Biuletyn WAT
Vol. LXII, Nr 1, 2013

Utrzymywanie wymaganego poziomu bezpieczeństwa platformy integracyjnej

JERZY STANIK

Wojskowa Akademia Techniczna, Wydział Cybernetyki,
Instytut Systemów Informatycznych, Zakład Informatycznych Systemów Zarządzania,
00-908 Warszawa, ul. S. Kaliskiego 2, jstanik@wat.edu.pl

Streszczenie. W artykule przedstawiono koncepcję utrzymywania wymaganego poziomu bezpieczeństwa platformy integracyjnej (PI). Wyróżniono i scharakteryzowano podstawowe elementy PI z punktu widzenia sterowania jej bieżącym poziomem bezpieczeństwa. Zaproponowano model platformy integracyjnej dla potrzeb utrzymania wymaganego poziomu bezpieczeństwa. Pożądaną bieżącą właściwość bezpieczeństwa PI uzyskuje się poprzez wygenerowanie odpowiedniej konfiguracji bezpieczeństwa PI ze zbioru rozwiązań dopuszczalnych. Zaproponowana koncepcja zapewniania bezpieczeństwa, uwzględniająca wpływ nie tylko bezpieczeństwa zasobów informacyjnych, lecz także zmian uwarunkowań pracy zarówno platformy integracyjnej (PI), systemu informacyjnego korporacji, jak i całej korporacji, stanowi własną propozycję autora.
Słowa kluczowe: bezpieczeństwo, system zarządzania bezpieczeństwem informacji, konfiguracja bezpieczeństwa, analiza ryzyka, platforma integracyjna

Wprowadzenie

Obserwowany w ostatnich latach szybki rozwój architektur korporacyjnych i platform integracyjnych (PI) wyprzedza w znacznym stopniu wiedzę na temat jakości i bezpieczeństwa przetwarzania informacji w takich systemach. Daje się również zauważyć brak formalnych i komercyjnych modeli systemów zarządzania bezpieczeństwem informacji (SZBI) oraz ogólnych metod formułowania i rozwiązywania zadań sterowania bieżącymi właściwościami użytkowymi w tych systemach, mających na celu utrzymanie wymaganego poziomu bezpieczeństwa informacji. Trudności zaproponowania receptury zarządzania bezpieczeństwem informacji

i zasad sterowania bieżącym poziomem bezpieczeństwa przede wszystkim wynikają ze specyficznych właściwości platform integracyjnych, które dziś stanowią podstawowe wyposażenie korporacji.

Spośród wielu definicji w teorii platform integracyjnych następująca definicja z [3] najbardziej odpowiada wymogom niniejszego artykułu: „Platforma integracyjna jest to zbiór powiązanych ze sobą elementów, którego celem jest stworzenie środowiska do współpracy systemów informatycznych w celu realizacji funkcji i/lub usług zlecanych przez użytkowników tych systemów".

W następstwie powyższej definicji PI nazywać będziemy uporządkowaną parę:

$$\mathrm{PI} = \langle E, R \rangle, \tag{1}$$

gdzie: E — skończony zbiór elementów PI;
R — skończony zbiór relacji określonych na zbiorze E.

Zbiór E opisujący skład platformy integracyjnej spełnia następujący warunek

$$E = \left\{ e_j : \xi(j,q), j \in J, q \in Q^j \right\}. \tag{2}$$

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".

Do zbioru specyficznych cech i właściwości PI można między innymi zaliczyć:

1) dynamiczne poszerzanie zakresu świadczonych usług zgodnie z faktycznymi potrzebami;
2) występowanie zmiennych i skomplikowanych sytuacji w pojawianiu się różnego typu zagrożeń i podatności zasobów informacyjnych przetwarzanych w ramach PI, implikowanych losowym strumieniem napływu z otoczenia zapotrzebowań na świadczenie różnego typu usług;
3) brak odpowiednich mechanizmów zapewniających bezpieczeństwo i interoperacyjność;
4) brak jednoznacznych kryteriów oceny bezpieczeństwa i interoperacyjności oraz sposobu ich pomiaru;
5) brak komercyjnych dostępnych metodyk projektowania i wdrażania SZBI dla korporacji.

Prawidłowa organizacja przetwarzania informacji i utrzymanie wymaganego poziomu bezpieczeństwa platform integracyjnych stanowią przedmiot zainteresowania zarówno kierownictwa korporacji jak i projektantów tych systemów.

Zdaniem autora wymagany poziom bezpieczeństwa informacji w ramach platformy integracyjnej można osiągnąć poprzez podejmowanie właściwych decyzji sterujących (zarządczych) inicjujących generowanie odpowiednich konfiguracji bezpieczeństwa PI.

W zależności od poziomu abstrakcji, z jakim patrzymy na architekturę PI, możemy wyróżniać i opisywać różne typy konfiguracji bezpieczeństwa. Przykładowo, przyjmując za kryterium podziału warstwowe ujęcie PI, można wyróżnić następujące konfiguracje bezpieczeństwa:

1) zasobowa konfiguracja bezpieczeństwa;
2) usługowa konfiguracja bezpieczeństwa;
3) kompozytowa konfiguracja bezpieczeństwa;
4) procesowa konfiguracja bezpieczeństwa;
5) biznesowa konfiguracja bezpieczeństwa;
6) platformowa konfiguracja bezpieczeństwa.

Uwzględniając różne typy zasobów i/lub aktywów platformy integracyjnej, a mianowicie:

1) informacje: bazy danych i pliki z danymi, kontrakty i umowy, dokumentacje systemowe, informacje badawcze, podręczniki użytkownika, materiały szkoleniowe, procedury operacyjne i wspierające, plany ciągłości działania, plany odtworzeniowe, ślady audytowe oraz informacje zarchiwizowane;
2) oprogramowanie: aplikacje, oprogramowanie systemowe, narzędzia rozwojowe i inne;
3) aktywa fizyczne: sprzęt komputerowy, urządzenia komunikacyjne, nośniki wymienne i inne urządzenia;
4) usługi: usługi przetwarzania i przesyłania, usługi ogólne: np. ogrzewanie, oświetlenie, zasilanie i klimatyzacja;
5) ludzie, ich kwalifikacje, umiejętności i doświadczenie;
6) wartości niematerialne, takie jak reputacja oraz wizerunek organizacji,

można wyróżniać „elementarne" lub „atomowe" konfiguracje bezpieczeństwa w danej grupie zasobów PI. W dalszej części pracy prowadzone rozważania zostały ograniczone tylko do *zasobów informacyjnych* i *zasobowych konfiguracji bezpieczeństwa.*

1. Model platformy integracyjnej dla potrzeb utrzymywania wymaganego poziomu bezpieczeństwa

Jako model platformy integracyjnej dla potrzeb sterowania i utrzymywania wymaganego poziomu bezpieczeństwa przyjęto uporządkowaną piątkę:

$$\langle PI, OB, KB, DS, FR \rangle, \tag{3}$$

gdzie: *PI* — platforma integracyjna traktowana jako obiekt chroniony;
OB — otoczenie platformy integracyjnej rozumiane jako środowisko bezpieczeństwa, zapewniające platformie utrzymywanie wymaganego

poziomu bezpieczeństwa; obecnie najpopularniejszym rozwiązaniem tego typu jest system zarządzania bezpieczeństwem informacji (SZBI);
KB — rodzina dopuszczalnych konfiguracji bezpieczeństwa;
DS — zbiór dopuszczalnych decyzji sterujących, zwanych dalej dyrektywami, przy pomocy których osoby z zespołu do spraw bezpieczeństwa korporacji mogą ustalać bieżące właściwości konfiguracji bezpieczeństwa;
FR — funkcja rekonfiguracji; odwzorowanie to wyznacza się na etapie projektowania PI, aby zapewniło ono uzyskiwanie pożądanego poziomu bezpieczeństwa. Pożądany poziom bezpieczeństwa można uzyskać poprzez wygenerowanie odpowiedniej konfiguracji bezpieczeństwa PI ze zbioru rozwiązań dopuszczalnych właściwości konfiguracji bezpieczeństwa.

Zbiór elementów *E* platformy integracyjnej można dekomponować następująco:

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

gdzie: E^{PP} — zbiór elementów podsystemu przetwarzania zasobów informacyjnych;
E^{OT} — zbiór elementów stanowiących otoczenie podsystemu sterowania poziomem bezpieczeństwa i podsystemu przetwarzania zasobów informacyjnych.

