Symulacja w Badaniach i Rozwoju
Vol. 7, No. 1-2/2016

Jerzy STANIK, Maciej KIEDROWICZ
Wojskowa Akademia Techniczna, Wydział Cybernetyki,
Instytut Systemów Informatycznych
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
E-mail: jerzy.stanik@wat.edu.pl, maciej.kiedrowicz@wat.edu.pl

Model służby bezpieczeństwa dla potrzeb utrzymywania wymaganego poziomu bezpieczeństwa informacji w organizacji

1 Wstęp

Obserwowany w ostatnich latach szybki rozwój systemów bezpieczeństwa organizacji oraz konieczność zagwarantowania wytycznych, umożliwiających uczciwe i zgodne z prawem przetwarzanie danych, wyprzedza w znacznym stopniu wiedzę na temat metod utrzymywania wymaganego poziomu bezpieczeństwa informacyjnego organizacji oraz projektowania i budowy systemów automatycznej kontroli bezpieczeństwa (SAKB). Daje się również zauważyć brak formalnych i komercyjnych modeli lub opisów służb bezpieczeństwa, mających na celu utrzymanie wymaganego poziomu bezpieczeństwa obiektom systemu informacyjnego organizacji (SIO). Trudności zaproponowania receptur określania reguł, modeli lub zasad sterowania bieżącym poziomem bezpieczeństwa elementom SIO przez służbę bezpieczeństwa, przede wszystkim wynikają ze specyficznych właściwości takich podsystemów jak:

- podsystem bezpiecznego przetwarzania informacji w SIO,
- podsystem zabezpieczeń, rozumiany jako element systemu zarządzania bezpieczeństwem informacji,
- podsystem wydzielonych stanowisk pracy osób funkcyjnych, tworzących strukturę służby bezpieczeństwa.

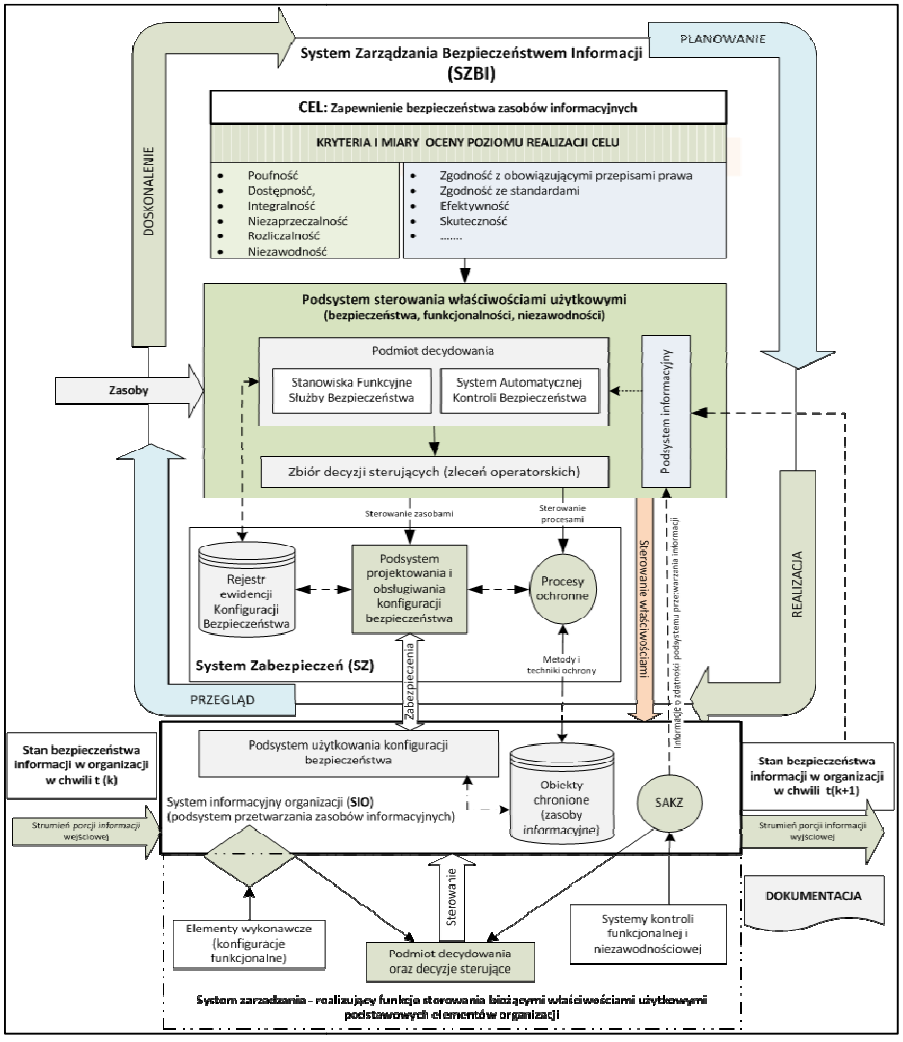
Wyżej wymienione podsystemy wchodzą w skład SZBI[1] i dziś stanowią podstawowe elementy umożliwiające sterowanie bieżącym poziomem bezpieczeństwa organizacji. Ilustrację graficzną organizacji z punktu widzenia sterowania jej bieżącymi właściwościami użytkowymi przedstawiono na rysunku 1.

Celem niniejszego artykułu jest sformułowania modelu służby bezpieczeństwa i uzasadnienie metody takiego sterowania bieżącymi właściwościami (np.: użytkowymi, funkcjonalnymi, niezawodnościowymi, bezpieczeństwa) wyżej wymienionych podsystemów, które zapewnia utrzymanie wymaganego poziomu bezpieczeństwa informacji w organizacji.

Zdaniem autorów wymagany poziom bezpieczeństwa informacji w organizacji można osiągnąć poprzez podejmowanie właściwych decyzji sterujących, które uaktywniają odpowiednie zbiory procesów ochronnych, przyczyniających się do podniesienia

[1] System Zarządzania Bezpieczeństwem Informacji - ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji

bieżącego poziomu bezpieczeństwa ochranianym. Procesy ochronne wykorzystują odpowiednie metody i techniki ochronne (zabezpieczenia) o charakterze technicznym i organizacyjnym. Relacje zachodzące między uaktywnionymi zabezpieczeniami tworzą odpowiednie konfiguracje bezpieczeństwa. Odpowiednie sterowanie właściwościami użytkowymi tych konfiguracji bezpieczeństwa pozwala utrzymywać wymagany poziom bezpieczeństwa informacji w organizacji.



Rys. 1. Ilustracja organizacji z punktu widzenia sterowania jej bieżącymi właściwościami bezpieczeństwa

Fig. 1. Illustration of the organization from the point of view of controlling its current security properties

Możliwość podejmowania decyzji sterujących warunkuje istnienie, w ramach SZBI organizacji, podsystemu sterowania właściwościami bezpieczeństwa systemu informacyjnego organizacji (SIO). Pojmując w ten sposób istotę bieżącego sterowania bezpieczeństwem informacji, w dalszych rozważaniach przyjmuje się, że ma ono dla SIO znaczenie podstawowe i bez jego spełnienia nie można mówić o skutecznym działaniu służb bezpieczeństwa.

Zakładamy, że celem działania służb bezpieczeństwa jest nadawanie obiektom przetwarzanych w ramach SIO (np.: procesom biznesowym, procesom przetwarzania informacji, ustalonym porcjom informacji - zasobom informacyjnym) w przedziale czasu $\Delta\dot{T}_p$, pożądanych stanów $\dot{\alpha_p}$, nie tylko w aspekcie funkcjonalnym, ale również z punktu widzenia bezpieczeństwa.

