ASSESSMENT OF THE USEFULNESS OF THE SECURITY CONFIGURATION

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 a method of assessment of the usefulness of the security configuration[1] (SC) from a set of available security configurations, after occurrence of an emergency situation. It is believed that the best security configuration is the one that not only ensures maintenance of the required security level of the information resources, but also provides the best values describing its utility properties. The values describing the utility properties of the security configuration and partial criteria for measuring their utility were proposed. The utility measures of the security configuration include performance, reliability and security indicators.

Key words: utility, security system, security configuration, loss of security

Introduction

To ensure the required level of security of an organization or high level of security of a given information system of such organization, which would protect it against risks, it is necessary to develop the protection strategy (plan, project) in accordance with a reliable methodology (STANIK, KIEDROWICZ, 2017; KIEDROWICZ, 2017), and then implement such project by experts, using appropriate technology and maintaining appropriate security configurations. The designed security configurations of technical or organizational nature should be to a large extent based on the results of the risk analysis, specifications of security requirements as well as general theory of security measures (i.a. it is required to assess utility of the current security configuration, verify resistance of the applied security measures to different types of attacks and re-configure the security system following the occurrence of various types of emergency situations and loss of the required level of security). 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 generated from among a set of permissible solutions (EHRGOTT, 2005) is possible on the basis of the detailed reconfiguration function Q, which - from the point of view of its essence - is a criterial function. Schematic representation of the organization from the perspective of the reconfiguration process – control of current properties of the security configuration is in figure 1.

The purpose of this article is to develop the security system model to formulate the issue of multicriteria optimization of the security configuration. To achieve the assumed goal, it was necessary to execute the following tasks, which at the same time constitute the scope of this article:

- definition of the subject, object and purpose of the operations of the security system,
- distinction of material values describing utility properties of the security system and security configuration,
- definition of the method for measuring utility properties of the security configuration,
- proposal of a set of partial criteria (criteria functions and quality indicators) for measuring utility of the security configuration,
- definition of the means for measuring utility of the security configuration to assess and chose the best configuration.

[1] Security configuration – a set of technical, organizational and human resources (security measures) as well as correlations between them, which reflect the quality, e.g. utility, security, performance and reliability features.

