MODEL OF AUTOMATED CONTROL AND MONITORING SYSTEM OF THE CURRENT LEVEL OF INFORMATION SECURITY

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

Jarosław Napiórkowski, M.Sc.
Cybernetics Faculty
Military University of Technology
Warsaw, Poland
e-mail: jaroslaw.napiorkowski@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 for maintaining the required level of information security in an organization. The model of automated control and monitoring system of the current level of information security was proposed. Basic system elements, such as: subject of activities, object of activities and purpose of activities were selected and characterized. Furthermore, the concept of security configuration and subsystem model for controlling the current level of information security in case of an emergency situation were defined. Theoretical considerations were illustrated with examples.

Key words: security configuration, loss of security level, control of security level, security risk

Introduction

The rapid growth of the information security systems in organizations as well as the necessity to provide appropriate guidelines allowing fair and legal data processing[1] observed over the last few years significantly goes ahead present knowledge of principles or methods for obtaining the required level of information security in the organization as well as designing and constructing automated control and monitoring systems of the current information security level. It is also noticeable that there are no formal or commercial models of risk analysis systems and security configuration management aimed at ensuring efficient protection of resources and hence allowing to maintain the required level of security for objects (information resources, also known as data sets) of the information system in the organization (ISO). The difficulties in proposing the formulas for determining the rules, models or principles of controlling the current level of security of the ISO elements are mainly caused by specific properties of the following subsystems:

- subsystem of secure information processing under the ISO,
- subsystem of security configuration properties control,
- subsystem of risk analysis,
- subsystem of divided workstations for persons authorized to process the data which constitute the Processing Subject,
- internal and external environment.

The above-mentioned subsystems are included in the automated control and monitoring system of the current information security level. Currently, the automated control and monitoring system of the current information security level in the organization is based on the approach resulting from business risk, allowing to control present level of security in the organization. Risk mitigation and provision of efficient

[1] 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.

protection means for the resources are the possibilities delivered by the automated control and monitoring system of the current information security level (HOFFMANN at al., 2016; KIEDROWICZ at al., 2018; KIEDROWICZ, 2018). The automated control and monitoring system of the current information security level in terms of control and monitoring of its utility properties is shown in figure 1.

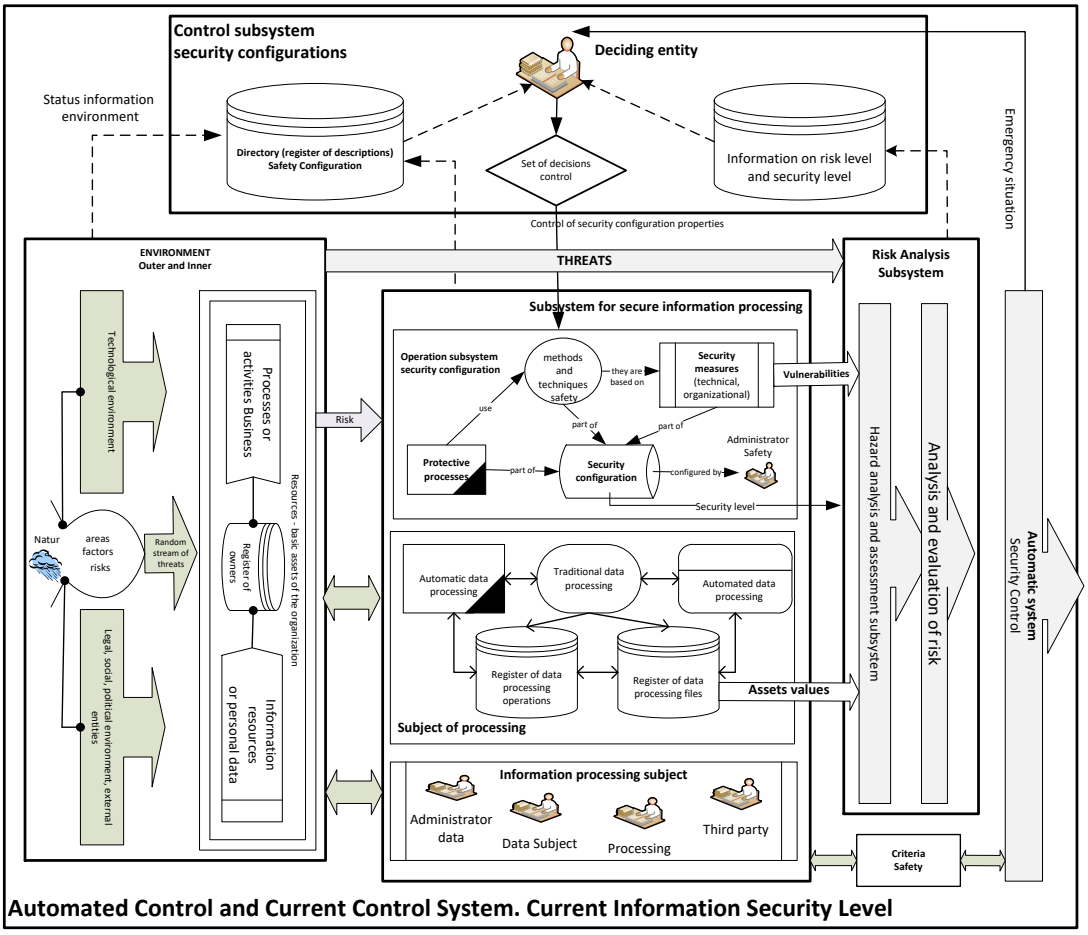

Fig.1. Automated control and monitoring system of the current information security level in terms of control and monitoring of its utility properties.
Source: Own work.