Przy określeniu bieżącego poziomu bezpieczeństwa informacji, akcentuje się trzy istotne zagadnienia, charakterystyczne dla konstrukcji artykułu:

- w bieżących chwilach czasu muszą istnieć możliwości bezpiecznego przetwarzania wymaganego zbioru zasobów informacyjnych,
- w stosunku do kluczowych wymaga się procesów biznesowych oraz wrażliwych zasobów informacyjnych[2] których wymaga się istnienia procesów ochronnych, które zapewniają utrzymanie odpowiednich atrybutów bezpieczeństwa[3] na akceptowalnym poziomie ryzyka[4],
- do utrzymania wymaganych atrybutów bezpieczeństwa, w stosunku do wybranej grupy zasobów SIO służby bezpieczeństwa ustanawiają, wdrażają i utrzymują ściśle określone konfiguracje bezpieczeństwa, zapewniające tym zasobom wymagany poziomu bezpieczeństwa lub akceptowalną wartość ryzyka.

W świetle powyższego bieżący poziom bezpieczeństwa zasobów SIO rozumiany jest, jako możliwość uaktywnienia w systemie informacyjnym organizacji właściwego zbioru zabezpieczeń. Relacje zachodzące pomiędzy tymi zabezpieczeniami tworzą zbiór dopuszczalnych konfiguracji bezpieczeństwa, skonstruowanych na bazie zbioru aktualnie sprawnych zabezpieczeń o charakterze technicznym lub organizacyjnym, będących w dyspozycji zespołu obsługiwania systemu zabezpieczeń.

2 Model służby bezpieczeństwa

Spośród wielu definicji w teorii bezpieczeństwa informacji następująca definicja (Stanik, 2017) najbardziej odpowiada wymogom niniejszego artykułu:

> „Służba bezpieczeństwa ta część całościowego systemu zarządzania bezpieczeństwem informacji o celowo zorientowanym działaniu, odnosząca się do projektowania, monitorowania i utrzymywania pożądanego zbioru

[2] Wrażliwy zasób informacyjny – każdy aktyw organizacji, utrata którego powoduje istotne szkody dla organizacji.

[3] Atrybut bezpieczeństwa informacji – tutaj: poufność, niezapzrzeczalnośc, dostępność, integralność, rozliczalnośc, niezawodność.

[4] Ryzyko akceptowalne – wielkość ryzyka, którą organizacja może zaakceptować bez żadnych dodatkowych działań zaradczych bądź zmian w funkcjonowaniu.

zabezpieczeń o charakterze technicznym i organizacyjnym, w oparciu o który można wygenerować pożądaną konfiguracje bezpieczeństwa".

Służba bezpieczeństwa zawiera strukturę organizacyjną, planowane działania, zakresy odpowiedzialności i narzędzia pracy umożliwiające sterowanie bieżącym poziomem bezpieczeństwa całej organizacji, jaki i jej elementami.

W następstwie powyższej definicji jako model służby bezpieczeństwa przyjmujemy uporządkowaną czwórkę:

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

gdzie:

PSF – podmiot działania, którym jest zbiór osób funkcyjnych wchodzących w skład służby bezpieczeństwa organizacji,

PDZ – przedmiot działania, którym są obiekty SIO, w stosunku do których należy utrzymywać wymagany poziom bezpieczeństwa,

$\mathbb{C}$ – cel działania służby bezpieczeństwa określony na przedmiocie działania,

NP – zbiór narzędzi pracy stanowiących wyposażenie stanowisk pracy podmiotu działania.

Wyżej wymienione elementy są przedmiotem rozważań w kolejnych podrozdziałach niniejszego artykułu.

2.1. Podmiot działania

Z punktu widzenia sterowania bieżącym poziomem bezpieczeństwa informacji, podmiotem działania może być:

- element automatycznego wypracowania decyzji sterujących, np. system automatycznej kontroli bezpieczeństwa (SAKB),
- zbiór osób funkcyjnych[5], powołanych w ramach struktury służby bezpieczeństwa lub SZBI danej organizacji, zwanych dalej podmiotem decydowania.

Wprowadźmy następujące oznaczenia:

SF – zbiór uporządkowanych czwórek: $sf_p =< O_p, P_p, PO_p, MB_p > \in \Theta \times 2^P \times 2^{PO} \times 2^{MB}$, zwanych dalej stanowiskami pracy; uwzględniając zbiór relacji $\{R_i; i \in I\}$ określonych na zbiorze SF, możemy wyróżnić różne struktury funkcjonalne służby bezpieczeństwa organizacji, gdzie:

Θ – zbiór osób funkcyjnych możliwych do powołania w ramach struktury służby bezpieczeństwa; zbiór tych osób jest ustalony na etapie projektowania SZBI,

P – zbiór obiektów SIO, których właścicielami są osoby funkcyjne, i w stosunku do których powinny one utrzymywać wymagany poziom bezpieczeństwa,

PO – zbiór procesów ochronnych wykorzystujących odpowiednie metody i techniki ochronne o charakterze technicznym lub organizacyjnym, których

[5] np.: ADO – administrator danych osobowych, ABI – administrator bezpieczeństwa informacji, ASI – administrator systemu informatycznego, itp.,

właścicielami są osoby funkcyjne wyróżnionych stanowisk pracy; procesy ochronne wspierają procesy przetwarzania informacji SIO w zakresie bezpieczeństwa oraz wpływają na ciągłość działania procesów biznesowych organizacji,

MB – zbiór mechanizmów bezpieczeństwa będących w dyspozycji osób funkcyjnych i stanowiących wyposażenie ich stanowisk pracy.

Każdy proces ochronny $po_p \in PO$ zdefiniowany jest następująco:

$$po_p = < r_p , \propto_p^{PO},\ ZD_p,\ OB_p ,\ MTO_p , ZTO_p >, \tag{2}$$

gdzie:

r_p – rodzaj p-tego procesu ochronnego,

$\propto_p^{PO}$ – cel działania p-tego procesu ochronnego,

ZD_p – zbiór działań, jakie należy wykonać aby osiągnąć cel działania p-tego procesu ochronnego,

OB_p – zbiór obiektów chronionych przez p-ty proces ochronny,

MTO_p – zbiór metod ochronnych p-tego procesu ochronnego,

ZTO_p – zbiór technik ochronnych p-tego procesu ochronnego.

Każdy mechanizm bezpieczeństwa $mb_p \in MB$ zdefiniowany jest następująco:

$$mb_p = < ch_p , \propto_p^{MB}, ZF_p, ZP_p >, \tag{3}$$

gdzie:

ch_p – charakter p-tego mechanizmu bezpieczeństwa,

$\propto_p^{MB}$ – cel działania p-tego mechanizmu bezpieczeństwa,

ZF_p – zbiór pełnionych funkcji bezpieczeństwa p-tego mechanizmu bezpieczeństwa,

ZP_p - zbiór podatności p-tego mechanizmu bezpieczeństwa.

