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

Ocena użyteczności systemu zabezpieczeń w systemie bezpieczeństwa informacji

1. Wstęp

Zapewnienie wymaganego poziomu bezpieczeństwa organizacji lub wysokiego poziomu bezpieczeństwa dla wybranych obszarów przetwarzania informacji wymaga opracowania strategii lub dobrego projektu zabezpieczeń, zgodnie ze sprawdzoną metodyką, a następnie wdrożenia tego projektu przez specjalistów z użyciem właściwie dobranych technologii oraz utrzymania skutecznych konfiguracji bezpieczeństwa[4]. Zaprojektowane konfiguracje bezpieczeństwa o charakterze technicznym lub organizacyjnym powinny być oparte w znacznej mierze na wynikach analizy ryzyka, specyfikacji wymagań bezpieczeństwa, a także ogólnej teorii zabezpieczeń (m.in. wymagane jest dokonanie oceny użyteczności bieżącej konfiguracji bezpieczeństwa, weryfikacji odporności zastosowanych zabezpieczeń na strategię różnego typu ataków oraz rekonfiguracji systemu zabezpieczeń wskutek wystąpienia różnego typu sytuacji awaryjnych – utraty wymaganego poziomu bezpieczeństwa).

W dostępnej literaturze przedmiotu nie znaleziono propozycji metod oceny skuteczności systemu zabezpieczeń skonstruowanego na podstawie konfiguracji bezpieczeństwa lub konfiguracji zabezpieczeń o charakterze technicznym lub organizacyjnym. Na wyróżnienie zasługuje metoda zaproponowana w pracy M. Szulima i M. Kuchty[5]. Metoda ta ma charakter metody jakościowej. Możliwość

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

[4] Konfiguracja bezpieczeństwa – zbiór zabezpieczeń o charakterze technicznym i organizacyjnym oraz relacje zachodzące między nimi, odzwierciedlające właściwości użytkowe konfiguracji bezpieczeństwa.

[5] M. Szulim, M. Kuchta, *Metoda analizy skuteczności systemu bezpieczeństwa obiektu*, „Biuletyn Wojskowej Akademii Technicznej" 2016, vol. LIX, nr 4.

praktycznego jej zastosowania jest ograniczona do bardzo wąskiej klasy wskaźników jakości. Nie może być wykorzystana do oceny użyteczności bieżącej konfiguracji bezpieczeństwa i procesu alokacji zabezpieczeń do poszczególnych konfiguracji bezpieczeństwa – procesu rekonfiguracji. Prace J. Napiórkowskiego, J. Stanika i R. Hoffmana[6] wykazują na rosnącą potrzebę automatyzacji procesu rekonfiguracji, związanej z opracowaniem procedur sterowania ryzykiem w procesach biznesowych.

Brak metod oraz kryteriów oceny skuteczności środków bezpieczeństwa (zabezpieczeń technicznych i organizacyjnych) utrudnia ilościową ocenę skuteczności systemu zabezpieczeń. Wymusza się zatem korzystanie z oceny jakościowej. Ocena jakościowa jest subiektywna, a jej wynik, akceptacja poziomu ochrony zasobu lub jego odrzucenie, zależy od wiedzy i doświadczenia osoby oceniającej. Skuteczna ochrona obszarów przetwarzania informacji wymaga stosowania różnego rodzaju konfiguracji zabezpieczeń, w tym wprowadzenia kilku lub kilkunastu zabezpieczeń technicznych i organizacyjnych jednocześnie. Po uwzględnieniu zbioru tych zabezpieczeń oraz różnych charakterystyk powiązań (relacji, właściwości) pomiędzy tymi zabezpieczeniami, mamy do czynienia z systemem zabezpieczeń.

Celem artykułu jest ukazanie i rekomendacja zarówno teoretycznych, jak i praktycznych podejść do oceny skuteczności systemu zabezpieczeń. Przy określeniu poziomu bezpieczeństwa w obszarach przetwarzania informacji w organizacji akcentuje się trzy istotne zagadnienia, charakterystyczne dla konstrukcji artykułu:

1) w bieżących chwilach muszą istnieć możliwości bezpiecznego wykonywania operacji przetwarzania danych (wymaganego zbioru zasobów informacyjnych),
2) w stosunku do zasobów wrażliwych[7] SIO wymaga się istnienia procesów ochronnych, które zapewniają utrzymanie odpowiednich atrybutów bezpieczeństwa[8] na akceptowalnym poziomie ryzyka[9],

---

[6] J. Napiórkowski, J. Stanik, R. Hoffmann, *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, Konferencja naukowa pt. „Współczesne wyzwania e-Gospodarki", 2016; J. Stanik, R. Hoffmann, *Model ryzyka procesów biznesowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Ekonomiczne Problemy Usług" 2017, 126/1, s. 325–338.

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

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

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

3) 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 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.