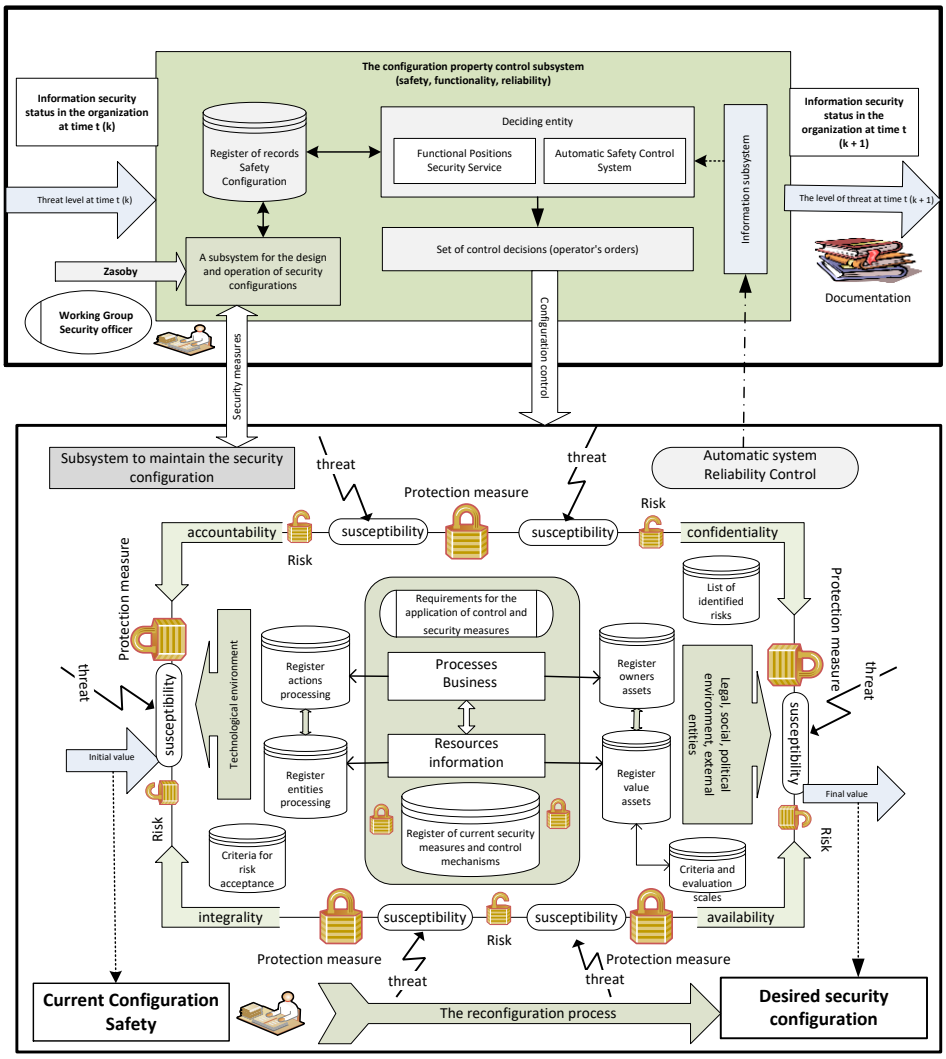

Fig. 1. Representation of the organization from the perspective of the reconfiguration process – control of current properties of the security configuration.
Source: Own study.

According to the authors, all intended elements were described in this article. Furthermore, to facilitate the understanding of the above-mentioned issues, we assume that the purpose of the security system is to assign appropriate $\dot{\alpha_p}$ statuses to the ISO objects (e.g. business processes, information processing processes, established bits of information - information resources), within the $\Delta\dot{T_p}$ time framework, not only in terms of their functionality or utility, but also security. When determining the current security level of information, three main issues, typical for the structure of the article, must be taken into consideration:

- at each particular moment of time, it must be possible to safely process the required set of information resources,
- key business processes and sensitive information resources are required[2], with respect to which protection processes need to be implemented to ensure maintenance of appropriate security attributes[3] at the acceptable risk level[4],
- To maintain the required security attributes, the security authorities shall establish, implement and maintain strictly predefined security configurations with respect to a selected set of ISO resources, ensuring their appropriate level of security or tolerable risk value.

[2] Sensitive information resource – each asset of the organization, whose loss may cause significant damages to the organization.
[3] Information security attribute – here: confidentiality, non-repudiation, availability, integrity, accountability, reliability.
[4] Acceptable risk – the level of risk which the organization may accept without any additional remedial actions or changes in its operations.

The security system and its subject, object and purpose of operations

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; KIEDROWICZ, 2018) 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. Following the above definition, we shall adopt the ordered four as the model for the information security system:

$$SB =< POF, PDZ, \mathbb{C}, KB >, \tag{1}$$

where:

- POF - 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 security system aimed at reducing the probability of risk of assets or information system of the organization. Their appropriate selection and 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 constitute the subject of deliberations in the subsequent subchapters of the article.

Object of activities

In terms of controlling the current level of information security, the object of activities may be the following:

1. an element of the automatic process for making steering decisions, e.g. the system of automatic security control system,
2. a group of officers, appointed within the framework of a team responsible for the design and handling of security configurations or Information Security Management System (ISMS) in a given organization, hereinafter referred to as the object of the decision making process.

Let us introduce the following symbols:

SF – a set of the ordered fours:

$$sf_p =< O_p, P_p, PO_p, MB_p > \in \Theta \times 2^P \times 2^{PO} \times 2^{MB}, \tag{2}$$

hereinafter referred to as positions; while considering the set of $\{R_i; i \in I\}$ correlations defined in the SF set, it is possible to distinguish different functional structures of the security system team, where:

- Θ - a group of officers appointed within the framework of the security system; the group of such persons is determined at the stage of designing the ISMS,
- P - a set of ISO objects, with respect to which the officers of the security system should maintain the required level of security,
- PO - a set of control mechanisms or protection processes, thanks to which it is possible to support the processing of the information in the ISO in terms of security and continuity of business processes in the organization,
- MB - a set of security measures available to officers of the security system.