Dodatkowo wprowadźmy następujące oznaczenia:

$\hat{U}$ – zbiór dopuszczalnych wielkości sterujących, przy pomocy których podmiot decydowania może ustalać bieżące właściwości następujących elementów:

- procesów ochronnych,
- obiektów chronionych,
- mechanizmów bezpieczeństwa,
- stanowisk pracy;

V_u – zbiór odpowiadających tym sterowaniom par $< p, q > \in \hat{P}^k \times \hat{Q}^k , \overline{k = 1,4}$,
gdzie:

$\hat{P}^k$– zbiór numerów wyróżnionych, odpowiednio dla: $k = 1$ - procesów ochronnych, $k = 2$ - obiektów chronionych, $k = 3$ – mechanizmów bezpieczeństwa, $k = 4$ – stanowisk pracy,

$\hat{Q}^k$ – zbiór numerów wyróżnionych, odpowiednio dla: $k = 1$ - procesów ochronnych, $k = 2$ - obiektów chronionych, $k = 3$ – mechanizmów bezpieczeństwa, $k = 4$ – stanowisk pracy,

$\hat{S}^k$ – wektor stanów wyróżnionych elementów, którego współrzędne określają stany poszczególnych elementów odpowiednio dla: $k = 1$ - procesów ochronnych, $k = 2$ – obiektów chronionych, $k = 3$ – mechanizmów bezpieczeństwa, $k = 4$ – stanowisk pracy.

Pod pojęciem stanu s_p, gdzie $p \in \hat{P}^k$, $\overline{k = 1{,}4}$, rozumie się wektor cech opisujących szczegółowo bieżące właściwości użytkowe p-tego elementu:

$$s_p = < a_p^q \in A_p^q : p \in \hat{P}, q \in \hat{Q} >, \tag{4}$$

gdzie:

a_p^q – współrzędne wektora stanu p-tego elementu wyrażające poszczególne cechy,

A_p^q – zbiór dopuszczalnych realizacji q-tej cechy p-tego elementu,

Wpływ sterowania na stan elementów $p \in \hat{P}^k$, $\overline{k = 1{,}4}$, a w następstwie na ich właściwości, można zapisać następująco:

$$\bigwedge_{<p,q> \in \hat{P}^k \times \hat{Q}^k} a_p^q = a_p^q[u(t)], u \in U, \overline{k = 1{,}4}, \tag{5}$$

w rezultacie zbiór sterowalnych:

a) na stan procesów ochronnych, można zdefiniować następująco:

$$\widehat{PO} = \left\{ po_p \in PO : \bigvee_{q \in \hat{Q}} [< p, q > \in V_u], p \in \hat{P}^1 \right\} \tag{6}$$

b) na stan obiektów chronionych, można zdefiniować następująco:

$$\widehat{OB} = \left\{ ob_p \; POB : \bigvee_{q \in \hat{Q}} [< p, q > \in V_u], p \in \hat{P}^2 \right\} \tag{7}$$

c) na stan mechanizmów bezpieczeństwa, można zdefiniować następująco:

$$\widehat{MB} = \left\{ mb_p \in MB : \bigvee_{q \in \hat{Q}} [< p, q > \in V_u], p \in \hat{P}^3 \right\}; \tag{8}$$

d) na stan mechanizmów bezpieczeństwa, można zdefiniować następująco:

$$\widehat{SF} = \left\{ sf_p \in SF : \bigvee_{q \in \hat{Q}} [< p, q > \in V_u], p \in \hat{P}^4 \right\}. \tag{9}$$

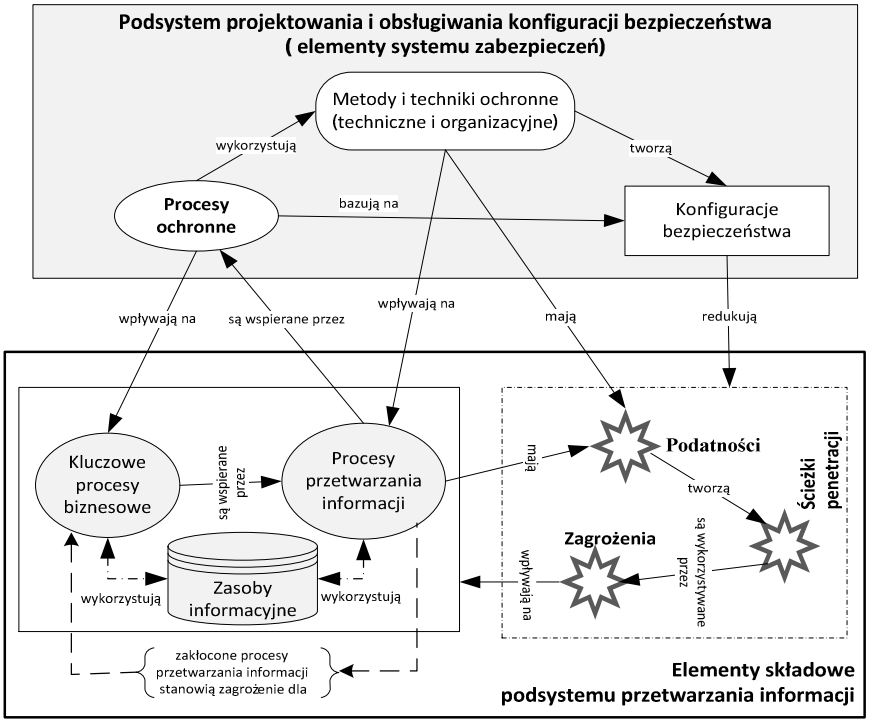
Na zbiorze sterowalnych procesów ochronnych lub obiektów chronionych, lub mechanizmów bezpieczeństwa, lub stanowisk pracy określa się cel $\propto^{SB}$ działania służby bezpieczeństwa.

2.2. Przedmiot działania

Z punktu widzenia sterowania bieżącym poziomem bezpieczeństwa informacji przedmiotem działania jest zbiór takich elementów $e_j \in E^{SIO}$, systemu informacyjnego organizacji (SIO), których stan pożądany może ustalać podmiot decydowania – służba bezpieczeństwa (rysunek 2). Elementami zbioru E^{SIO} mogą być (Liderman, 2012):

- kluczowe procesy biznesowe,
- procesy przetwarzania informacji,
- porcje informacji (zasoby informacyjne) gromadzone lub przetwarzane w ramach SIO, zwane dalej obiektem lub zasobem informacyjnym.

Każdy zasób informacyjny $z \in Z$ oznacza się numerem $p \in P^{SIO}$ i opisuje się go zbiorem C_p^{SIO} nazw cech. Jeżeli wszystkie różniące się zbiory cech C_p^{SIO}, jakimi są opisane poszczególne zasoby informacyjne, ponumerujemy zmienną $b = \overline{1,B}$ (którą nazwiemy typem zasobu informacyjnego - obiektu), to dwa obiekty są tego samego typu (np. „b"), gdy opisują je identyczne zbiory cech. Zbiory Q_p^{SIO} numerów cech opisujących obiekt $p \in P^{SIO}$ i odpowiadające im zbiory nazw cech C_p^{SIO} nie mogą być puste dla każdego $p \in P^{SIO}$, gdzie P^{SIO} jest zbiorem numerów wyróżnionych zasobów informacyjnych. Zakładamy, że dla każdej cechy $q \in Q^{SIO}$ jest określony zbiór A_q^{SIO} możliwych realizacji a_q cechy.



Rys. 2. Ilustracja sytemu informacyjnego organizacji z punktu widzenia sterowania jego bezpieczeństwem informacji.

Fig. 2. Illustration of the information system of the organization from the point of view of controlling its information security.