Zbiór *R* relacji określony na zbiorze *E* można dekomponować następująco:

$$R = R^{PP} \cup R^{SP}, \tag{5}$$

gdzie: $R^{PP} \subset E^{PP} \times E^{PP}$ — zbiór relacji pomiędzy elementami podsystemu przetwarzania zasobów informacyjnych zapewniających określone jego działanie;
$RS^{SP} \subset E^{PS} \times E^{PP}$ — zbiór relacji pomiędzy elementami otoczenia podsystemu przetwarzania zasobów informacyjnych i podsystemu przetwarzania zasobów informacyjnych.

Działanie platformy integracyjnej można zdefiniować następująco:

1. W odniesieniu do podsystemu przetwarzania informacji — jako uporządkowana para:

$$DZ^{PP} = \langle \alpha^{PP}, Z^{PP} \rangle, \tag{6}$$

gdzie: E^{PP} — cel działania podsystemu sterowania;
Z^{PP} — zbiór zadań (sterowań) zapewniających osiągnięcie celu α^{PP}.

2. W odniesieniu do otoczenia podsystemu przetwarzania informacji — jako uporządkowana para:

$$DZ^{OP} = \langle \alpha^{OP}, Z^{OP} \rangle, \tag{7}$$

gdzie: α^{OP} — cel działania podsystemu sterowania;
Z^{OP} — zbiór zadań (sterowań) zapewniających osiągnięcie celu α^{OP}.

Otoczenie platformy integracyjnej rozumiane jest jako środowisko bezpieczeństwa PI, które stanowią następujące elementy:

1) podsystem sterowania poziomem bezpieczeństwa;
2) podsystem inwentaryzacji zasobów;
3) podsystem analizy zagrożeń i oceny ryzyka;
4) podsystem projektowania i obsługi zabezpieczeń.

Możliwość podejmowania decyzji sterujących warunkuje istnienie w otoczeniu PI — środowisku bezpieczeństwa PI następujących elementów:

1) podsystemu sterowania zarówno właściwościami użytkowymi platformy integracyjnej, jak i właściwościami bezpieczeństwa platformy integracyjnej;
2) podsystemu analizy i oceny ryzyka, dostarczającego podsystemu sterowania, informacji o możliwości realizacji zagrożenia bezpieczeństwa informacji przetwarzanej w ramach platformy integracyjnej, wyrażonej w postaci bieżącej wartości ryzyka rezydualnego (szczątkowego) i/lub bieżących wartości atrybutów bezpieczeństwa informacji, platformy integracyjnej, korporacji;
3) podsystemu projektowania, wdrażania i obsługiwania zabezpieczeń.

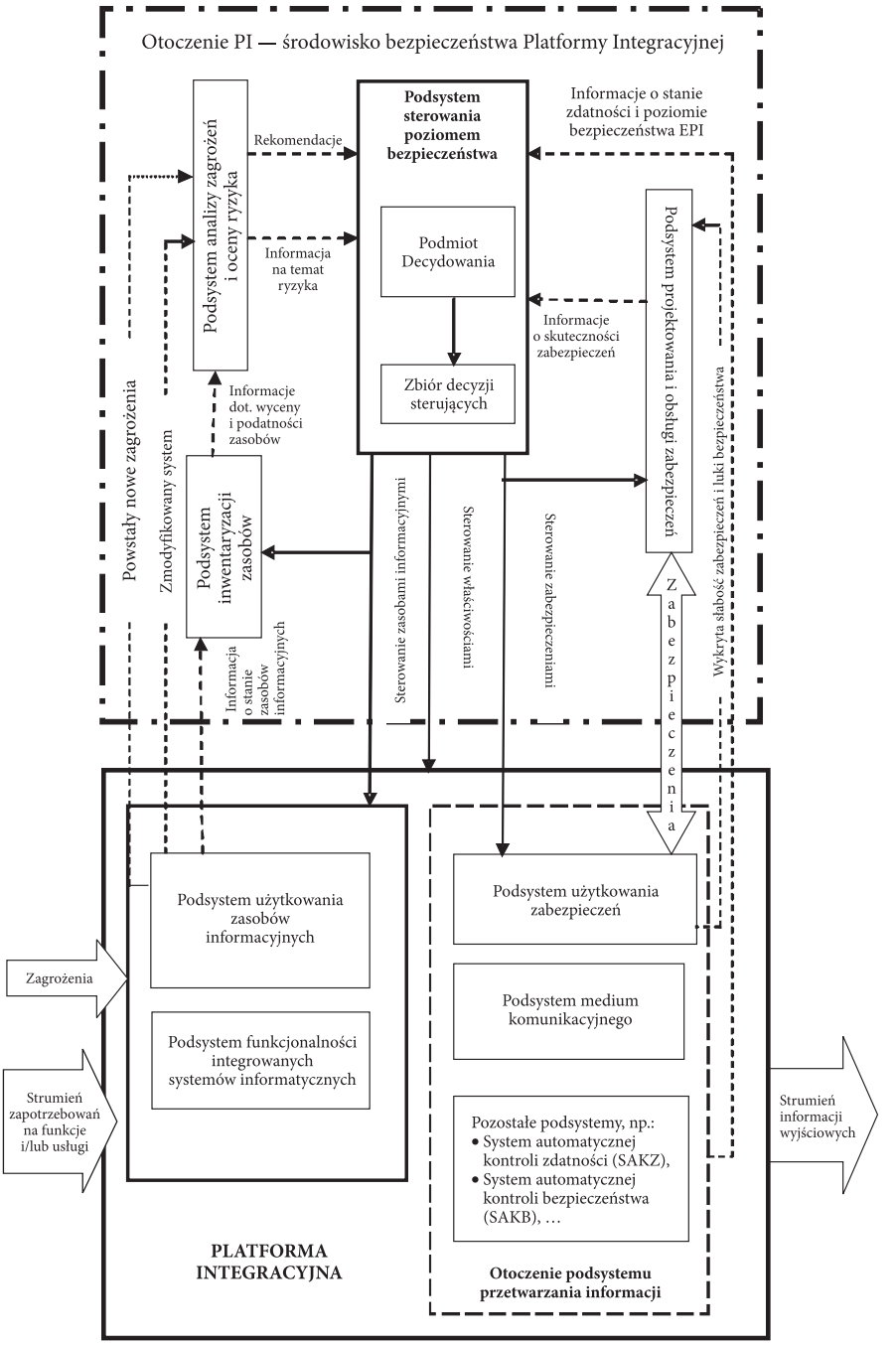
Graficzną ilustrację PI, z punktu widzenia sterowania jej bieżącym poziomem bezpieczeństwa, przedstawiono na rysunku 1.

Pod pojęciem konfiguracji bezpieczeństwa rozumie się odpowiednio zaprojektowany i zaimplementowany zbiór mechanizmów bezpieczeństwa o ściśle określonych funkcjach bezpieczeństwa. Każda funkcja bezpieczeństwa jest precyzyjnie pełniona w ściśle określonych warunkach realnego zagrożenia, podatności i w określonym czasie w środowisku PI. Od precyzji tego działania zależy bezpieczeństwo zasobów informacyjnych, a w następstwie bezpieczeństwo PI.

Zbiór potencjalnych konfiguracji bezpieczeństwa PI można zdefiniować następująco:

$$\left\{ KB_p = \left\langle zi_p, AB_p, MB_p \right\rangle ; p \in P \right\}, \tag{8}$$

gdzie: KB_p — konfiguracja bezpieczeństwa dla p-tego zasobu informacyjnego;
$zi_p \in ZI$ — p-ty zasób informacyjny;
$AB_p \in 2^{AB}$ — zbiór atrybutów bezpieczeństwa przypisanych do p-tego zasobu informacyjnego;
$MB_p \in 2^{MB}$ — zbiór mechanizmów bezpieczeństwa tworzących p-tą konfigurację bezpieczeństwa.



Rys. 1. Ilustracja PI z punktu widzenia sterowania poziomem bezpieczeństwa. Źródło: opracowanie własne

W celu stworzenia możliwości kompensacji utraty wymaganego poziomu bezpieczeństwa, wymagane jest określenie na etapie projektowania PI zbioru dopuszczalnych decyzji sterujących, zwanych dalej dyrektywami, przy pomocy których osoby z zespołu do spraw bezpieczeństwa korporacji mogą ustalać takie bieżące właściwości konfiguracji bezpieczeństwa, które zapewniają osiągnięcie wymaganego poziomu bezpieczeństwa PI.

