Jerzy Stanik[1], Jarosław Napiórkowski[2],
Maciej Kiedrowicz[3]

Model służby bezpieczeństwa na potrzeby utrzymywania wymaganego poziomu bezpieczeństwa informacji w organizacji

1. Wstęp

Obserwowany w ostatnich latach szybki rozwój systemów bezpieczeństwa organizacji oraz konieczność zagwarantowania wytycznych RODO[4], umożliwiających uczciwe i zgodne z prawem przetwarzanie danych, wyprzedza w znacznym stopniu wiedzę na temat metod i technik utrzymywania wymaganego poziomu bezpieczeństwa informacyjnego organizacji oraz projektowania i budowy skutecznych systemów kontroli bezpieczeństwa. Prace J. Stanika, M. Kiedrowicza i R. Waszkowskiego[5] wskazują na rosnącą potrzebę automatyzacji procesu utrzymywania wymaganego poziomu bezpieczeństwa informacyjnego w organizacjach związaną z opracowaniem struktur służby bezpieczeństwa. W pracach J. Stanika i M. Kiedrowicza[6] wykazano między innymi, że sprowadzenie zadania utrzymywania właściwego poziomu bezpieczeństwa informacji do poziomu

[1] Wojskowa Akademia Techniczna, Wydział Cybernetyki.
[2] Wojskowa Akademia Techniczna, Wydział Cybernetyki.
[3] Wojskowa Akademia Techniczna, Wydział Cybernetyki.

[4] Rozporządzenie, nazywane GDPR (od angielskiej nazwy *General Data Protection Regulation*), a w Polsce znane pod nazwą RODO (Rozporządzenie Ogólne o Ochronie Danych Osobowych) stosowane jest od 25 maja 2018 r. w całej Unii Europejskiej.

[5] J. Stanik, M. Kiedrowicz, R. Waszkowski, *Security and Risk as a Primary Feature of the Production Process*, Intelligent Systems in Production Engineering and Maintenance, Springer 2019, s. 701–709, DOI:10.1007/978–3–319–97490-3_66; J. Stanik, M. Kiedrowicz, *Method for Assessing Efficiency of the Information Security Management System*, MATEC Web of Conferences 2018, vol. 210.

[6] J. Stanik, *System Risk Model of the IT System Supporting the Processing of Documents at Different Levels of Sensitivity*, MATEC Web of Conferences 2017, vol. 125; M. Kiedrowicz, *Multi-faceted Methodology of the Risk Analysis and Management Referring to the IT System Supporting the Processing of Documents at Different Levels of Sensitivity*, MATEC Web of Conferences 2017, vol. 125.

specjalizowanych procedur organizacyjnych pozwala służbom bezpieczeństwa efektywnie sterować pożądanym poziomem bezpieczeństwa informacyjnego. W pracach tychże autorów[7] proces rekonfiguracji struktur służby bezpieczeństwa rozpatrywany jest jako alokacja zadań (operacji przetwarzania), sformułowanych do rozwiązania zagadnienia rekonfiguracji w trybie *off-line*.

Daje się również zauważyć brak formalnych i komercyjnych modeli służb bezpieczeństwa, mających na celu utrzymanie wymaganego poziomu bezpieczeństwa obiektów systemu informacyjnego organizacji (SIO) lub kluczowych obszarów bezpieczeństwa (np. ochrony danych osobowych). Trudności zaproponowania receptur określania reguł, modeli, struktur lub zasad sterowania bieżącym poziomem bezpieczeństwa elementom SIO przez służbę bezpieczeństwa wynikają przede wszystkim ze specyficznych właściwości takich podsystemów, jak:

- podsystem bezpiecznego przetwarzania informacji w wydzielonych obszarach przetwarzania informacji lub całym systemie informacynym organizacji (SIO),
- podsystem zabezpieczeń, rozumiany jako element systemu zarządzania bezpieczeństwem informacji,
- podsystem wydzielonych stanowisk pracy osób funkcyjnych, tworzących strukturę służby bezpieczeństwa oraz inne podsystemy organizacji będące składowymi SZBI[8].