Wprowadźmy następujące oznaczenia:

D – zbiór decyzji sterujących, zwanych dalej dyrektywami, przy pomocy których osoby funkcyjne ze swoich stanowisk pracy, mogą ustalać właściwości bezpieczeństwa zasobów informacyjnych;

V_D – zbiór odpowiadających tym sterowaniom par $< p, q > \in P^{sio} \times Q^{SIO}$,

gdzie:

P^Z – zbiór numerów wyróżnionych zasobów informacyjnych,

Q^Z – zbiór numerów wyróżnionych cech zasobów informacyjnych,

$\underline{a}(t)$ – wektor stanu wyróżnionych zasobów informacyjnych, którego współrzędne określają stany bezpieczeństwa poszczególnych obiektów w chwili t.

Pod pojęciem stanu $a^p(t)$, $p \in P^{SIO}$ p-tego obiektu rozumie się wektor cech opisujących szczegółowo jego bieżące właściwości bezpieczeństwa:

$$a^p(t) =< a_q^p(t) \in \ddot{A}_p^q : p \in P^{SIO}, q \in Q^Z > \tag{10}$$

gdzie:

$a_q^p(t)$ – współrzędne wektora stanu p-tego obiektu, wyrażające poszczególne cechy,

$\ddot{A}_p^q$ – zbiór dopuszczalnych realizacji q-tej cechy p-tego obiektu,

Q^Z – zbiór numerów wyróżnionych cech obiektów.

Wpływ decyzji, podejmowanych przez osoby funkcyjne, na bieżący stan bezpieczeństwa w chwili t można zapisać następująco:

$$\bigwedge_{<p,q>\in P^{SIO}\times Q^{SIO}} a_p^q(t) = a_p^q[d(t)],\ d \in D\ . \tag{11}$$

W rezultacie zbiór zasobów, których stan bieżący (a w następstwie bieżący poziom bezpieczeństwa) mogą ustalać osoby funkcyjne, można zdefiniować następująco:

$$OB = ZI = \left\{zi_p \in E^{SIO} : \bigvee_{q\in Q^{SIO}} [< p, q >\in V_D],\ p \in P^{SIO}\right\}. \tag{12}$$

Podsumowując, w dalszej rozważanych niniejszego artykułu, przedmiotem działania dla służ bezpieczeństwa są zasoby informacyjne przetwarzane w ramach SIO.

2.3. Cel działania służby bezpieczeństwa

Działanie służby bezpieczeństwa można zdefiniować:

1. w odniesieniu do sterowania właściwościami bezpieczeństwa zasobów informacyjnych SIO jako uporządkowana para:

$$DZ^{SIO} =<\propto^{SIO}, Z^{SIO} >, \tag{13}$$

gdzie:

$\propto^{SIO}$ – cel działania SIO w kontekście bezpieczeństwa informacji,

Z^{SIO} – zbiór zadań bezpiecznego przetwarzania informacji, zapewniających osiągnięcie celu $\propto^{SIO}$.

2. w odniesieniu do sterowania właściwościami użytkowymi stanowisk pracy osób funkcyjnych, powołanych w ramach służby bezpieczeństwa jako uporządkowana para:

$$DZ^{SF} =<\propto^{SF}, Z^{SF} >, \tag{14}$$

gdzie:

$\propto^{SF}$ – cel działania służby bezpieczeństwa,

Z^{SF} – zbiór zadań (sterowań), zapewniających osiągnięcie celu $\propto^{SF}$,

Wprowadźmy następujące oznaczenia:

$\dot{P}(t)$ – zbiór numerów zasobów informacyjnych zgromadzonych w SIO do chwili t i wymagających dalszego bezpiecznego przetwarzania,

$[t_0^{p\cdot}, \dot{T}^p]$ – dopuszczalny przedział czasu, w którym obiekt o numerze $p \in \dot{P}(t)$ powinien mieć zachowane atrybuty bezpieczeństwa - posiadać wymagany poziom bezpieczeństwa.

$\dot{W}_p$ – pożądana właściwość bezpieczeństwa p-tego obiektu informacyjnego uzyskana w przedziale czasu $[t_0^{p\cdot}, \dot{T}^p]$ gdzie:

t_0^p, – chwila zarejestrowania p-tego obiektu w SIO

$\dot{T}^p$ – chwila wyrejestrowania (usunięcia) p-tego obiektu z SIO.

$Q^{SIO}(w)$ – zbiór numerów cech obiektu informacyjnego, na których określona jest własność „w" .

Stwierdzenie czy zasób informacyjny o numerze $p \in \dot{P}(t)$ posiada własność „w" wymaga określenia dla tego obiektu podzbiorów $\propto_p^q (w) \subset \dot{A}_p^q$ realizacji cech, dla każdej cechy $q \in Q^{SIK}(w)$. Jeżeli realizacje cech $a_q^p(t)$ p-tego obiektu w chwili $t \in [\dot{t}_0^p, \dot{T}^p]$ należą do tych podzbiorów $\propto_p^q (w)$, to mówimy, że obiekt o numerze $p \in \dot{P}(t)$ posiada własność „w".

Przyjmując, ze dla każdego obiektu $p \in P^{SIO}$ znane są zbiory $\dot{Q}_P$ cech, na wartościach których określone są podzbiory $\propto_p^q (w) \equiv \dot{\propto}_p^q,\ q \in \dot{Q}_P$, cel służb bezpieczeństwa można zdefiniować następująco:

$$\propto^{SB} \equiv \propto^{SIO} \left\{ \dot{\propto}_p^q : < p, q > \in V_D\ , p \in \dot{P}(t), q \in Q^{SIO} \right\}. \tag{15}$$

Z punktu widzenia możliwości osiągania celu służb bezpieczeństwa, każdy zasób informacyjny$z_p \in Z$ i przetwarzany w ramach SIO można opisać:

$$z_p = < b_p, O_p^b, w_p^b, Q\left(w_p^b\right), \dot{\propto}\left(w_p^b\right), R_p^b > \tag{15}$$

gdzie:

b_p – typ p-tego zasobu informacyjnego,

O_p^b – osoba funkcyjna będą właścicielem p-tego zasobu informacyjnego b-tego typu,

w_p^b, – właściwość bezpieczeństwa p-tego zasobu informacyjnego b-tego typu,

$Q\left(\dot{w}_p^b\right)$ – zbiór numerów cech na których określone są podzbiory $\propto_p^q \left(w_p^b\right)$,

$\dot{\propto}\left(w_p^b\right)$ – zbiór pożądanych stanów p-tego obiektu b-tego typu,

R_p^b – zbiór relacji wiążących b_p z $\dot{\propto}\left(w_p^b\right)$.

3 Model podsystemu sterowania poziomem bezpieczeństwa informacji

Jako model podsystemu sterowania bieżącym poziomem bezpieczeństwa zasobów informacyjnych przyjęto uporządkowaną piątkę (Stanik, 1987):

$$< SF, U, KB, FR, Q >, \tag{16}$$

gdzie:

SF – zbiór stanowisk pracy osób funkcyjnych, powołanych w ramach struktury służby bezpieczeństwa organizacji,

U – zbiór numerów typów sytuacji awaryjnych (zbiór numerów utraty bezpieczeństwa SIO), wyróżnionych na podstawie analizy skutków jakie one powodują,

KB – rodzina dopuszczalnych konfiguracji bezpieczeństwa,

FR – ogólna funkcja rekonfiguracji,

Q – ogólna funkcja rekonfiguracji.