The purpose of this article is to formulate the model of the automated control and monitoring system of the current information security level, use of the risk-based approach and provide grounds for the method of such control of current properties (e.g. functional, reliability, security properties) of the above-mentioned subsystems, which ensures maintenance of the required level of information security in the organization.

The risk-based approach is an important and promising concept, which constitutes the core of the General Data Protection Regulation. According to such principle, the manner of fulfilling the obligations imposed on the administrator or Processing Entity depends on the nature, scope, context and purpose of data processing as well as on the risk of infringement of rights and freedoms of person whom such data concern and the risk of infringement of interests of the administrator/processing entity. The risk-based approach means that the administrators and processing entities are not provided with strictly defined security means and procedures, e.g. access control, encryption, accountability or method for monitoring the processing processes. Instead, the administrators and processing entities are obliged to independently conduct a detailed analysis of the data processing process and assess the risks to which the data processing may be exposed in a given case. The aforesaid approach allows to concentrate on the situations of highest risk, while maintaining the appropriate level of protection when the risk is lower and does not require a whole set of means as provided for in the General Data Protection Regulation.

Pursuant to the risk-based approach, it is necessary to:

1. adapt the means of protection of the processed information resources, including personal data, to the risk scale. They are assessed in terms of the loss of basic security attributes, e.g. confidentiality, integrity and availability of data, while considering their scope, special significance (sensitivity), context and purposes of processing, hence, also the issues related to ensuring the security of the processing services (reliability, integrity and availability of the information processing system) as well as authenticity and accountability of data and processing entities.
2. concentrate on searching for means reducing the probability of occurrence of the most severe risks and means mitigating the effects of such risks.
3. maintain the required level of security of information resources in the organization (STANIK at al., 2016).

The risk-based approach is nothing new. It has been based on the present, almost 40-year old legislative and judicative acquis developed in Europe. Article 17 sec. 1 of Directive 95/46 includes examples of risks, which may occur while processing the information resources and personal data, and requires adoption of such security measures, which shall guarantee appropriate security level adequate to the risks that may occur while data processing and adequate to the character of the protected data.

Basic terms concerning the automated control and monitoring system of the current level of information security

Automated control and monitoring system of the current level of information security

Among many definitions adopted in the theory of system engineering, the following definition seems to best meet the requirements of this article:

"The system refers to a material object with intentionally organized operations, whose components - apart from technical or organizational elements - are also human resources (people) with predefined algorithms of action".

As a result of the above-mentioned definition, the automated control and monitoring system of the current level of information security shall be called:

$$\text{ZSKiSBPBI} =< E, R, DZ > \tag{1}$$

where:

E – a finite set of elements of the $\{e_j; j \in J\}$ system,

R – a finite set of $\{R_i; i \in I\}$ correlations defined in set E,

whereas:

$J = \{1,2,3, \ldots \text{J}\}$ – the set of indices of set E, whereas $I = \{1,2,3, \ldots \text{I}\}$ – the set of indices of set R,

DZ – the purpose of system operations.

The E set describing the system composition meets the $E = \{e_j : \xi(j,q), j \in J, q \in Q^j\}$ requirements. The $\xi(j,q)$ value shall be construed as the following sentence formula:

"The element number $j \in J$ is characterized by feature number $q \in Q^j$, where Q^j is the set of indices of the C^j set of elements number "j".

The set of E elements of the automated control and monitoring system of the current level of information security may decomposed in the following manner:

$$E = E^{PS} \cup E^{PP} \cup E^{AR} \cup E^{OT} \tag{2}$$

where:

E^{PS} – the set of elements of the subsystem for controlling the security configuration properties,

E^{PP} – the set of elements of the subsystem for information processing,

E^{AR} – the set of elements of the subsystem for risk analysis,

E^{OT} – the set of elements that constitute both external and internal environment - i.e. environment of the information processing subsystem.

Among the elements of the subsystem for controlling the security configuration properties, in the E^{AR} risk analysis subsystem and E^{PP} elements of information processing, it is possible to distinguish the following functional components:

$$E^{PS} = E^{PS}_{PD} \cup E^{PS}_{PR} \cup E^{PS}_{OT}$$
$$E^{AR} = E^{AR}_{PD} \cup E^{AR}_{PR} \cup E^{AR}_{OT}$$

$$E^{PP} = E^{PP}_{PD} \cup E^{PP}_{PR} \cup E^{PP}_{OT}$$

where:

E^{PS}_{PD} – the set of elements of the controlling subsystem, which constitute the decision-making subject,
E^{PS}_{PR} – the set of elements of the controlling subsystem, which constitute its subject,
E^{PS}_{OT} – the set of elements of the controlling subsystem, which constitute the environment of its subject and object,
E^{AR}_{PD} – the set of elements of the risk analysis subsystem, which constitute its subject of operations,
E^{AR}_{PR} – the set of elements of the risk analysis subsystem, which constitute its object,
E^{AR}_{OT} – the set of elements of the risk analysis subsystem, which constitute the environment of its subject and object,
E^{PP}_{PD} – the set of elements of the information processing subsystem, which constitute its subject of processing,
E^{PP}_{PR} – the set of elements of the information processing subsystem, which constitute its subject,
E^{PP}_{OT} – the set of elements of the information processing subsystem, which constitute the environment of its subject and object.