Ilustrację graficzną organizacji z punktu widzenia sterowania jej bieżącymi właściwościami użytkowymi przedstawiono na rysunku 1.

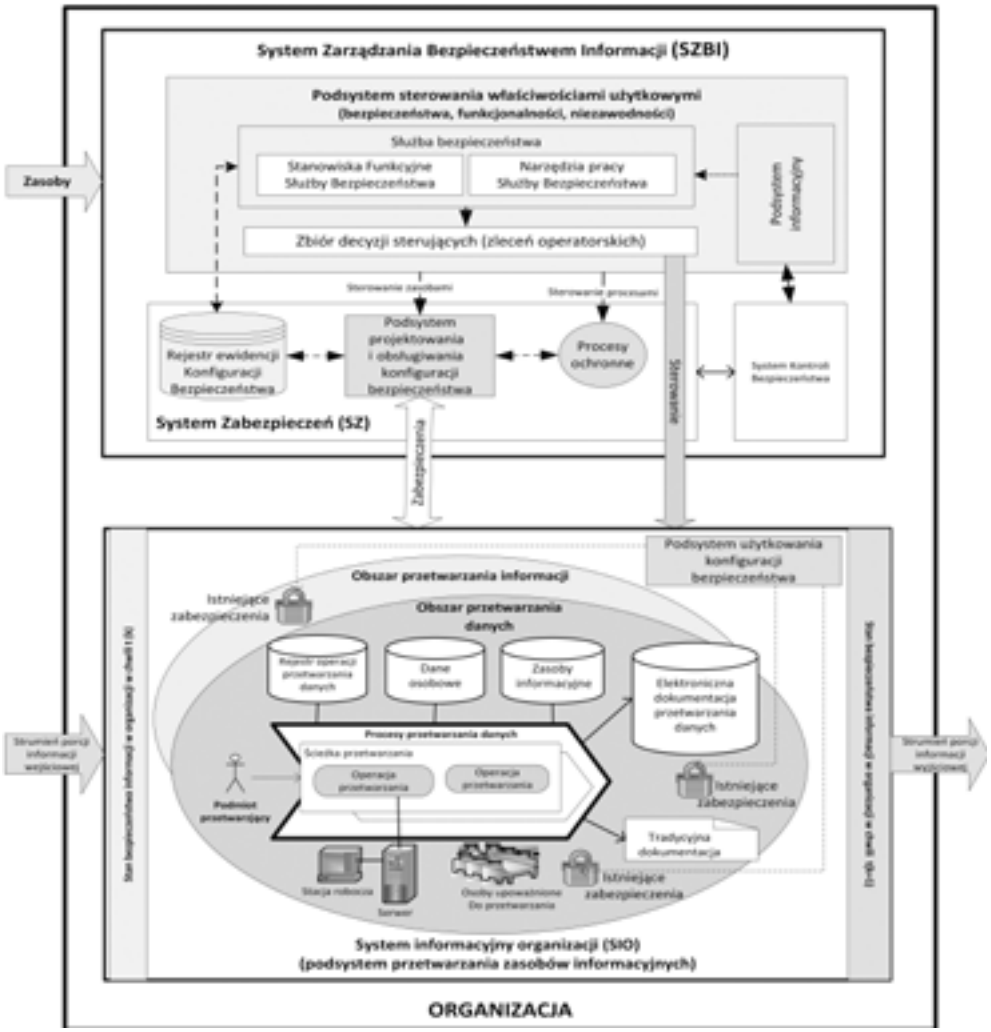
Celem niniejszego artykułu jest sformułowanie modelu służby bezpieczeństwa i uzasadnienie metody takiego sterowania bieżącymi właściwościami (np. użytkowymi, funkcjonalnymi, niezawodnościowymi, bezpieczeństwa) jego składnikami (wyżej wymienionymi podsystemami), które zapewnia utrzymanie wymaganego poziomu 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

[7] J. Stanik, M. Kiedrowicz, *Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych*, 01/2017, 126, s. 339–354, DOI:10.18276/epu.2017.126/1–33; J. Stanik, M. Kiedrowicz, *Models and Method for the Risk Assessment of an Intellectual Resource*, WSEAS Transactions on Information Science and Applications 09/2017; 14(2017), s. 174–183.

