the security system.

* Corresponding author: maciej.kiedrowicz@wat.edu.pl

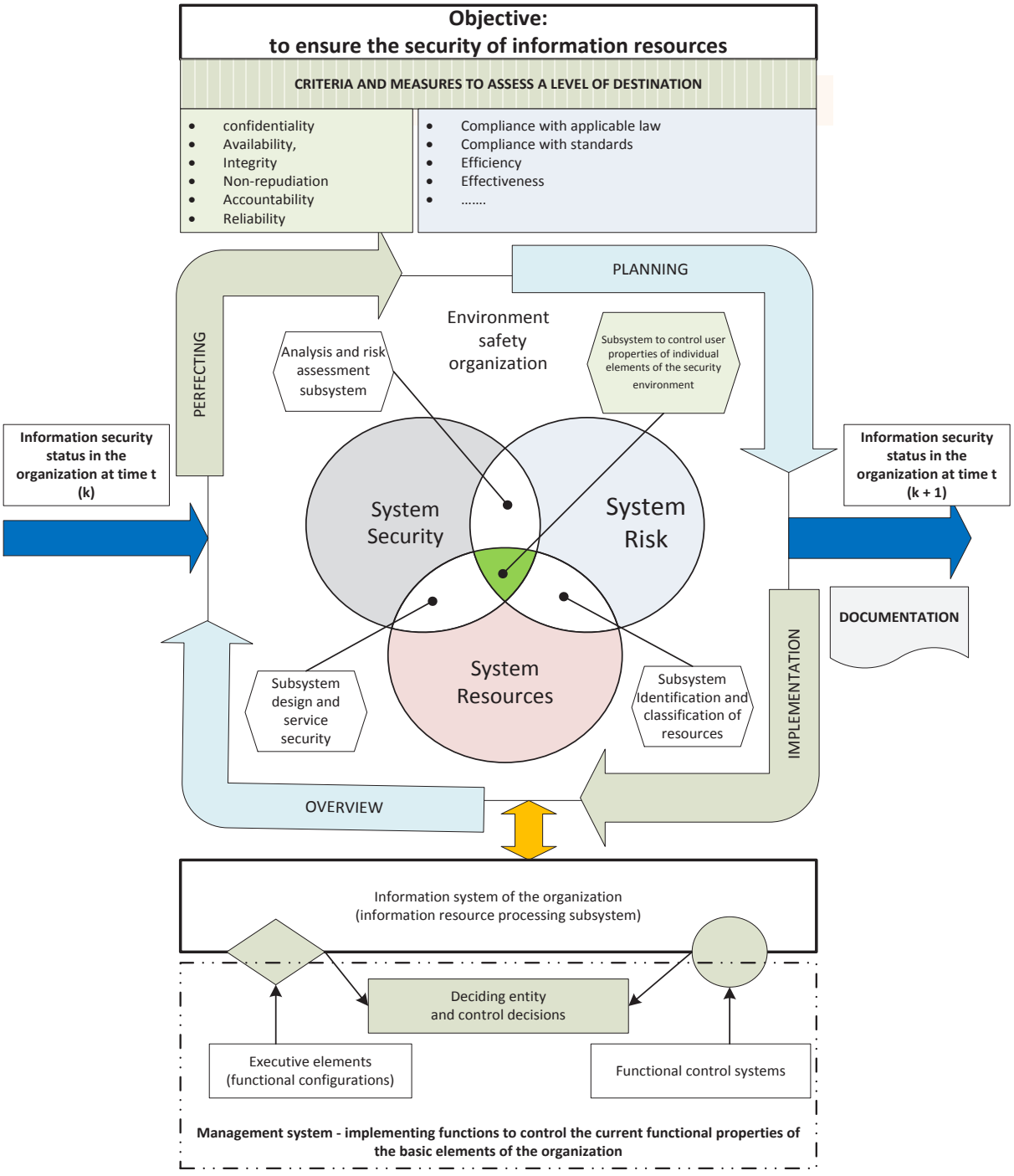

Fig. 1 Diagram of the organization from the point of view of controlling current performance characteristics – functional aspect and security aspect.