Z punktu widzenia możliwości sterowania bieżącymi właściwościami stanowisk pracy a w następstwie bieżącym poziomem bezpieczeństwa zasobów informacyjnych, każde stanowisko pracy można opisać następująco, w sposób rozszerzony:

$$\widehat{sf}_p =< O_p, P_p, \quad PO_p, D_p, \quad MB_p > \in \Theta \times 2^P \times 2^{PO} \times 2^D \times 2^{MB} \tag{17}$$

gdzie:

O_p – nazwa powołanego zasobu osobowego p-tego stanowiska pracy – kod osoby funkcyjnej, itp.: ABI, IOD lub ASI,

P_p – zbiór obiektów SIO, których właścicielem jest osoba funkcyjna p=tego stanowiska, i w stosunku do których powinna utrzymywać wymagany poziom bezpieczeństwa,

PO_p – zbiór procesów ochronnych przypisanych do p-tego stanowiska pracy, inicjowanie których wpływa na poziom bezpieczeństwa podstawowych aktywów organizacji (procesów biznesowych lub zasobów informacyjnych),

D_p – zbiór decyzji sterujących (dyrektyw, zleceń, decyzji nakazowych, itp.) dostępnych dla osoby funkcyjnej przypisanej do p-tego stanowiska pracy.

MB_p – zbiór mechanizmów bezpieczeństwa będących w dyspozycji osoby funkcyjnej p-tego stanowiska pracy.

Awaria rozumiana jest jako zdarzenie, powstałe w chwili t_i, spowodowane wystąpieniem różnicy między pożądaną właściwością konfiguracji bezpieczeństwa a jego bieżącą konfiguracją bezpieczeństwa. Odpowiada to warunkowi:

$$KB^{WY}(t_i) \supset KB^{MO}(t_i)\ , \tag{18}$$

gdzie:

$KB^{WY}(t_i) = \bigcup_{i:\, z_i \in OB^{WY}(t_i)} KB_g$ – pożądana konfiguracja bezpieczeństwa, jaką należy powołać do zapewnienia wymaganego poziomu bezpieczeństwa

zasobom informacyjnym należącym do zbioru $z_i \in OB^{WY}(t_i)$; można ją rozpatrywać jako mnogościową sumę konfiguracji bezpieczeństwa dla zasobów $z_i \in OB^{WY}(t_i)$, przy czym : $KB_g = \langle z_g, O_g, MB_g \rangle$, gdzie:

- z_g – zasób informacyjny ochraniany przez g-ta konfigurację bezpieczeństwa,
- O_g – podzbiór zasobów osobowych możliwych do zaangażowania przy zapewnianiu utrzymania atrybutów bezpieczeństwa przypisanych do z_g zasobu informacyjnego,
- MB_g- zbiór mechanizmów bezpieczeństwa tworzących g-tą konfiguracje bezpieczeństwa,

$\mathrm{KB}^{\mathrm{MO}}(\mathrm{t_i}) = \bigcup_{\mathrm{i}:\, z_i \in OB^{MO}(t_i)} \mathrm{KB_g}$. – możliwa do skonstruowania, w chwili $\mathrm{t_i}$, konfiguracja bezpieczeństwa, w oparciu o aktualnie sprawne mechanizmy bezpieczeństwa o charakterze technicznym lub organizacyjnym;

$OB^{WY}(t_i)$ – zbiór zasobów informacyjnych, w stosunku do których od chwili t_i nie istnieje możliwość utrzymania wymaganego poziomu bezpieczeństwa,

$OB^{MO}(t_i) \in \Theta B(t)$ - zbiór zasobów informacyjnych, w stosunku do których od chwili t_i istnieje krytyczna możliwość utrzymania wymaganego poziomu bezpieczeństwa w oparciu o aktualnie powołane konfiguracje bezpieczeństwa; tzn. jeśli w chwili t_i wystąpi konieczność ochrony nowo - wprowadzonego zasobu informacyjnego do SIO , to wystąpi tzw. utrata bieżącego wymaganego poziomu bezpieczeństwa,

$\Theta B(t)$ – rodzina zbiorów możliwych do utworzenia na zbiorze na zbiorze OB(t).

Wprowadźmy następującą notację dowolnej konfiguracji bezpieczeństwa:

$$KB_{kl} = \langle OB^{kl}, O^k, MB^l \rangle , \tag{19}$$

gdzie:

- OB^{kl} – zbiór zasobów informacyjnych systemu informacyjnego organizacji chronionych przez kl-tą konfiguracją bezpieczeństwa,
- O^k – zbiór osób funkcyjnych zaangażowanych do zapewniania bezpieczeństwa zasobów informacyjnych należących do zbioru OB^{kl},
- MB^l – zbiór mechanizmów bezpieczeństwa o charakterze technicznym lub organizacyjnym tworzących kl-tą konfiguracją bezpieczeństwa.

Znajomość konfiguracji bezpieczeństwa KB_{kl} stwarza możliwość przyporządkowania każdemu zbiorowi OB^{kl}, przy ustalonym zbiór MB^l mechanizmów bezpieczeństwa (zabezpieczeń organizacyjnych i technicznych) odpowiadający mu zbiór O^k. Konfiguracja bezpieczeństwa KB_{kl} jest realizowalna wtedy i tylko wtedy, gdy zbiorowi OB^{kl} przy ustalonych elementach zbioru MB^l można przyporządkować taki $zbiór\ O^k$, który zapewni utrzymanie wymaganego poziomu bezpieczeństwa zbiorowi zasobów informacyjnych OB^{kl}.

Można uwzględnić, że w następstwie powyższego zbiór, OB^{kl} , przy ustalonym zbiorze MB^l jest w relacji ze zbiorem OB^{kl}, tzn. $OB^{kl}\ KB_{kl}\ O^k$. Zatem możemy rozpatrywać konfigurację bezpieczeństwa (16) jako analog systemu terminalnego w ujęciu

(Mesarowicz, 1976), w którym wejściami są zasoby informacyjne ze zbioru OB^{kl}, a wyjściami elementy ze zbioru O^k.

Przestrzeń możliwych sytuacji awaryjnych tworzy produkt kartezjański $A = 2^{OB} \times 2^{O} \times 2^{MB}$. Element $a_{nms} =< OB_n, O_m, MB_s > \in A$ określa typ sytuacji awaryjnej. Przyjmijmy, że dla każdego typu awarii określona jest wartość funkcji $\chi(nms) = u$ definiująca numer sytuacji awaryjnej.

Zakłada się, służba bezpieczeństwa wyposażona jest w podsystem wizualizacji, podsystem automatycznej kontroli bezpieczeństwa (SAKB) oraz zespół kontrolno – diagnostycznego, które są w stanie zidentyfikować wszystkie typy sytuacji awaryjnych (sytuacji utraty bezpieczeństwa). Pod pojęciem sytuacji awaryjnej typu $a \in A$ o numerze u $\in U$ rozumie się zbiory OB_n, O_m, MB_s pozostające po wystąpieniu sytuacji awaryjnej o numerze u $\in U$.