Set R of correlations defined in set E may be decomposed in the following manner:

$$R = R^{PS} \cup R^{PP} \cup R^{AR} \cup R^{SP} \quad (3)$$

where:

$R^{PS} \subset E^{PS} \times E^{PS}$ – the set of correlations between elements of the security configuration control subsystem, ensuring specific operation of such subsystem,
$R^{PP} \subset E^{PP} \times E^{PP}$ – the set of correlations between elements of the information processing subsystem, ensuring specific operations of such subsystem,
$R^{AR} \subset E^{AR} \times E^{AR}$ – the set of correlations between elements of the risk analysis subsystem, ensuring specific operations of such subsystem,
$R^{SP} \subset E^{PS} \times E^{PP}$ – the set of correlations between elements of the control system and information processing subsystem,
$R^{SR} \subset E^{PS} \times E^{AR}$ – the set of correlations between elements of the control system and risk analysis subsystem.

The system operations may be defined in the following way for the analyzed category of the system:

1. with respect to the control of the utility properties of the security configuration, as an ordered pair:

$$DZ^{KB} = <\propto^{KB}, Z^{KB}>, \quad (4)$$

where:
$\propto^{KB}$ – the purpose of the control subsystem,
Z^{KB} – the set of tasks (controls) allowing to achieve the $\propto^{KB}$ goal,

2. with respect to the information (information resources) processing subsystem, as an ordered pair:

$$DZ^{pp} = <\propto^{PP}, Z^{PP}>, \quad (5)$$

where:
$\propto^{PP}$ – the purpose of operations of the information processing subsystem,
Z^{PP} – the set of information processing operations allowing to achieve the $\propto^{PP}$ goal,

3. with respect to the risk analysis subsystem, as an ordered pair:

$$DZ^{AR} = <\propto^{AR}, Z^{AR}>, \quad (6)$$

where:
$\propto^{AR}$ – the purpose of operations of the risk analysis subsystem,
Z^{AR} – the set of tasks allowing to achieve the $\propto^{AR}$ goal.

It is assumed that the purpose of operations of the subsystem for controlling the security configuration is to maintain the required level of the information (information resources) security through appropriate adaptation of the means of information protection to the scale of risk of losing the information security attributes. Such goal may be achieved by controlling the utility properties of the information resources in the information processing subsystem. The aforementioned resources refer to technical, organizational or human resources.

It is assumed that the purpose of operations of the risk analysis subsystem is to decrease negative impact of risk on the functioning of the information processing subsystem and undertake appropriate actions aimed at combating and mitigating the risk. It is also assumed that risk identification as well as qualitative and quantitative risk assessment and monitoring constitute part of the Z^{AR} set. The risk analysis comes down to identification of the most vulnerable assets in the organization (places where the probability that any of such risks materializes is relatively high), which allows to determine which assets should be dealt with in the first place and for which assets some security measures (technical, organizational or HR) should be implemented.

It is assumed that the purpose of operations of the information processing subsystem is to manage the processing of the information resources (sets of data) so as to ensure continuity of the security attributes assigned thereto, such as: confidentiality, integrity, availability, non-repudiation or accountability. Such goal may be achieved by mitigating the risk of infringement of rights and freedoms as well as business goals or consent given to process the data. The specificity of the information processing subsystem is the fact that all physical actions are in the form of operations on the information or data, whose source is the environment of such subsystem.

It is assumed that the following shall be included in the Z^{PP} set:

1. collecting, gathering, storing, using, making available, passing and removing according to the needs of the entity. The tasks are implemented in a traditional, automated or automatic manner using IT equipment,
2. information processing tasks in compliance with the adopted technological principles.

Furthermore, it is assumed that:

1. part of the information processing operations may be executed using a computer system, whereas the other part requires approval of the processing entity,
2. part of the information processing operations may be executed automatically by the entity of the information processing subsystem.

Subject, object and purpose of the system operations

In terms of controlling the current level of the information security, the operator shall be an element of the automated system for making steering decisions, e.g. automated security control system or data administrator, hereinafter referred to as the decision-making entity. In such case, the subject shall be the set of such $e_j \in E$ elements, whose desired status may be determined by the decision-making entity. Therefore, the following symbols shall be introduced:
SF – the set of ordered pairs: $sf_p =< O_p , IT_p > \in \Theta \times 2^{IT}$, hereinafter referred to as positions;

where:

- Θ – a group of officers appointed at the stage of designing the system, who shall participate in the information processing process, hereinafter referred to as the processing entity,
- IT – the set of IT devices, which constitute the workplace equipment of the processing entity,
- $\hat{U}$ – the set of permissible steering values, thanks to which the decision-making entity may determine current utility values of the positions of the processing entity,
- V_u – the set of $< p, q > \in \hat{P} \times \hat{Q}$ pairs corresponding to such steering values, where: $\hat{P}$ – the set of numbers of the selected positions of the processing entity, $\hat{Q}$ – the set of numbers of characteristic features of the positions;
- $\hat{S}$ – the vector of the status of special conditions of the position, whose coordinates define the status of particular position.

