MULTICRITERIA OPTIMIZATION USED FOR THE INFORMATION SECURITY – IDEAL AND ANTI-IDEAL

Maciej Kiedrowicz, Ph.D.
Cybernetics Faculty
Military University of Technology
Warsaw, Poland
e-mail: maciej.kiedrowicz@wat.edu.pl

Jerzy Stanik, Ph.D.
Cybernetics Faculty
Military University of Technology
Warsaw, Poland
e-mail: jerzy.stanik@wat.edu.pl

Abstract

The article outlines the concept of assessing the utility of the security configuration, using two reference points (ideal and anti-ideal). The concept is in line with the natural intention of getting closer to the ideal point. In case of several such solutions, it is possible to obtain the solution that would move the least desirable situations as far as possible. In methodological context, the article consists of two layers. The first layer includes the security configuration model, including values describing the utility properties and partial criteria for measuring utility. The second layer refers to the issue of multicriteria optimization of the security configuration and proposed method of its resolution.

Key words: security configuration, utility of configuration, polioptimization task, multicriteria optimization methods

Introduction

The efficiency of the information processing process in an organization to a large extent depends on the present qualitative properties, e.g. functionality, reliability, utility, security of the security system (SS). Therefore, it is crucial to appropriately control the current properties of the SS by generating the most desired security configurations[1] from among the set of permissible solutions after the occurrence of an emergency situation[2]. The most desired security configuration is the one, which not only ensures maintenance of the required level of security, but also has the best utility properties. The issue was analyzed as the task of multicriteria optimization of the security configuration. The issue constitutes the main theme of the article and determines its framework. The subject of the article is composed of the following elements:

1. Development of models of the Security System and Security Configuration allowing to consider the interdependence between the current level of security and random changes of risk factors having material impact on the safety of the information processing processes.
2. Proposal of the values describing the utility properties of the security configuration and partial criteria for measuring their utility.
3. Formulation of the issue of multicriteria optimization of the security configuration and proposed method of its resolution.

The re-configuration process is executed on the basis of the detailed Q reconfiguration function, which - from the point of view of its essence - constitutes a criterial function. Schematic representation of the configuration from the perspective of the reconfiguration process is in figure 1.

The figure shows two important groups of elements:

1. basic components of the security configuration and some of the selected interdependencies between them,

[1] Security configuration – a set of technical, organizational and human security measures as well as correlations between them, which reflect the quality, e.g. utility, security, performance and reliability features.
[2] Emergency situation – an event that occurred due to the difference between the desired property of the SS and its current utility feature.

2. basic components of the reconfiguration process and interdependencies between them, reflecting the manner of transformation from the current, ineffective security configuration into the desired security configuration.

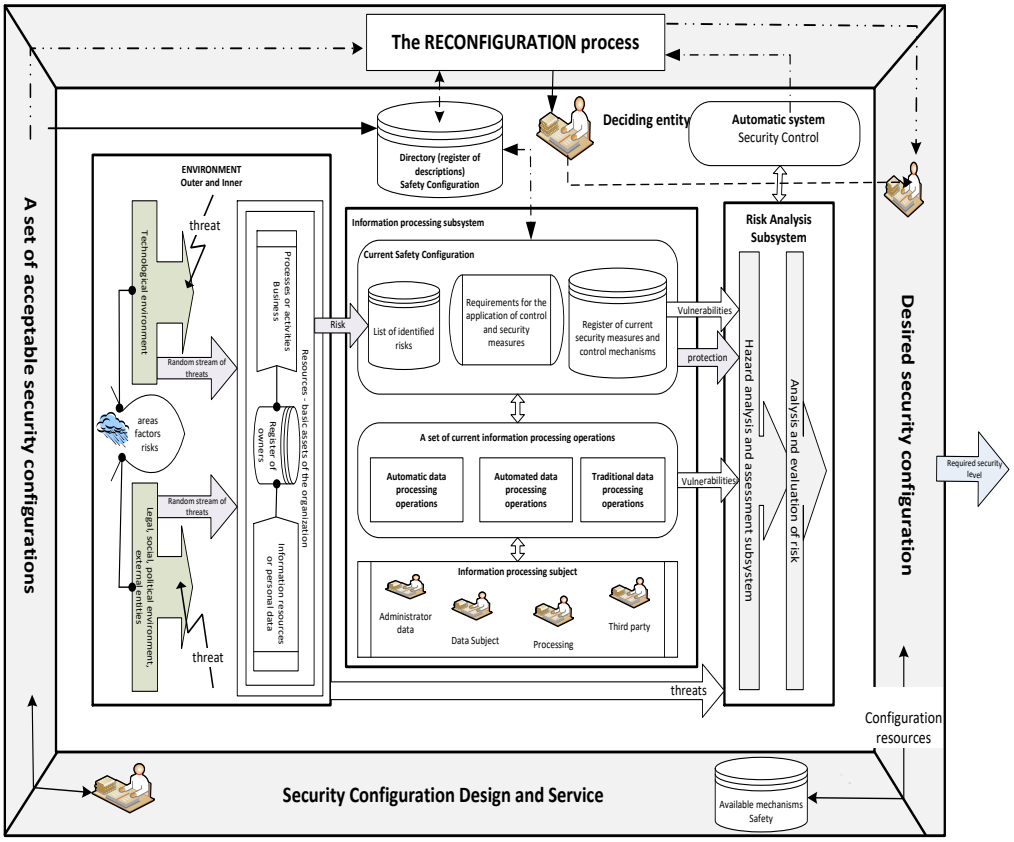

Fig. 1. Illustration of the configuration from the perspective of the reconfiguration process.
Source: Own study.

After the occurrence of an emergency situation – loss of the required level of security, it is essential to generate permissible or optimum security configuration to efficiently continue the process of safe information processing in the information system of the organization (ISO). The optimum 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.

Security configuration as a fundamental pillar of the information security system

Information security system

When compared with other definitions of the information security theory, the following definition seems to be the most accurate in terms of the requirements (STANIK et al., 2016; HOFFMANN et al., 2016) hereof:

> "The security system constitutes a part of the whole system for information security management with predefined actions concerning the design, monitoring and maintenance of the desired set of technical and organizational security measures, based on which it is possible to generate the required security configuration".

The security system includes an organizational structure, planned actions, scopes of responsibilities and work tools allowing to control the current level of security of the entire organization as its elements. The security system constitutes one of the key links in the Information Security Management Systems (KIEDROWICZ, 2018; KIEDROWICZ, 2017; KIEDROWICZ, STANIK, 2017).