1 Security Configuration

The following notation of any security configuration shall be introduced

$$KB_{klmn} = \langle A^{klmn}, AT^k, ZG^l, ZP^m, MB^n \rangle \quad (1)$$

where:

- A^{klmn} – a set of information resources of the information system in the organization subject to protection by the klmn-th security configuration,
- AT^k – a set of security attributes assigned to the information resources belonging to A^{klmn} set,
- ZP^m – a set of vulnerability describing weak points of the information resources from A^{klmn} set,
- ZG^l – a set of risks that may use the vulnerability of the information resources from A^{klmn} set,
- MB^n – a set of security mechanisms creating the klmn-th security configuration.

* Corresponding author: maciej.kiedrowicz@wat.edu.pl

The knowledge of security KB_{klmn} makes it possible to assign to each the set A^{klmn}, , with the predefined AT^k, ZG^l, ZP^m sets, corresponding set MB^n of security mechanism (organizational and technical security measures). The security configuration KB_{klmn} shall be efficient only when the set of information A^{klmn}, with predefined ZG^l, ZP^m, may have such a MB^n set assigned thereto, which ensures resources of the A^{klmn} set required security level. It may be assumed that, as a result of the above, the A^{klmn} set, with the predefined Cartesian product $R^{klm} = \langle AT^k, ZG^l, ZP^m \rangle$, shall be in relation with the MB^n set, i.e. $A^{klmn}\ KB_{klmn}\ R^{klm}$. Therefore, it is possible to analyze the security configuration (1) as an analogous to the terminal system according to [4] based on which the information resources from the A^{klmn} set constitutes the input data, whereas the elements of the MB^n set - the output data.

If a given information resource $a_g \in A$ may be protected by the security mechanism $mb_j \in$ MB, then, by providing the feasibility relation R_x, ($R_x \subset A \times MB$), for which the expression

$$\langle a_g, mb_j \rangle \in R_x , \tag{2}$$

is correct, it is possible to define the set of the security mechanisms, involved in the protection of a single information resource a_g.

In such case, the set of the aforesaid security mechanisms shall be determined in the following way:

$$MB_g = \{mb_j \in MB : a_g R_x mb_j, \}. \tag{3}$$

While considering the property (2), the relation R_x may be replaced with the GxJ matrix

$$X = [x_{gj}], \tag{4}$$

whose elements

$$x_{gj} = \begin{cases} 1, when,\ a_g R_x mb_j, \\ 0, in\ other\ cases. \end{cases} \tag{5}$$

The elements of the matrix shall meet the following conditions:

$$\sum_{j=1}^{J} x_{gj} \geq 1\ for\ g = \overrightarrow{1,G}, \tag{6}$$

$$\sum_{g=1}^{G} x_{gj} \geq 1\ for\ j = \overrightarrow{1,J}. \tag{7}$$

In the subsequent part of the article, only such security systems which meet the following condition shall be considered:

$$\left(\Lambda_{A_g \subset A^{klmn}} \vee_{KZ_g \in A^{klmn}} {}_{\times 2^{AT\,k} \times 2^{ZG\,l} \times 2^{ZP\,m} \times 2^{MB\,n}}\ KZ_g \subset KB^{klmn}\right) \Leftrightarrow \left(A_g\ KZ_g MB_g\right). \tag{8}$$

In the above-mentioned relation, KZ_g means the security configuration of the g-th task. While considering the (1) configuration, KZ_g may be defined in the following manner:

$$KZ_g = \langle a_g, AT^g, ZG^g, ZP^g, MB^g \rangle, \tag{9}$$

where:

- a_g – information resources protected by the g-th security configuration,
- AT^g – a set of security attributes assigned to a_g of the information resources,
- ZG^g – a set of risks that may have impact on the a_g information resources,
- ZP^g – a set of vulnerability factors of the information resources, which may be used by the risks from the set, ZG^g
- MB^g – a set of security mechanisms creating the g-th security configuration.

The knowledge of configuration of security measures for the information resources makes it possible to assign the MB^g set of security mechanisms (measures) corresponding to the $a_g \in A$ resource, with the predefined AT^g, ZG^g, ZP^g sets.

On the basis of the above considerations, it is evident that the condition

$$KB_{klmn} = \bigcup_{g:\, a_g \in A^{klmn}} KZ_g \tag{10}$$

is justified for the analyzed group of security systems.

In such case, any security configuration KB_{klmn} may be analyzed as a multitude of the configurations of security measures for the resources $a_g \in A^{klmn}$.