The s_p status, where $p \in \hat{P}$, for the p^{th} position shall be deemed to mean the vector of characteristics describing in detail the current utility properties:

$$s_p =< a_p^q \in A_p^q : p \in \hat{P}, q \in \hat{Q} > \tag{7}$$

where:

a_p^q – coordinates of the vector of status of the pth position, expressing individual features,
A_p^q – the set of permissible implementation of the qth feature of the pth position.

The impact of such control on the position and hence their characteristics may be noted in the following manner:

$$\Lambda_{<p,q>\in \hat{P}\times\hat{Q}}\ a_p^q = a_p^q[u(t)], u \in U, \tag{8}$$

As a result, the set of controlled positions may be defined as follows:

$$\widehat{SF} = \{sf_p \in \text{SF} : \vee_{q\in\hat{Q}}[< p, q >\in V_u\ ], p \in \hat{P}\}.$$

The $\propto^{SP}$ goal of the operations of the information processing subsystem is determined in the set of the controlled positions.

In terms of the information processing process, the processing entity in the automated control and monitoring system of the current level of information security shall be the $\widehat{SF}$ set of positions, whereas the subject of operations shall be the set of such $e_j \in E^O$ elements, where the purpose of operations of the information processing subsystem is determined. Some bites of information (information resources) collected or processed by the information processing subsystem may be elements of the E^O set. Such bites of information define actual information objects in the organization (e.g. data of natural persons, descriptions of basic assets in the organizations, descriptions of supporting assets, etc.). They are formed by the information processing subsystem according to certain rules and are subject to further processing. Each bite of information, hereinafter referred to as the information object (information resource) is marked with p ∈ P^O number and described by the set of C_p^O feature names.

If all different sets of C_p^O features used to describe individual information resources are numbered with $b = \overline{1, B}$ variable (to be called the type of the information resource or object), then, two objects shall be of the same type (e.g. "b") when described by identical sets of features. The sets of Q_p^O numbers of features describing the $p \in P^O$ object and the sets of C_p^O feature names corresponding thereto may not be empty for each $p \in P^O$, where P^O is the set of numbers of the selected information resources. It is assumed that for each $q \in Q^O$ feature, the A_q^O set of possible implementation of the a_q feature shall be defined.

Therefore, the following symbols shall be introduced:

D – the set of steering decisions, hereinafter referred to as orders, used by the Processing Entity (officers) from its positions to initiate the data processing operations and hence influence the current properties of the information resources (also including the properties of the security attributes assigned thereto);

V_D – the set of $< p, q >\in P^Z \times Q^Z$ pairs corresponding to such steering values,
where:
P^Z – the set of numbers of the selected information resources,
Q^Z – the set of numbers of the selected features of the information resources,

$\underline{a}(t)$ – the vector of status of the selected information resources, whose coordinates determine the processing statuses of particular objects at moment t, also including in terms of security (e.g. loss or continuity of confidentiality, integrity, non-repudiation, availability and accountability).

The $a^p(t)$ status, $p \in P^O$ of the pth object shall be deemed to mean the vector of features describing in detail its current quality - properties related to utility, security, reliability, etc.:

$$a^p(t) =< a_q^p(t) \in \ddot{A}_p^q : p \in P^Z, q \in Q^Z > \tag{9}$$

where:
$a_q^p(t)$ – coordinates of the vector of status of the pth object, expressing individual features,
$\ddot{A}_p^q$ – the set of permissible implementation of the qth feature of the pth object,
Q^Z – the set of numbers of the selected features of the object.

The impact of decisions made by the processing entity on the current security status, at moment t, may be noted in the following manner:

$$\Lambda_{<p,q>\in P^Z\times Q^Z}\ a_p^q\ (t) = a_p^q[d(t)],\ d \in D. \tag{10}$$

As a result, the set of resources, whose current status (and hence current level of security) may be determined by officers, may be defined as follows:

$$OB = ZI = \{zi_p \in E^O : \bigvee_{q \in Q^z} [< p, q > \in V_D],\ p \in P^Z\}. \quad (11)$$

In terms of possibilities of controlling current properties of the automated control and monitoring system of the current level of information security and processing information therein, each position may be described in the following extended manner:

$$\widehat{sf_p} =< nz_p, ROP_p, RZI_p, \acute{S}B_p, ZL_p > \quad (12)$$

where:

nz_p – the name of an activated human resource of the pth position (e.g. code of the information processing entity),

ROP_p – the set (register) of the information processing operations assigned to the pth position (a list of processing operations that may be performed at the pth position),

RZI_p – the set (register) of the data sets assigned to the pth position (a list of information resources owned by the person from the pth position),

$\acute{S}B_p$ – the set of security measures of technical and organizational nature, which may be activates in the information processing system from the pth position,

ZL_p – the set of steering decisions (orders) assigned to the pth position, used by the processing entity to initiate processing from the ROP_p set.