Following the above definition, we shall adopt the ordered four as the model for the security system:

$$SZ =< POF, PDZ, \mathbb{C}, KB >, \quad (1)$$

where:

PSF - the subject of activities of the security system refers to a group of officers, who perform different roles in the data processing process, entitled to make decisions in that respect,

PDZ - the object of activities, i.e. the ISO objects, with respect to which the data must be processed and the security maintained at the required level,

$\mathbb{C}$ - the purpose of operations as defined in the object of activities,

KB - the set of permissible security configurations, which constitutes a basic element of the object of activities in terms of maintaining the required level of security.

The set of permissible security configurations shall be considered a comprehensive, consistent and non-contradictory subsystem of the security system aimed at reducing the probability of risk of assets or information system of the organization. Appropriate selection of such security configurations (set of permissible security configuration) and their efficient use allow to significantly reduce the cost of security of the organization, additionally ensuring appropriate level of security - tolerable level of protection. The above-mentioned elements are the subject of considerations in the subsequent subchapters of this article.

Security configuration

The grounds for the security configuration model shall be a correlation between the set of the information processing processes (recorded actions) and the set of activated technical, organizational, process and human security measures, after the occurrence of serious circumstances[3], hereinafter referred to as the emergency situation. In case of some types of the emergency situations, it may turn out that it is possible to safely process the data or maintain the required level of information security by various sets of activated security measures or protection processes. In such cases, it is necessary to choose one of them – the best from the point of view of a specific criterion.

The following notation of any security configuration shall be introduced

$$KB_{kl} = \langle OB^{kl}, PO^{k}, MB^{l} \rangle \tag{2}$$

where:

OB^{kl} – the set of the data processing processes or operations (information resources and personal details) in the information system of the organization protected by the klth security configuration,

PO^{k} – the set of control mechanisms or protection processes aimed at meeting business, legal and other requirements for the processing of data, including personal details, which belong to the OB^{kl} set,

MB^{l} – the set of security mechanisms creating the klth security configuration.

The knowledge of the KB_{kl} security configuration makes it possible to assign the MB^{l} set corresponding to each OB^{kl}, set, with the predefined PO^{k} set of security mechanisms (organizational and technical security measures). The KB_{kl} security configuration is implemented only when it is possible to assign such $zbiór\ PO^{k}$, to the OB^{kl} set, with predefined elements of the MB^{l} set, which shall guarantee the maintenance of the required level of security for the OB^{kl} set of information resources. It may be assumed that as a result of the above, the OB^{kl} set, with the predefined MB^{l} set, remains in correlation with the PO^{k} set, i.e. $OB^{kl}\ KB_{kl}\ PO^{k}$. Therefore, it is possible to analyze the security configuration (2) as analogous to the terminal system, in which the elements from the OB^{kl} set constitute input data, whereas the elements of the PO^{k} or MB^{l} set - output data.

If a given $z_g \in OB$ data processing process may keep the required level of security through the $po \in PO$ protection process and subset of security measures from the MB^{l} set, then, by providing the R_x feasibility correlation, ($R_x \subset OB \times PO \times 2^{MB}$), in case of which the following formula $\langle z_g, po_j, MB_n \rangle \in R_x$ is correct, it is possible to determine the sets of protection processes and security measures used to protect a single z_g data processing process.

In the subsequent part of the article, only such situations are analyzed, which meet the following condition:

$$\left(\bigwedge_{z_g \subset OB^{kl}} \bigvee_{KB_g \in KB^{kl} \times 2^{PO_g} \times 2^{MB_g}} KB_g \subset KB^{kl}\right) \Leftrightarrow \left(z_g\ KB_g PO_g KB_g MB_g\right). \tag{3}$$

[3] Serious circumstances – the occurrence of one of the following events: inefficiency or uselessness of the security measures, inability to perform the data processing due to significant disruption of the processing environment, e.g. the occurrence of a large number of risks or vulnerability factors, etc.

In the above-mentioned relation, KB_g means the security configuration of the g[th] information resource. While considering the (2) configuration, KB_g may be defined in the following manner:

$$KB_g = \langle z_g, PO_g, MB_g \rangle, \tag{4}$$

where:

z_g – the data processing process protected by the g[th] security configuration,

OP_g – the set of protection processes used to maintain the required level of security of the z_g[th] data processing process,

MB_g – the set of security measures creating the g[th] security configuration.

The knowledge of the security configuration for the data processing process creates a possibility of assigning the MB_g set to the $z_g \in OB$ process, with the predefined PO_g set. On the basis of the above considerations, it is evident that the following condition is true for the analyzed class of the security systems:

$$KB_{kl} = \bigcup_{g:\, OB_g \in OB^{kl}} KB_g. \tag{5}$$

In such case, any KB_{kl} security configuration may be analyzed as a multitude of the security configurations for the particular $z_g \in OB^{kl}$ data processing processes.

Depending on the types of the data processing processes, which need to be protected through the protection processes and security measures, with the predefined security configuration, it is possible to activate, at a given moment, several or even a dozen or so KB_g action security configurations. It should be stressed that the data processing process subject to protection requires specific protection processes and technical or organizational security measures to ensure the acceptable security level.

Values describing utility properties of the security system

In case of an emergency situation related to the loss of the required level of security, it should be possible to activate (using protection processes and efficient security mechanisms - security measures) several different permissible security configurations. In such cases, it is necessary to choose one of them. It is obvious that the chosen security configuration must be the best in every aspect. Therefore, it is necessary to comprehensively assess - in terms of criteria functions - all variants of the permissible security configuration, including many values (characteristics) describing its utility and security properties. The rating shall be composed of many partial ratings. Such task may be executed only upon establishment of the set of representative characteristics reflecting the purpose of operations of the security system, manner of its operation and rules of use, determining the system's utility[4] or efficiency[5].

In such a manner, the subjectivity of the rating is decreased, thus, it is possible to:

1. reduce the number of criteria functions and quality indicators, which constitute grounds for such rating and choice of the optimal or suboptimal security configuration,
2. ensure proportionality of the significance (weight) of particular values and criteria functions,
3. reasonably assess the utility of the security system with a specific security configuration.
4. With the above in mind, it is possible to state the following with respect to the utility of the security configuration in the security system, distinguishing the following values (characteristics):
5. sensitivity[6] of the security system to the loss of the required level of security,
6. time of generation of the security configuration,
7. efficiency of the operations of the information processing subsystem,
8. redundancy with respect to the technical security measures,
9. redundancy with respect to the protection processes.