Subject of activities

In terms of controlling the current level of information security, the subject of activities shall be a set of such $e_j \in E^{SIO}$ elements, information system of the organization (ISO), whose required status may determine the object of the decision making process. The following may be the elements of the E^{SIO} set:

- key business processes,
- information processing processes,
- bits of information (information resources) collected or processed under ISO, hereinafter referred to as an object or information resource.

Every $z \in Z$ information resource shall be marked with $p \in P^{SIO}$ number and described using the C_p^{SIO} set of property names. If all different sets of C_p^{SIO} features used to describe particular information resources are numbered with $b = \overline{1,B}$ variable (which shall be called a type of the information resource - object), the two objects shall be of the same type (e.g. "b"), when described by the identical sets of features. The sets of Q_p^{SIO} numbers of features describing the $p \in P^{SIO}$ object and sets of C_p^{SIO} feature names corresponding thereto may not be empty for each $p \in P^{SIO}$, where P^{SIO} constitutes the set of numbers of the distinguished information resources. We assume that the A_q^{SIO} set of potential implementation of the a_q feature shall be determined for each $q \in Q^{SIO}$ feature.

Purpose of operations of the security system

The operations of the security system may be defined as the following ordered pair:

$$DZ^{SZ} = <\propto^{SZ}, Z^{SZ}>, \tag{3}$$

where:

$\propto^{SZ}$ – the purpose of operations of the security system in terms of safety of the information processing,

Z^{SZ} – the set of tasks related to safe processing of information allowing to achieve the goal $\propto^{SZ}$.

Let us introduce the following symbols:

$\dot{P}(t)$ – the set of numbers of the information resources collected in the ISO by the time t, and with respect to which it is required to continue safe processing,

$[t_0^{p\cdot}, \dot{T}^p]$ – permissible time framework, during which the object number $p \in \dot{P}(t)$ should retain the security attributes - i.e. should have the required level of security,

$\dot{W}_p$ – the desired security feature of the pth information object obtained during the $[t_0^{p\cdot}, \dot{T}^p]$ time framework, where:

t_0^p, – time of registering the pth object in the ISO

$\dot{T}^p$ – time of de-registering (removing) the pth object in the ISO

$Q^{SIO}(w)$ – the set of features of the information object, based on which the "w" property is determined.

To determine whether the information resource number $p \in \dot{P}(t)$ has the "w" property, it is necessary to define for such object the $\propto_p^q (w) \subset \dot{A}_p^q$ subsets of the feature implementation, for each $q \in Q^{SIK}(w)$ feature. If the $a_q^p(t)$ features of the pth object implemented at the $t \in [\dot{t}_0^p, \dot{T}^p]$ time belong to the $\propto_p^q (w)$ subsets, it is possible to state that the object number $p \in \dot{P}(t)$ has the "w" property. When assuming that the sets of $\dot{Q}_P$ features, whose values are used to define the $\propto_p^q (w) \equiv \dot{\propto}_p^q$, $q \in \dot{Q}_P$ subsets, are known for each $p \in P^{SIO}$ object, the purpose of the security system may be determined in the following manner:

$$\propto^{SZ} \equiv \propto^{SZ} \left\{ \dot{\propto}_p^q : < p, q > \in V_D , p \in \dot{P}(t), q \in Q^{SIO} \right\}. \tag{4}$$

In terms of a possibility of achieving the goal of the security system operations, each $z_p \in Z$ information resource processed under the ISO may be described in the following manner:

$$z_p = < b_p, O_p^b, w_p^b, Q\left(w_p^b\right), \dot{\propto}\left(w_p^b\right), \dot{R}_p^b, G_p^b, S_p^b, R_{GS}^b > \tag{5}$$

where:

b_p – the type of the pth information resource,

O_p^b – the officer responsible for maintaining the required level of security with respect to the p[th] information resource of the "b" type,
w_p^b, – security feature of the p[th] information resource of the "b" type,
$Q\left(w_p^b\right)$ – the set of feature numbers, based on which the $\propto_p^q \left(w_p^b\right)$ subsets are defined,
$\dot{\propto}\left(w_p^b\right)$ – the set of desired statuses of the p[th] "b" type object,
R_p^b – the set of correlations linking b_p with $\dot{\propto}\left(w_p^b\right)$,
G_p^b – the set of potential risks of the p[th] information resource of "b" type,
S_p^b – the set of vulnerability of the p[th] information resource of "b" type,
R_{GS}^b – the correlation linking G_p^b with S_p^b.