The goal of operations of the automated control and monitoring system in terms of its purpose is considered equivalent of the goal of the information processing subsystem. It may be defined by specifying the desired security statuses of the established group of information resources.

Therefore, the following symbols shall be introduced:

$\dot{P}(t)$ – the set of numbers of the information resources collected in the information processing subsystem by moment t, which require further safe processing,

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

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

t_0^p, – the time of collecting (registering) the pth object in the information processing subsystem,

$\dot{T}^p$ – the time of deregistering (removing) the pth object in the information processing subsystem,

$Q^{PPI}(w)$ – the set of numbers of the information object features, where the $w \in \dot{W}_p$ property is defined.

To determine whether the information resource number $p \in \dot{P}(t)$ has the "w" property, it is necessary to define the $\propto_p^q (w) \subset \dot{A}_p^q$ subsets of implemented features, for each $q \in Q^{PPI}(w)$ feature. If the implementation of the $a_q^p(t)$ features of the pth object at the time $t \in [\dot{t}_0^p, \dot{T}^p]$ belongs to such $\propto_p^q (w)$ subsets, it is possible to state that the object number $p \in \dot{P}(t)$ has the "w" property.

When assuming obviousness of the sets of the $\dot{Q}_P$ features, on whose values the $\propto_p^q (w) \equiv \dot{\propto}_p^q,\ q \in \dot{Q}_P$ subsets are determined, for each $p \in P^{PPI}$ object, the purpose of the automated control and monitoring system may be defined in the following manner:

$$\propto^{ZSKiSBPBI} \equiv \propto^{PPI} \{\dot{\propto}_p^q : < p, q > \in V_D\ , p \in \dot{P}(t), q \in Q^{PPI}\}. \quad (13)$$

In terms of a possibility of achieving the goal of the automated control and monitoring system, every $z_p \in \dot{P}(t)$ information resource, processed under the information processing subsystem, may be described in the following manner:

$$z_p =< b_p, O_p^b, w_p^b, Q\ (w_p^b), \dot{\propto}\ (w_p^b), R_p^b > \quad (14)$$

where:

b_p – the type of the pth information resource,

O_p^b – the officer being the owner of the pth information resource of b type,

w_p^b, – the property (security level) of the pth information resource of b type,
$Q\left(\dot{w}_p^b\right)$ – the set of numbers of properties, where the $\propto_p^q \left(w_p^b\right)$ subsets are defined,
$\dot{\propto}\left(w_p^b\right)$ – the set of the desired security statuses of the pth object of b type,
R_p^b – the set of correlations between b_p and $\dot{\propto}\left(w_p^b\right)$.

System model for controlling the current level of information security

An ordered five was adopted as the system model for controlling the current level of information security:

$$< SF, U, KB, FR, Q >, \tag{15}$$

where:
SF – the set of positions of persons processing the data,
U – the set of numbers of the types of emergency situations (the set of numbers of the lost security levels under the ISO), selected on the basis of the analysis of effects that such emergency situations may cause,
KB – the family of permissible security configurations,
FR – the general reconfiguration function,
Q – the general reconfiguration function.

Any failure shall be deemed to mean an event that occurred at time t_i due to the difference between the desired property of the security configuration and its current security configuration. It is in line with the following condition:

$$KB^{WY}(t_i) \supset KB^{MO}(t_i), \tag{16}$$

where:
$KB^{WY}(t_i) = \bigcup_{i:\, z_i \in OB^{WY}(t_i)} KB_g$ – the desired security configuration, which needs to be initiated to ensure the required level of security of the n information resources, which belong to the $z_i \in OB^{WY}(t_i)$ set; it may be analyzed as a multitude of security configurations for the $z_i \in OB^{WY}(t_i)$ information resources, whereas: $KB_g = \langle z_g, O_g, MB_g \rangle$,
where:
z_g– the information resource protected by the gth security configuration,
O_g – the subset of human resources, which may be used to ensure the maintenance of the security attributes assigned to the z_g information resources,
MB_g– the set of security mechanisms creating the gth security configuration,
$\mathrm{KB^{MO}(t_i)} = \bigcup_{\mathrm{i:\, z_i \in OB^{MO}(t_i)}} \mathrm{KB_g}$. – the security configuration, which may be constructed at time $\mathrm{t_i}$, based on technical or organizational security mechanism in currently proper condition;
$OB^{WY}(t_i)$ – the set of information resources, with respect to which, as of time t_i, the required security level may not be maintained,
$OB^{MO}(t_i) \in \Theta\mathrm{B}(t)$ – the set of information resources, with respect to which, as of time t_i, it is possible to maintain the required level of security, based on the currently initiated security configurations; i.e. if at time t_i it is necessary to protect the information resource newly introduced to the ISO, the current required level of security is lost,
$\Theta\mathrm{B}(t)$ – the set of sets which may be created on the OB(t) set.

