AUTOMATYKA • 2007 • Tom 11 • Zeszyt 1–2

Piotr Sienkiewicz*

# Optymalizacja w zarządzaniu bezpieczeństwem systemów

## 1. Wprowadzenie

Każda epoka ma własny, niepowtarzalny nakaz chwili. I pierwszym jej wymogiem jest stworzenie efektywnego systemu bezpieczeństwa, zapewniającego redukcję poczucia zagrożenia i redukcję realnych zagrożeń dla bezpiecznego funkcjonowania systemów różnej natury i różnej wartości. Chodzi bowiem o minimalizację skumulowanego ryzyka, gdyż istnienie niebezpieczeństw (zagrożeń) może prowadzić do utraty kontroli nad procesami, co może być przyczyną kryzysów i konfliktów, zakłócenia procesów rozwojowych, a nawet katastrof (upadków) systemów. O społeczeństwie informacyjnym mówi się niekiedy jako o „społeczeństwie ryzyka", natomiast jako jeden z głównych dylematów współczesności wymienia się wybór między poczuciem bezpieczeństwa a poczuciem wolności, albowiem tych dwóch wartości nie da się pozyskać w jednakowo pożądanym stopniu.

Klasyczną sytuację decyzyjną stanowi wybór między działaniem bezpiecznym, tj. takim, który zapewnia określone korzyści, a działaniem ryzykownym, które może przynieść sukces (np. z prawdopodobieństwem $p$), lecz może także przynieść porażkę (z prawdopodobieństwem $1-p$). Tego typu sytuacje są przedmiotem teorii decyzji, analizującej między innymi postawy decydentów, wyrażające skłonność bądź awersję do ryzyka.

Zarządzanie ryzykiem obejmuje zarówno przedsięwzięcie o charakterze ewaluacyjnym (analityczno-ocenowym), jak i działania planistyczno-kontrolne, mające na celu minimalizację (redukcję) ryzyka lub utrzymania go na poziomie dopuszczalnym. Zarządzanie bezpieczeństwem można w szczególności sprowadzić do zagadnienia zarządzania ryzykiem, bowiem ryzyko stanowi ilościowy wyraz funkcjonowania systemów w środowisku, w którym znajdują się aktywne źródła zagrożeń dla bezpieczeństwa systemów.

W artykule przedstawiono wybrane ogólne modele systemów w warunkach zagrożeń, podkreślając możliwości podejmowania działań optymalizacyjnych w procesie zarządzania bezpieczeństwem.

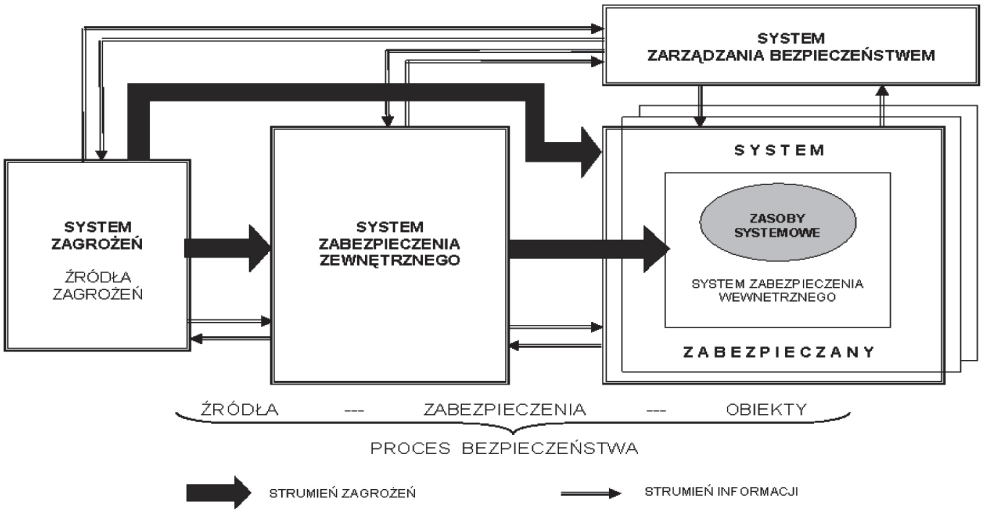
* Warszawska Wyższa Szkoła Informatyki

## 2. System bezpieczeństwa

W analizie systemowej bezpieczeństwa założono, że na efektywność systemu mają wpływ [7]:

- niezawodność systemu, czyli zdolność do sprawnego (bez uszkodzeń, awarii, błędów itp.) funkcjonowania w określonym czasie;
- bezpieczeństwo systemu, czyli zdolność do skutecznego zabezpieczenia przed skutkami zagrożeń zewnętrznych.