[8] 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.

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



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

Źródło: opracowanie własne.

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 służby bezpieczeństwa.

Zakładamy, że celem działania służb bezpieczeństwa jest nadawanie obiektom przetwarzanym 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, lecz także z punktu widzenia bezpieczeństwa.

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

- w bieżących chwilach muszą istnieć możliwości bezpiecznego przetwarzania wymaganego zbioru zasobów informacyjnych,
- w stosunku do kluczowych procesów biznesowych oraz wrażliwych zasobów informacyjnych[9] wymaga się istnienia procesów ochronnych, które zapewniają utrzymanie odpowiednich atrybutów bezpieczeństwa[10] na akceptowalnym poziomie ryzyka[11],
- 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 poziom bezpieczeństwa lub akceptowalną wartość ryzyka.

W świetle powyższego bieżący poziom bezpieczeństwa zasobów SIO rozumiany jest jako możliwość uaktywnienia przez służbę bezpieczeństwa właściwego zbioru zabezpieczeń w systemie informacyjnym organizacji. 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.

---

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

[10] Atrybut bezpieczeństwa informacji – tutaj: poufność, niezaprzeczalność, dostępność, integralność, rozliczalność, niezawodność.

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

2. Model służby bezpieczeństwa

W literaturze fachowej nie znaleziono definicji służby bezpieczeństwa do ochrony informacji w organizacji. Następująca definicja najbardziej odpowiada wymogom niniejszego artykułu:

Służba bezpieczeństwa to część całościowego systemu zarządzania bezpieczeństwem informacji o celowo zorientowanym działaniu, odnosząca się do projektowania, monitorowania i utrzymywania pożądanego zbioru zabezpieczeń o charakterze technicznym i organizacyjnym, na podstawie których można wygenerować pożądaną konfigurację bezpieczeństwa, zapewniającą utrzymanie akceptowalnego poziom bezpieczeństwa organizacji.

Służba bezpieczeństwa zawiera strukturę organizacyjną, planowane działania, zakresy odpowiedzialności i narzędzia pracy umożliwiające sterowanie bieżącym poziomem bezpieczeństwa zarówno całej organizacji, jak i jej elementów składowych.

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

$$\mathrm{SB} = <C, STO, NP>, \tag{1}$$

gdzie:
C – cel działania służby bezpieczeństwa,
STO – struktura organizacyjna służby bezpieczeństwa, przy czym:
NP – zbiór narzędzi pracy stanowiących wyposażenie stanowisk pracy podmiotu działania.

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

2.1. Struktura organizacyjna służby bezpieczeństwa

Jako model struktury organizacyjnej przyjmujemy uporządkowaną parę:

$$STO = <E, R> \tag{2}$$

gdzie:
E – skończony zbiór elementów struktury $\{e_j;\ j \in J\}$,
R – skończony zbiór relacji $\{R_i;\ i \in I\}$ określonych na zbiorze E, przy czym: $J = \{1, 2, 3, \ldots, J\}$ – zbiór indeksów zbioru E, zaś $I = \{1, 2, 3, \ldots, \mathrm{I}\}$ – zbiór indeksów zbioru R.

Zbiór E opisujący skład służby bezpieczeństwa spełnia warunek

$$. \; E = \left\{ ej : \xi\left(j,q\right), j \in J, q \in Q^j \right\}. \tag{3}$$

Wielkość $\xi(j, q)$ interpretujemy, jako następującą formułę zdaniową:
„Element o numerze $j \in J$ charakteryzuje cecha o numerze $q \in Q^j$, gdzie Q^j jest zbiorem indeksów zbioru C^j cech elementu o numerze j".

Zbiór E elementów można zdekomponować następująco:

$$E = E^{PS} \cup E^{PP} \cup E^{OT} \tag{4}$$

gdzie:
E^{PS} – zbiór elementów podsystemu sterowania właściwościami bezpieczeństwa wydzielonych obszarów przetwarzania,
E^{PP} – zbiór elementów tworzących obszary przetwarzania (podsystem przetwarzania informacji),
E^{OT} – zbiór elementów stanowiących środowisko zewnętrzne i wewnętrzne – otoczenie podsystemu przetwarzania informacji.