The above-mentioned values describing the properties of the security system with a specific security configuration do not constitute any closed set. It is possible to introduce other (not mentioned herein) values, which concern, for example, bandwidth or capacity of the security configuration.

Let us introduce the following symbols:

Ω – the set of values describing utility properties of the security configuration,

[4] Easy operation and meeting the actual needs of the user.
[5] Verification whether the undertaken activities produced the expected results.
[6] ability of the security system to react to the change of type and amount of the information subject to further processing under the ISO,

KB^u_{dop} – the set of permissible security configurations in case of the emergency situation (loss of security), number "u",
Q – the set of distinguished criteria functions,
W – the set of vectors of implementation of particular values from the Ω set,
f_{1-5} – the vector-valued function assigning a vector of implementation of particular values to each permissible security configuration.

While considering the above values (describing the utility properties of the security configuration), the Ω set may be presented in the following manner:

$$\Omega = \{\Omega_i, i = \overline{1,5}\}. \tag{6}$$

Let us assume that for each Ω_i value, the W_i set of possible implementation is determined. In such case, the ordered set of implementation of the $< f_1(KB), f_2(KB), f_3(KB), f_4(KB), f_5(KB) >$ value shall correspond to the permissible $KB \in KB^u_{dop}$ security configuration, recorded shortly $f(KB)$ or

$$\underline{w} =< w_1, w_2, w_3, w_4, w_5 >. \tag{7}$$

The functions assigning to each permissible $KB \in KB^u_{dop}$ configuration the implementation of its i[th] value, may be presented in the following manner:

$$f_i : KB^u_{dop} \longrightarrow W_i, f_i(KB) = w_i, i = \overline{1,5}. \tag{8}$$

$$\overline{f}: KB^u_{dop} \longrightarrow W_1 \times W_2 \times W_3 \times W_4 \times W_5;\ \overline{f}(KB) = \underline{w} \text{ vector function.} \tag{9}$$

According to further considerations on $\underline{w}$ vectors of implementation of the values describing the utility properties of the security configurations, it may be assumed that the security configurations with the same type of implementation of such values are indistinguishable and have the same use value for the assessor (in terms of utility). Such assumption is true only when the distinguished values reflect basic material utility properties of the security configuration.

The $W = \overline{f}(KB^u_{dop})$ set of permissible $KB \in KB^u_{dop}$ security configurations does not have to include all possible combinations of implementation of the values $(W_1 \times W_2 \times W_3 \times W_4 \times W))$ and usually does not include. Some types of implementation of the Cartesian product $(W_1 \times W_2 \times W_3 \times W_4 \times W))$ correspond, in practice, to impermissible or unfeasible variants. The vectors of implementation of values reflecting the utility properties of the security configuration are not value determinants in general. The criteria functions, depending on the vectors of implementation of such values, are used to show the utility of the security configuration. Therefore, the criteria functions are the functions of $\underline{w}$ or $\overline{f}$: (KB) vectors defined in the following manner:

$$Q_m: W \longrightarrow Y_m, m = \overline{1,M} \text{ or } Q_m: \overline{f}\left(KB^u_{dop}\right) \longrightarrow Y_m, m = \overline{1,M} \tag{10}$$

where:
W, $\overline{f}\left(KB^u_{dop}\right)$ – the sets of vectors of implementation of values,
M – the number of distinguished criteria functions.

The permissible security configurations may be rated using the following vectors:

$$\overline{Q}(KB) = \left(Q_1\left(\overline{f}(KB)\right), Q_2\left(\overline{f}(KB)\right), Q_3\left(\overline{f}(KB)\right), Q_4\left(\overline{f}(KB)\right), \dots, Q_M\left(\overline{f}(KB)\right)\right)$$

or (11)

$$\underline{Q}(KB) = (Q_1(KB), Q_2(KB), Q_3(KB), \dots, Q_M(KB)).$$

In case of $Q_m, m \in \hat{M}$ criteria functions, their extremization are not provided for, but preferences are to be established. The preferences mean that the level of each distinguished criterion must be achieved equally or exceeded unequally, i.e.:

$$Q_m(KB) \geq \hat{y}_m,\ m \in \hat{M} \tag{12}$$

where:

$\hat{y}_m$ – the level of preference (aspiration) for the mth criteria function,

$\widehat{M}$ – the set of numbers of criteria functions, with respect to which no extremization is provided for.

The aspiration level values are determined by experts from the security system team, depending on what is demanded from such system.

To find optimal or suboptimal security configuration, the following stages must be executed:

1. Definition and measurement of values describing utility properties of the security configuration,
2. Definition of the set of criteria functions,
3. Formulation of the issue of multicriteria optimization,
4. Solution of the task of multicriteria optimization,

The issues 1 and 2 constitute the subject of the article (STANIK, KIEDROWICZ, 2018), whereas the issues 3 and 4 constitute the subject of this article.

Formulation of the issue of multicriteria optimization of the security configuration

The formulation of the issue of a multicriteria optimization of the security configuration is justified only in such cases when in case of an emergency situation, it is possible to generate (with efficient technical, organizational and human resources) several permissible security configurations. In case of many different (with materially different values of the distinguished quantities) permissible security configurations, the problem is usually to choose the best configuration, which shall meet the requirements determined at the stage of designing the SS to the greatest extent possible. Such choice may be made only in the event when the assessor determines (for assessed security system class) the vector criteria function and domination dependency in the criterial space.

Forms of the distinguished criteria functions

In case of the security system, the utility of the security configuration may be rated and compared in a reliable manner using the following qualitative indicators

1. $Q_1(KB_x)$ - sensitivity of the security system to the loss of the required level of security,
2. $Q_2(KB_x)$ - time of generation of the security configuration,
3. $Q_3(KB_x)$ - efficiency of the operations of the information processing subsystem,
4. $Q_4(KB_x)$ - redundancy with respect to the technical security measures,
5. $Q_5(KB_x)$ - assessment of even load of the security configuration with the technical security measures

The above-mentioned indicators are defined in the following manner:

$$Q_1(KB_x) = y_1 = \frac{\overline{\overline{OB}}_x^{MAX} - \overline{\overline{OB}}^u}{\overline{\overline{OB}}}, x \in X; \tag{13}$$

where:

$\overline{\overline{OB}}_x^{MAX}, \overline{\overline{OB}}^u, \overline{\overline{OB}}$ – cardinality OB_x^{MAX}, OB^u , OB sets;

whereas:

OB_x^{MAX} – the set of information resources, including a maximum number of information resources, with respect to which it is possible to maintain the level of security as part of the KB_xth security configuration,

OB^u – the set of information resources, with respect to which it is necessary to maintain the required level of security as of the time of occurrence of the emergency situation number "u", with the predefined O^u and MB^u sets.