2. Miejsce i rola systemu zabezpieczeń w środowisku bezpieczeństwa organizacji

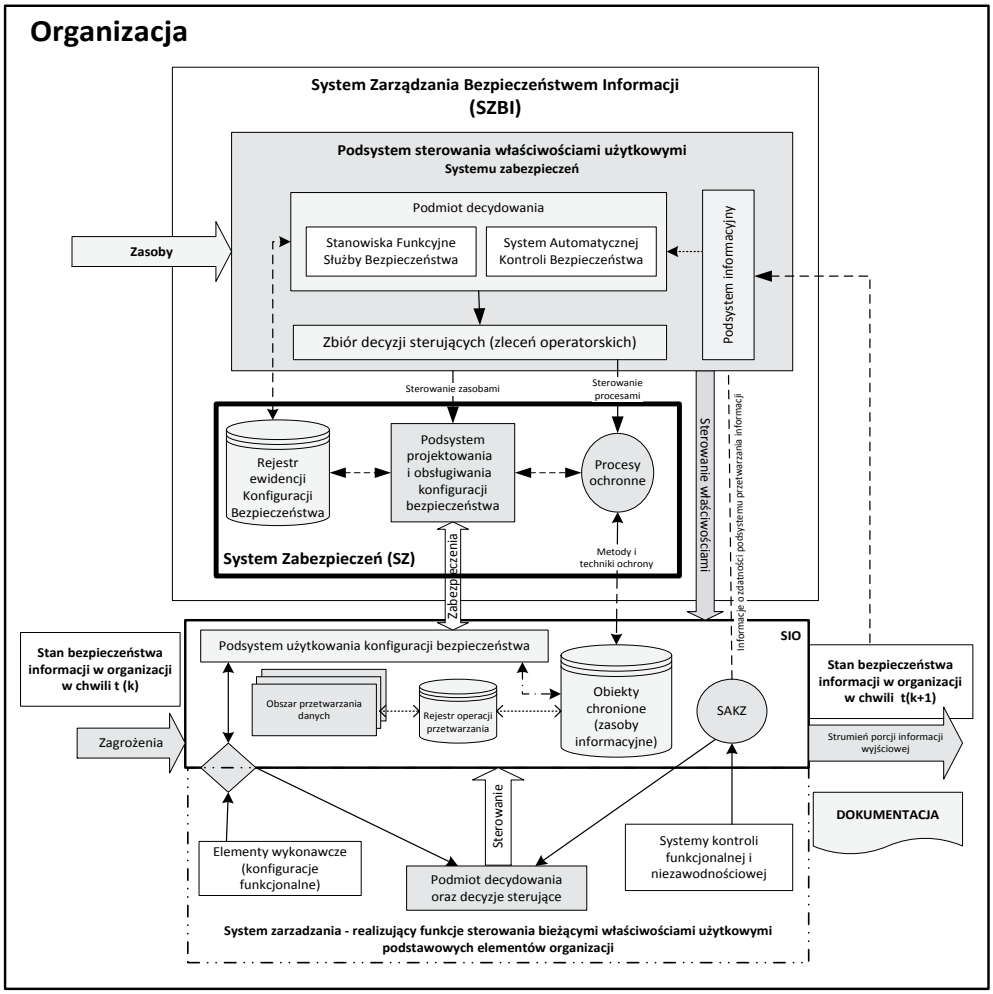
System zabezpieczeń jest częścią składową systemu zarządzania bezpieczeństwem organizacji i obejmuje ochronę zarówno wyróżnionych obszarów przetwarzania informacji, jak i ich infrastruktury przed celowymi lub przypadkowymi zniszczeniami. Schematyczną ilustrację organizacji z punktu widzenia sterowania bieżącym poziomem bezpieczeństwa obszarów przetwarzania systemu informacyjnego przedstawiono na rysunku 1.

Na rysunku tym wyróżniono następujące elementy:

- Podsystem obszarów przetwarzania informacji (System Informacyjny Organizacji),
- System zabezpieczeń (SZ),
- Środowisko bezpieczeństwa organizacji, w którym realizowane są funkcje sterowania poziomem bezpieczeństwa zasobów informacyjnych,
- Pozostałe systemy zarządzania, realizujące funkcje sterowania właściwościami użytkowymi podsystemu informacyjnego organizacji.

Ogólnie, w sensie opisowym, określa się, że dany system zabezpieczeń działa skutecznie, jeżeli osiąga cel – realizuje postawione mu zadania. Jednakże, aby można było w kategoriach wymiernych określać: pożądany zakres działań zapobiegawczych, przygotowawczych oraz sił i środków niezbędnych do skutecznego reagowania na wystąpienia danego rodzaju zagrożenia, tj. skutecznego zapewnienia pożądanego poziomu bezpieczeństwa obszaru przetwarzania danych,

niezbędne jest przyjęcie miary (wskaźnika) skuteczności. Pozwoli to oceniać i analizować możliwości przyjęcia i koszt proponowanych rozwiązań (koncepcji), zapewnienia obszarowi przetwarzania danych (w szczególności jego elementom składowym) pożądanego poziomu bezpieczeństwa informacyjnego.