W zbiorach E^{PS} elementów podsystemu sterowania właściwościami obszarów bezpieczeństwa oraz E^{PP} elementów przetwarzania informacji można wyróżnić następujące składniki funkcjonalne:

$$E^{PS} = E^{PS}_{PD} \cup E^{PS}_{PR} \cup E^{PS}_{OT} \tag{5}$$

$$E^{PP} = E^{PP}_{PD} \cup E^{PP}_{PR} \cup E^{PP}_{OT} \tag{6}$$

gdzie:
E^{PS}_{PD} – zbiór elementów podsystemu sterowania, stanowiących podmiot decydowania,
E^{PS}_{PR} – zbiór elementów podsystemu sterowania, stanowiących jego przedmiot,
E^{PS}_{OT} – zbiór elementów podsystemu sterowania, stanowiących otoczenie jego podmiotu i przedmiotu,
E^{PP}_{PD} – zbiór elementów podsystemu przetwarzania informacji, stanowiących jego podmiot przetwarzania,
E^{PP}_{PR} – zbiór elementów podsystemu przetwarzania informacji, stanowiących jego przedmiot,
E^{PP}_{OT} – zbiór elementów podsystemu przetwarzania informacji, stanowiących otoczenie jego podmiotu i przedmiotu.

Zbior R relacji określony na zbiorze E można zdekomponować następująco:

$$R = R^{PS} \cup R^{PP} \cup R^{SP} \tag{7}$$

gdzie:
$R^{PS} \subset E^{PS} \times E^{PS}$ – zbiór relacji pomiędzy elementami podsystemu sterowania poziomem bezpieczeństwa, zapewniających określone jego działanie,
$R^{PP} \subset E^{PP} \times E^{PP}$ – zbiór relacji pomiędzy elementami podsystemu przetwarzania informacji, zapewniających określone jego działanie,
$R^{SP} \subset E^{PS} \times E^{PP}$ – zbiór relacji pomiędzy elementami systemu sterowania i podsystemu przetwarzania informacji.

2.1.1. Podmiot działania

Z punktu widzenia sterowania bieżącym poziomem bezpieczeństwa informacji, podmiotem działania jest zbiór osób funkcyjnych[12], powołanych w ramach struktury służby bezpieczeństwa lub istniejącego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) danej organizacji, zwanych dalej podmiotem decydowania.

Wprowadźmy następujące oznaczenia:
SF – zbiór uporządkowanych czwórek:

$$, sf_p = < O_p, P_p, PO_p, MB_p > \in \Theta \times 2^P \times 2^{PO} \times 2^{MB} \tag{8}$$

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 (np. inspektor bezpieczeństwa, specjalista ds. bezpieczeństwa, LABI, AS, itp.); zbiór tych osób jest ustalony na etapie projektowania struktury służby bezpieczeństwa lub SZBI;
P – zbiór obiektów przetwarzania informacji tworzących SIO, których właścicielami są osoby funkcyjne i w stosunku do których powinny one utrzymywać wymagany poziom bezpieczeństwa;
PO – zbiór operacji przetwarzania informacji lub procesów ochronnych wykorzystujących odpowiednie metody i techniki ochronne o charakterze technicznym

[12] Np. AD – administrator danych, SOD – specjalista ochrony danych, LABI – lokalny administrator bezpieczeństwa informacji, ASI – administrator systemu informatycznego itp.

lub organizacyjnym, których właścicielami są osoby funkcyjne wyróżnionych stanowisk pracy; procesy ochronne wspierają operacje przetwarzania informacji SIO w zakresie bezpieczeństwa oraz wpływają na ciągłość działania procesów biznesowych organizacji,
MB – zbiór środków lub mechanizmów bezpieczeństwa będących w dyspozycji osób funkcyjnych i stanowiących wyposażenie ich stanowisk pracy.