OB – the set of of the information resources in the ISO determined at the stage of design.

$$Q_2(KB_x) = y_2 = \frac{1}{N_x}\sum_{i=1}^{N_x} t_i^x, x \in X; \tag{14}$$

where:

N_x – the number of experiments conducted in the security system in the KB$_x$th security configuration.

t$_i^x$ – the time of generation of the KB$_x$th security configuration in the ith experiment.

The strive towards shortening the generation time allows to:

1. reduce a possibility of interrupting the continuity of business processes in the organization, in particular the information processing process,
2. reduce a possibility of interrupting the information receipt process in the ISO environment due to temporary break in operation of the system.

$$Q_3(KB_x) = y_3 = \begin{cases} \sum_{r\in R_x}\left(\overline{K}_r^x - K_{KR,r}^x\right), jeżeli\ \bigwedge_{r\in R_x}\overline{K}_r^x\ \geq K_{KR,r}^x \\ -1, jeseli\ \bigvee_{r\in R_x}\overline{K}_r^x < K_{KR,r}^x \end{cases}, x \in X; \quad (15)$$

where:

$\overline{K}_r^x$ – the average number of the rth type protection processes initiated as part of the $KB_x{}^{th}$ security configuration,

$K_{KR,r}^x$ – the number of the rth type protection processes necessary to construct the security configuration critical in emergency situations,

R_x – the set of types of the protection processes initiated in the $KB_x{}^{th}$ security configuration.

$$Q_4(KB_x) = y_1 = \frac{\overline{\overline{OB}}_x^{MAX} - \overline{\overline{OB}}^u}{\overline{\overline{OB}}}, x \in X; \quad (16)$$

where:

$\overline{\overline{MB}}_x^{MAX}, \overline{\overline{MB}}^u, \overline{\overline{MB}}$ – cardinality MB_x^{MAX},MB^u , MB sets;

whereas:

MB_x^{MAX} – the set of the security mechanisms, including a maximum number of the security mechanisms implemented as part of the $KB_x{}^{th}$ security configuration

MB^u – the set of security mechanisms, with respect to which it is necessary to maintain the required level of security as of the time of occurrence of the emergency situation number "u", with the predefined O^u and PO^u sets.

MB – the set of security mechanisms established at the stage of designing the security system.

It is obvious that the value of such indicator should significantly exceed the critical value.

$$Q_5(KB_x) = y_5 = \begin{cases} \frac{min\left\{\sum_{j\in B_x^i} n_{ji},\ldots,\sum_{j\in B_x^i} n_{jI_x}\right\}}{max\left\{\sum_{j\in B_x^i} n_{ji},\ldots,\sum_{j\in B_x^i} n_{jI_x}\right\}}, jeżeli\ \bigvee_{<i,k>\in I^x\times I^x}\left(\bigwedge_{j\in B_x} n_{ij}\ \neq n_{kj}\ \right); \\ 1,\ jeżeli\ \bigwedge_{<i,k>\in I^x\times I^x}\left(\bigwedge_{j\in B_x} n_{ij} = n_{kj}\right) \end{cases} \quad (17)$$

where:

I_x – the set of numbers of technical security measures included in the $KB_x{}^{th}$ of the security configuration,

B_x – the set of numbers of the types of technical security measures used under the ith protection process, included in the $KB_x{}^{th}$ security configuration,

n_{ij} – the number of technical security measures of the jth type initiated under the ith protection process.

Formulation of the issue of multicriteria optimization of the security configuration

Having established:

$\widehat{KB}_{dop}^u$ – the set of permissible security configurations in case of an emergency situation (loss of security), number "u", with respect to which tighten requirements for the values describing their utility properties are met

Q – vector criteria function,

$\geq$ – domination dependency in the criteria space.

The task of multicriteria optimization of the security configuration may be noted in the following manner (CICHOSZ, BOREK, 2007; PŁONKA, 2013):

$$(\widehat{KB}_{dop}^u, Q, \geq), \quad (18)$$

whereas:

1. The set of permissible security configurations may have the following form:

$$\widehat{KB}_{dop}^{u} = \left\{KB_x \in KB_{dop}^{u} : \; Q_2(KB_x) \leq T_{dop} \wedge Q_3(KB_x) \geq 0, x \in X\right\} \tag{19}$$

where:

$\widehat{KB}_{dop}^{u}$ – the set of permissible security configurations in case of the emergency situation (loss of security), number "u", defined in the following manner:

$Q_2(KB_x)$ – the time of generation of the KB_xth security configuration,

T_{dop} – permissible time of generation of the KB_xth security configuration,

$Q_3(KB_x)$ – efficiency indicator of the operations of the information processing subsystem,

X – the set of indices of the elements in the $\widehat{KB}_{dop}^{u}$ set,

2. Vector criteria function is defined in the following manner:

$$\widehat{Q: KB}_{dop}^{u} \longrightarrow Y, Q(\,KB_x) = \underline{y} \tag{20}$$

where:

$\underline{y}$ – the vector of partial rating of security configurations,

Y – the criteria space defined in the following manner:

$$Y = \left\{\underline{y} = \underline{Q}(KB_x) \in \mathcal{R}^5 : KB_x \in \widehat{KB}_{dop}^{u}\right\}, \tag{21}$$

whereas:

$\underline{Q}(KB_x)$– the rating vector of the KB_xth security configuration in the following form:

$$\underline{Q}(KB_x) = (Q_1(KB_x), Q_2(KB_x), Q_3(KB_x), Q_4(KB_x), Q_5(KB_x)); \tag{22}$$

where particular components of the $\underline{Q}(KB_x)$ rating vector for the KB_x security configuration shall be construed in the following manner:

$Q_1(KB_x) = y_1$ – indicator of sensitivity of the security system to the loss of the required level of security,

$Q_2(KB_x) = y_2$ – time of generation of the security configuration,

$Q_3(KB_x) = y_3$ – efficiency indicator of the operations of the information processing subsystem, with the predefined security configuration,

$Q_4(KB_x) = y_4$ – redundancy indicator with respect to the technical security measures,

$Q_5(KB_x) = y_5$ – indicator of even load of the security configuration with the technical security measures.