Security configuration

The following notation of any security configuration shall be introduced

$$KB_{kl} = \langle OB^{kl}, PO^k,\ MB^l \rangle \tag{6}$$

where:
OB^{kl} – the set of information resources of the information system in the organization subject to protection by the kl[th] security configuration,
PO^k – the set of protection processes implemented to ensure security of the information resources belonging to the OB^{kl} set,
MB^l – the set of technical, organizational and human security measures, which constitute the kl[th] 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 (9) as analogous to the terminal system, in which the information resources from the OB^{kl} set constitute input data, whereas the elements of the PO^k set - output data. If a given $z_g \in OB$ information resource may be protected by way of the $po \in PO$ protection process, then, by providing the R_x feasibility correlation, ($R_x \subset OB \times PO$), in case of which the following formula: $\langle z_g, po_j \rangle \in R_x$ is correct, it is possible to determine the set of protection processes used to protect a single z_g information resource. Depending on the types of information resources, 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 resource security configurations. In such case, any KB_{kl} security configuration may be analyzed as a multitude of the security configurations for the $z_g \in OB^{kl}$ resources, i.e.:

$$KB_{kl} = \bigcup_{g:\, OB_g \in OB^{kl}} KB_g. \tag{7}$$

It should be stressed that the information resources subject to protection require specific technical or organizational security measures to ensure the acceptable security level.

Values describing utility properties of the security system

In case of loss of the required level of security, it should be possible to activate (using efficient security mechanisms - technical and organizational security measures) several other protection processes or 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 assessment shall be com-

posed of many partial assessments. 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[5] or efficiency[6].

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

1. reduce the number of criteria functions and quality indicators, which constitute grounds for such assessment 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.

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):

1. Sensitivity[7] of the security system to the loss of the required level of security,
2. Time of generation of the security configuration,
3. Efficiency of the operations of the information processing subsystem,
4. Redundancy with respect to the technical security measures,
5. 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,

KB_{dop}^{u} – 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:

$$\Omega = \{\Omega_i, i = \overline{1,5}\}. \tag{8}$$

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 $KB \in KB_{dop}^{u}$ security configuration, recorded shortly $f(KB)$ or

$$\underline{w} =< w_1\ , w_2\ , w_3\ , w_4\ , w_5\ >. \tag{9}$$

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

$$f_i :\ KB_{dop}^{u} \longrightarrow W_i\ , f_i(KB) =\ w_i\ , i = \overline{1,5}. \tag{10}$$

$$\bar{f}: KB_{dop}^{u} \longrightarrow W_1 \times W_2 \times W_3 \times W_4 \times W_5\ ;\ \bar{f}(KB) = \underline{w} \text{ vector function.} \tag{11}$$

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 $W = \overline{f}(KB_{dop}^{u})$ set of permissible $KB \in KB_{dop}^{u}$ 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.

[5] Easy operation and meeting the actual needs of the user.

[6] Verification whether the undertaken activities produced the expected results.

[7] Ability of the security system to react to the change of type and amount of the information subject to further processing under the ISO,

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:

$$Q_m: W \longrightarrow Y_m\ , m = \overline{1, M} \text{ or } Q_m: \overline{f}\left(KB_{dop}^{u}\right) \longrightarrow Y_m\ , m = \overline{1, M} \tag{12}$$

where:

W, $\overline{f}\left(KB_{dop}^{u}\right)$ – the sets of vectors of implementation of values,

M – the number of distinguished criteria functions.

The permissible security configurations may be assessed 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

$$\underline{Q}(KB) = (Q_1(KB), Q_2(KB), Q_3(KB), \dots, Q_M(KB)\ ). \tag{13}$$

In case of $Q_m, m \in \widehat{M}$ 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.:

$$Q_m(KB) \geq\ \hat{y}_m,\ \ m \in \widehat{M} \tag{14}$$

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.