Każda operacja przetwarzania informacji $po_p \in PO$ zdefiniowana jest następująco:

$$po_p = \left\langle r_p \ , \ \propto_p^{PO}, KZI_p, PP_p \ , MTO_p \ , ZTO_p \right\rangle, \tag{9}$$

gdzie:
r_p – rodzaj *p*-tej operacji przetwarzania,
$\propto_p^{PO}$ – cel przetwarzania,
KZI_p – kategoria zasobu informacyjnego, w stosunku do którego operacja ma zastosowanie,
PP_p – podstawa prawna wykonania operacji przetwarzania,
MTO_p – zbiór metod ochronnych do wykonania *p*-tej operacji przetwarzania,
ZTO_p – zbiór technik ochronnych do wykonania *p*-tej operacji przetwarzania.

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

$$mb_p = \left\langle ch_p \ , \ \propto_p^{MB}, ZF_p, ZPZ_p \ ZP_p \right\rangle, \tag{10}$$

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,
ZPZ_p – zbiór potencjalnych zagrożeń możliwych do wyeliminowania przez zastosowanie tego mechanizmu,
ZP_p – zbiór podatności *p*-tego mechanizmu bezpieczeństwa.

Dodatkowo wprowadźmy następujące oznaczenia:
$\hat{U}$ – zbiór dopuszczalnych wielkości sterujących, za pomocą których podmiot decydowania może ustalać bieżące właściwości następujących elementów:
- operacji przetwarzania,
- obszarów przetwarzania lub obiektów chronionych w tych obszarach (np. zasobów informacyjnych, danych osobowych itp.)
- mechanizmów bezpieczeństwa,
- stanowisk pracy;

V_u – zbiór odpowiadających tym sterowaniom par:

$$\langle p,\ q\rangle \in \hat{P}^k\hat{Q}^k\ ,\ \overline{k=1,4}, \tag{10}$$

gdzie:
$\hat{P}^k$ – zbiór numerów wyróżnionych odpowiednio dla: $k = 1$ – operacji przetwarzania, $k = 2$ – obszarów przetwarzania, $k = 3$ – mechanizmów bezpieczeństwa, $k = 4$ – stanowisk pracy,
$\hat{Q}^k$ – zbiór numerów wyróżnionych, odpowiednio dla: $k = 1$ – operacji przetwarzania, $k = 2$ – obszarów przetwarzania, $k = 3$ – mechanizmów bezpieczeństwa, $k = 4$ – stanowisk pracy,
$\hat{S}^k$ – wektor stanów wyróżnionych elementów, którego współrzędne określają stany poszczególnych elementów odpowiednio dla: $k = 1$ – operacji przetwarzania, $k = 2$ – obszarów przetwarzania, $k = 3$ – 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:

$$s_p = \left\langle a_p^q\ \in A_p^q\ :\ p \in \hat{P},\ q \in \hat{Q}\right\rangle \tag{11}$$

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:

$$\bigwedge_{\langle p,q\rangle \in \hat{P}^k\hat{Q}^k} a_p^q = a_p^q\left[u(t)\right],\ u \in U,\ \overline{k=1,4}. \tag{12}$$

W rezultacie zbiór sterowalnych:

a) na stan operacji przetwarzania można zdefiniować następująco:

$$\widehat{PO} = \left\{po_p\ \in\ PO\ :\ \bigvee_{q\in\hat{Q}}\left[\ \langle p,q\rangle \in V_u\ \right],\ p \in \hat{P}^1\right\}, \tag{13}$$

b) na stan obszarów przetwarzania można zdefiniować następująco:

$$\widehat{OB} = \left\{ob_p\ \ POB\ :\ \bigvee_{q\in\hat{Q}}\left[\ \langle p,q\rangle \in V_u\ \right],\ p \in \hat{P}^2\right\}, \tag{14}$$

c) na stan mechanizmów bezpieczeństwa, można zdefiniować następująco:

$$\widehat{MB} = \left\{mb_p\ \in\ MB\ :\ \bigvee_{q\in\hat{Q}}\left[\ \langle p,q\rangle \in V_u\ \right],\ p \in \hat{P}^3\right\}, \tag{15}$$

d) na stan stanowisk pracy, można zdefiniować następująco:

$$\widehat{SF} = \left\{ sf_p \in SF : \bigvee_{q \in \hat{Q}} \left[\langle p,q \rangle \in V_u \right], p \in \hat{P}^4 \right\}. \tag{16}$$

Na zbiorze sterowalnych operacji przetwarzania lub obszarów przetwarzania, lub mechanizmów bezpieczeństwa, lub stanowisk pracy określa się cel $\propto^{SB}$ działania służby bezpieczeństwa.