Bezpieczeństwo systemu jest własnością charakteryzującą odporność na powstanie sytuacji niebezpiecznych, czyli takich, w których powstaje konieczność ochrony wewnętrznych wartości systemu przed zewnętrznymi zagrożeniami.




**Rys. 1.** Ogólny model zarządzania bezpieczeństwem systemów [7]

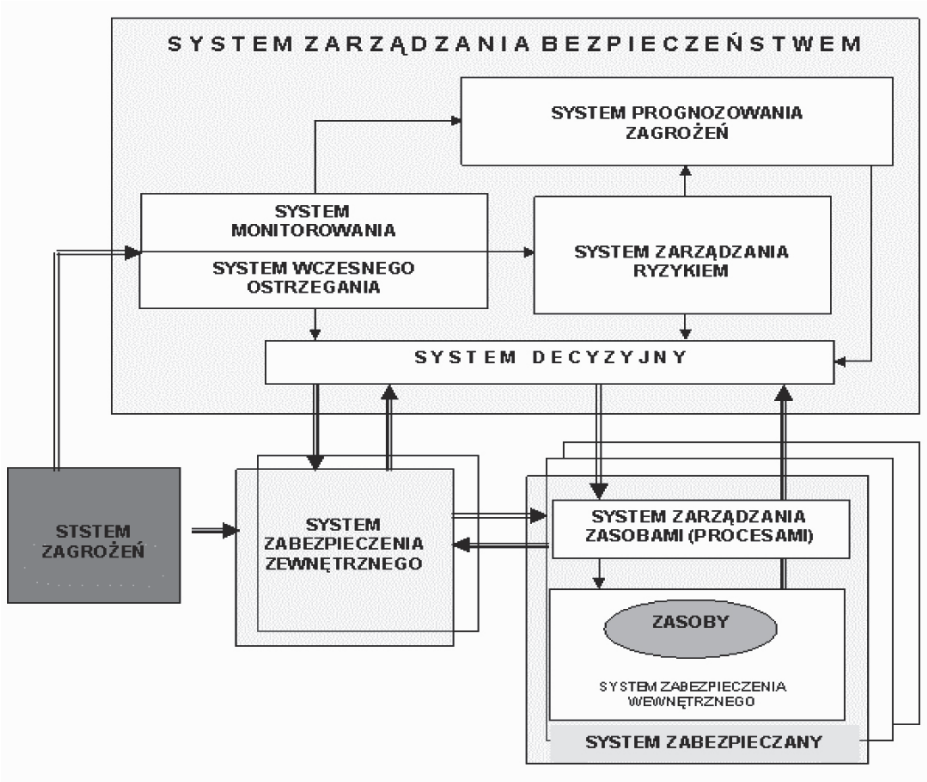
Przyjęto, że ogólny model systemu bezpieczeństwa składa się z komponentów takich, jak (rys. 1):

- system zagrożeń (zbiór źródeł zagrożeń i relacji między nimi), będący swoistym generatorem zagrożeń;
- system zabezpieczany (obiekt zagrożeń), dysponujący zasobami systemowymi o określonej wartości, chronionymi przez system zabezpieczania wewnętrznego (lokalnego);
- system zarządzania bezpieczeństwem zapewniający sterowanie systemem zabezpieczenia zewnętrznego (nadrzędnego).

Proces bezpieczeństwa można rozpatrywać jako relacje między: źródłem zagrożeń, zabezpieczeniami a obiektami zagrożeń.

Każdy lokalny system zabezpieczony informuje nadrzędny system zarządzania o stanie swojego bezpieczeństwa i prognozowanych zagrożeniach.

System nadrzędny na podstawie informacji o stanie systemu zagrożeń oraz informacji o stanach systemów lokalnych planuje zasoby systemu zabezpieczenia zewnętrznego, które mogą zapewnić skuteczną ochronę zasobów poszczególnych obiektów zagrożeń.