2. Charakterystyka wybranych podsystemów

2.1. Podsystemy platformy integracyjnej

Specyfiką podsystemu przetwarzania informacji jest fakt, że wszystkie czynności fizyczne dotyczą operacji na informacjach, których źródłem są integrowane systemy informatyczne.

Zakłada się, że do zbioru Z^{PP} zadań realizowanych przez platformę zalicza się:

1) sterowanie przepływem komunikatów pomiędzy integrowanymi systemami informatycznymi według ustalonych „tras";
2) przechowywanie i kolejkowanie komunikatów w przypadku chwilowej niedostępności docelowego sytemu informatycznego;
3) zadania zbierania, przechowywania i udostępniania informacji, zgodnie z potrzebami użytkownika, w sposób automatyczny, za pomocą urządzeń informatyki;
4) zadania przetwarzania informacji, zgodnie z opracowaną logiką PI i przyjętymi regułami technologicznymi.

W dalszej części pracy rozważania zostały ograniczone tylko do dwóch podsystemów, a mianowicie:

1) podsystemu użytkowania zasobów informacyjnych;
2) podsystemu użytkowania zabezpieczeń.

2.1.1. Podsystem użytkowania zasobów informacyjnych

Z punktu widzenia procesu przetwarzania zasobów informacyjnych podmiotem działania w PI jest zbiór stanowisk pracy — stanowiska pracy użytkowników końcowych, zaś przedmiotem zbiór takich elementów $e_j \in E^{\mathrm{PI}}$, na których określony jest cel działania podsystemu przetwarzania informacji.

Elementami zbioru E^{PI} są porcje informacji odebrane przez podsystem przetwarzania informacji (rys. 1). Porcje te charakteryzują zapotrzebowania na aplikacje lub usługi zlecane przez użytkowników platformy integracyjnej. Są one automatycznie uformowane według określonych standardów przez oprogramowanie zapewniające komunikację systemów informatycznych i podlegają dalszemu przetwarzaniu.

Każdą porcję informacji, stanowiącą zasób informacyjny, oznacza się numerem $p \in P^{PI}$ i opisuje się ją zbiorem C_p^{PI} nazw cech.

Jeżeli wszystkie różniące się zbiory cech, jakimi są opisane poszczególne zasoby informacyjne, ponumerujemy zmienną $b = \overline{1,B}$ (którą nazwiemy typem zasobu informacyjnego), to dwa zasoby są tego samego typu (np. „b"), gdy opisują je identyczne zbiory cech. Zbiory Ω_p^{PI} numerów cech, opisujących zasób i odpowiadające im zbiory nazw cech C_p^{PI}, nie mogą być puste dla każdego $p \in P^{PI}$, gdzie P^{PI} jest zbiorem numerów wyróżnionych zasobów informacyjnych. Zakładamy, że dla każdej cechy $\omega \in \Omega^{PI}$ jest określony zbiór A_ω^{PI} możliwych realizacji α_ω cechy.

Zakłada się, że celem działania podsystemu użytkowania zasobów informacyjnych jest uzyskanie zasobów informacyjnych o pożądanych właściwościach użytkowych. Są to informacje wyjściowe o charakterze usługowym. Usługi świadczone są na rzecz użytkowników platformy — integrowanych systemów informatycznych.

Elementami podsystemu przetwarzania informacji, w ramach platformy integracyjnej, są uaktywnione porcje informacji o numerach $p \in P(t)$, zwane również zasobami informacyjnymi. Relacje zachodzące między uaktywnionymi zasobami informacyjnymi tworzą różne konfiguracje funkcjonalne.

Celem działania podsystemu przetwarzania informacji jest nadawanie zasobom informacyjnym w przedziale czasu ΔT_p pożądanych stanów α_p. Oczywiście stan początkowy α_p^0 w chwili $t_0 < t$ jest różny od pożądanego. W celu osiągnięcia stanu pożądanego, w PI musi istnieć możliwość realizacji procesu przetwarzania informacji przeprowadzającego ich stan z α_p^0 do stanu $\overset{*}{\alpha}_p$.

Załóżmy, że na etapie projektowania PI określony został wzorcowy proces bezpiecznego przetwarzania informacji, obejmujący wszystkie możliwe typy zasobów informacyjnych należące do zbioru *P*. Z punktu widzenia poszczególnych typów zasobów można dokonać podziału tego procesu na poszczególne typy i związane z nimi cele.

Poszczególne typy procesów ponumerowane są zmienną $b = \overline{1,B}$. Każdy typ procesu, określony parą $\langle a^b, t \rangle$, scharakteryzowany jest stanem początkowym i końcowym.

Analizując procesy przetwarzania bieżących zasobów informacyjnych na tle wzorcowych typów procesów, dla każdego typu zasobu informacyjnego możemy określić zbiór procesów etapowych oraz związanych z nimi celów cząstkowych i wzorcowych konfiguracji bezpieczeństwa.

Procesy składowe należy wykonać w ustalonym porządku, aby osiągnąć:

a) stan pożądany z informacyjnego i/lub funkcjonalnego punktu widzenia,
b) ustalony poziom bezpieczeństwa zasobu informacyjnego.

Jeżeli założymy, że dla każdego zasobu informacyjnego typu $b \in B$ ustalony jest początkowy i końcowy numer etapu procesu typu *b*, oraz przyjmując, że osiągnięcie celu cząstkowego o wyższym numerze jest uwarunkowane osiągnięciem celu

o numerze niższym, to dla każdego typu zasobu informacyjnego można określić ciąg numerów etapów procesu typu *b* i odpowiadający mu ciąg wzorcowych konfiguracji bezpieczeństwa, których wykonanie zapewnia osiągnięcie zamierzonego celu w aspekcie funkcjonalnym i bezpieczeństwa. Z punku widzenia sterowania bezpieczeństwem postać ciągu (np. dla zasobu informacyjnego typu *b*) można zapisać następująco:

$$\mathrm{K}^b = \{1,2,3,4,...K_b\}. \tag{9}$$

W dalszej części opracowania problem generowania właściwych konfiguracji funkcjonalnych nie będzie rozpatrywany, ponieważ wykracza poza ramy tematu i dotyczy problemu utrzymania wymaganego poziomu jakości, a dokładniej bieżącej niezawodności. Dalsze rozważania dotyczą tylko generowania konfiguracji zabezpieczeń.

2.1.3. Podsystem użytkowania zabezpieczeń

Elementami podsystemu użytkowania zabezpieczeń są uaktywnione konfiguracje bezpieczeństwa, które zapewniają wymagany poziom bezpieczeństwa dla przetwarzanych zasobów informacyjnych.

Pod pojęciem konfiguracji bezpieczeństwa rozumie się odpowiednio zaprojektowany i zaimplementowany zbiór mechanizmów bezpieczeństwa o ściśle określonych funkcjach bezpieczeństwa. Każda funkcja bezpieczeństwa jest precyzyjnie pełniona w ściśle określonych warunkach realnego zagrożenia, podatności i określonym czasie w środowisku PI. Od precyzji tego działania zależy bezpieczeństwo zasobów informacyjnych, a w następstwie bezpieczeństwo PI.

Zbiór potencjalnych konfiguracji bezpieczeństwa PI można zdefiniować następująco:

$$\left\{KB_p = \left\langle zi_p, AB_p, MB_p \right\rangle; p \in P\right\}, \tag{10}$$

gdzie: $zi_p \in ZI$ — *p*-ty zasób informacyjny, dla którego została wygenerowana konfiguracja bezpieczeństwa;
$AB_p \in 2^{AB}$ — zbiór atrybutów bezpieczeństwa przypisanych do *p*-tego zasobu informacyjnego;
$MB_p \in 2^{MB}$ — zbiór mechanizmów bezpieczeństwa tworzących *p*-tą konfigurację bezpieczeństwa.