Assessment and measurement of values describing utility properties of the security configuration

The characteristics of the values mentioned in point 1 describing the utility properties of the security configuration may be determined (measured) by choosing one of the following options:

1. Measurements based on actual security systems, with predefined security configuration in simulated conditions of incoming risks and vulnerability of information resources and security measures of technical and organizational nature, or while using the security system in various test or actual conditions;
2. The measurements conducted in the simulated security system, with the predefined security configurations.

The first method applies to already existing and used Information Security Management Systems, whereas the second one - to the designed Information Security Management Systems.

Sensitivity assessment of the system with the predefined security configuration

Sensitivity characteristics of the security system with the predefined security configuration are assessed with respect to the type and number of information resources, subject to further protection (with respect to which it is necessary to maintain the required level of security) after the occurrence of an emergency situation.

The method for assessing sensitivity of the security system with the predefined security configuration to quantitative changes of the types of bits of informations is as follows:

1. When using the $\underline{F} = (F^{OB}, F^{PO}, F^{MB})$ vector function for identifying the emergency situation – loss of the required level of security, for example number "u", the following must be determined:
   a) The set of 2^{OB} information resources under the ISO, with respect to which the security needs to be maintained at a required level, as of the time of the loss of the required level of security,

b) The 2^{PO} set of protection processes, which may be initiated after the occurrence of an emergency situation,
c) The 2^{MB} set of efficient technical and organizational mechanisms.

2. Having determined the OB^u, PO^u, MB^u sets, it is essential to establish the set of permissible security configurations, ensuring the maintenance of the required level of security of the information resources in the OB^u set. The set of permissible security configurations my be presented in the following manner:

$$KB_{dop}^u = \left\{KB_x^u \in 2^{\widehat{OB}^u} \times 2^{PO^u} \times 2^{MB^u} : OB_x^{MAX} \supseteq OB^u, x \in X^u\right\}, \quad (15)$$

where:
$\widehat{OB}^u$ – the set of information resources, with respect to which it is possible to achieve the required level of security, with the predefined O^u and MB^u sets.
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,
X^u – the set of indices of the KB_{dop}^u set.

3. Assuming that the security system with the KB_xth security configuration is:
a) insensitive to emergency situations if $OB_x^{MAX} \equiv OB$
b) sensitive to emergency situation if $OB^u \subset OB_x^{MAX}$,
c) critically sensitive if $OB_x^{MAX} \equiv OB^u$.

Method for measuring the generation time of the system with the predefined security configuration

The generation time of the security system with the predefined security configuration shall be understood as the sum total of the duration time of the initiated protection processes by the decision-making entity, counted from the occurrence of the emergency situation - loss of the required level of security as of the generation time of the security system with an appropriate security configuration. The duration of such actions shall be deemed to mean average time set for the multiple development of the aforesaid configuration for the same emergency situation. Therefore, the setting of the generation values of the security system with the predefined security configuration requires statistical surveys.

Efficiency assessment of the operations of the information processing subsystem with the predefined security configuration

The efficiency of the operations of the information processing subsystem is assessed with respect to the types of protection processes and the number of such types that may be initiated to maintain the required level of security of the information resources.

The method of efficiency assessment of the operations of the information processing subsystem with the predefined security configuration may be as follows:

1. The R_x set of types of the protection processes initiated as part of the KB_xth security configuration is determined for the established PO_x set,
2. The[8] efficiency measure is set for each $r \in R_x$ type. H_r^x.
3. on the basis of the knowledge of the following:
a) vector efficiency measure of the information processing subsystem

$$\underline{H}^x = \left(H_1^x, H_2^x, \dots, H_r^x, \dots, H_{R_x}^x\right) \quad (16)$$

where:
H_r^x – vector coordinates showing expected values of the relative effects of operations of particular protection processes,
R_x – number of the distinguished protection processes initiated in the KB_xth security configuration,

b) vector of statuses of all protection processes initiated in the KB_xth security configuration