**Rys. 2.** Model systemu zarządzania bezpieczeństwem jako dwupoziomowe sterowanie [7]

Aby realizować przedsięwzięcia zapewniające bezpieczeństwo systemów lokalnych, system nadrzędny tworzą określone podsystemy (rys. 2):

- system decyzyjny: dokonuje przydziału zasobów przeznaczonych na ochronę systemów lokalnych w ramach dopuszczalnej strategii bezpieczeństwa;
- system monitorowania i wczesnego ostrzegania: zbiera bieżące informacje o stanie sytuacji bezpieczeństwa i identyfikuje symptomy zagrożeń;
- system prognozowania zagrożeń: tworzy podstawy do planowania działań;
- system zarządzania ryzykiem: zapewnia ocenę ryzyka i planuje przedsięwzięcia zmierzające do minimalizacji ryzyka, co stanowi podstawę do określenia dopuszczalnych strategii bezpieczeństwa.

W kontekście powyższego ogólnego modelu wartość ryzyka zależy od zagrożeń, podatności (odporności) na zagrożenia, dotkliwości skutków zagrożeń.

## 3. Wybrane modele

### 3.1. Bezpieczeństwo informacyjne

Klasyczny model Clementsa systemu bezpieczeństwa tworzą następujące elementy [2]:

$O$ – zbiór zabezpieczonych obiektów;
$T$ – zbiór zagrożeń;
$M$ – zbiór środków bezpieczeństwa;
$V$ – zbiór miejsc wrażliwych na atak – jest on rzutem zbioru $T \times O$ na zbiór uporządkowanych par $V_L = <t_i, o_j, m_k>$, które są ścieżkami penetracji systemu;
$B$ – zbiór barier, czyli przekształceniem zbioru $T \times O \times M$ do uporządkowanych trójek $b_i = <t_i, o_j>$, będący zbiorem punktów bezpieczeństwa w systemie.

System bezpieczeństwa $S = < O, T, M, V, B>$ jest całkowicie zabezpieczony, jeśli w nim istnieje zabezpieczenie dla każdej znanej ścieżki penetracji. W takim systemie relacja $<t_i, o_j> \in V$ implikuje zachowanie relacji $<t_i, o_j, m_k> \in B$. Jeśli implikacja ta nie jest prawdziwa, to $o_j$ jest nie chronione.

Zarządzanie bezpieczeństwem systemu $S$ można sprowadzić do optymalizacji rozdziału środków bezpieczeństwa do ścieżek penetracji tak, aby zapewnić systemowi całkowite zabezpieczenie przy spełnieniu warunku ograniczającego koszty lub czas zabezpieczenia przed zagrożeniami.

W modelu „chroniącego intruza" [2] zakłada się, że intruz pragnie zdobyć określone informacje o określonej wartości, i na to przeznacza określone środki $X$. W celu ochrony informacji, odpowiedzialny za ich bezpieczeństwo przeznacza na ochronę $Y$ zasobów, przy czy przyjmuje się, że nie należy przeznaczać dużych zasobów do ochrony informacji o znikomej wartości. Niech $I(X, Y)$ określa przewidywalną ilość informacji uzyskaną przez intruza przeznaczającego $X$ zasobów na przełamanie zabezpieczeń $Y$ zastosowanych przez chroniącego; niech $f(\cdot)$ będzie wartością jednostek informacji uzyskanych przez intruza, a $g(\cdot)$ – wartością tych informacji dla chroniącego.

Dla danych $X$ i $Y$ zysk netto intruza wyniesie

$$\upsilon(X, Y) = f(I(X, Y)) - X,$$

straty netto dla chroniącego

$$\mu(X, Y) = g(I(X, Y)) + Y.$$

Intruz określa swoje nakłady $X$ w celu zmaksymalizowania wartości funkcji $\upsilon(X, Y)$, natomiast obrońca wyznacza nakłady $Y$, tak by zminimalizować wartości funkcji $\mu(X, Y)$.

### 3.2. Bezpieczeństwo inwestycji

W analizach ryzyka i bezpieczeństwa inwestycji uwagę zwraca model H. Markowitza [8], który może stać się podstawą do formułowania problemów, optymalizacji strategii bezpiecznego inwestowania. Załóżmy, że miarą efektywności inwestycji jest stopa zwrotu [4]

$$R_t = \frac{P^*(t) - P(t-1)}{P(t-1)},$$

gdzie:

$P(t-1)$ – kapitał zainwestowany w okresie $t-1$,

$P^*(t)$ – przychód uzyskany z inwestycji w czasie $t$.

Najczęściej zakłada się, że $R_t$ ma rozkład normalny z daną wartością przeciętną ($R$) i wariancją ($\delta^2$).