Zbiór dopuszczalnych konfiguracji bezpieczeństwa, po utracie bezpieczeństwa *określa się* na podstawie znajomości:

- OB^p – zbioru zasobów informacyjnych, w stosunku do których należy utrzymywać wymagany poziom bezpieczeństwa,
- O^p – zbioru zasobów osobowych (osób funkcyjnych) będących w dyspozycji po wystąpieniu sytuacji awaryjnej o numerze u $\in U$,
- $MB^p \in$ MP – zbiór możliwych do wdrożenia konfiguracji bezpieczeństwa w oparciu o zbiory sprawnych zabezpieczeń o charakterze technicznym lub organizacyjnym, pozostałych po wystąpieniu sytuacji utraty bezpieczeństwa o numerze u $\in U$,

według następującej reguły:

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

Powyższe oznacza, ze do zbioru KB_{dop}^{u} dopuszczalnych konfiguracji bezpieczeństwa, po utracie możliwości zapewnienia wymaganego poziomu bezpieczeństwa zasobom informacyjnym SIO, zalicza się wszystkie konfiguracje bezpieczeństwa, zbudowane dla różnych wariantów zbiorów osobowych i zbioru zabezpieczeń o charakterze technicznym lub organizacyjnym, pozostających po wystąpieniu sytuacji awaryjnej, zapewniających utrzymanie wymaganego poziomu bezpieczeństwa w stosunku do bieżącego zbioru zasobów informacyjnych $OB\ (t) \in \Theta B(t)$. Każda konfiguracja bezpieczeństwa ze zbioru KB_{dop}^{u} zapewnia utrzymanie akceptowalnego poziomu bezpieczeństwa zasobów informacyjnych ze zbioru OB^{kl}.

Odwzorowanie FR wyznacza się na etapie projektowania systemu sterowania bieżącym poziomem bezpieczeństwa lub na etapie ustanawiania systemu zabezpieczeń, jako podstawowego elementu SZBI, aby zapewniło ono uzyskiwanie pożądanych celów działania Służby Bezpieczeństwa oraz podsystemu przetwarzania informacji w trakcie ich eksploatacji, mimo wystąpienia sytuacji awaryjnej. Po wystąpieniu sytuacji awaryjnej – utraty wymaganego poziomu bezpieczeństwa, aby można było skutecznie

kontynuować proces bezpiecznego przetwarzania informacji w SIO, należy wygenerować dopuszczalną lub optymalną konfigurację bezpieczeństwa. Wygenerowanie optymalnej konfiguracji bezpieczeństwa spośród zbioru rozwiązań dopuszczalnych, realizowane jest w oparciu o szczegółową funkcję rekonfiguracji Q, która z punktu widzenia swojej istoty jest funkcją kryterialną.

4 Model podsystemu sterowania poziomem bezpieczeństwa zasobów informacyjnych - przykład

4.1. Opis formalny służby bezpieczeństwa

Przedmiotem rozważań jest służba bezpieczeństwa hipnotycznej organizacji. Funkcję sterowania poziomem bezpieczeństwa w niej spełnia osoba funkcyjna, pełniąca np. obowiązki ABI/IOD[6] lub ASI[7]. Jego stanowisko pracy wyposażone jest w następujące zasoby o charakterze technicznym lub organizacyjnym:

a) środki wizualizacji danych opisujących bieżący stan bezpieczeństwa zasobów informacyjnych przetwarzanych w SIO, np. system automatycznej kontroli bezpieczeństwa SIO ,
b) środki IT, przy pomocy których ABI może przekazywać zlecenia (decyzje sterujące, polecenia, itp.) w celu ustalania bieżących stanów bezpieczeństwa zasobów informacyjnych poprzez powoływanie odpowiednich konfiguracji bezpieczeństwa, ze zbioru konfiguracji dopuszczalnych ustalonych na etapie projektowania.

Zbiór dopuszczalnych decyzji sterujących (zleceń) ma postać:

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

Poszczególne elementy zbioru ZL interpretowane są następująco:

zl_1 – powołaj system zabezpieczeń o konfiguracji bezpieczeństwa, zdefiniowanej w rejestrze ewidencji struktur systemu zabezpieczeń na i – tej pozycji (np. zdefiniowanej w 5-tym wierszu tego rejestru),

zl_2 – uaktywnij w systemie zabezpieczeń (o bieżącej konfiguracji bezpieczeństwa) wskazane zabezpieczenie techniczne lub organizacyjne,

zl_3 – odłącz/usuń w systemie zabezpieczeń (o bieżącej konfiguracji bezpieczeństwa) wskazane zabezpieczenie techniczne lub organizacyjne,

zl_4 – powołaj w służbie bezpieczeństwa (o bieżącej strukturze bezpieczeństwa) wskazane stanowisko pracy,

zl_5 – odwołaj w służbie bezpieczeństwa (o bieżącej strukturze bezpieczeństwa) wskazane stanowisko pracy,

[6] IOD – Inspektor ochrony danych osobowych, czyli ABI po nowemu. ABI – Administrator bezpieczeństwa informacji, w skrócie ABI, to osoba fizyczna powołana przez administratora danych osobowych (ADO), która zajmuje się zapewnianiem przestrzegania przepisów o ochronie danych osobowych.

[7] Administrator systemów informatycznych (ASI). Osoba pełniąca tę funkcje nadzoruje bezpieczeństwo przetwarzania danych w systemach informatycznych. Funkcja ASI wynika bardziej z praktyki niż z samych przepisów prawa.

zl_6 – przydziel do określonego stanowiska pracy wskazany proces ochronny,

zl_7 – odbierz od określonego stanowiska pracy wskazany proces ochronny.

Z punktu widzenia procesu zarządzania bezpieczeństwem zasobów informacyjnych podmiotem działania jest zbiór *PO* procesów ochronnych zarządzanych przez osoby funkcyjne ze zbioru *O*, przypisane do zbioru *SF* sterowalnych stanowisk pracy, powołanych w ramach bieżącej struktury bezpieczeństwa organizacji. Zbiory $\tilde{P}$ numerów zarządzanych procesów ochronnych oraz$\tilde{Q}$ numerów wyróżnionych cech tych procesów mają następującą postać:

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

$$\tilde{Q} = \{1,2,3,4,5\}.$$

Poszczególne elementy zbioru $\tilde{Q}$ interpretowane są następująco:

1 – proces ochronny jest powołany w ramach bieżącej konfiguracji bezpieczeństwa,

2 – proces ochronny nie jest powołany w ramach bieżącej konfiguracji bezpieczeństwa

3 – proces ochronny posiada (ma zaimplementowane) wszystkie metody i techniki ochronne (zabezpieczenia) o charakterze technicznym lub organizacyjnym ustalone na etapie projektowania

4 – proces ochronny posiada niezbędną liczbę zabezpieczeń zapewniających jego prawidłowe funkcjonowania

5 – proces ochronny nie posiada wystarczającej liczby zabezpieczeń zapewniających jego prawidłowego funkcjonowania.