Znając:

— zbiór $ZI(t)$ aktualnie przetwarzanych zasobów informacyjnych w podsystemie przetwarzania informacji,

— zbiory $MB_p(t)$ aktualnie dostępnych mechanizmów bezpieczeństwa dla każdego aktualnie przetwarzanego zasobu informacyjnego,
— bieżące wartości $ab_p^h(t) \in WAB_p^a,\ h \in H, p \in P$ atrybutów bezpieczeństwa dla każdego zasobu informacyjnego,
gdzie:
H — zbiór numerów nazw atrybutów bezpieczeństwa;
WAB_p^h — zbiór dopuszczalnych wartości h-tego atrybutu bezpieczeństwa dla p-tego zasobu informacyjnego,

możemy określić, jaki jest bieżący poziom bezpieczeństwa platformy integracyjnej, a następnie nim sterować.

Wprowadźmy następujące oznaczenia:
D — zbiór dopuszczalnych decyzji sterujących, zwanych dalej dyrektywami, przy pomocy których osoby z Forum Bezpieczeństwa mogą ustalać bieżące właściwości mechanizmów bezpieczeństwa,
V_d — zbiór odpowiadających tym sterowaniom par:

$$\langle k,l \rangle \in K \times L, \tag{11}$$

gdzie: K — zbiór numerów konfiguracji bezpieczeństwa;
L — zbiór numerów wyróżnionych cech konfiguracji bezpieczeństwa;
$\underline{c(t)}$ — wektor stanu wyróżnionych konfiguracji bezpieczeństwa, którego współrzędne określają stany konfiguracji bezpieczeństwa dla poszczególnych zasobów informacyjnych w chwili t.

Pod pojęciem stanu $c^k(t), k \in K$ k-tej konfiguracji bezpieczeństwa rozumie się wektor cech opisujących jego bieżące właściwości bezpieczeństwa:

$$c^k(t) = \left(c_l^k(t) \in C_l^k : k \in K, l \in L\right), \tag{12}$$

gdzie: $c_j^k(t)$ — współrzędne wektora stanu k-tej konfiguracji bezpieczeństwa, wyrażające poszczególne cechy bezpieczeństwa;
C_j^k — zbiór dopuszczalnych realizacji l-tej cechy k-tej konfiguracji bezpieczeństwa;
L — zbiór numerów wyróżnionych cech konfiguracji.

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

$$\bigwedge_{\langle k,l \rangle \in K \times L} c_l^k(t) = c_l^k\left[d(t)\right], d \in D. \tag{13}$$

W rezultacie zbiór konfiguracji bezpieczeństwa, których stan bieżący (a w następstwie bieżące właściwości bezpieczeństwa PI) mogą ustalać osoby z Forum Bezpieczeństwa, można zdefiniować następująco:

$$\overline{KB} = \left\{ kb_k \in KB : \bigvee_{l \in \bar{L}} \left[\langle k, l \rangle \in V_D \right], k \in K \right\}. \tag{14}$$

Z punktu widzenia możliwości sterowania bieżącymi właściwościami bezpieczeństwa PI i przetwarzania w niej zasobów informacyjnych, każdą konfigurację bezpieczeństwa można opisać następująco w sposób rozszerzony:

$$\overline{kb}_k = \left\langle zi_k^p, AB_k^p, MB_k, D_k, rs_k^p \right\rangle, k \in K, p \in P, \tag{15}$$

gdzie: zi_k^p — nazwa *p*-tego zasobu informacyjnego, dla którego powołano *k*-tą konfigurację bezpieczeństwa;
AB_k^p — zbiór atrybutów bezpieczeństwa przypisanych do *p*-tego zasobu informacyjnego, dla którego powołano *k*-tą konfigurację bezpieczeństwa;
MB_k — zbiór mechanizmów bezpieczeństwa wchodzących w skład *k*-tej konfiguracji bezpieczeństwa;
D_k — zbiór decyzji sterujących (dyrektyw) niezbędnych do wygenerowania *k*-tej konfiguracji bezpieczeństwa;
rs_k^p — wartość ryzyka szczątkowego, jaka pozostała dla *p*-tego zasobu informacyjnego po zastosowaniu zbioru MB_k mechanizmów bezpieczeństwa.

Przypomnijmy, że celem działania podsystemu użytkowania zabezpieczeń jest powoływanie w przedziale czasu $\Delta \overset{*}{T}_p$ zbioru konfiguracji o numerach $k \in K(t)$, które zapewniają osiągnięcie wymaganych wartości $ab_p^b(t) \in WAB_p^b$, $b \in B(t), p \in P(t)$ atrybutów bezpieczeństwa dla każdego aktualnie przetwarzanego zasobu informacyjnego.

2.2. Podsystemy środowiska bezpieczeństwa

2.2.1. Podsystem sterowania poziomem bezpieczeństwa

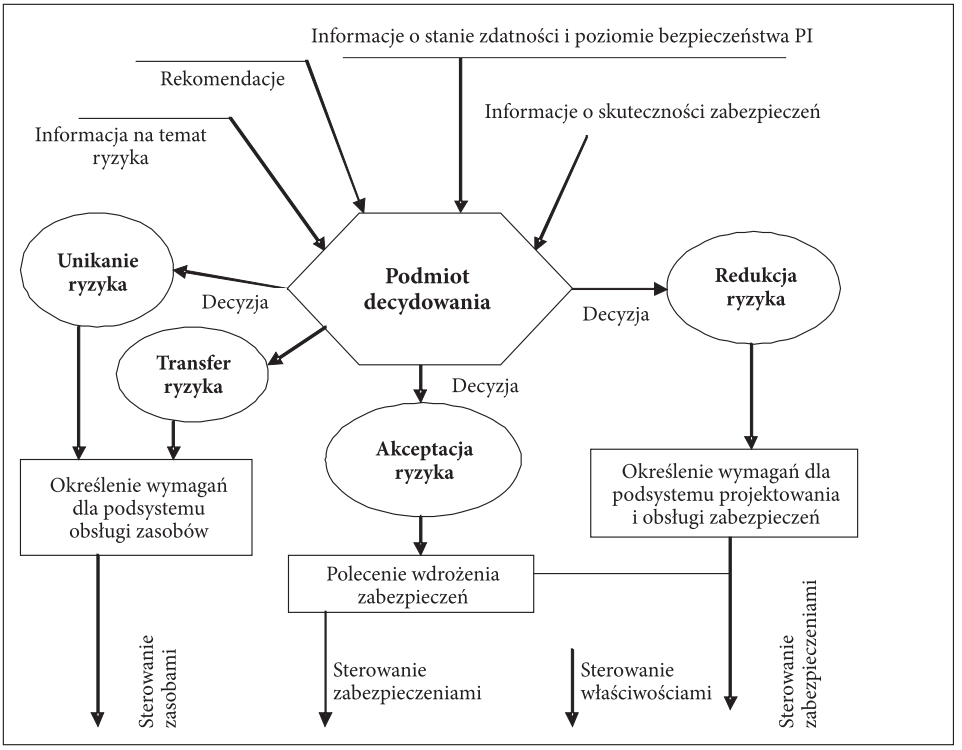
Zakłada się, że celem działania podsystemu sterowania bezpieczeństwem jest utrzymanie wymaganego bieżącego poziomu bezpieczeństwa PI. Cel ten można osiągnąć poprzez bieżące sterowanie konfiguracjami bezpieczeństwa podsystemu użytkowania zabezpieczeń.

Elementami podsystemu sterowania bezpieczeństwem są:

1) podmiot decydowania, którym jest element automatycznego wypracowania decyzji sterujących lub Forum Bezpieczeństwa Organizacji;
2) zbiór decyzji sterujących (dyrektyw) uaktywnianych przez element decyzyjny.

Graficzną ilustrację PSPB przedstawiono na rysunku 2. Wyróżniono na nim cztery istotne elementy decyzyjne znane jako podstawowe strategie postępowania z ryzykiem:

— unikanie,
— transfer ryzyka,
— redukcja ryzyka,
— akceptacja ryzyka.



Rys. 2. Wybrane elementy podsystemy sterowania poziomem bezpieczeństwa. Źródło: opracowanie własne

Podmiot decydowania, podejmując jedną z wyżej wymienionych decyzji, korzysta z informacji dostarczonych przez elementy otoczenia PSPB w postaci:

1) informacji na temat ryzyka (raportu z analizy i oceny ryzyka);
2) rekomendacji kierownika zespołu analizy zagrożeń i oceny ryzyka w zakresie strategii postępowania z ryzykiem;
3) informacji o stanie zasobów informacyjnych PI;
4) informacji o otoczeniu PI (strumień informacji wyjściowych).