Przy wyborze strategii inwestycji brane są pod uwagę dwie podstawowe charakterystyki:

1) zwrot z portfela

$$R_p \sum_{i=1}^{n} R_i x_i,$$

2) wariancja z portfela

$$V_p = \sum_{i=1}^{n} \left[ x_i^2 \delta^2 + \sum_{\substack{j=1 \\ j \neq 1}} x_i x_j \delta_{ij} \right],$$

gdzie:

$x_i$ – część całkowitych nakładów na $i$-te akcje,

$\delta_{ij}$ – kowariancja między $i$-tą a $j$-tą akcją.

Problem optymalizacji polega na znalezieniu takiej strategii $\overset{*}{x} \in \Omega$, że

$$R_p(\overset{*}{x}) = \max_{x \in \Omega} R_p(x),$$

gdzie:

$$\Omega = \{x : \sum_{i=1}^{n} x_i = 1, \quad x_i \geq 0, \quad V_p(x) \leq V\}.$$

Załóżmy, że dana jest funkcja użyteczności inwestora w postaci zaproponowanej przez R. Kulikowskiego [4]

$$U(Z, Y) = YF\left(\frac{Z}{Y}\right),$$

gdzie:

$Z = PR$,

$P$ – inwestycja początkowa,

$Y = P(R - \lambda\delta)$,

$\lambda$ – wartość kosztów ryzyka,

$F(\cdot)$ – funkcja wklęsła.

Wprowadza się funkcję bezpieczeństwa

$$S = \frac{Y}{Z} = 1 - \lambda \frac{\delta}{R},$$

a wtedy użyteczność portfela ma postać

$$\Phi(x) = \sum_{i=1}^{n} Y_i F\left(\frac{x_i}{s_i}\right),$$

gdzie:

$$Y_i = P_i R_i S_i > 0,$$

$$S_i = 1 - \lambda \frac{\delta_i}{R_i} > 0.$$

Wykazano [4], że istnieje jednoznaczna strategia $\overset{*}{x}$ taka, że $\Phi(\overset{*}{x}) = \max_{x \in \Omega} \Phi(x)$, gdzie

$$\Omega = \{x_i : \sum_{i=1}^{n} P_i R_i x_i = Z,\ x_i > 0,\ i = 1, ..., n\}.$$

## 4. Zakończenie

Przykłady zarządzania bezpieczeństwem wskazują na istotne znaczenie problemu optymalizacji przydziału środków przeznaczonych na zabezpieczenie działania przed zagrożeniami w celu maksymalizacji wartości użyteczności przy dopuszczalnym poziomie ryzyka. W szczególności problem zarządzania bezpieczeństwem może zostać sprowadzony do dwupoziomowego sterowania rozdziałem środków zabezpieczenia (nakładów na bezpieczeństwo) między systemy lokalne, których systemy zabezpieczenia zewnętrznego nie gwarantują pożądanego poziomu bezpieczeństwa (dopuszczalnego ryzyka).

Można sformułować następującą tezę: inwestycje w system bezpieczeństwa należą do najbardziej użytecznych z punktu widzenia potrzeb społecznych. Jednakże należy zabezpieczać przed zagrożeniami przede wszystkim te obiekty, których wartość jest istotna, a spowodowane przez zagrożenia straty mogą być szczególnie dotkliwe. Koszty bezpiecznego funkcjonowania systemów stale rosną, przeto zarządzanie bezpieczeństwem, w tym zarządzanie ryzykiem należy z pewnością zaliczyć do najważniejszych dla zapewnienia trwałego, czyli bezpiecznego i zrównoważonego rozwoju społecznego.

## Literatura

[1] Dorosiewicz S.: *Elementy analizy portfelowej – ujęcie matematyczne.* Warszawa, SGH 2003
[2] Hoffman L.J.: *Poufność w systemach informacyjnych*. Warszawa, WNT 1982
[3] Jaźwiński J., Ważyńska-Fiok K.: *Bezpieczeństwo systemów*. Warszawa, PWN 1993

[4] Krawczak M., Jakubowski A., Konieczny P., Kulikowski R., Miklewski A., Szkatuła G.: *Aktywne zarządzanie inwestycjami finansowymi*. Warszawa, EXIT 2003
[5] Paszkowski S.: *Dwupoziomowe sterowanie wielkiego systemu*. Warszawa, WAT 1967
[6] Sienkiewicz P.: *Analiza systemowa*. Warszawa, Bellona 1995
[7] Sienkiewicz P.: *Teoria i inżynieria bezpieczeństwa systemów*. Monografia nr 3, Kraków, AGH 2005
[8] Tarczyński W.: *Fundamentalny portfel papierów wartościowych*. Szczecin, USz 1999