Selection criteria of optimal security configuration:

$$Q_1(KB_x) = y_1 = \frac{\overline{\overline{OB}}_x^{MAX} - \overline{\overline{OB}}^{u}}{\overline{\overline{OB}}} \longrightarrow max$$

$$Q_2(KB_x) = y_2 = -\frac{1}{N_x}\sum_{i=1}^{N_x} t_i^x \longrightarrow max$$

$$Q_3(KB_x) = y_3 = \sum_{r \in R_x}\left(\overline{K}_r^x - K_{KR,r}^x\right) \longrightarrow max$$

$$Q_4(KB_x) = y_1 = \frac{\overline{\overline{OB}}_x^{MAX} - \overline{\overline{OB}}^{u}}{\overline{\overline{OB}}} \longrightarrow max$$

$$Q_5(KB_x) = y_5 = \frac{min\left\{\sum_{j \in B_x^i} n_{ji}, \ldots, \sum_{j \in B_x^i} n_{jI_x}\right\}}{max\left\{\sum_{j \in B_x^i} n_{ji}, \ldots, \sum_{j \in B_x^i} n_{jI_x}\right\}} \longrightarrow max$$

Methods of resolving the issue of multicriteria optimization of the security configuration

Resolution of the $(\widehat{KB}_{dop}^{u}, Q, \geq)$ polyoptimization task comes down to the establishment of the set of dominating solutions. The set has the following form:

$$KB_D^{\geq} = \left\{ \dot{KB} \in \widehat{KB}_{dop}^{u} : Q_m\left(\dot{KB}\right) = \max_{KB \in \widehat{KB}_{dop}^{u}} Q_m(KB), m = \overline{1,5} \right\}. \quad (23)$$

Once nonempty $KB_D^{\geq}$ set is obtained, the procedure is finished.

Every $KB \in KB_D^{\geq}$ security configuration is characterized by the values describing its utility properties. Better than the security configuration belonging to the $\widehat{KB}_{dop}^{u} \backslash KB_D^{\geq}$ set. Any security configuration from the $KB_D^{\geq}$ set of dominating solutions may be considered the optimal security configuration in terms of the adopted criterion.

In practice, it is often the case that the set of dominating solutions is an empty set. In such situation, it is essential to choose the solution from the set of permissible solutions. The set of permissible solutions is usually quite "extensive". Therefore, a practical dilemma arises: which solution should be applied? A comparison of the permissible security configurations using the rating vector is difficult and labor-intensive. Therefore, it is recommended to use such solution, which would be a natural generalization of the optimization concept, including one global criteria function aggregating all partial criteria functions. The methods of reliable measurement of the values describing the utility properties of the security configurations and methods for determining the values of particular criteria functions are known. However, no general methods for aggregating partial ratings are available. The aggregation process requires great caution. It is especially misleading to aim at achieving general rating in the form of one number. According to fig. 2, when adopting, for the purpose of general rating of the security configuration utility, the "distance" of the analyzed security configuration from the model configuration (e.g. determined at the stage of designing the SS), many materially different permissible security configurations (with materially different values of the distinguished quantities) produce such results.

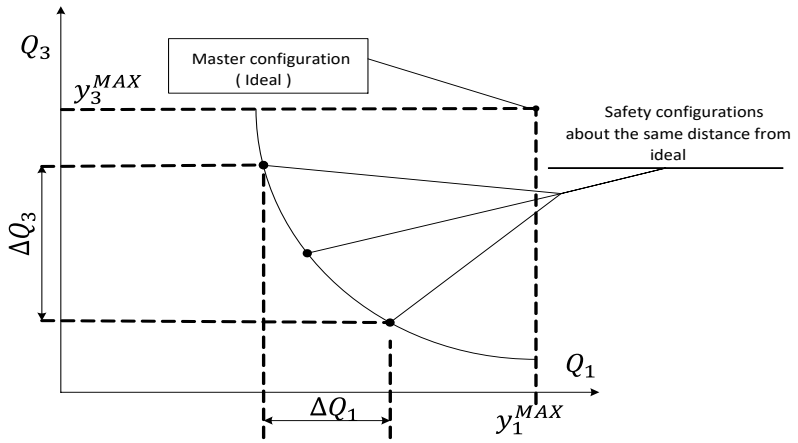

Fig. 2. Comparison of various security configurations with the model rating[7].
Source: Own study.

Figure 2 shows potential problems that may be encountered in case of aggregating partial rates of the utility of the security configuration. By distinguishing many partial quality indicators, it is possible to assess the utility of the permissible security configurations in the form of a vector (10). Therefore, a ranking of the rated security configurations from "the best" to "the worst" and selection of the only one best security configuration (without ordering other configurations) may be a difficult task. It is an exceptional situation when one of the rated security configurations is better than other configurations in terms of all criteria (i.e. the value of each criteria function for such security configuration is higher or lower than the value of the same criteria function for other permissible security configurations (Fig.3)). Such situation means that there is an nonempty set of dominating solutions.

[7] This and other figures show the limitation to the two-dimensional space (resulting from the fact that it is easier to illustrate) despite the fact that five partial criteria functions are being analyzed. The distance in the figure is the Euclidean distance (parameter p=2 was adopted).

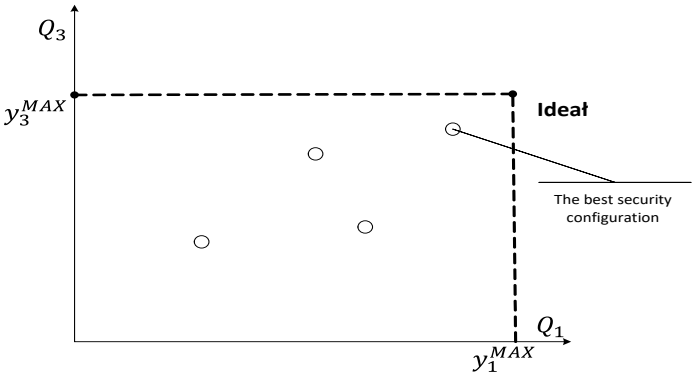

Fig. 3. Domination of one security configuration over others.
Source: Own study.

A serious problem occurs when none of the permissible security configurations significantly "dominates" over other security configurations (see: fig. 4).

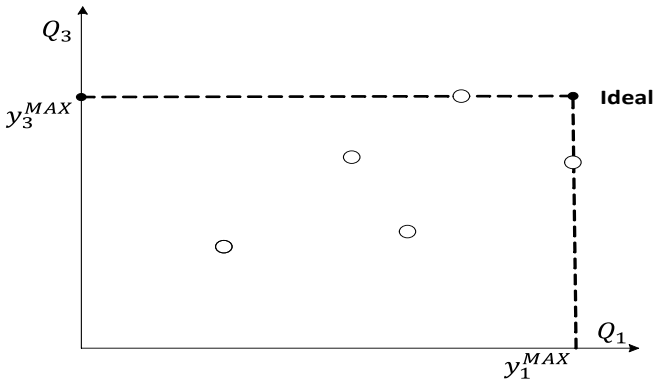

Fig. 4. Absence of domination of one permissible security configuration over others.
Source: Own study.