2.2.2. Podsystem inwentaryzacji zasobów

Elementami podsystemu inwentaryzacji zasobów informacyjnych są:
1) zespół do spraw inwentaryzacji i klasyfikacji zasobów informacyjnych;
2) metodyka wyceny istotności zasobów informacyjnych.

Podczas określania wartości zasobu należy rozważyć, jaki wpływ na funkcjonowanie korporacji będzie miała jego utrata, awaria lub inne problemy z nim związane. Im większy wpływ, tym większa wartość zasobu. Wartość najlepiej oceniać z punktu widzenia znaczenia dla biznesu i wyrażać w pieniądzu, ale w przypadku takich zasobów jak wizerunek firmy czy też wiedza pracowników trudno jest określić ich wartość kwotowo. Można przyjąć inny sposób oceny wartości — względną ocenę istotności zasobu w stosunku do pozostałych zasobów. Stosując skalę np. trójstopniową, ważne jest określenie znaczenia poszczególnych wystąpień, np.:
1) wysoka — utrata lub naruszenie bezpieczeństwa aktywu[1] powoduje przerwanie procesów biznesowych,
2) średnia — utrata lub naruszenie bezpieczeństwa aktywu powoduje utrudnienia w normalnym funkcjonowaniu procesu biznesowego,
3) pomijalna — utrata lub naruszenie bezpieczeństwa aktywu nie ma wpływu na funkcjonowanie procesu biznesowego;

gdzie pozycja „wysoka" oznacza największe znaczenie, a „pomijalna" — najmniejsze znaczenie.

2.2.3. Podsystem analizy zagrożenia i oceny ryzyka

Elementami podsystemu analizy zagrożenia i oceny ryzyka są:
1) zespół analizy ryzyka,
2) metodyka identyfikacji zagrożeń, podatności oraz analizy i szacowania ryzyka,
3) zbiór informacji na temat podatności i wyceny zasobów informacyjnych.

Chcąc skutecznie zabezpieczyć zasoby, należy wiedzieć przed czym, czyli jakie zagrożenia mogą wystąpić w przypadku konkretnego zasobu informacyjnego. Dobrą praktyką jest wskazywanie przede wszystkim rzeczywistych zagrożeń — tzn. takich, które mogą wystąpić i występują w korporacji (konkretne awarie, braki zasilania, „wypaplanie" informacji, kradzież itp.). Z punktu widzenia kompletności szacowania ryzyka powinna być brana pod uwagę jak największa liczba zagrożeń (również tych mało prawdopodobnych), ale należy pamiętać, że istotnym elementem procesu analizy ryzyka jest możliwość uzyskania aktualnych i miarodajnych wyników. Zbyt rozbudowany proces analizy (znaczne wydłużenie czasu jego realizacji) o mniej

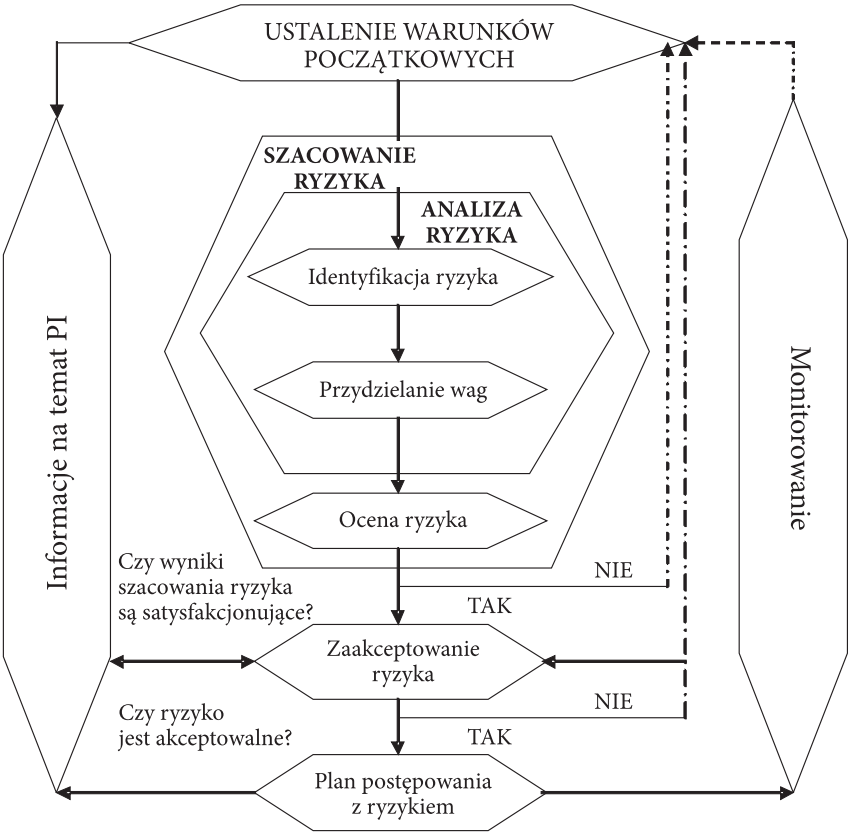
[1] Aktywa, wszystko, co ma wartość dla organizacji [ISO/IEC 13335-1:2004].

istotne elementy może spowodować, że w momencie jego zakończenia wyniki analizy ryzyka będą już nieaktualne.

Nie wszystkie zagrożenia występują z tą samą częstotliwością, stąd wprowadzone zostało pojęcie możliwości realizacji zagrożenia. Dobrą praktyką, która sprawdziła się w czasie szacowania ryzyka, jest stosowanie skali nie większej niż 3-stopniowa, np.: wysokie, średnie, niskie, gdzie: możliwość realizacji zagrożenia:

1) wysokie — występuje często (np. raz w miesiącu) lub regularnie z ustaloną częstotliwością;
2) średnie — wystąpiło w ostatnim roku lub zdarza się nieregularnie;
3) niskie — nie wystąpiło ani razu w ciągu ostatniego roku,

gdzie prawdopodobieństwo „wysokie" oznacza najwyższe prawdopodobieństwo, a „niskie" najniższe.



Rys. 3. Idea metodyki analizy i szacowania ryzyka. Źródło: opracowanie własne

Jeśli już wiadomo, co chronimy (zasoby informacyjne), dlaczego (istotność), przed czym (zagrożenia), to należy jeszcze określić słabe strony zasobów, tzn. cechy i/lub właściwości zasobu, które mogą zostać wykorzystane przez zagrożenie. Ostatnimi elementami domykającymi tę analizę są kwestie związane z oceną wpływu zagrożenia na atrybuty bezpieczeństwa (np. poufność, integralność i dostępność, niezaprzeczalność, rozliczalność itp.) oraz określenie skuteczności wdrożonych zabezpieczeń. Wpływ/skutek wystąpienia zagrożenia na atrybut bezpieczeństwa można opisać następująco:

1) krytyczny — wystąpienie zagrożenia powoduje zaistnienie efektu biznesowego, wysoki koszt, utratę wizerunku firmy, brak możliwości realizacji zadań;
2) średni — wystąpienie zagrożenia może wywołać efekt biznesowy lub stanowi duże utrudnienie w pracy;
3) niski — wystąpienie zagrożenia nie powoduje wystąpienia żadnego efektu biznesowego lub jest on marginalny;
4) nie dotyczy — wystąpienie zagrożenia nie ma wpływu na zasób,

gdzie wpływ „krytyczny" oznacza najwyższą wartość (największy wpływ), a „niski" — najniższą wartość (najmniejszy wpływ). Dobrą praktyką jest opracowanie własnej metodyki analizy i szacowania ryzyka (patrz rys. 3).

2.2.4. Podsystem projektowania i obsługi zabezpieczeń

Elementami podsystemu projektowania i obsługi zabezpieczeń są:

1) zespół projektowania różnych typów konfiguracji bezpieczeństwa, którego zadaniem jest opracowywanie zbioru propozycji zasobowych konfiguracji bezpieczeństwa na podstawie dostarczonych specyfikacji wymagań bezpieczeństwa platformy integracyjnej oraz zaakceptowanej polityki bezpieczeństwa korporacji;
2) zespół oceny skuteczności zabezpieczeń uaktywnionych w podsystemie przetwarzania informacji PI;
3) zespół obsługi mechanizmów bezpieczeństwa, którego zadaniem jest przywracanie zdatności zabezpieczeniom, w stosunku do których wykryto podatności i/lub słabości w dotychczasowym ich użytkowaniu;
4) zespół do spraw inwentaryzacji i klasyfikacji potencjalnych zabezpieczeń fizycznych, technicznych, programowych, proceduralnych i organizacyjnych.