Każdy sterowalny proces ochronny $po_p \in PO; p = \overline{1,9}$, zgodnie z określeniem (2), $po_p = < r_p, \propto_p^{PO}, ZD_p, OB_p, MTO_p, ZTO_p >$, opisany jest następująco:

$po_1 =$ < 1,C1, $\{d_2, d_3\}$, $\{z_2, z_3\}$, { $MO1, MO2, MO3$ }, { $MT3, MT4$}>;

$po_2 =$ < 1,C4, $\{d_1, d_3, d_5\}$, $\{z_1, z_5\}$, $\{MO2, MO3\}$, { $MT1, MT2$}>;

……

$po_8 =$ < 1,C5, $\{d_2, d_4, d_5\}$, $\{z_4\}$, $\{MO4, MO5\}$, { $MT1, MT3$}>;

gdzie:

1,2,3,……8 – rodzaje procesu ochronnego, jednoznacznie określające ich funkcjonalność w systemie zabezpieczeń przy czym: 1-wykrywanie, 2-odstraszanie, 3-zapobieganie, 4-redukowanie, 5-odtwarzanie, 6-monitorowanie, 7-uświadamianie, 8- udoskonalanie,

C1, C2, C3, C4, C5 – cel działania procesu ochronnego, przy czym: C1 - zapewnienie odpowiedniego poziomu ochrony logicznej, C2 - zapewnienie odpowiedniego poziomu ochrony fizycznej, C3 - zapewnienie ochrony wskazanej grupie elementów SIO, C4 – zapewnienie ochrony wskazanego elementu systemu informatycznego, C5 – wspomaganie wskazanego zasobu informacyjnego,

d_i – działanie, zadanie lub czynność będące składową procesu ochronnego, inicjowane ze stanowiska pracy osób funkcyjnych,

z_2 , z_3 – chronione zasoby informacyjne przez dany proces ochronny,

$MO1$, $MO2$, $MO3$ – metoda ochrony (np.: procedura, instrukcja, szkolenie, itp.),

$MT1$, $MT2$, $MT3$, $MT4$, $MT5$ – technika ochrony (np.: środki sprzętowe, środki programowe, środki programowo-sprzętowe, środki osobowe).

Przedmiotem działania są porcje informacji gromadzonych lub przetwarzanych przez SIO. Zbiór porcji informacji – zasobów informacyjnych określony jest zależnością $OB = ZI = \{zi_p \in E^{SIO} : \bigvee_{q \in Q^{SIO}} [< p, q > \in V_D],\ p \in P^{SIO}\}$.

W definicji tej zbiory P^{SIO} numerów wyróżnionych obiektów oraz Q^{SIO} numerów wyróżnionych cech tych zasobów informacyjnych maja następującą postać:

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

Poszczególne elementy zbioru Q^{SIO} interpretowane są następująco: 1- numer identyfikacyjny obiektu, 2 – nazwa, 3 – zbiór przypisanych atrybutów bezpieczeństwa, 4 - wartość wymaganego poziomu bezpieczeństwa w aspekcie przypisanych atrybutów bezpieczeństwa 5 - wycena zasobu w aspekcie możliwych szkód, jakie poniesie organizacja wskutek utraty przypisanych atrybutów bezpieczeństwa lub wymaganego poziomu bezpieczeństwa, 6 - zbiór aktualnie posiadanych podatności, 7- aktualna wartość podatności w kontekście zbioru aktualnie posiadanych podatności, 8 - zbiór aktualnie przypisanych zabezpieczeń technicznych, 9 - zbiór aktualnie przypisanych zabezpieczeń organizacyjnych, 10 -wartość ryzyka szczątkowego, 11- klauzula poufności,

Każdy obiekt o numerze $p \in P^{SIO}$, zgodnie z rozważeniami przedstawionym w punkcie 1.2. określony jest zależnością

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

W definicji tej zbiory $B, W, \dot{Q}^b, \dot{\propto}^b, R^b, b \in B$ mają następującą postać:

A. zbiór typów obiektów $B = \{1,2,3\}$, gdzie elementy tego zbioru interpretowane są następująco: 1- dane osobowe, 2- dane niejawne, 3-dane wrażliwe.

B. Zbiór właściwości bezpieczeństwa W= $\{1,2\}$, gdzie elementy tego zbioru interpretowane są następująco: 1- zasób ma zachowane atrybuty bezpieczeństwa , 2- zasób utracił podstawowe atrybuty bezpieczeństwa.

C. Zbiory $\dot{Q}^b\ ;\ b = \overline{1,3}$,
   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. Zbiory $\dot{\propto}^b\ ;\ b = \overline{1,3}$,
   a. $\dot{\propto}^1 = \{1,2,3,4\}$
   b. $\dot{\propto}^2 = \{3,4,5\}$,
   c. $\dot{\propto}^3 = \{4,5\}$,

   Elementy zbiorów $\dot{\propto}^b$ interpretowane są następująco: 1- poziom bezpieczeństwa podstawowy, 2- poziom bezpieczeństwa podwyższony, 3- poziom bezpieczeństwa wysoki, 4- ryzyko akceptowalne, 5- ryzyko tolerowane.

E. Zbiory $R^b;\ b = \overline{1,3}$,

$$R^1 = Z^1 \times \dot{\propto}^1 = \{< z_1^1, 1 >, < z_2^1, 2 >, < z_3^1, 3 > < z_4^1, 4 >\}$$
$$R^2 = Z^2 \times \dot{\propto}^2 = \{< z_1^2, 3 >, < z_2^2, 4 >, < z_3^2, 5 >\}$$
$$R^3 = Z^3 \times \dot{\propto}^3 = \{< z_1^3, 4 >, < z_2^3, 5 >\}$$

Elementami zbiorów Z^b; $b = \overline{1,3}$ są etapowe działania (zadania), które powinien wykonać podmiot działania (osoba funkcyjna $o_p \in O_p^b$) aby obiekt (zasób informacyjny) typu $b \in B$ osiągnął stan pożądany ze zbioru $\dot{\propto}^b$.

Poszczególne etapowe zadania ze zbioru $\{ Z^b;\ b = \overline{1,3}\}$ są opisane następująco:

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

Zbiór wszystkich zadań etapowych ma więc następującą $Z = \{z_g,\ g = \overline{1,9}\}$.

Zakładając, że uaktywnianie każdej procedury $PR_i, i = \overline{1,11}$ wymaga wprowadzenia przez osobę funkcyjną zlecenia $d_i \in D$ inicjującego i-tą procedurę oraz wizualizację danych wejściowych DMB_i niezbędnych poprawnego wykonania się tej procedury, to każde etapowe zadanie można zapisać następująco:

$$z_g = [< d_i, DMB_i >: i \in I_g \ \wedge DMB_i \subset DMB_g],$$

gdzie:

I_g – zbiór numerów procedur uaktywnianych podczas realizacji g-tego zadania etapowego,

DMB_g – zbiór danych wejściowych zapewniających prawidłowe wykonanie ciągu procedur realizujących g-te zadanie etapowe.

Zakładając, że znana jest funkcja $\varphi_g(PR_i) = j$, ustalająca numer „j" dyrektywy inicjującej procedurę o numerze „i" w zadaniu etapowym rodzaju „g", to każde zadanie etapowe można zapisać (w postaci uproszczonej) jako ciąg numerów dyrektyw (zleceń), np.: $z_1 = [1,2]$, …, $z_9 = [1,2,3,4,6,9]$.

Cel działania służby bezpieczeństwa ma postać

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

Poszczególne zbiory $\dot{\propto}^b$ określone są następująco: $\dot{\propto}^1 = \{1,2,3,4\}$; $\dot{\propto}^2 = \{3,4,5\}$, $\dot{\propto}^3 = \{4,5\}$. Przyjmujemy, że dopuszczalny przedział czasu , w którym obiekt (zasób informacyjny) $p \in P^{SIO}(t)$ winien osiągnąć stan pożądany, nie może przekraczać 3 dni.