In the events when it is impossible to explicitly indicate "the best" security configuration in the set of permissible solutions, it is necessary to find a way of ordering the security configurations (or at least a method for finding the best one). It is possible to reject such security configurations from the $\widehat{KB}_{dop}^{u}$ set of permissible security configurations, whose properties are worse (i.e. the value of each criteria function is less satisfactory to the assessor) than those of others (see: fig. 5).

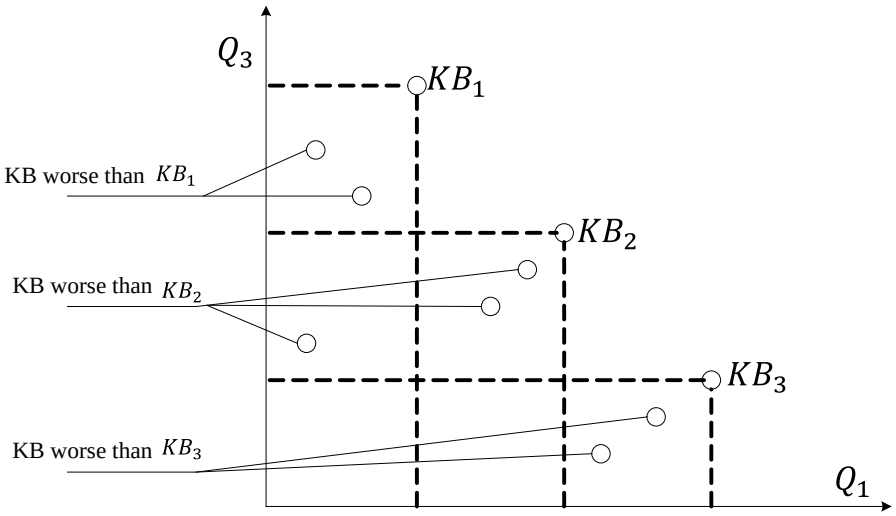

Fig. 5. Domination of KB_1, KB_2 *i* KB_3 over other permissible security configurations.
Source: Own study.

The set of security configurations, which may not be eliminated in the above-mentioned manner, shall be called the set of undominated security configurations. Such set (BLASZCZYNSKI et al., 2007) constitutes an inverse image of the set of undominated results.

$$KB_N^{\geq} = Q^{-1}(Y_N^{\geq}). \tag{24}$$

The set of undominated results has the following form:

$$Y_N^{\geq} = \left\{\underline{y} \in Y \ : nie\ istnieje\ \underline{z} \in Y, \underline{z} \neq \underline{y}, że\ \left(\underline{z}, \underline{y}\right) \in \geq \right\}. \tag{25}$$

The manner of choosing the suboptimal security configuration from the set of undominated solutions may be as follows:

1. First, such solutions that do not achieve the required level of values of the determined criteria functions shall be eliminated from the set. The representation of narrowing the set of permissible solutions is in fig. 6.

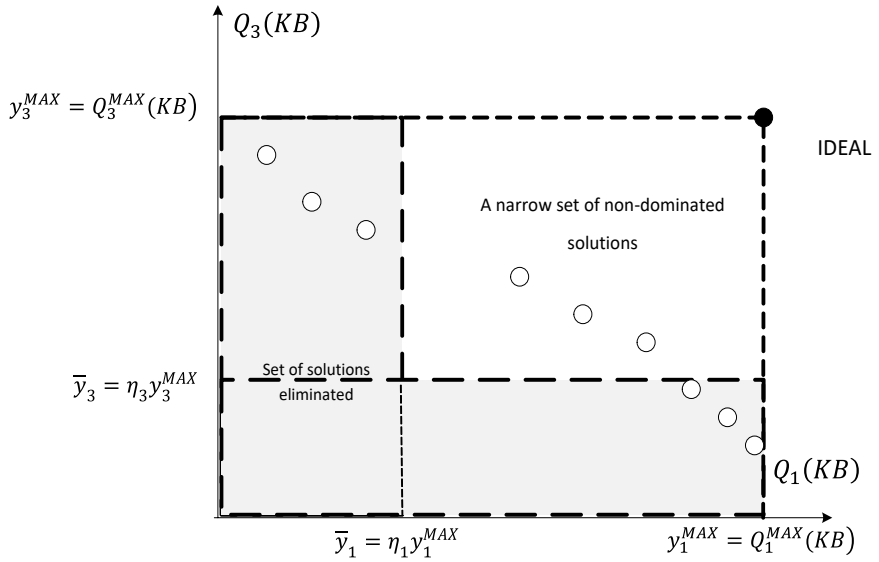

Fig.6. Narrowed set of undominated solutions.
Source: Own study.

The narrowed $\overline{KB} \equiv KB_N^{\hat{y}}$ set may be defined recursively

$$KB_m^{\hat{y}} = \left\{KB \in KB_{m-1}^{\hat{y}} : Q_m(KB) \geq \hat{y}_m\right\}, m \in \{1,2,3,4,5\}, KB_D^{\hat{y}} = Y_N^{\geq} \tag{26}$$

where:

$\hat{y}_m$ – the level of aspiration (preference) for the mth criteria function.

The process of narrowing the set may be continued until a single solution is obtained through the change of the value of η_m , $m = \overline{1,5}$ coefficients. When high values of η_m coefficients are adopted, the idea of such behavior may be distorted by eliminating (at some stage of the recursive procedure) all undominated solutions. Therefore, the values of η_m coefficients should be selected from the following ranges: $\frac{\hat{y}_m}{\dot{Q}_m} \leq \eta_m \leq 1, m \in \{1,2,3,4,5\}$, where $\dot{Q}_m = \max_{KB \in \overline{KB}_N^{\geq}} Q_m(KB)$, not to allow acceptance of the situation. If the aforesaid situation occurs, i.e. $\vee_{m\in\{1,2,3,4,5\}} KB_m = \phi$, the η_m ($m \in \{1,2,3,4,5\}$ coefficient should be decreased so that the $\wedge_{m\in\{1,2,3,4,5\}} KB_m^{\eta} \neq \phi$ conditions are met.