[8] The measure is set at the stage of designing the security level by the risk analysis team

$$\underline{K}^x = \left(K_1^x, K_2^x, \dots, K_r^x, \dots, K_{R_x}^x\right) \quad (17)$$

where:
- K_r^x – vector coordinates showing the count of the protection processes initiated in the KB_xth security configuration,
- R_x – number of types of the distinguished protection processes initiated in the KB_xth security configuration,

c) vector of statuses of critical protection processes initiated in the KB_xth security configuration

$$\underline{K}_{KR}^x = \left(K_{KR,1}^x, K_{KR,2}^x, \dots, K_{KR,r}^x, \dots, K_{KR,R_x}^x\right) \quad (18)$$

where:
- $K_{KR,r}^x$ – vector coordinates showing the count of the protection processes of particular types included in the KB_xth security configuration,
- R_x – number of the distinguished types of the protection processes included in the KB_xth security configuration.

The correlations between the K_r^x and $K_{KR,r}^x$ values are determined, where ($K_{KR,r}^x = K_r^x \cdot H_r^x$) means an average number of the protection processes initiated to protect the information resources under the ISO.

4. Assuming that the subsystem for the processing of the information resources, in which the KB_xth security configuration was activated, is:
   a) efficient if $\bigvee_{r \in R_x} K_r^x \geq K_{KR,r}^x$,
   b) inefficient if $\bigvee_{r \in R_x} K_r^x < K_{KR,r}^x$,

Assessment of the existence of security redundancy in the information processing subsystem with the predefined security configuration

The existence of security redundancy in the information processing subsystem shall be assessed with respect to the types and number of such types of security measures that may be initiated in the KB_xth security configuration for the purpose of maintaining the required level of security of the information resources.

The method for assessing the existence of security redundancy in the information processing subsystem may be as follows due to quantitative changes in the security measures:

1. In case of the already established OB_x, PO_x, MB_x sets, it is essential to determine the R_x set of security mechanisms initiated as part the KB_xth security configuration, ensuring safe processing of the information resources from the OB_x set.
2. While using the $\gamma: 2^{PO} \longrightarrow 2^{MB}$ transformation, it is required to determine the MB^u set of technical and organizational resources, necessary to provide the information resources from the set OB^u
3. Assuming that in the ISO of the KB_xth security configuration:
   a) security redundancy exists if $MB_x \supset MB^u$,
   b) security redundancy does not exist if $MB_x \equiv MB^u$.

Assessment of even load of the security configuration with the technical security measures

Even load of the KB_xth security configuration with the technical security measures shall be assessed with respect to the types and number of such types of security measures that may be initiated in the KB_xth security configuration for the purpose of maintaining the required level of security of the information resources.

The method of assessment of even load of the KB_xth security configuration with technical security measures may be as follows:

1. For the already established ZT_x set, the following is determined:
   a) the I_x set of numbers of efficient security measures implemented as part of the KB_xth security configuration and ensuring safe processing of the information resources from the OB_x set,
   b) the J_x set of numbers of the protection processes implemented as part of the KB_xth security configuration and ensuring safe processing of the information resources from the OB_x set,
   c) the B_x set of types of the technical security measures included in the KB_xth security configuration,

d) the $N_x = [n_{ij}]$ matrix, size I × J, whose elements show the number of technical security measures from the j[th] type to the i[th] protection process, initiated under the KB_x[th] security configuration.

2. Assuming that the protection processes included in the KB_x[th] security configuration are:
   a) evenly loaded if

$$\wedge_{<i,k>\in I_x \times I_x}\left(\wedge_{j\in B_x} n_{ij} = n_{kj}\right), i \neq k$$

   b) unevenly loaded if

$$\vee_{<i,k>\in I_x \times I_x}(\vee_{j\in B_x} n_{ij} = n_{kj}), i \neq k\ .$$

Forms of the distinguished criteria functions

In case of the security system, the utility of the security configuration may be assessed 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:

$$Q_1(KB_x) = y_1 = \frac{\overline{\overline{OB}}_x^{MAX} - \overline{\overline{OB}}^u}{\overline{\overline{OB}}}, x \in X; \tag{19}$$

where :

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

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_x[th] 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.