Rysunek 1. Ilustracja organizacji z punktu widzenia sterowania bieżącym poziomem bezpieczeństwa obszarów przetwarzania systemu informacyjnego

Źródło: opracowanie własne.

3. Wielkości opisujące właściwości użytkowe systemu bezpieczeństwa

Po wystąpieniu sytuacji utraty wymaganego poziomu bezpieczeństwa powinna istnieć możliwość uaktywnienia (przy wykorzystaniu sprawnych mechanizmów bezpieczeństwa – zabezpieczeń o charakterze technicznym i organizacyjnym) kilku różnych procesów ochronnych lub dopuszczalnych konfiguracji bezpieczeństwa. W takich przypadkach istnieje konieczność wyboru jednej z nich. Oczywiste jest, że należałoby wybrać konfigurację bezpieczeństwa najlepszą pod każdym względem. Wymaga to „poddania" wariantów dopuszczalnych konfiguracji wszechstronnej ocenie, uwzględniającej wiele wielkości (charakterystyk) opisujących jej właściwości użytkowe i bezpieczeństwa, przeprowadzonej względem różnych funkcji kryterialnych. Ocena ta będzie się wtedy składać z wielu ocen cząstkowych. Zamiar taki można zrealizować tylko wówczas, gdy zostanie ustalony zbiór reprezentatywnych charakterystyk odzwierciedlających cel działania systemu zabezpieczeń, sposób jego funkcjonowania oraz zasady jego eksploatacji, przesądzające o jego użyteczności[10] lub skuteczności[11]. Postępując w ten sposób, zmniejsza się subiektywność oceny, a zarazem można:

- ograniczyć liczbę funkcji kryterialnych i wskaźników jakości, stanowiących podstawę oceny i wyboru optymalnej lub suboptymalnej konfiguracji bezpieczeństwa,
- zapewnić współmierność znaczenia (wagi) poszczególnych wielkości i funkcji kryterialnych,
- racjonalnie ocenić użyteczność systemu zabezpieczeń o określonej konfiguracji bezpieczeństwa.

Mając na uwadze powyższe rozważania, można określić użyteczność konfiguracji bezpieczeństwa dla systemu zabezpieczeń, wyodrębniając następujące wielkości (charakterystyki):

- wrażliwość[12] systemu zabezpieczeń na sytuacje utraty wymaganego poziomu bezpieczeństwa,
- czas generowania konfiguracji bezpieczeństwa,
- efektywność działania podsystemu przetwarzania informacji,

[10] Łatwość obsługi i dopasowanie do rzeczywistych potrzeb użytkownika.

[11] Sprawdzenie, czy nasze działania dały nam oczekiwane rezultaty.

[12] Zdolność systemu zabezpieczeń przejawiająca się reagowaniem na zmianę typów i ilości typów informacji, podlegających dalszemu bezpiecznemu przetwarzaniu w SIO.

- redundancję w odniesieniu do zabezpieczeń o charakterze technicznym,
- redundancję w odniesieniu do procesów ochronnych.

Zaproponowane wyżej wielkości, opisujące właściwości systemu zabezpieczeń o ustalonej konfiguracji bezpieczeństwa, nie stanowią zamkniętego zbioru. Można wprowadzić inne (tutaj nieuwzględnione), dotyczące np. przepustowości lub wydajności konfiguracji bezpieczeństwa.

Wprowadźmy następujące oznaczenia:
Ω – zbiór wielkości opisujących właściwości użytkowe konfiguracji bezpieczeństwa,
KB^{u}_{dop} – zbiór dopuszczalnych konfiguracji bezpieczeństwa po wystąpieniu sytuacji awaryjnej (sytuacji utraty bezpieczeństwa) o numerze u,
Q – zbiór wyróżnionych funkcji kryterialnych,
W – zbiór wektorów realizacji poszczególnych wielkości ze zbioru Ω,
f_{1-5} – funkcja wektorowa przyporządkowująca każdej dopuszczalnej konfiguracji bezpieczeństwa wektor realizacji poszczególnych wielkości.

Uwzględniając powyższe wielkości (opisujące właściwości użytkowe konfiguracji bezpieczeństwa), zbiór Ω można przedstawić nastepujaco:

$$\Omega = \left\{ \Omega_{i},\ i = \overline{1,5} \right\}. \tag{1}$$

Przyjmijmy, że dla każdej wielkości Ω_i określony jest zbiór W_i możliwych jej realizacji. Wówczas każdej, dopuszczalnej konfiguracji bezpieczeństwa $KB \in KB^{u}_{dop}$ odpowiada uporządkowany zbiór realizacji jej wielkości:

$$\left\langle f_1(KB),\ f_2(KB),\ f_3(KB),\ f_4(KB),\ f_5(KB) \right\rangle, \tag{2}$$

zapisany krótko:

$$f(KB) \text{ lub } \underline{w} = \left\langle w_1, w_2,\ w_3, w_4, w_5 \right\rangle. \tag{3}$$