The following notation of any security configuration shall be introduced:

$$KB_{kl} = \langle OB^{kl}, O^k, MB^l \rangle \tag{17}$$

where:
OB^{kl} – the set of information resources of the information system in the organization subject to protection by the klth security configuration,
O^k – the set of officers responsible for ensuring security of the information resources, which belong to the OB^{kl} set,
MB^l – the set of security mechanisms of technical or organizational nature, which created the klth security configuration.

The knowledge of the KB_{kl} security configurations makes it possible to assign to each OB^{kl}, set, with the predefined MB^{l}, the O^{k} set of security mechanism (organizational and technical security measures) corresponding thereto. The KB_{kl} security configuration may be implemented only when it is possible to assign such *zbiór* O^{k}, to the OB^{kl} set, with the predefined elements of the MB^{l} set, ensuring the maintenance of the required level of security of the set of OB^{kl} information resources.

Therefore, it may be stated that as a consequence of the above, the OB^{kl} set, with the predefined MB^{l} set, remains in correlations with the OB^{kl} set, i.e. $OB^{kl}\ KB_{kl}\ O^{k}$. Therefore, it is possible to analyze the security configuration (17) as an analogous to the terminal system, based on which the information resources from the set OB^{kl} constitutes the input data, whereas the elements of the set O^{k} - the output data.

Space for potential emergency situations creates creates the Cartesian product $A = 2^{OB} \times 2^{O} \times 2^{MB}$. The $a_{nms} =< OB_n, O_m, MB_s >\in A$ element determines the type of an emergency situation. Let us assume that for each type of the emergency situation, there is function value $\chi(nms) = u$ defining the number of the emergency situation.

It is assumed that the decision-making entity is equipped with visualization subsystem, security control subsystem and control and diagnostic complex, which may identify all type of emergency situations (loss of security). The $a \in A$ type emergency situation, number u $\in U$ shall be deemed to mean OB_n, O_m, MB_s sets that remain after the emergency situation number u $\in U$ occurs.

The set of the permissible security configurations, upon the loss of security, shall be defined on the basis of the knowledge of:

OB^{p} – a set of information resources, with respect to which the required security level shall be maintained,

O^{p} – a group of human resources (officers) available after the occurrence of the emergency situation, number u $\in U$,

$MB^{p} \in$ MP – a set of implementable security configurations on the basis of sets of efficient technical or organizational security measures, which remain after the loss of security event, number u $\in U$,

according to the following formula:

$$KB_{dop}^{u} = \begin{cases} \{KB_{kl} = \langle OB^{kl}, O^{k}, MB^{l} \rangle \in \Theta B_p \times \Theta_p \times MP_p : \\ OB^{kl} \supset OB^{p}\},\ jeżeli\ \bigvee_{\langle k,l \rangle \in K^{u} \times L^{u}} (OB^{kl} \supseteq OB^{p}). \\ \Phi\ \ w\ przeciwnych\ przypadkach - zbiór\ pusty. \end{cases} \tag{18}$$

The above means that the KB_{dop}^{u} set of permissible security configurations, shall include - upon loss of the required level of security of the information resources under the ISO - all security configurations, constructed for different variants of human resources as well as the set of technical or organizational security measures, which remain after the occurrence of the emergency situation, ensuring the required level of security with respect to the current set of the $OB\ (t) \in \Theta B(t)$ information resource. Each security configuration from the set KB_{dop}^{u} guarantees maintenance of the acceptable security level of the information resources from the set OB^{kl}.

The representation of radio waves is determined at the stage of designing the control system for the current level of security or at the stage of determining the security system to ensure accomplishment of the desired purpose of activities of the processing entity and the information processing subsystem during their exploration, despite the occurrence of the emergency situation. After the occurrence of the emergency situation – loss of the required level of security, it is essential to generate permissible or optimum security configuration to be able to efficiently continue the process of safe information processing under the ISO (KIEDROWICZ, 2017; KIEDROWICZ, STANIK, 2017). 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.

Model of subsystem for controlling the level of security of the information resources – example

Formal description

The automated control and monitoring system of the current level of information security in a hypothetical organization is the subject of the considerations herein. The officer performing the duties of IOD[2]

[2] IOD – Inspector for the Protection of Personal Data, i.e. former ABI. ABI – Information Security Administrator, i.e. ABI, a natural person appointed by the personal data administrator (ADO), responsible for ensuring compliance with the regulations on personal data protection.

or ASI[3] shall be also responsible for controlling the level of security. The position of such officer shall be equipped with the following technical or organizational resources:

- data visualization means describing the current level of security of the informations resources processed under the ISO, e.g. the system of automated security control ISO,
- IT means used by the IOD to assign work (steering decisions, instructions, etc.) to determine the current levels of security of the information resources by initiating appropriate security configurations from the set of permissible configurations determined at the stage of design.

The set of permissible steering decision (orders) has the following form:

$$ZL = \{zl_i; i = \overline{1,7}\}.$$

Particular elements of the ZL set shall be interpreted in the following manner:
zl_1 – initiate the set of security measures with the security configuration defined in the register of structures of the security system on the i th position (e.g. defined in the 5th row of such register),
zl_2 – activate the indicated technical or organizational security measure in the security system (with current security configuration),
zl_3 – switch on/off the indicated technical or organizational security measure (with current security configuration) in the security system,
zl_4 – establish the indicated job (with current security structure) in the security service,
zl_5 – cancel the indicated job (with current security structure) from the security service,
zl_6 – assign the indicated protection process to the specific position,
zl_7 – remove the indicated protection process from the specific position.