$$Q_2(KB_x) = y_2 = \frac{1}{N_x}\sum_{i=1}^{N_x} t_i^x, x \in X; \tag{20}$$

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 i[th] 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.

$$Q_3(KB_x) = y_3 = \begin{cases} \sum_{r\in R_x}\left(\overline{K}_r^x - K_{KR,r}^x\right), jeżeli\ \wedge_{r\in R_x} \overline{K}_r^x \geq K_{KR,r}^x \\ -1, jeseli\ \vee_{r\in R_x} \overline{K}_r^x < K_{KR,r}^x \end{cases}, x \in X; \tag{21}$$

where:

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

$K_{KR,r}^x$ – the number of the r[th] 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.

$$Q_4(KB_x) = y_1 = \frac{\overline{\overline{OB}}_x^{MAX} - \overline{\overline{OB}}^u}{\overline{\overline{OB}}}, x \in X; \quad (23)$$

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_xth 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.

$$Q_5(KB_x) = y_5 = \begin{cases} \frac{min\left\{\sum_{j\in B_x^i} n_{ji},\ldots,\sum_{j\in B_x^i} n_{jI_x}\right\}}{max\left\{\sum_{j\in B_x^i} n_{ji},\ldots,\sum_{j\in B_x^i} n_{jI_x}\right\}}, jeżeli\ \bigvee_{<i,k>\in I^x\times I^x}\left(\bigwedge_{j\in B_x} n_{ij} \neq n_{kj}\right); \\ 1,\ jeżeli\ \bigwedge_{<i,k>\in I^x\times I^x}\left(\bigwedge_{j\in B_x} n_{ij} = n_{kj}\right) \end{cases} \quad (24)$$

where:

I_x – the set of numbers of technical security measures included in the KB_xth 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_xth security configuration,

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

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

The works on optimization of the security systems have been carried out worldwide for many years. The approach based on the information resource risk and current control of the utility properties of the security configuration is nothing new (STANIK et al., 2016; KIEDROWICZ, STANIK, 2017). The adoption of such rules in the security systems is aimed at protecting the processed information resources in a reasonable manner (the higher risk of losing security attributes, the more advanced protection measures).

The conditions of the information society make it 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 security system with respect to the maintenance of the required security level within the required time limit,
3. high quality and security of the information processing processes - information processes through:
   a) reasonable adoption of steering decisions related to the initiation of appropriate security configurations,
   b) application of scientific methods and good practices while assessing the utility of the security system and choosing the best security configuration.

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. 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.

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.
- while studying the literature on security audits (POLACZEK, 2014; ISO, 2013; ISO 2015).

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)[9].

References

EHRGOTT, M. 2005. *Multicriterial optimization*, 2nd edition, Springer, Berlin.

HOFFMANN, R., KIEDROWICZ, M., STANIK, J. 2016. *Evaluation of information safety as an element of improving the organization's safety management*. 20th International Conference on Circuits, Systems, Communications and Computers (CSCC 2016), MATEC Web of Conferences, vol. 76.

ISO / IEC 27002: 2015. *Technika informatyczna - Techniki bezpieczeństwa - Kodeks postępowania w zakresie kontroli bezpieczeństwa informacji (Information technology - Security techniques - Code of conduct in the field of information security control).*

ISO / IEC 27004: 2013. *Technika informatyczna - Techniki zabezpieczeń - Zarządzanie bezpieczeństwem informacji – pomiary (Information technology - Security techniques - Information security management - measurements)*.

KIEDROWICZ, M. 2018. *Metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych (Methodology of risk management in the security of information resources)*. Collegium of Economic Analysis Annals, 49: 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, vol. 14, p. 174-183.

POLACZEK, T. 2014. *Audyt bezpieczeństwa informacji w praktyce (Information security audit in practice)*, Helion, Warsaw.

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, pp. 321-336.

STANIK, J., KIEDROWICZ, M. 2017. *Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych (Multifaceted methodology of risk analysis and management of business processes)*. Scientific Papers of the University of Szczecin, Economic Problems of Services, 126:p. 339-3354.

[9] The Regulation of the European Parliament and Council (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC (General Data Protection Regulation). http://www.giodo.gov.pl/pl/1520284/9745.