4.2 Sterowanie bieżącym poziomem bezpieczeństwa przez służby bezpieczeństwa

Załóżmy, że opisana w punkcie 1. służba bezpieczeństwa działa przez dłuższy okres czasu $[t_0, t]$, gdzie t_0 – chwila rozpoczęcia procesu przetwarzania informacji w SIO, t-chwila bieżąca. Podczas eksploatacji SIO ulegają zmianie pożądanie (wymagane) i bieżące właściwości użytkowe i bezpieczeństwa zarówno w zakresie służby bezpieczeństwa jak i SIO. Przyjmijmy również, że w chwili $t_i = t$ system

automatycznej kontroli poziomu bezpieczeństwa (SAKB) lub osoba funkcyjna wykrył sytuację awaryjną. Odpowiada to warunkowi: $KB^{WY}(t_i) \supset KB^{MO}$.

W celu zapewnienia wymaganego poziomu zasobom informacyjnym ze zbioru $OB^{WY}(t_i)$ Inspektor Ochrony Danych lub ABI inicjuje zlecenie zl_1, które spowoduje wygenerowanie i wdrożenie nowej konfiguracji bezpieczeństwa, zapewniającej utrzymanie wymaganego poziomu bezpieczeństwa. Postać zlecenia inicjującego powołanie w systemie zabezpieczeń nowej konfiguracji bezpieczeństwa może być następująca: RTO n, gdzie:

- RTO zabezpieczeń - kod zlecenia inicjującego wdrożenie odpowiedniego zbioru zabezpieczeń technicznych i organizacyjnych,
- n - numer wiersza w rejestrze ewidencji dopuszczalnych konfiguracji bezpieczeństwa, odpowiadający numerowi sytuacji awaryjnej.

Numer sytuacji awaryjnej określony jest przez osobę funkcyjną lub automatycznie przez SAKB na podstawie znajomości:

- zbioru zasobów informacyjnych w stosunku do których wymagane jest zapewnienie odpowiednich poziomów bezpieczeństwa,
- zbioru aktualnie sprawnych lub użytecznych mechanizmów bezpieczeństwa o charakterze technicznym, organizacyjnym i osobowym,
- zbioru osób funkcyjnych będących w dyspozycji służby bezpieczeństwa organizacji.

Przyjmijmy, że wystąpiła sytuacja awaryjna o numerze n=5. Dla tej sytuacji (o numerze 5) zbiory OB^5, SF^5, MB^5 są następujące:

$OB^5 = \{zi_2, zi_5, zi_6, zi_7, zi_8, zi_{11}\}$,

$SF^5 = \{sf_1, sf_2, sf_3\}$,

$MB^5 = \{mb_1, mb_2, mb_3, mb_5, mb_7, mb_8, mb_{10}, mb_{12}, mb_{13}\}$.

5 Podsumowanie

Na świecie od dłuższego czasu prowadzone są prace nad standaryzacją i optymalizacją systemów zabezpieczeń aktywów organizacji w tym zasobów informacyjnych. Warunki społeczeństwa informacyjnego wymagają, aby każdy system zabezpieczeń charakteryzowały następujące właściwości:

1) stała gotowość, czyli utrzymywanie wymaganego poziomu bieżącej funkcjonalności, niezawodności i skuteczności w zakresie utrzymywania pożądanego poziomu bezpieczeństwa, niezależnie od występujących sytuacji awaryjnych,
2) wysoka operatywność z punktu widzenia sterowania właściwościami użytkowymi rozumiana, jako terminowe i zdecydowane reagowanie na wszystkie sytuacje awaryjne oraz podejmowanie decyzji sterujących przywracających skuteczność systemu w aspekcie utrzymywania wymaganego poziomu bezpieczeństwa w wymaganym czasie,

Artykuł nie stanowi gotowej „recepty" na projektowanie i budowę skutecznych systemów zabezpieczeń w aspekcie zapewniania wymaganego poziomu bezpieczeństwa zasobów informacyjnych. Należy go traktować, jako propozycję autorów częściowego

rozwiązania problemu ustanawiania i budowy SZ, który umożliwiałby bieżące sterowania poziomem bezpieczeństwa systemu informacyjnego organizacji. Zaproponowany sposób podejścia do problematyki bezpieczeństwa, ukierunkowanej na proces rekonfiguracji, wynika między innymi ze spostrzeżeń i kilkuletnich doświadczeń autorów nagromadzonych:

a) podczas obserwacji ustanawiania i wdrażania takich systemów zabezpieczeń w organizacjach i korporacjach,
b) w trakcie prowadzenia projektów badawczo-wdrożeniowych
c) w trakcie prac naukowo-badawczych i dyskusji seminaryjnych dotyczących bezpieczeństwa korporacji.

Aktualnie, punktem odniesienia przy budowie Systemu Zabezpieczeń (SZ) są międzynarodowe standardy ISO 27001, ISO 27005 oraz zbiór dobrych praktyk w obszarze analizy ryzyka oraz bezpieczeństwa informacyjnego i bezpieczeństwa informacji.

Literatura

1. ISO / IEC 27002: 2015 Technika informatyczna - Techniki bezpieczeństwa - Kodeks postępowania w zakresie kontroli bezpieczeństwa informacji
2. ISO / IEC 27004: 2013 Technika informatyczna - Techniki zabezpieczeń - Zarządzanie bezpieczeństwem informacji – pomiary
3. Liderman K.: Bezpieczeństwo informacyjne, PWN, 2012
4. Mesarovic M. D.: Matematyczna teoria systemów ogólnych [w:] *Ogólna teoria systemów. Klir G.* J. red. WNT, Warszawa 1976
5. Polaczek T.: *Audyt bezpieczeństwa informacji w praktyce*, Helion, 2014
6. Stanik J., Kiedrowicz M.: Model ryzyka procesów biznesowych. *Zeszyty Naukowe Uniwersytetu Szczecińskiego*, Ekonomiczne Problemy Usług, (2017).
7. Stanik J.: *Utrzymywanie wymaganego poziomu bieżącej niezawodności funkcjonalnej komputerowego systemu zautomatyzowanego dowodzenia*, praca doktorska, Warszawa 1987 r.
8. http://www.zut.edu.pl/fileadmin/pliki/abi/9/RYZYKO_ODO-1.pdf (21.03.2018)
9. http://www.zut.edu.pl/fileadmin/pliki/abi/9/RYZYKO_ODO-2.pdf (21.03.2018)

Streszczenie

W artykule przedstawiono koncepcję utrzymywania wymaganego poziomu bezpieczeństwa przez służbę bezpieczeństwa organizacji. Zaproponowano model służby bezpieczeństwa dla potrzeb utrzymania wymaganego poziomu bezpieczeństwa. Wyróżniono i scharakteryzowano podstawowe elementy służby bezpieczeństwa, takie jak: podmiot działania, przedmiot działania oraz cel działania. Ponadto zdefiniowano pojęcie konfiguracji bezpieczeństwa oraz model podsystemu sterowania bieżącym poziomem bezpieczeństwa informacji w przypadku wystąpienia sytuacji awaryjnej. Rozważania teoretyczne zostały poparte przykładem.

Słowa kluczowe: służba bezpieczeństwa, system zabezpieczeń, konfiguracja bezpieczeństwa, utrata poziomu bezpieczeństwa

The model of security service for the needs of maintaining the required level of information security in the organization

Streszczenie

The article presents the concept of maintaining the required level of security by the security service of the organization. A model of security service was proposed for maintaining the required level of security. The basic elements of the security service were distinguished and characterized, such as the subject of action, the subject of the activity and the purpose of the action. In addition, the concept of security configuration and the subsystem model for controlling the current level of information security in the event of an emergency situation were defined. Theoretical considerations have been supported by an example.

Keywords: security service, security system, security configuration, loss of security