Wprowadźmy następujące oznaczenia:

MB — zbiór uporządkowanych par $mb_i = \langle zb_i, FB_i \rangle \in ZB \times 2^{FB}$ zwanych dalej mechanizmami bezpieczeństwa,

gdzie: *ZB* — zbiór potencjalnych zabezpieczeń PI, ustalonych na etapie projektowania,

FB — zbiór potencjalnych funkcji bezpieczeństwa (np. wykrywanie, odstraszanie, zapobieganie, ograniczanie, poprawianie, odtwarzanie, monitorowanie, uświadamianie itp.), jakie mogą pełnić zabezpieczenia ze zbioru *ZB*;

ZI — zbiór potencjalnych zasobów informacyjnych przetwarzanych w ramach PI;

AB — zbiór nazw potencjalnych atrybutów bezpieczeństwa dla zasobów informacyjnych;

U — zbiór dopuszczalnych wielkości sterujących, przy pomocy których podmiot decydowania może ustalać bieżące właściwości mechanizmów bezpieczeństwa;

V_u — zbiór odpowiadających tym sterowaniom par $\langle i, j \rangle \in I \times J$,
gdzie: *I* — zbiór numerów wyróżnionych mechanizmów bezpieczeństwa;
J — zbiór numerów wyróżnionych cech mechanizmów bezpieczeństwa;
S — wektor stanów wyróżnionych mechanizmów bezpieczeństwa, którego współrzędne określają stany poszczególnych mechanizmów bezpieczeństwa.

Pod pojęciem stanu $s_i, i \in I$ *i*-tego mechanizmu bezpieczeństwa rozumie się wektor cech opisujących szczegółowo jego bieżące właściwości użytkowe z punktu widzenia bezpieczeństwa:

$$s_i = \left\langle a_i^j \in A_i^j : i \in I, j \in J \right\rangle, \tag{16}$$

gdzie: a_i^j — współrzędne wektora stanu *i*-tego mechanizmu bezpieczeństwa wyrażające poszczególne cechy bezpieczeństwa;
A_i^j — zbiór dopuszczalnych realizacji *j*-tej cechy *i*-tego mechanizmu bezpieczeństwa;
J — zbiór numerów wyróżnionych cech mechanizmów.

Wpływ sterowania na stan mechanizmów bezpieczeństwa, a w następstwie na ich właściwości bezpieczeństwa, można zapisać następująco:

$$\bigwedge_{\langle i,j \rangle \in I \times J} a_i^j(t) = a_i^j\left[u(t)\right], u \in U. \tag{17}$$

W rezultacie zbiór sterowalnych mechanizmów bezpieczeństwa można zdefiniować następująco:

$$\overline{MB} = \left\{ mb_i \in MB : \bigvee_{j \in J} \left[\langle i, j \rangle \in V_u \right], i \in I \right\}. \tag{18}$$

Na zbiorze $\overline{MB}$-sterowalnych mechanizmów bezpieczeństwa określa się cel działania podsystemu sterowania poziomem bezpieczeństwa.

Z punktu widzenia procesu bezpiecznego przetwarzania zasobów informacyjnych podmiotem działania w PI jest zbiór *MB* mechanizmów bezpieczeństwa, zaś przedmiotem zbiór takich elementów $e_j \in E^{PI}$, na których określony jest cel działania podsystemu przetwarzania informacji.

Elementami zbioru E^{PI} są porcje informacji odebrane przez podsystem przetwarzania informacji (rys. 1). Porcje te są automatycznie uformowane, według określonych zasad, przez podsystem przetwarzania informacji i podlegają dalszemu przetwarzaniu. Każdą porcję informacji, zwaną również zasobem informacyjnym PI, oznacza się numerem $p \in P$ i opisuje się zbiorem C_p nazw cech. Porcje te charakteryzują rzeczywiste zapotrzebowania użytkowników PI na usługi[2].

3. Opis platformy integracyjnej dla potrzeb sterowania poziomem bezpieczeństwa

Podczas sterowania poziomem bezpieczeństwa interesują nas tylko pewne a priori nieznane chwile, w których należy podejmować decyzje sterujące. Stany PI w takich chwilach czasu będziemy nazywali stanami istotnymi z punktu widzenia sterowania bezpieczeństwem informacji. Zakładamy, że w przedziale czasu między każdymi dwoma stanami istotnymi istnieje możliwość wykonywania wszystkich zadań przetwarzania zasobów informacyjnych wynikających z odebranych zapotrzebowań na usługi zlecanych przez użytkowników platformy integracyjnej. Wystąpienie stanu istotnego jest spowodowane pojawieniem się różnicy między pożądanym stanem bezpieczeństwa PI a jej bieżącym stanem bezpieczeństwa. Wystąpienie takiego zdarzenia powoduje przejście PI ze stanu „bezpiecznego" do stanu „bieżącej utraty bezpieczeństwa" i nazywane jest „utratą wymaganego poziomu bezpieczeństwa PI".

Przyczyną takiego przejścia mogą być następujące zdarzenia:

1) pojawienie się nowych zapotrzebowań na usługi zlecane przez użytkowników platformy integracyjnej;
2) pojawienie się nowych funkcjonalności integrowanych systemów informatycznych;
3) pojawienie się nowych i/lub dotychczas niezidentyfikowanych zagrożeń, podatności, mających istotny wpływ na poziom bezpieczeństwa informacji;
4) zidentyfikowanie nowych luk bezpieczeństwa, mających istotny wpływ na poziom bezpieczeństwa informacji;

[2] Na podstawie IBM (http://www.ibm.com) „Usługa jest to logiczna reprezentacja powtarzalnej aktywności biznesowej, która ma określony wynik, jest niezależna, może składać się z innych usług oraz jest czarną skrzynką dla jej konsumenta".

5) wystąpienie niesprawności i nieużyteczności aktualnie zaimplementowanych mechanizmów bezpieczeństwa, które uniemożliwiają zapewnienie wymaganego poziomu bezpieczeństwa;
6) zmodyfikowanie PI.

Wystąpienie zdarzenia określonego w punkcie 1, 2, 3, 4, 5 lub 6, względnie 1 i 2 i 3 i 4 i 5 i 6 lub dowolna ich kombinacja, nazywane „utratą wymaganego poziomu bezpieczeństwa PI", wykrywane jest przez podsystemy SAKZ i SAKB i natychmiast sygnalizowane do podsystemu sterowania bezpieczeństwem informacji. Zadaniem podsystemu sterowania jest skorygowanie różnicy między pożądanym poziomem bezpieczeństwa a jego bieżącym poziomem. Jeśli odchylenie to nie zostanie skorygowane przez podsystem sterowania, to PI nie osiągnie określonego celu. Z powyższego wynika, że warunkiem koniecznym osiągania przez PI zamierzonego celu, z punku widzenia bezpieczeństwa, jest utrzymanie wymaganego poziomu bezpieczeństwa informacji. Akceptowalny poziom bezpieczeństwa ustalany jest przez Kierownika Jednostki Organizacyjnej i gwarantuje skuteczne realizowanie procesu przetwarzania informacji w ramach platformy integracyjnej.

Po wystąpieniu sytuacji „utrata wymaganego poziomu bezpieczeństwa PI", aby można było skutecznie kontynuować proces przetwarzania informacji, musi nastąpić zmiana bieżących właściwości konfiguracji bezpieczeństwa w podsystemie użytkowania zabezpieczeń (PUZ). Pożądany, bieżący poziom bezpieczeństwa PI można uzyskać poprzez wygenerowanie odpowiedniej konfiguracji bezpieczeństwa PI (zbioru zabezpieczeń i funkcji bezpieczeństwa dających wymaganą wartość poszczególnym atrybutom bezpieczeństwa i ryzykom szczątkowym dla aktualnie przetwarzanych zasobów informacyjnych). Takie działanie nosi nazwę rekonfiguracji bezpieczeństwa, inaczej rekonfiguracji podsystemu użytkowania zabezpieczeń. Zakres i sposób przeprowadzenia rekonfiguracji może być:

1) wypracowany automatycznie przez podsystem sterowania i zainicjowany po akceptacji przez osobę funkcyjną, wchodzącą w skład Forum Bezpieczeństwa;
2) ustalony w sposób zautomatyzowany przez Zespół Analizy Zagrożeń i Oceny Ryzyka i przez niego rekomendowany do osoby funkcyjnej z Forum Bezpieczeństwa;
3) ustalony przez Forum Bezpieczeństwa i przez niego zainicjowany.