Funkcje przypisujące każdej dopuszczalnej konfiguracji $KB \in KB^{u}_{dop}$ realizację jej i-tej wielkości można zapisać następująco:

$$f_i : KB^{u}_{dop} \to W_i,\ f_i(KB) = w_i,\ i = \overline{1,5}. \tag{4}$$

Funkcja wektorowa

$$\overline{f} : KB^{u}_{dop} \to W_1 \times W_2 \times W_3 \times W_4 \times W_5;\ \overline{f}(KB) = \underline{w}. \tag{5}$$

W dalszych rozważaniach, dotyczących wektorów $\underline{w}$ realizacji wielkości opisujących właściwości użytkowe konfiguracji bezpieczeństwa, zakładamy, że konfiguracje bezpieczeństwa o takich samych realizacjach tych wielkości są nierozróżnialne dla oceniającego (z punktu widzenia użyteczności) i mają dla niego taką samą wartość użytkową. Założenie to jest prawdziwe wtedy i tylko wtedy, gdy wyróżnione wielkości odzwierciedlają podstawowe ważne właściwości użytkowe konfiguracji bezpieczeństwa.

Zbiór $W = \overline{f}\left(KB^{u}_{dop}\right)$ dopuszczalnych konfiguracji bezpieczeństwa $KB \in KB^{u}_{dop}$ nie musi zawierać wszystkich możliwych kombinacji realizacji wielkości $(W_1 \times W_2 \times W_3 \times W_4 \times W)$ i przeważnie nie zawiera. Niektóre realizacje iloczynu kartezjańskiego $(W_1 \times W_2 \times W_3 \times W_4 \times W)$ odpowiadają, w praktyce, wariantom niedopuszczalnym lub nierealizowalnym.

Wektory realizacji wielkości odzwierciedlających właściwości użytkowe konfiguracji bezpieczeństwa nie mają w ogólności charakteru wartościującego. Do wyrażania użyteczności konfiguracji bezpieczeństwa służą funkcje kryterialne, zależne od wektorów realizacji tych wielkości W, więc funkcje kryterialne są to funkcje wektorów $\underline{w}$ lub $\overline{f}:(KB)$ określone następująco:

$$Q_m : W \to Y_m,\ m = \overline{1,M} \ \text{ lub } \ Q_m : \overline{f}\left(KB^{u}_{dop}\right) \to Y_m,\ m = \overline{1,M} \tag{6}$$

gdzie:
W, $\overline{f}\left(KB^{u}_{dop}\right)$ – zbiory wektorów realizacji wielkości,
M – liczba wyróżnionych funkcji kryterialnych.

Dopuszczalne konfiguracje bezpieczeństwa można ocenić przy użyciu wektorów:

$$\overline{Q}(KB) = \left(Q_1\left(\overline{f}\left(KB\right)\right), Q_2\left(\overline{f}\left(KB\right)\right), Q_3\left(\overline{f}\left(KB\right)\right), Q_4\left(\overline{f}\left(KB\right)\right), \ldots, Q_M\left(\overline{f}\left(KB\right)\right)\right)$$

lub

$$\underline{Q}(KB) = \left(Q_1(KB), Q_2(KB), Q_3(KB), \ldots, Q_M(KB)\right). \tag{7}$$

Dla niektórych funkcji kryterialnych $Q_m,\ m \in \hat{M}$ nie przewiduje się ich ekstremalizacji, natomiast dla tych funkcji ustala się preferencje[13]. Są one rozumiane

[13] A. Ameljańczyk, M. Kiedrowicz, *Multicriteria Methods for Identifying Patterns in the Analysis of the Flow of "Dangerous Financial Documents"*, 22th International Conference on Circuits, Systems, Communications and Computers (CSCC 2018), MATEC Web of Conference 2018, vol. 210, 04010, DOI: 10.1051/matecconf/201821004010.

w ten sposób, że poziom każdego wyróżnionego kryterium musi być osiągnięty równościowo lub przewyższony nierównościowo, czyli:

$$Q_m\left(KB\right) \geq \hat{y}_m,\ m \in \hat{M} \tag{8}$$

gdzie:
$\hat{y}_m$ – poziom preferencji (aspiracji) dla m-tej funkcji kryterialnej,
$\hat{M}$ – zbiór numerów funkcji kryterialnych, dla których nie przewiduje się ekstremalizacji.

Wartości poziomów aspiracji ustalone są przez ekspertów zespołu obsługi systemu zabezpieczeń w zależności od wymagań stawianych temu systemowi.