Depending on the type of the information resources, which need to be protected by the security system with the predefined security configuration, several or even a dozen or so resource KZ_g configurations of security measures may be activated at a given time. It should be stressed that the information resources subject to protection require specific technical or organizational security measures to ensure the acceptable security level. In case of loss of the required security level, the security configuration in the security system shall be deemed to mean sets of technical and organizational security measures, remaining after the loss of security and allowing protection of only the $\check{A} \subset A^p$ set, where A^p – the set of the information resources, with respect to which the required security level must be maintained.

The set of the permissible security configurations for the security system <u>*shall be defined*</u>, upon its loss of security, on the basis of the knowledge of:

- A^p – a set of information resources, with respect to which the required security level shall be maintained,
- ZG^p – a set of risks that may have impact on the information resources form the set A^p,
- ZP^p – a set of vulnerability factors of the information resources from the set A^p, which may be used by the risks from the set, ZG^p
- MB^p – a set of the operational security mechanisms remaining after the loss of security,

according to the following formula:

$$KB_{dop}^{v} = \begin{cases} \{KB_{klmn} = \langle A^{klmn}, AT^{k}, ZG^{l}, ZP^{m}, MB^{n} \rangle \in Å x B x \Omega x \Pi x \times \Psi : \\ A^{klmn} \supset A_p\}, if \ \vee_{\langle k,l,m,n \rangle \in K^v \times L^s \times M^r \times N^u} (A^{klmn} \supseteq A^{p}). \\ \Phi in \ other \ cases - set \ empty. \end{cases} \quad (11)$$

where:

- $Å$ – a family of sets of information resources, which may have to be protected in case of lost efficiency of the SS,
- B – a family of sets of security attributes, which may be assigned to information resources,
- Ω – a family of sets of risks, in case of which the security mechanisms must be applied,
- Π – a family of sets of vulnerability of information resources,
- Ψ – a family of sets of security mechanisms, which may be used after the loss of efficiency of the SS,
- K^v – a set of indices of the family elements B,
- L^s – a set of indices of the family elements Ω,
- M^r – a set of indices of the family elements Π,
- N^u – a set of indices of the family elements Ψ,

The above means that all security configuration, built for different variants of the AT^k, ZG^l, ZP^m sets and set of security measures MB^n shall be included in the set KB_{dop}^{v} of permissible security configurations of the security system after the loss of efficiency. Each security configuration from the KB_{dop}^{v} set guarantees maintenance of the acceptable security level of the information resources from the A^{klmn} set.

2. Desired property of the security system

The desired property of the security system shall be deemed to mean a possibility of ensuring the acceptable security system for the security attributes assigned to the information resources of the security system [5-6]. It is assumed that the set of such resources $a_g \in A$ shall change discreetly over time. The set of the information resources, which shall have efficient protection as of the specific period of time $t_i \in \Delta\dot{T}_p$ may be presented in the following way:

$$A(t_i) = \{a_g^b \in A : g \in G(t). b \in B(t)\}, \quad (12)$$

where:

- a_g^b – information resources, with respect to which efficient protection shall be implemented,
- A – a set of information resources, with respect to which efficient protection shall be implemented,
- G(t) – a set of numbers of the information resources processed in the information system of the organization as of t moment,
- B(t) – a set of numbers of the types of the information resources processed in the information system of the organization as of t moment.

3. Current property of the security system

The current property of the security system shall be deemed to mean a possibility of activating the set of appropriate security configurations in the Security System of the Organization, while using currently operational and useful technical and/or organizational security measures that remain at the disposal of the team responsible for designing and operating the security mechanisms [7-10].

While assuming that the transformations β, γ are known, where:

$$\beta: 2^{A} \times 2^{AT} \longrightarrow 2^{MB}, \beta(A^{klmn}, AT^{l}) = MB^{klmn} \quad (13)$$

$$\gamma: 2^{ZG} \times 2^{ZP} \longrightarrow 2^{MB}, \gamma(ZG^{l}, ZP^{m}) = MB^{klmn} \quad (14)$$

and knowing the set of currently available security mechanisms: MB(t) and sets: ZG(t), ZP(t), it is possible to define a family of sets Å(t) of the information resources, with respect to which it is possible to maintain the acceptable security level as of t moment $\in \Delta\dot{T}_p$.