3.1. Bieżący poziom bezpieczeństwa PI

W niniejszym artykule bieżący poziom bezpieczeństwa PI rozumiany jest jako aktualna pozytywna ocena możliwości przetwarzania obowiązujących zasobów informacyjnych, w sposób bezpieczny, niezależnie od występujących sytuacji awaryjnych. Ocena ta powinna być zawsze pozytywna, ponieważ od PI wymagane jest zapewnienie ciągłości realizacji funkcji zlecanych przez użytkowników

integrowanych systemów informatycznych — usług i/lub procesów biznesowych. Oznacza to, że w bieżącej chwili musi istnieć możliwość bezpiecznego przetwarzania wszystkich porcji informacji odebranych z otoczenia. Pojmując w ten sposób istotę obowiązującego bezpieczeństwa, w dalszych rozważaniach przyjmuje się, że ma ono dla PI znaczenie podstawowe i bez jej spełnienia nie można zapewnić skutecznego poziomu bezpieczeństwa i przydatności PI.

Należy podkreślić, że dla PI zbiór zapotrzebowań na usługi może zmieniać się w czasie rzeczywistym. Jest on implikowany zbiorem funkcji zlecanych przez użytkowników PI. Zlecenia te pojawiają się na wejściu podsystemu przetwarzania informacji w sposób losowy.

Przypomnijmy, że celem działania podsystemu przetwarzania informacji jest nadawanie zasobom informacyjnym w przedziale czasu $\Delta \overset{*}{T}_p$ pożądanych stanów $\overset{*}{\alpha}_p$, nie tylko w aspekcie funkcjonalnym, lecz także z punktu widzenia atrybutów bezpieczeństwa.

W podanym (na wstępie) określeniu bieżącego poziomu bezpieczeństwa akcentuje się dwa istotne zagadnienia charakterystyczne dla konstrukcji artykułu:

1) w bieżących chwilach muszą istnieć możliwości realizowania wymaganego zbioru zadań przetwarzania zasobów informacyjnych, implikowanych zbiorem losowo napływających zleceń na usługi od użytkowników PI;
2) do bezpiecznego wykonania poszczególnych zadań przetwarzania informacji oraz zapewnienia bezpieczeństwa zasobom informacyjnym, podsystem użytkowania zabezpieczeń angażuje ściśle określone konfiguracje bezpieczeństwa w celu zapewnienia wymaganego poziomu bezpieczeństwa PI.

W świetle powyższego bieżący poziom bezpieczeństwa rozumiany jest jako możliwość uaktywnienia w podsystemie użytkowania zabezpieczeń zbiorów właściwych konfiguracji bezpieczeństwa, przy wykorzystaniu w nich zbioru aktualnie sprawnych zabezpieczeń i zbioru będących w dyspozycji. Zakładając, że znane jest β przekształcenie:

$$\beta : 2^D \to 2^{MB}; \beta\left(D^{kl}\right) = MB^{kl} \tag{19}$$

oraz znając zbiór $MB(t)$ aktualnie sprawnych mechanizmów bezpieczeństwa i zbiór $MB(t)$ mechanizmów bezpieczeństwa będących w dyspozycji, można określić rodzinę zbiorów $MB(t)$ konfiguracji możliwych do powołania w podsystemie użytkowania zabezpieczeń. Uwzględniając zależność (21), rodzinę zbiorów $MB(t)$ można przedstawić następująco:

$$MB(t) = \left\{ MB^{kl} \subset MB : MB^{kl} = \beta\left(D^{kl}\right); \left\langle MD^k, MB^l \right\rangle \in 2^{MD(t)} \times 2^{MB(t)} \right\}. \tag{20}$$

3.2. Pożądany poziom bezpieczeństwa platformy integracyjnej

Pożądany poziom bezpieczeństwa rozumiany jest jako możliwość wykonywania wszystkich zadań ze zbioru $Z^{PP}(t)$ wynikających z odebranych zleceń od użytkowników PI w sposób bezpieczny (poprzez zachowanie wszystkich atrybutów bezpieczeństwa dla wszystkich aktualnie przetwarzanych zasobów informacyjnych). Przyjmuje się, że zbiór tych zadań zmienia się dyskretnie w czasie.

Zbiór zadań przetwarzania informacji, które należy wykonać od chwili osiągnięcia przez PI pożądanego stanu bezpieczeństwa PI, można przedstawić następująco:

$$Z^{PP}(t_i) = \left\{ zi_g^b \in Z : b \in B(t_i), g \in G(t_i) \right\}, \tag{21}$$

gdzie: zi_p^b — zadanie przetwarzania informacji, które zaleźy wykonać w odniesieniu do zasobu informacyjnego typu b;
Z — zbiór możliwych zadań realizowanych przez PI, określony na etapie projektowania PI;
$B(t_i)$ — zbiór numerów zadań przetwarzania informacji wymaganych do wykonania od chwili t_i, wynikających z odebranych zleceń (typów porcji informacji przez podsystem przetwarzania informacji) do chwili t_i;
$G(t_i)$ — zbiór numerów typów porcji informacji (zasobów informacyjnych) wymagających dalszego przetwarzania.

3.3. Utrata bezpieczeństwa platformy integracyjnej

Utrata bezpieczeństwa platformy integracyjnej rozumiana jest jako zdarzenie powstałe w chwili t_i, spowodowane wystąpieniem różnicy między pożądanym poziomem bezpieczeństwa PI a jej bieżącym poziomem bezpieczeństwa. Wystąpienie takiego zdarzenia interpretowane jest jako „utrata poziomu bezpieczeństwa" w chwili t_i.

Odpowiada to warunkowi:

$$\overset{wym.do.wyk}{Z}(t_i) \supset \overset{moz.do.wyk}{Z}(t_i) \vee \overset{istniejaca}{KB}(t) \subset \overset{wymagana}{KB}(t), \tag{22}$$

gdzie: $\overset{wym.do.wyk}{Z}(t_i)$ — zbiór zadań przetwarzania informacji wymaganych do wykonania przez podsystem przetwarzania informacji do chwili t_i, wynikających z odebranych od użytkowników zapotrzebowań na usługi do chwili t_i;
$\overset{moz.do.wyk}{Z}(t_i)$ — zbiór zadań przetwarzania informacji możliwych do wykonania w podsystemie przetwarzania informacji o bieżącej konfiguracji funkcjonalnej i bieżącej konfiguracji bezpieczeństwa;

$\overset{istniejaca}{KB}(t_i)$ — istniejąca konfiguracja bezpieczeństwa w podsystemie użytkowania zabezpieczeń;

$\overset{wymagana}{KB}(t_i)$ — wymagana konfiguracja bezpieczeństwa w podsystemie użytkowania zabezpieczeń implikowana zbiorem $\overset{wym.do.wyk}{Z}(t_i)$ zadań przetwarzania informacji wymaganych do wykonania przez podsystem przetwarzania informacji od chwili t_i.

Przestrzeń możliwych rodzajów utrat bezpieczeństwa PI tworzy produkt kartezjański:

$$A = 2^Z \times 2^H \times 2^{MB} \times 2^D, \tag{23}$$

gdzie: Z — zbiór zadań możliwych do wykonywania w podsystemie przetwarzania informacji,

MB — zbiór możliwych konfiguracji bezpieczeństwa PI.

Element:

$$a_{phnd} = \langle Z_u, H_h, MB_n, D_d \rangle \in A \tag{24}$$

określa typ utraty bezpieczeństwa PI.