Once a one-element $\overline{KB}$ set is obtained, the procedure is finished.

2. A method of compromise solutions may be suggested for the set of the security configurations, which remained after the elimination process (described in point 1), as the continuation of the procedure.

The method is considered one of the ways of solving the polyoptimization tasks, using the so-called scalarization of partial criteria.

Let us assume that X security configurations numbered $x \in \bar{X} = \{1,2,\dots,X\}$ are left in the $\overline{KB}$ set. The configurations shall be rated using five (M = 5) different quality indicators. $\overline{y}_{mx} \in \mathcal{R}^1$ shall mean the value of the mth criteria function of the xth security configuration, wheres $\overline{y}_m$ - the rating scale relating to the mth criteria function.

$$\overline{y}_m \in [\overline{y}_m^{MIN}, \overline{y}_m^{MAX}] \in \mathcal{R}^1 \tag{27}$$

where:
$\overline{y}_m^{MIN}, \overline{y}_m^{MAX}$ – the minimum and maximum value of the criteria function, number "m".

Furthermore, let us assume that the security configuration is highly rated if the value achieved by every criteria function is higher. At the beginning, it is crucial to normalize the value of criteria functions, e.g. in the following manner:

$$\overline{y}_{mx} = \frac{\overline{y}_{mx}}{\overline{y}_m^{MAX} - \overline{y}_m} \quad \text{or} \quad \overline{y}_{mx} = \frac{\overline{y}_{mx}}{\overline{y}_m^{MAX}}. \tag{28}$$

The $\overline{y}_x = (\overline{y}_{1x}, \overline{y}_{2x}, \overline{y}_{3x}, \overline{y}_{4x}, \overline{y}_{5x},) \in \mathcal{R}^5$ vector shall be considered representative of the security configuration number "x".

The set

$$\overline{Y} = \{\overline{y}_m^N \in \mathcal{R}^5 : x \in \overline{X}\}. \tag{29}$$

shall be called the normalized space for the security configuration ratings. The vector

$$\overline{y}_m^{N,MAX} = (\overline{y}_1^{MAX}, \overline{y}_2^{MAX}, \overline{y}_3^{MAX}, \overline{y}_4^{MAX}, \overline{y}_5^{MAX}) \tag{30}$$

shall be called the normalized ideal point, representing the model (ideal) security configuration. To determine the "total" scalar rating of the security configuration, the following function shall be used:

$$R_p^{\overline{y}^{MAX}}(\overline{y}_x) = \|\overline{y}^{N,MAX} - \overline{y}_x^N\|_p = \sqrt[p]{\sum_{m=1}^{M}(\overline{y}_m^{MAX} - \overline{y}_{mx})^p}, \overline{y}_{mx} \in \overline{Y}. \tag{31}$$

The set of "the best" security configurations from the $\overline{KB}$ set (the closest to the ideal in terms of the adopted distance measure) shall be determined in the following manner:

$$KB^{R^{\overline{y}^{N,MAX}}} = Q^{-1}(\overline{Y}^{R^{\overline{y}^{N,MAX}}}). \tag{32}$$

In the above formulation, $\overline{Y}^{R^{\overline{y}^{N,MAX}}}$ is the set of "the best" ratings of the security configuration - from the ideal to the closest to the ideal in terms of the adopted distance measure. The set has the following form:

$$\overline{Y}^{R^{\overline{y}^{N,MAX}}} = \left\{ \overline{y}_x^{N,O} \in \overline{Y} : R_p^{\overline{y}^{MAX}}(\overline{y}_x^{N,O}) = \min_{\overline{y}_x^N \in \overline{Y}^N} R_p^{\overline{y}^{MAX}}(\overline{y}_x), x \in \hat{X} \right\} \tag{33}$$

where:
$\overline{Y}^N$ – the normalized criteria space (all values of criteria functions fall within the range $< 0,1 >$).
$R^{\overline{y}^{N,MAX}}(\overline{y}_x^N)$ – norm in the $\overline{Y}^N$ criteria space (distance of the $\overline{y}_x$ xth rating of the security configuration from the ($\overline{y}_m^{MAX}$ ideal point)).

The norm in the $R^{\overline{y}^{N,MAX}}(\overline{y}_x^N)$ – of the $\overline{Y}^N$ criteria space is defined in the following manner:

$$R^{\overline{y}^{N,MAX}}(\overline{y}_x^N) = \|\overline{y}^{N,MAX} - \overline{y}_x^N\| = \sqrt[2]{\sum_{m=1}^{5}(\overline{y}_m^{MAX} - \overline{y}_{mx})^2}. \quad (34)$$

Fig. 7 shows graphic interpretation of the assessed distance of the security configuration for the two indicators: Q_1 and Q_3.

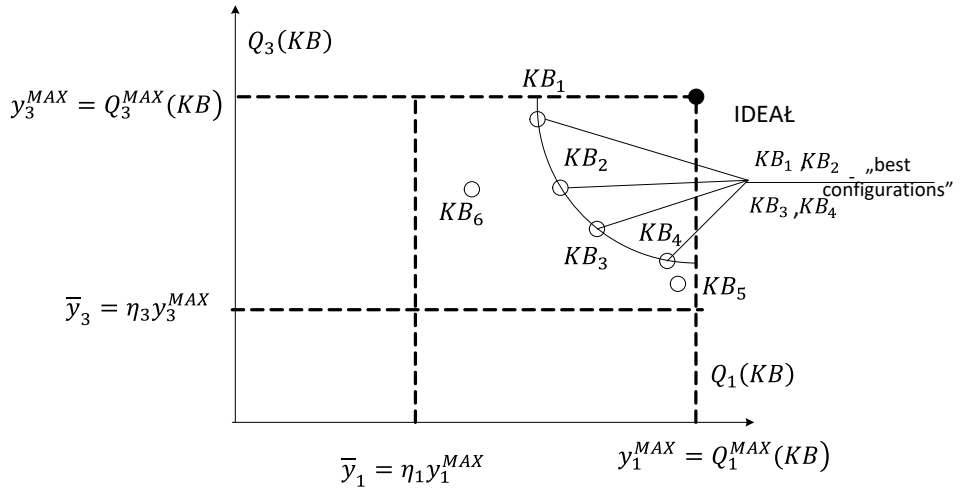

Fig. 7. Assessed distance of the security configurations.
Source: Own study.