Sposób rozwiązywania zadania poszukiwania konfiguracji bezpieczeństwa, optymalnej lub suboptymalnej, sprowadza się do zrealizowania następujących etapów:

- Ocena i pomiar wielkości opisujących właściwości użytkowe konfiguracji bezpieczeństwa,
- Określenie zbioru funkcji kryterialnych,
- Sformułowanie problemu optymalizacji wielokryterialnej,
- Rozwiązanie zadania optymalizacji wielokryterialnej.

4. Postacie wyróżnionych funkcji kryterialnych

Dla SZ wystarczająco wiernie można ocenić i porównać użyteczność konfiguracji bezpieczeństwa, przyjmując do ich oceny następujące wskaźniki jakości:

- $Q_1\left(KB_x\right)$ – wrażliwość systemu zabezpieczeń na sytuacje utraty wymaganego poziomu bezpieczeństwa,
- $Q_2\left(KB_x\right)$ – czas generowania konfiguracji bezpieczeństwa,
- $Q_3\left(KB_x\right)$ – efektywność działania podsystemu przetwarzania informacji,
- $Q_4\left(KB_x\right)$ – redundancja w odniesieniu do zabezpieczeń o charakterze technicznym,
- $Q_5\left(KB_x\right)$ – ocena równomiernego obciążenia konfiguracji bezpieczeństwa zabezpieczeniami technicznymi.

Wyżej wymienione wskaźniki określone są następująco:

$$Q_1\left(KB_x\right) = y_1 = \frac{\overline{\overline{OB_x}}^{MAX} - \overline{\overline{OB}}^{u}}{\overline{\overline{OB}}},\ x \in X; \tag{9}$$

gdzie: $\overline{\overline{OB_x}}^{MAX}$, $\overline{\overline{OB}}^{u}$, $\overline{\overline{OB}}$ – moce zbiorów OB_x^{MAX}, OB^u, OB; przy czym:

- OB_x^{MAX} – zbiór zasobów informacyjnych, obejmujący maksymalną liczbę zasobów informacyjnych, w stosunku do których istnieje możliwość utrzymania poziomu bezpieczeństwa w ramach KB_x-tej konfiguracji bezpieczeństwa;
- OB^u – zbiór zasobów informacyjnych, w stosunku do których istnieje konieczność utrzymania wymaganego poziomu bezpieczeństwa, od chwili wystąpienia sytuacji awaryjnej o numerze u, przy ustalonych zbiorach O^u i MB^u;
- OB – zbiór zasobów informacyjnych SIO ustalonych na etapie projektowania.

$$Q_2\left(KB_x\right) = y_2 = \frac{1}{N_x}\sum_{i=1}^{N_x} t_i^x,\ x \in X; \tag{10}$$

gdzie:

- N_x – liczba przeprowadzonych eksperymentów w SZ o KB_x-tej konfiguracji bezpieczeństwa.
- t_i^x – czas generowania KB_x-tej konfiguracji bezpieczeństwa w i-tym eksperymencie.

Dążenie do skracania tego czasu stwarza możliwości:

- zmniejszenia prawdopodobieństwa przerwania ciągłości działania procesów biznesowych organizacji, a w szczególności procesu przetwarzania informacji,
- zmniejszenia prawdopodobieństwa przerwy w odbiorze informacji z otoczenia SIO wskutek chwilowego przerwania użytkowania systemu.

$$Q_3\left(KB_x\right) = y_3 = \begin{cases} \sum\limits_{r\in R_x}\left(\bar{K}_r^x - K_{KR,r}^x\right), \text{ jeżeli } \bigwedge\limits_{r\in R_x} \bar{K}_r^x \geq K_{KR,r}^x \\ -1, \text{ jeżeli } \bigvee\limits_{r\in R_x} \bar{K}_r^x < K_{KR,r}^x \end{cases},\ x \in X; \tag{11}$$

gdzie:

$\bar{K}_r^x$ – średnia liczba procesów ochronnych r-tego typu powołanych w ramach KB_x-tej konfiguracji bezpieczeństwa,

$K_{KR,r}^x$ – liczba procesów ochronnych r-tego typu niezbędna do skonstruowania konfiguracji bezpieczeństwa krytycznej na sytuacje awaryjne,

R_x – zbiór typów procesów ochronnych powołanych w ramach KB_x-tej konfiguracji bezpieczeństwa.

$$Q_4\left(KB_x\right) = y_1 = \frac{\overline{\overline{OB_x}}^{MAX} - \overline{\overline{OB}}^{u}}{\overline{\overline{OB}}},\ x \in X; \tag{12}$$

gdzie: $\overline{\overline{MB_x}}^{MAX}$, $\overline{\overline{MB}}^{u}$, $\overline{\overline{MB}}$ – moce zbiorów MB_x^{MAX}, MB^u, MB; przy czym:

- MB_x^{MAX} – zbiór mechanizmów bezpieczeństwa, obejmujący maksymalną liczbę mechanizmów bezpieczeństwa, zaimplementowanych w ramach KB_x-tej konfiguracji bezpieczeństwa,
- MB^u – zbiór mechanizmów bezpieczeństwa, w stosunku do których istnieje konieczność utrzymania wymaganego poziomu bezpieczeństwa, od chwili wystąpienia sytuacji awaryjnej o numerze u, przy ustalonych zbiorach O^u i PO^u,
- MB – zbiór mechanizmów bezpieczeństwa ustalonych na etapie projektowania SZ.