From the point of view of management of the security of information resources, the subject of activities shall be the *PO* set of protection processes managed by officers from the *O* set, assigned to the *SF* set of controllable positions, established under the current security structure of the organization. The set of $\tilde{P}$ numbers of the managed protection processes and $\tilde{Q}$ numbers of the distinguished features of such process have the following format:

$$\tilde{P} = \{1,2,3,4,5,6,7,8,9\},$$
$$\tilde{Q} = \{1,2,3,4,5\}.$$

Particular elements of the $\tilde{Q}$ set shall be interpreted in the following manner:
1 - security measure initiated as part of the current security configuration,
2 - security measure not initiated as part of the current security configuration,
3 - security configuration having all protection methods and techniques (implemented) of technical or organizational nature, established at the stage of design,
4 - security configuration having a sufficient number of security measures ensuring proper functioning of the set,
5 - security configuration not having a sufficient number of security measures ensuring proper functioning of the set.

The subjects of activities are bites of information gathered or processed under the ISO. The set of information bites - information resources is determined on the basis of the $OB = ZI = \{zi_p \in E^{SIO} : \bigvee_{q \in Q^{SIO}} [< p, q > \in V_D],\ p \in P^{SIO}\}$ correlation.

According to this definition, the sets of P^{SIO} numbers of the distinguished objects and Q^{SIO} numbers of the distinguished features of such information resources have the following format:

$$P^{SIO} = \{1,2, \ldots . 20\}, \quad Q^{SIO} = \{1,2, \ldots . 8\}$$

Particular elements from the Q^{SIO} set shall be interpreted in the following manner: 1- identification number of the object, 2 - name, 3 - set of assigned security attributes, 4 - value of the required level of security in terms of the assigned security attributes, 5 - valuation of the resource in terms of potential damages that the organization may incur due to the loss of the assigned security attributes or required level of security, 6 - set of current vulnerability factors, 7 - current vulnerability value in the context of the set of current vulnerability, 8 - set of currently assigned technical security measures, 9 - set of currently assigned organizational security measures, 10 - value of residual risk, 11 - confidentiality clause.

[3] Information system administrator (ASI). A person responsible for the safety of data processing in the information systems. The ASI function is more determined by the practical experience than by the provisions of law.

Each object number $p \in P^{SIO}$ shall be defined by the following correlation in accordance with deliberations herein.

$$OB = Z =< b_p, O_p^b\ w_p^b, Q\ (w_p^b), \dot{\propto}\ (w_p^b), R_p^b >$$

According to the definition, the $B, W, \dot{Q}^b, \dot{\propto}^b, R^b, b \in B$ sets have the following form:

A. The set of the type $B = \{1,2,3\}$ objects, where the elements are interpreted in the following manner: 1- personal data, 2 - confidential data, 3 - sensitive data.
B. The set of W= $\{1,2\}$ security properties, where the elements are interpreted in the following manner: 1 - resource maintained security attributes, 2 - resource lost basic security attributes.
C. $\dot{Q}^b\ ;\ b = \overline{1,3}$ sets,
   a. $\dot{Q}^1 = \{1,2,4,8.9.10\}$
   b. $\dot{Q}^2 = \{1,2,3,4,5,6,7,8,9,10,11\}$,
   c. $\dot{Q}^3 = \{1,2,3,4,5,8,9,10\}$,
D. $\dot{\propto}^b\ ;\ b = \overline{1,3}$ sets,
   a. $\dot{\propto}^1 = \{1,2,3,4\}$
   b. $\dot{\propto}^2 = \{3,4,5\}$,
   c. $\dot{\propto}^3 = \{4,5\}$,
   Elements of the $\dot{\propto}^b$ sets shall be interpreted in the following manner: 1 - basic level of security, 2 - medium level of security, 3 - high level of security, 4 - acceptable risk, 5 - tolerable risk.
E. $R^b;\ b = \overline{1,3}$ sets,
   $R^1 = Z^1 \times \dot{\propto}^1 = \{< z_1^1, 1 >, < z_2^1, 2 >, < z_3^1, 3 >< z_4^1, 4 >\}$
   $R^2 = Z^2 \times \dot{\propto}^2 = \{< z_1^2, 3 >, < z_2^2, 4 >, < z_3^2, 5 >\}$
   $R^3 = Z^3 \times \dot{\propto}^3 = \{< z_1^3, 4 >, < z_2^3, 5 >\}$

The elements of the $Z^b;\ b = \overline{1,3}$ sets are activities (tasks) performed in stages, which the subject of activities ($o_p \in O_p^b$ officer) should perform to allow the object (information resource) type $b \in B$ form the $\dot{\propto}^b$ set achieve the desired state.