2.1.2. Przedmiot działania

Z punktu widzenia sterowania bieżącym poziomem bezpieczeństwa informacji przedmiotem działania jest zbiór takich elementów $e_j \in E^{SIO}$, obszarów przetwarzania lub systemu informacyjnego organizacji (SIO), których stan pożądany może ustalać podmiot decydowania – służba. Elementami zbioru E^{SIO} mogą być[13]:

- kluczowe procesy biznesowe,
- procesy przetwarzania informacji,
- obszary przetwarzania,
- 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.

Wprowadźmy następujące oznaczenia:

D – zbiór decyzji sterujących, zwanych dalej dyrektywami, za pomocą których osoby funkcyjne ze swoich stanowisk pracy mogą ustalać właściwości bezpieczeństwa elementów SIO lub zasobów informacyjnych;

V_D – zbiór odpowiadających tym sterowaniom par:

$$\langle p,\ q \rangle \in P^{sio} Q^{SIO}, \tag{17}$$

[13] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.

gdzie:
$a^p(t) = \langle a_q^p(t) \in \ddot{A}_p^q : p \in P^{SIO},\ q \in Q^Z \rangle$ – zbiór numerów wyróżnionych zasobów informacyjnych,
$a^p(t) = \langle a_q^p(t) \in \ddot{A}_p^q : p \in P^{SIO},\ q \in Q^Z \rangle$ – zbiór numerów wyróżnionych cech zasobów informacyjnych,
$a^p(t) = \langle a_q^p(t) \in \ddot{A}_p^q : p \in P^{SIO},\ q \in Q^Z \rangle$ – 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:

$$a^p(t) = \langle a_q^p(t) \in \ddot{A}_p^q : p \in P^{SIO},\ q \in Q^Z \rangle \tag{18}$$

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:

$$\bigwedge_{\langle p,q \rangle \in P^{SIO} Q^{SIO}} a_p^q(t) = a_p^q[d(t)],\ d \in D. \tag{19}$$

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

$$OB = ZI = \left\{ zi_p \in E^{SIO} : \bigvee_{q \in Q^{SIO}} [\langle p,q \rangle \in V_D],\ p \in P^{SIO} \right\}. \tag{20}$$

Podsumowując: w dalszej części rozważań niniejszego artykułu przedmiotem działania dla służb bezpieczeństwa są zasoby informacyjne przetwarzane w ramach SIO.

2.2. Cel działania służby bezpieczeństwa

Działanie służby bezpieczeństwa można zdefiniować:

1) w odniesieniu do sterowania właściwościami bezpieczeństwa zasobów informacyjnych SIO jako uporządkowaną parę:

$$DZ^{SIO} = \langle \propto^{SIO},\ Z^{SIO} \rangle, \tag{21}$$

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 uporządkowaną parę:

$$DZ^{SF} = \left\langle \propto^{SF}, Z^{SF} \right\rangle, \tag{22}$$

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,

$[t_0^p, \dot{T}^p]$ – 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 $[t_0^p, \dot{T}^p]$, 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 $t \in [t_0^p, \dot{T}^p]$ należą do tych podzbiorów $\propto_p^q (w)$, to mówimy, że obiekt o numerze $p \in \dot{P}(t)$ posiada własność w.