Oczywiste jest dążenie, aby wartość tego wskaźnika w znacznym stopniu przekraczała wartość krytyczną.

$$Q_5\left(KB_x\right) = y_5 = \begin{cases} \dfrac{\min\left\{\sum\limits_{j\in B_x^i} n_{ji},\ldots,\sum\limits_{j\in B_x^i} n_{jI_x}\right\}}{\max\left\{\sum\limits_{j\in B_x^i} n_{ji},\ldots,\sum\limits_{j\in B_x^i} n_{jI_x}\right\}}, \text{ jeżeli } \bigvee\limits_{\langle i,k\rangle\in I^x\times I^x}\left(\bigwedge\limits_{j\in B_x} n_{ij}\neq n_{kj}\right); \\ 1, \text{ jeżeli } \bigwedge\limits_{\langle i,k\rangle\in I^x\times I^x}\left(\bigwedge\limits_{j\in B_x} n_{ij}= n_{kj}\right) \end{cases} \tag{13}$$

gdzie:

I_x – zbiór numerów zabezpieczeń technicznych wchodzących w skład KB_x-tej konfiguracji bezpieczeństwa

B_x – zbiór numerów typów zabezpieczeń technicznych, wykorzystanych w ramach i-tego procesu ochronnego, wchodzącego w skład KB_x-tej konfiguracji bezpieczeństwa,

n_{ij} – liczba zabezpieczeń technicznych j-tego typu powołanych w ramach i-tego procesu ochronnego.

Sformułowanie zadania wielokryterialnej optymalizacji konfiguracji bezpieczeństwa oraz sposób jego rozwiązania zostały w tym artykule pominięte.

5. Ilościowa miara skuteczności Systemu Zabezpieczeń

Charakterystyki zaproponowane w punkcie 4., opisujące właściwości użytkowe konfiguracji bezpieczeństwa, można wyznaczać (mierzyć), wybierając jeden z dwu możliwych wariantów.

1. Pomiary na rzeczywistych systemach zabezpieczeń o ustalonych konfiguracjach bezpieczeństwa w warunkach symulowanego napływu zagrożeń i symulacji występowania podatności zasobów informacyjnych i zabezpieczeń o charakterze technicznym i organizacyjnym lub w trakcie użytkowania systemu zabezpieczeń przy różnych warunkach ćwiczebnych lub rzeczywistych.
2. Pomiary w symulowanym systemie zabezpieczeń o założonych konfiguracjach bezpieczeństwa.

Pierwszy sposób ma zastosowanie w odniesieniu do istniejących i eksploatowanych systemów zarządzania bezpieczeństwem informacji (SZBI), natomiast drugi do projektowanych SZBI.

Poziom bezpieczeństwa zasobów informacyjnych systemu informacyjnego organizacji jest wypadkową skuteczności działania aktualnie powołanych konfiguracji zabezpieczeń w ramach systemu zabezpieczeń. W systemie zabezpieczeń można wyróżnić dwa rodzaje konfiguracji zabezpieczeń:

1) konfiguracje zabezpieczeń technicznych,
2) konfiguracje zabezpieczeń organizacyjnych.

Konfiguracje zabezpieczeń organizacyjnych odzwierciedlają zarządcze i administracyjne aspekty bezpieczeństwa informacji, w tym odpowiedzialność w zakresie postępowania z ryzykiem. Konfiguracje zabezpieczeń technicznych odzwierciedlają aspekty techniczne i dotyczą przede wszystkim: bezpieczeństwa sprzętu, zarządzania systemami i sieciami, kontroli dostępu do sieci, kontroli dostępu do systemów operacyjnych, kontroli dostępu do aplikacji i informacji, przetwarzania mobilnego i pracy na odległość, poprawnego przetwarzania w aplikacjach, zabezpieczeń kryptograficznych oraz bezpieczeństwa plików systemowych. Dobrą praktyką jest stosowanie różnych kombinacji zabezpieczeń zarówno organizacyjnych, jak i technicznych.

Konfiguracja zabezpieczeń może spełniać wiele funkcji, np.: redukowanie, zapobieganie, odstraszanie, wykrywanie, monitorowanie, uświadomienie, odtwarzanie, udoskonalenie.

Celem działania SZ jest zapewnienie wyróżnionym zasobom informacyjnym możliwości realizacji przypisanych im zadań w warunkach zakłóceń ich funkcjonowania przez zagrożenia i podatności. Stopień realizacji tak określonego celu SZ zależy od stopnia realizacji celów przez jego konfiguracje zabezpieczeń, którymi są KZ. Zatem o poziomie skuteczności systemu zabezpieczeń stanowią poziomy skuteczności ich konfiguracji zabezpieczeń.