In practice, there may be several rated security configurations from the $\overline{KB}$ set, with the same assessed distance from the ideal point (fig. 7). It means that the set

$$\overline{Y}^{R^{\overline{y}^{MAX}}} = \left\{\overline{y}_x^{N,O} \in \overline{Y}: R_p^{\overline{y}^{MAX}}(\overline{y}_x^{N,O}) = \min_{\overline{y}_x^N \in \overline{Y}^N} R_p^{\overline{y}^{MAX}}(\overline{y}_x), x \in \hat{X}\right\} \neq \phi. \quad (35)$$

In such cases, it is essential to choose the solution from the set of undominated solutions.

$$KB_N^{R_{\overline{y}}^{N,MAX}} = Q^{-1}(\overline{Y}^{R^{\overline{y}^{N,MAX}}}), \quad (36)$$

1. Choose any solution and complete the procedure,
2. Choose the solution using the method of the security configuration rating with respect to the anti-ideal point.

Therefore, two criteria for the configuration rating shall be used:

1. distance from the ideal, which should be the shortest,
2. distance from the anti-ideal, which should be the longest.

It should be stressed that moving further away from the anti-ideal does not have to mean getting closer to the ideal (fig. 8).

The issue of assessing the utility of the security configurations, using two reference points (the ideal and anti-ideal - bipolar optimization) was omitted in this article.

Summary

The security of the information (including personal details) processing processes (operations) to a large extent depends on the current utility properties of the security configuration. The desired security configuration may be obtained by reconfiguring the security system. The most desired security configuration is the one which not only allows to process the information resources so as to ensure the required level of security or maintain the continuity of security attributes, but also the one which is characterized by the best utility properties.

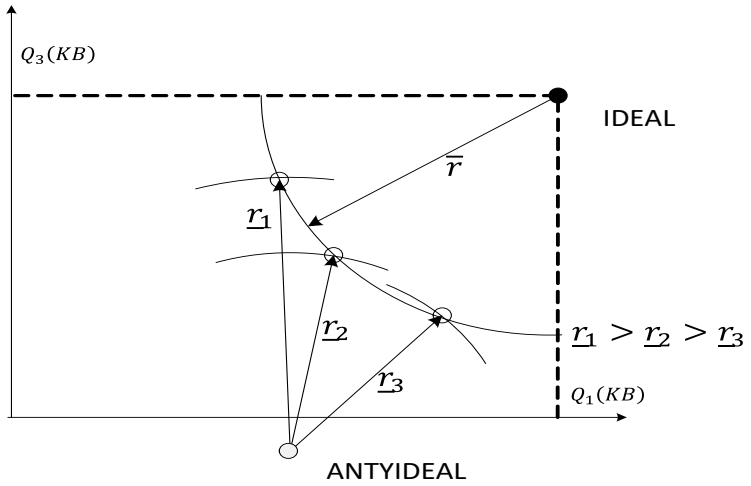

Fig. 8. Different distances from the anti-ideal with the same distance from the ideal.
Source: Own study.

On the basis of the considerations included in this article, the following conclusions may be drawn:

1. To eliminate the impact of a failure – to maintain the required level of the information security, it is justified to distinguish the two phases:
   a) Definition of the set of permissible security configurations of a given emergency situation,
   b) Optimization of the security configuration in case of a given emergency situation.
2. To optimize the security configuration, it is intentional to use the method of resolution of such task, as suggested in chapter 2.3.
3. The suggested method for controlling current utility properties of the security configuration, as the basic element of the security system, should constitute an integral part of the Information Security Management System.
4. The proposed concept of assessing the utility of the security configuration may be also used at the stage of designing the ISMS as the "privacy by design" principle recommended under the General Data Protection Regulation (GDPR) (Regulation (EU) No. 2016/679 of the European Parliament and the Council).
5. The article does not provide the "recipe" for design and implementation of efficient security configurations, which are the basic link of the security systems. It is merely a proposal of the authors for partial solution of the problem related to the determination and construction of the security system, which would allow current maintenance of the security level of the information system in any organization.
6. The proposed method for assessing utility of the security configuration is aimed at the reconfiguration and optimization of the security configuration, with an identified emergency situation – loss of the required level of security.
7. The 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:
   - during observations of the construction and implementation of such security systems in the organizations and corporations,
   - during research and implementation projects,
   - during scientific and research projects as well as seminar discussions relating to the issue of corporate security.
8. Using the results outlined herein, it is recommended to pursue further research in the following areas:
   - improvement of the structure of the security configuration models, while considering, among other things, the guidelines, motives and recommendations under the GDPR,
   - increase of precision of the proposed model by including more detailed utility properties of the security configuration and qualitative features of the security system.

The authors are convinced that further research in the above-mentioned fields may lead to the justified construction of the data protection systems or security systems with better utility parameters.

References

BLASZCZYŃSKI, J., GRECO, S., SŁOWIŃSKI, R. 2007. *Multi-criteria classification - A new scheme for application of dominance-based decision rules*. European Journal of Operational Research, 181(3).

CICHOSZ, K., BOREK, T. 2007. *Wprowadzenie do optymalizacji wielokryterialnej (Introduction to multi-criteria optimization)*, AGH, Krakow.

HOFFMANN, R., KIEDROWICZ, M., STANIK, J. 2016. *Risk management system as the basic paradigm of the information security management system in an organization*. 20th International Conference on Circuits, Systems, Communications and Computers (CSCC 2016), MATEC Web of Conferences, vol. 76.

KIEDROWICZ, M. 2018. *Metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych. (Methodology of risk management in the security of information resources)*. In: Collegium of Economic Analysis Annals, Publisher: Warsaw School of Economics (SGH) Collegium of Economic Analysis, vol 49, p. 287-305.

KIEDROWICZ, M. 2017. *Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity*. 21st International Conference on Circuits, Systems, Communications and Computers (CSCC 2017), MATEC Web of Conferences, vol. 125.

KIEDROWICZ, M., STANIK, J. 2017. *Models and method for the risk assessment of an intellectual resource*. WSEAS Transactions on Information Science and Applications, 14: 174-183.

PŁONKA, S., 2013. *Wielokryterialna optymalizacja procesów wytwarzania części maszyn (Multicriteria optimization of manufacturing processes of machine parts)*, WNT, Warsaw.

ROZPORZĄDZENIE Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE - ogólne rozporządzenie o ochronie danych (Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation), http://www.giodo.gov.pl/pl/1520284/9745.

STANIK, J., NAPIÓRKOWSKI, J., HOFFMANN, R. 2016. *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji (The risk analysis and the risk management as basic components of the safety management system of the organization)*. Scientific Papers of the University of Szczecin, Economic Problems of Services. vol. 123, p. 321-336.