Przyjmując, że 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:

$$\propto^{SB} \equiv \propto^{SIO} \left\{ \dot{\propto}_p^q : \langle p,q \rangle \in V_D \ , p \in \dot{P}(t), \ q \in Q^{SIO} \right\}. \tag{24}$$

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

$$z_p = \left\langle b_p,\ O_p^b,\ w_p^b,\ Q\left(w_p^b\right), \dot{\propto}\left(w_p^b\right),\ R_p^b > \right\rangle \tag{25}$$

gdzie:
b_p – typ p-tego zasobu informacyjnego,

O_p^b – osoba funkcyjna będąca właścicielem p-tego zasobu informacyjnego b-tego typu,
w_p^b – właściwość bezpieczeństwa p-tego zasobu informacyjnego b-tego typu,

$Q\left(w_p^b\right)$ – 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. Podsumowanie

Na świecie od dłuższego czasu prowadzone są prace nad standaryzacją i optymalizacją systemów zabezpieczeń aktywów organizacji, w tym zasobów informacyjnych SIO. 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 zapewnienia 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 struktur organizacyjnych służby bezpieczeństwa lub systemów zabezpieczeń w aspekcie zapewniania wymaganego poziomu bezpieczeństwa zasobów informacyjnych SIO. Należy go traktować jako propozycję autorów częściowego rozwiązania problemu ustanawiania i budowy struktury organizacyjnej służby bezpieczeństwa, która umożliwiałby bieżące sterowanie poziomem

bezpieczeństwa systemu informacyjnego organizacji. Zaproponowany sposób podejścia do problematyki utrzymywania wymaganego poziomu bezpieczeństwa, ukierunkowanej na proces rekonfiguracji, wynika między innymi ze spostrzeżeń i kilkuletnich doświadczeń autorów nagromadzonych:

- podczas obserwacji ustanawiania i wdrażania takich struktur organizacyjnych oraz systemów zabezpieczeń w organizacjach,
- w trakcie prowadzenia projektów badawczo-wdrożeniowych,
- w trakcie prac naukowo-badawczych i dyskusji seminaryjnych dotyczących bezpieczeństwa danych osobowych.

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

Bibliografia

ISO/IEC 27004: 2013 Technika informatyczna – Techniki zabezpieczeń – Zarządzanie bezpieczeństwem informacji – pomiary.

Kiedrowicz M., *Multi-faceted Methodology of the Risk Analysis and Management Referring to the IT System Supporting the Processing of Documents at Different Levels of Sensitivity*, MATEC Web of Conferences, vol. 125(2017).

Liderman K., *Bezpieczeństwo informacyjne*, PWN, Warszawa 2012.

Polaczek T., *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice 2014.

Stanik J., *System Risk Model of the IT System Supporting the Processing of Documents at Different Levels of Sensitivity*, MATEC Web of Conferences 2017, vol. 125.

Stanik J., Hoffmann R., Napiórkowski J., *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2016, nr 123, s. 321–336.

Stanik J., Kiedrowicz M., *Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych*, 01/2017, 126, s. 339–354, DOI:10.18276/epu.2017.126/1–33.

Stanik J., Kiedrowicz M., *Models and Method for the Risk Assessment of an Intellectual Resource*, WSEAS Transactions on Information Science and Applications 09/2017; 14(2017), s. 174–183.

Stanik J., Kiedrowicz M., *Method for Assessing Efficiency of the Information Security Management System*, MATEC Web of Conferences 2018, vol. 210.

Stanik J., Kiedrowicz M., Waszkowski R., *Security and Risk as a Primary Feature of the Production Process*, Intelligent Systems in Production Engineering and Maintenance, s. 701–709, Springer 2019; DOI:10.1007/978–3–319–97490-3_66.

Źródła sieciowe

http://www.zut.edu.pl/fileadmin/pliki/abi/9/RYZYKO_ODO-1.pdf (dostęp: 21.08.2018).
http://www.zut.edu.pl/fileadmin/pliki/abi/9/RYZYKO_ODO-2.pdf (dostęp: 21.08.2018).

* * *

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

Abstract

The article presents the concept of a security service model for the needs of maintaining the required level of information security of an organization's information resources. The model of the security service was defined and its basic elements were characterized, such as: the objective of the security service, the organizational structure and the subject of action.

Keywords: security service, structure of security service, subject and object of operation of the security service