W pracach dotyczących teorii oceny skuteczności i efektywności, a w szczególności w odniesieniu do systemów zabezpieczeń, jako pożądane właściwości miary skuteczności podaje się:

- zgodność z celem działania systemu,
- zgodność ze wskaźnikiem skuteczności działania systemu nadrzędnego,
- wrażliwość na zmiany wartości wielkości charakteryzujących istotne właściwości użytkowe systemu i jego elementów składowych,
- możliwość wyznaczenia jej wartości,
- możliwość interpretacji zmian jej wartości.

Istotę proponowanego podejścia do ilościowej analizy skuteczności SZ przedstawimy poniżej.

Oznaczmy przez:

W – miarę skuteczności działania SZ,

Ω – zbiór możliwych wartości miary W,

I – zbiór numerów konfiguracji, wchodzących w skład SZ, $I = \{i: \ i = 1, I\}$,

J – zbiór numerów funkcji zabezpieczeń, wchodzących w skład SZ, $J = \{i: \ i = 1, J\}$.

W_I – wielkość charakteryzującą skuteczność i-tej konfiguracji, w_i – realizacja wielkości W_I, przy czym $w_i \in W$,

W_{Ij} – wielkość charakteryzującą skuteczność działania i-tej konfiguracji o j-tych funkcjach zabezpieczeń,

w_{ij} – realizację wielkości W_{Ij}, przy czym $w_{ij} \in W$.

„Udział" w skuteczności działania i-tej konfiguracji o j-tych funkcjach zabezpieczeń i przed ustalonym rodzajem zagrożeń określać będziemy za pomocą zależności:

$$W_{Ij} = W - W_{\bar{ij}} \text{ lub } W_{Ij} = \frac{W - W_{\bar{ij}}}{W} \tag{14}$$

przy czym $W_{\bar{ij}}$ – skuteczności działania SZ bez udziału i-tej konfiguracji o j-tych funkcjach zabezpieczeń. Zwraca się uwagę, że przy przyjętym sposobie oceny „udziału" i-tej konfiguracji o j-tych funkcjach zabezpieczeń zachodzą zależności:

$$W_i \neq \sum_{j \in J} W_{ij}; \ W \neq \sum_{i \in I} W_i \tag{15}$$

Powyższe wynika zarówno z możliwości występowania synergii efektów współdziałania konfiguracji zabezpieczeń organizacyjnych i technicznych, jak i różnych funkcji w nim uczestniczących. Skuteczność działania poszczególnych konfiguracji zabezpieczeń w zapewnieniu bezpieczeństwa funkcjonowania systemu informacyjnego organizacji będziemy zatem określać poprzez wpływ ich uczestnictwa w przedmiotowym przedsięwzięciu na wartość miary skuteczności tego systemu i skuteczności SZ.

Zaproponowane powyżej podejście do oceny skuteczności działania SZ lub jego elementów składowych (konfiguracji zabezpieczeń) pozwala określać użyteczność (rolę i wagę) zarówno SZ oraz jego konfiguracji mechanizmów bezpieczeństwa w zapewnieniu bezpieczeństwa zasobów informacyjnych systemu informacyjnego organizacji.

6. Podsumowanie

Bezpieczeństwo informacji było i nadal jest bardzo ważne. Środkiem do jego zapewnienia jest skuteczny system zarządzania bezpieczeństwem informacji, a jego „motorem" musi być skuteczny system zabezpieczeń – to generalna konkluzja.

System zabezpieczeń działa skutecznie, jeżeli osiąga cel – realizuje postawione mu zadania. Jednakże, aby można było w kategoriach wymiernych określać: pożądany zakres mechanizmów bezpieczeństwa niezbędnych do skutecznego reagowania na wystąpienia danego rodzaju zagrożenia lub podatności, tj. skutecznego zapewnienia zasobom informacyjnym pożądanego poziomu bezpieczeństwa, niezbędne jest przyjęcie miary (wskaźnika) skuteczności dla każdej konfiguracji zabezpieczeń. Pozwoli to oceniać i analizować skuteczność SZ oraz poziom bezpieczeństwa systemu informacyjnego organizacji.

Skuteczność działania SZ zależy od następujących czynników:

- liczebności ochranianych zasobów informacyjnych systemu informacyjnego,
- zbioru zagrożeń i podatności, jakimi charakteryzują się poszczególne zasoby informacyjne,
- ilościowego i jakościowego doboru konfiguracji technicznych i/lub organizacyjnych,
- skuteczności poszczególnych konfiguracji zabezpieczeń,
- sposobu zarządzania konfiguracjami mechanizmów bezpieczeństwa,
- sposobu podejścia do oceny skuteczności (zastosowanej metody oceny skuteczności).