Przyjmijmy, że dla każdego typu utraty bezpieczeństwa określona jest wartość funkcji definiująca numer utraty bezpieczeństwa.

$$\lambda(phnd) = \nu \in \mathrm{N}. \tag{25}$$

Zakłada się, że rozpatrywana klasa systemów wyposażona będzie w programowy zespół kontrolno-diagnostyczny, wykrywający wszystkie typy utraty poziomu bezpieczeństwa. W celu jednoznacznego określenia sytuacji — utraty bezpieczeństwa, podsystem sterowania poziomem bezpieczeństwa PI będzie wykorzystywał następujące funkcje identyfikacji:

1) zbiór dyrektyw

$$F^D : A \to 2^D; f^D(a_v) = D_d, \tag{26}$$

2) zbiór sprawnych mechanizmów bezpieczeństwa

$$F^{MB} : A \to 2^{MB}; f^{MB}(a_v) = MB_n, \tag{27}$$

3) zbiór atrybutów bezpieczeństwa

$$F^H : A \to 2^H, f^H(a_v) = H_h, \tag{28}$$

4) zbiór zadań przetwarzania informacji

$$F^Z : A \to Z, f^Z(a_v) = Z_p. \tag{29}$$

Ponadto zakłada się, że dla każdego typu $\alpha \in A$ rodzaje utraty bezpieczeństwa o numerze v oraz zbiory Dd, MB_n, H_h są skończone i określone na etapie projektowania SZBI.

3.4. Funkcja rekonfiguracji

W celu stworzenia możliwości kompensacji utraty wymaganego poziomu bezpieczeństwa wymagane jest określenie na etapie projektowania PI zbioru dopuszczalnych decyzji sterujących, zwanych dalej dyrektywami, przy pomocy których osoby z zespołu do spraw bezpieczeństwa korporacji mogą ustalać takie bieżące właściwości konfiguracji bezpieczeństwa, które zapewniają osiągnięcie wymaganego poziomu bezpieczeństwa PI. Przejście PI ze stanu „brak wymaganego poziomu bezpieczeństwa" do stanu „osiągnięto wymagany poziom bezpieczeństwa" można opisać za pomocą następującego odwzorowania:

$$FR : \mathrm{KB} \rightarrow \mathrm{KB} \tag{30}$$

określonego następująco:

$$fr(KB^n) = KB^m; n, m \in \mathrm{N}, n \neq m, \tag{31}$$

gdzie: N — zbiór liczb naturalnych;
KB^n — zbiór dopuszczalnych konfiguracji bezpieczeństwa przed wystąpieniem stanu utraty bezpieczeństwa o numerze n;
KB^m — zbiór dopuszczalnych konfiguracji bezpieczeństwa po wystąpieniu stanu utraty bezpieczeństwa o numerze m.

Odwzorowanie FR wyznacza się na etapie projektowania PI lub ustanawiania systemu zarządzania bezpieczeństwem informacji (SZBI) korporacji, aby zapewniło ono uzyskanie wymaganych właściwości bezpieczeństwa PI w trakcie jej eksploatacji. Pożądaną bieżącą właściwość bezpieczeństwa PI można uzyskać poprzez wygenerowanie odpowiedniej konfiguracji bezpieczeństwa ze zbioru rozwiązań dopuszczalnych. Po wystąpieniu stanu utraty bezpieczeństwa, aby można było skutecznie kontynuować bezpieczny proces przetwarzania zasobów informacyjnych, należy wygenerować optymalną lub suboptymalną konfigurację bezpieczeństwa. Wygenerowanie optymalnej lub suboptymalnej konfiguracji bezpieczeństwa spośród zbioru rozwiązań dopuszczalnych realizowane jest w oparciu o szczegółową funkcję rekonfiguracji Q, która z punktu widzenia swojej istoty jest funkcją kryterialną. Sformułowanie zadania wielokryterialnej optymalizacji konfiguracji bezpieczeństwa i zaproponowanie metody jego rozwiązania będzie przedmiotem następnego artykułu.

4. Podsumowanie

Na świecie od dłuższego czasu prowadzone są prace nad standaryzacją bezpieczeństwa rozwiązań informatycznych, a w szczególności platform integracyjnych w architekturze SOA. Firmy wykorzystujące lub planujące wykorzystanie platformy integracyjnej z reguły stają przed problemem, jak zapewnić bezpieczeństwo platformy przy zachowaniu jej interoperacyjności i wymaganej wydajności. Jakkolwiek platformy integracyjne zgodne z paradygmatem SOA są bardzo obiecującym i intensywnie rozwijającym się obszarem rynku informatycznego, to jednak pełne wykorzystanie ich zalet wymaga rozwiązania wielu problemów, w szczególności tych związanych z zapewnieniem bezpieczeństwa. Wśród nich jedną z niewątpliwie pierwszorzędnych kwestii jest utrzymywanie wymaganego poziomu bezpieczeństwa. Zalecany model PDCA jest zbyt mało praktyczny.

Warunki społeczeństwa informacyjnego wymagają, aby każdą elektroniczną platformę integracyjną charakteryzowały następujące właściwości:

1) stała gotowość, czyli utrzymywanie wymaganego poziomu bieżącej niezawodności funkcjonalnej i wymaganego poziomu bieżącego bezpieczeństwa, niezależnie od występujących sytuacji awaryjnych,
2) wysoka operatywność z punktu widzenia sterowania właściwościami użytkowymi PI, rozumiana jako terminowe i zdecydowane reagowanie na wszystkie sytuacje awaryjne oraz podejmowanie decyzji sterujących właściwościami bezpieczeństwa w wymaganym czasie,
3) wysoka jakość i bezpieczeństwo realizowanych procesów, usług i zadań przetwarzania informacji poprzez:
   a) zasadne podejmowanie decyzji sterujących,
   b) terminowe przekazywanie do otoczenia PI informacji będących wynikami świadczenia usług,
   c) stosowanie naukowych metod organizacji przetwarzania informacji w PI również z punktu bezpieczeństwa.

Artykuł nie stanowi gotowej „recepty" na zapewnianie bezpieczeństwa platform integracyjnych. Należy go traktować jako propozycję autora częściowego rozwiązania problemu ustanawiania SZBI zapewniającego wymagany poziom bezpieczeństwa platform integracyjnych. Zaproponowany sposób podejścia do problematyki bezpieczeństwa, ukierunkowanej na korporacje wykorzystujące platformy integracyjne, wynika między innymi ze spostrzeżeń i kilkuletnich doświadczeń autora zgromadzonych:

a) podczas obserwacji ustanawiania i wdrażania takich systemów w korporacjach,
b) w trakcie prac naukowo-badawczych i dyskusji seminaryjnych dotyczących bezpieczeństwa korporacji.

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

Artykuł został opracowany na podstawie referatu prezentowanego na Konferencji SE'2012 — Systems Engineering 2012.

Artykuł wpłynął do redakcji 7.11.2012 r. Zweryfikowaną wersję po recenzji otrzymano w lutym 2013 r.

LITERATURA

[1] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa, 2006.

[2] B. Brodecki, P. Sasak, M. Szychowiak, *Security Policy Definition Framework for SOA-based systems*, Proceedings of the 10th Int'l Conference on Web Information Systems Engineering, LNCS 5802, Springer-Verlag, 2009.

[3] T. Górski, *Platformy integracyjne. Zagadnienia wybrane*, PWN S.A., Warszawa, 2012.

[4] IT-SOA, *Nowe technologie informacyjne dla elektronicznej gospodarki i społeczeństwa informacyjnego oparte na paradygmacie SOA*, Projekt realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka: Działanie 1.3.1, http://www.soa.edu.pl.

[5] J. Stanik, *Utrzymywanie wymaganego poziomu bieżącej niezawodności funkcjonalnej komputerowego systemu zautomatyzowanego dowodzenia*, praca doktorska, Warszawa, 1987.

[6] Raport Techniczny ISO/IEC TR 13335-1 *Technika informatyczna — Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*, Część 1. *Pojęcia i modele bezpieczeństwa systemów informatycznych*.

[7] Raport Techniczny ISO/IEC TR 13335-2 *Technika informatyczna — Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*, Część 2. *Zarządzanie i planowanie bezpieczeństwa systemów informatycznych*.

[8] Raport Techniczny ISO/IEC TR 13335-3 *Technika informatyczna — Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*, Część 3. *Techniki zarządzania bezpieczeństwem systemów informatycznych*.

J. STANIK

Maintenance of security required level of electronic integration platform

Abstract. The paper presents the concept of maintaining the required level of electronic integration platform (EPI) security. There were identified and characterized the basic elements of EPI from the viewpoint of controlling the current level of security. Electronic model of integration platform was proposed for maintaining the required level of security. The desired property of the current EPI security is achieved by generating the appropriate security configuration from the set of feasible solutions. The proposed concept of security maintenance takes into account the security of information resources, changes in operating conditions of electronic integration platform, company's information system and the entire corporation. This concept is the author's own proposal.

Keywords: security, information security management system, security configuration, risk analysis, integration platform