While considering correlations (13), (14), a family of Å(t) sets of the information resources may be presented in the following manner:

$$Å(t) = \begin{Bmatrix} \dot{A}^{klmn} \subset A : \dot{A}^{klmn} = \gamma\big(\beta(ZG^{l}, ZP^{m})\big), \\ \langle ZG^{l}, ZP^{m} \rangle \in 2^{ZG(t)} \times 2^{ZP(t)} \end{Bmatrix}, \quad (15)$$

where:

- A – a set of the current information resources of the information system in the organization,
- ZG(t) – a set of risks identified at t moment,
- ZP(t) – a set of risk identified at t moment with respect to the A set of the information resources,
- MB^{klmn} – a set of currently operational security mechanisms

4. Loss of efficiency of the security system

The loss of efficiency of the security system shall be deemed to mean an event that occurred at $t_i \in \Delta\dot{T}_p$ moment due to the discrepancy between the desired property of the security system and its current property. The occurrence of such event shall be construed as the "loss" of efficiency of the security system at t_i. moment. What corresponds to condition [11]:

$$A^{POŻĄD}(t) \supset A^{BIEŻ}(t) \quad (16)$$

where:

- $A^{POŻĄD}(t)$ – a set of the IS information resources, with respect to which it is required to maintain the values of the security attributes at the acceptable level,
- $A^{BIEŻ}(t)$ – a set of the IS information resources, with respect to which it is possible to maintain

the values of the security attributes at the acceptable level.

The Cartesian product creates space for possible scenarios of the loss of efficiency of the security system

$$U = 2^A \times 2^{ZG} \times 2^{ZP} \times 2^{MB}. \quad (17)$$

The $u_{klmn} = \langle A^k, ZG^l, ZP^m, MB^n \rangle \in U$ element defines the type of the loss of efficiency of the security system.

Let us assume that for each type of the loss of efficiency, the value of the $\lambda(\text{klmn}) = v$ function, defining the number of the loss of efficiency, e.g. value of the residual risk, is determined.

To explicitly define the loss of efficiency of the security system, among other things, the following identification functions in the information system or security system shall be used:

a) The set of currently operational security mechanisms:

$$F^{MB}: U \longrightarrow 2^{MB}, F^{MB}(u_v) = \widehat{MB^s} \quad (18)$$

b) The set of risks

$$F^{ZG}: U \longrightarrow 2^{ZG}, F^{ZG}(u_v) = ZG^l \quad (19)$$

The set of vulnerability factors

$$F^{ZP}: U \longrightarrow 2^{ZP}, F^{ZP}(u_v) = ZP^m \quad (20)$$

The set of the current information resources that require efficient protection

$$F^{A}: U \longrightarrow 2^{A}, F^{A}(u_v) = A^p \quad (21)$$

Furthermore, it is assumed that for each type of the loss of efficiency of the SS $u \in U$, number v, the $\widehat{MB^s}$, ZG^l, ZP^m, A^p sets shall be closed and determined at the stage of designing the security system.

5. Reconfiguration function

To create a possibility of compensation for the loss of efficiency of the security system, it is required to determine, at the stage of designing the SS set, all permissible steering decisions, hereinafter referred to as directives, without which members of the team responsible for the security of the organization may determine the aforesaid current properties of the security system by committing or rolling back the security configurations or configurations of security measures, which ensure achievement of the required security level of the IS information resources. The transition of the SS from the "loss of efficiency" status to the "achieved efficiency" status may be described through the following formula:

$$FR: KB \longrightarrow KB \quad (22)$$

Defined as:

$$FR(KB^z) = KB^v \; gdzie \; z, v \in V; z \neq v \quad (23)$$

where:

- V – a set of natural numbers,
- KB^z – a set of permissible security configurations before the loss of efficiency, number z,
- KB^v – a set of permissible security configurations after the loss of efficiency, number v.

The representation of FR shall be determined at the stage of designing the SS or establishing the Information Security Management System (ISMS) in the organization, to ensure the obtaining of the desired properties of the SS during its use. The desired current security property of the SS may be obtained by generating appropriate security configurations or configurations of security measures from the set of permissible solutions. After the loss of efficiency of the SS, it is essential to generate optimum or suboptimum security configuration for the purpose of continuing efficient processing of the information resources. The optimum or suboptimum security configuration is generated among the set of the permissible solutions on the basis of the detailed Q reconfiguration function, which - from the point of view of its essence - constitutes a criterial function. The subject of the next article shall be the formulation of the multicriterial task for optimization of the security configuration and method of its execution.