Skuteczny system zabezpieczeń może powstrzymywać zagrożenia oraz sprawiać, że będą mniej efektywne i mniej prawdopodobne. Skuteczność działania SZ i KZ rozumiana jest jako pozytywnie oceniana zgodność uzyskiwanych wyników z celem działania danego systemu bezpieczeństwa organizacji.

Przykładowymi miarami skuteczności działania SZ mogą być, np.:

- stopień (wskaźnik) zgodności zastosowanych mechanizmów bezpieczeństwa (zabezpieczeń) w powołanych konfiguracjach SZ z listą zabezpieczeń wyspecyfikowanych w standardach, np. zgodność z normami PN-ISO/IEC 27001:2014–12 lub PN-ISO/IEC 27002:2014–12;
- wartość ryzyka zredukowanego $\Delta R = R_p - R_k$, gdzie R_p wartość ryzyka początkowego, R_k wartość ryzyka końcowego; ryzyko po zastosowaniu mechanizmów bezpieczeństwa;
- wskaźnik osiągnięcie ryzyka akceptowalnego;
- inne metody.

W związku ze stale zmieniającymi się warunkami zewnętrznymi organizacji zachodzi konieczność modyfikacji wdrożonych zabezpieczeń, co wymusza stosowanie następujących działań[14]:

- monitorowania i oceny skuteczności zabezpieczeń zarówno organizacyjnych, jak i technicznych;
- identyfikacji ryzyka i opracowania zasad postępowania z ryzkiem;
- wdrożenia zmodyfikowanych zabezpieczeń,
- opracowywania aktualnych deklaracji stosowania zabezpieczeń.

Do utrzymania pożądanego stanu zabezpieczeń systemu informacyjnego powinny być stosowane dwie podstawowe metody:

1) audyt systemu informacyjnego, tj. jednorazowe lub okresowo powtarzające się całościowe szacowanie poziomu bezpieczeństwa;
2) monitorowanie systemu informacyjnego, tj. działanie o charakterze ciągłym, mające na celu nadzór nad zmieniającym się systemem, jego użytkownikami oraz środowiskiem.

Konfiguracje zabezpieczeń mogą pełnić różne funkcje. Aby konfiguracje zabezpieczeń technicznych lub organizacyjnych były skuteczne, należy je starannie zaprojektować, a po wdrożeniu poddawać testowaniu w ramach prowadzonego audytu SZ.

Przy projektowaniu, wyborze oraz ocenie skuteczności zabezpieczeń należy uwzględniać trzy komplementarne punkty widzenia:

1) jak zredukować ryzyko utraty atrybutów bezpieczeństwa chronionych zasobów (orientacja na ryzyko lub atrybuty bezpieczeństwa),
2) jak wyeliminować lub zredukować prawdopodobieństwo zagrożeń poszczególnych zasobów (orientacja na zagrożenia),
3) co można zrobić, aby uchronić zasoby przed zagrożeniami lub podatnościami (orientacja na zasoby).

[14] J. Stanik, R. Hoffmann, op. cit.

Niemniej jednak nie należy wprowadzać zabezpieczeń, jeśli poziom ryzyka jest akceptowalny, nawet wtedy, jeśli istnieją podatności, gdyż nie są znane zagrożenia, które te podatności mogłyby wykorzystać. Wszystkie te ograniczenia determinują wybór konkretnych zabezpieczeń.

Bibliografia

Ameljańczyk A., Kiedrowicz M., *Multicriteria Methods for Identifying Patterns in the Analysis of the Flow of "Dangerous Financial Documents"*, 22th International Conference on Circuits, Systems, Communications and Computers (CSCC 2018), MATEC Web of Conference, vol. 210, 04010(2018), DOI: 10.1051/matecconf/201821004010.

ISO/IEC 27004: 2016 Technika informatyczna – Techniki zabezpieczeń – Zarządzanie bezpieczeństwem informacji – pomiary.

Napiórkowski J., Stanik J., Hoffmann R., *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, Konferencja naukowa pt. „Współczesne wyzwania e-Gospodarki", 2016.

Stanik J., Hoffmann R., *Model ryzyka procesów biznesowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Ekonomiczne Problemy Usług" 2017, 126/1, 325–338..

Szulim M., Kuchta M., *Metoda analizy skuteczności systemu bezpieczeństwa obiektu*, „Biuletyn Wojskowej Akademii Technicznej" 2016, vol. LIX, nr 4.

Źródła sieciowe

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

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

* * *

Evaluation of the usefulness of a security system in the information security system

Abstract

The article presents a method of assessing the usefulness of a security system (SS) and selecting the best from a set of solitary solutions after an emergency situation. It is believed that the best security system is the one that not only ensures that the required level of security of information resources is maintained, but it is characterized by the best values describing its useful properties. It is proposed that this problem should be considered as a task of multi-criteria optimization. Values describing

functional properties of SS and partial criteria of measures of its usefulness have been proposed. The functional usability, reliability and security indicators are quantitative measures of the utility of SS.

Keywords: usability, security system, security configuration