Individual tasks from $\{Z^b;\ b = \overline{1,3}\}$ set performed in stages are described in the following manner:

$z_1 \equiv z_1^1 =< DMB_1, \{PR_1, PR_2\} >,$
$z_2 \equiv z_2^1 =< DMB_2, \{PR_1, PR_3, PR_5, PR_8\} >,$
$z_3 \equiv z_3^1 =< DMB_3, \{PR_1, PR_2, PR_6, PR_7\} >,$
……
$z_8 \equiv z_1^3 =< DMB_8, \{PR_1, PR_2, PR_4, PR_5, PR_6, PR_7, PR_{10}, PR_{11}\} >,$
$z_9 \equiv z_2^3 =< DMB_9, \{PR_1, PR_2, PR_3, PR_4, PR_6, PR_9\} >.$

The purpose of activities of the processing entity is the form of

$$\propto^{SB} = \{\dot{\propto}_p^q \subset \dot{\propto}^b, b = \overline{1,3}\}.$$

Particular elements from the $\dot{\propto}^b$ set shall be interpreted in the following manner: $\dot{\propto}^1 = \{1,2,3,4\}$; $\dot{\propto}^2 = \{3,4,5\}$, $\dot{\propto}^3 = \{4,5\}$. Let us assume that the acceptable time frame, during which the $p \in P^{SIO}(t)$ object (information resources) should reach the desired state may not exceed 3 days.

Control of the current level of security

Let us assume that the system described in chapter 1 operates for a longer period of time $[t_0, t]$, where t_0 – moment of starting the information processing process under the ISO, t - current time. While using the ISO, both desired (required) and current utility and security properties are subject to change in terms of the subject of processing and ISO. Let us assume that at $t_i = t$ moment, the system of automated security control or processing entity detected an emergency situation. It is in line with the following condition: $KB^{WY}(t_i) \supset KB^{MO}$.

To provide the required level of security of the information resources from the $OB^{WY}(t_i)$ set, the Inspector for the Protection of Personal Data shall initiate the zl_1 order, which generates and implements the new security configuration, ensuring maintenance of the required level of security. The order initiating the new security configuration in the security system may be as follows: RTO n,
where:

- RTO of security measures - code of the order initiating implementation of an appropriate set of technical and organizational security measures,
- n - number of the row in the register of permissible security configurations, corresponding to the number of the emergency situation.

The number of the emergency situation is defined by an officer or automatically by the automated security control system based on the knowledge of:

- the set of information resources with respect to which it is required to ensure appropriate levels of security,
- the set of currently efficient or useful security mechanisms of technical, organizational and personnel nature,
- the set of officers at the disposal of the security services of the organization.

Let us assume that emergency situation number n=5 occurred. In case of this situation (number 5), the OB^5, SF^5, MB^5 sets are the following:

$$OB^5 = \{zi_2, zi_5, zi_6, zi_7, zi_8, zi_{11}\},$$
$$SF^5 = \{sf_1, sf_2, sf_3\},$$
$$MB^5 = \{mb_1, mb_2, mb_3, mb_5, mb_7, mb_8, mb_{10}, mb_{12}, mb_{13}\}.$$

Summary

Fast-paced technological progress and globalization brought new challenges in the fields of information security and personal data protection. The scope of collection and exchange of the information resources significantly increased. Thanks to the technology, both private companies and public bodies may use in its activities the information resources, in particular personal data, on an unprecedented scale.

Risk mitigation and provision of efficient protection means for the resources are the possibilities delivered by the automated control and monitoring system of the current information security level. The automated control and monitoring systems of the current information security level, which apart from:

- irregularities caused by failure of hardware,
- irregularities or new vulnerability of protection means,
- new risks,
- lost secure processing of some information resources,

changes in the work conditions due to the real-time changes in demand for the scope of services offered by the system. In such systems, a number of mechanisms preventing the effects of emergency situation, for example developed systems of automated control of the level of security, systems of automated control of suitability, hardware and software mechanisms for failure tolerance, risk analysis systems, mechanisms for security system reconfiguration, systems for controlling current utility properties, etc. were introduced. The resources of the above-mentioned systems are used, to a varying degree, to implement particular tasks of the information processing, whereas any changes in their use are determined by different emergency situations.

For many years now, the works on standardization and optimization of the automated control and monitoring systems of the current information security level have been carried out. According to the conditions of the information society, it is necessary for each security system to have the following properties:

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

The article does not offer the recipe for the design and construction of the efficient automated control and monitoring systems of the current information security level. It is merely a proposal of the authors for partial solution of the problem related to the determination and construction of the system, which would allow present control of the security level of the information system in the organization. The proposed approach to the issue of security, aimed at the reconfiguration process, results, among other things, from the observations and long-term experience of the authors gained:

- during observations of the construction and implementation of such 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 information security.

References

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., STANIK, J., NAPIÓRKOWSKI, J. 2018. *Standardy bezpieczeństwa w cyklu życia systemu zabezpieczeń systemu informacyjnego organizacji. (Safety standards in the life cycle of the organization's information system security system)*. Collegium of Economic Analysis Annals, Publisher: Warsaw School of Economics (SGH) Collegium of Economic Analysis, vol 49, p. 347-369.

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.

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, 123: 321-336.

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).

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)*.

http://www.zut.edu.pl/fileadmin/pliki/abi/9/RYZYKO_ODO-1.pdf (access 21.03.2018).

http://www.zut.edu.pl/fileadmin/pliki/abi/9/RYZYKO_ODO-2.pdf (access 21.03.2018).