Summary

For many years now, the work on standardization and optimization of the security system with respect to the assets of an organization, including its information assets, has been carried out. According to the conditions of the information society, it is necessary for each security system to have the following properties:

1) continuous readiness, i.e. maintenance of the required level of current functionality, reliability and efficiency in terms of the maintenance of the desired security level, regardless of the emergency situations that may occur,
2) high operability in terms of controlling the performance properties, understood as timely and definite reaction to all emergency situations, and making steering decisions to restore efficiency of the system with respect to the maintenance of the required security level within the required time limit.

The article does not offer the recipe for the design and construction of efficient security system in terms of ensuring the required security level of the information resources. It is merely a proposal of the authors for partial solution of the problem related to the determination and construction of the SS, which would allow present control of the security level of the information system in the organization. The proposed approach to the issue of security, aimed at the reconfiguration process, results, among other things,

from the observations and long-term experience of the authors gained:

1) during observations of the construction and implementation of such security systems in the organizations and corporations,
2) during research and implementation projects,
3) during scientific and research projects as well as seminar discussions relating to the issue of corporate security.

Currently, the ISO 27001, ISO 27005 and ISO 27006 [12-15] international standards as well as a set of good practices in the field of risk analysis and information security shall constitute the reference point while building the Security System (SS).

References

1. M. Kiedrowicz, J. Stanik, *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity*, (in:) B. F. Kubiak and J. Maślankowski (eds), *Information Management in Practice*, pp. 231-249 (2015)
2. M. Kiedrowicz, J. Stanik, *Models and Method for the Risk Assessment of an Intellectual Resource*, WSEAS Transactions on Information Science and Applications, **14**, pp. 174-183 (2017)
3. J. Stanik, M. Kiedrowicz, *Model ryzyka procesów biznesowych.* Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług, Szczecin (2017)
4. M. D. Mesarovic, *Matematyczna teoria systemów ogólnych*, (in:) G. J. Klir (ed.), *Ogólna teoria systemów,* WNT, Warsaw (1976)
5. R. Hoffmann, M. Kiedrowicz, J. Stanik, *Evaluation of information safety as an element of improving the organization's safety management*, MATEC Web of Conferences, **76** (2016)
6. M. Kiedrowicz, *Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity,* MATEC Web of Conferences, **125** (2017)
7. A. Najgebauer, R. Antkiewicz, D. Pierzchała, J. Rulka, *Quantitative Methods of Strategic Planning Support: Defending the Front Line in Europe*, in *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017*, Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 656), ISSN: 2194-5357, (2017)
8. D. Pierzchała, R. Antkiewicz, M. Dyk, R. Kasprzyk, A. Najgebauer, Z. Tarapata, *Modelling, simulation and computer support of the Polish criminal procedure*, in: *Information Systems Architecture and Technology. The Use of IT Technologies to Support Organizational Management in Risky Environment*, ed. Z. Wilimowska, L. Borzemski, A. Grzech, J. Świątek, ISBN 978-83-7493-858-7, pp. 51-60, Wrocław, (2014)
9. Z. Tarapata, M. Zabielski, R. Kasprzyk, K. Szkółka, *Profile Cloning Detection in Online Social Networks*, Computer Science and Mathematical Modelling, vol. **3**, pp.39-46, (2016)
10. A. Najgebauer, R. Antkiewicz, M. Chmielewski, M. Dyk, R. Kasprzyk, D. Pierzchała, J. Rulka, Z. Tarapata, *The Qualitative and Quantitative Support Method for Capability Based Planning of Armed Forces Development*, LNAI, Springer, vol. 9012, pp. 224-234, (2015)
11. J. Stanik, *Utrzymywanie wymaganego poziomu bieżącej niezawodności funkcjonalnej komputerowego systemu zautomatyzowanego dowodzenia, praca doktorska,* WAT, Warszawa (1987)
12. ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements*, pp. 10-22, Geneva (2013)
13. ISO/IEC 27006:2015 *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems*, pp. 29-34, Geneva (2013)
14. PN-ISO/IEC 27005 *Technika informatyczna, Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji,* PKN (2013)
15. PN-ISO 31000:2012 *Zarządzanie ryzykiem - Zasady i wytyczne*, PKN (2012)