Imed EL FRAY, Jerzy PEJAŚ, Tomasz HYLA

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Wydział Informatyki, Katedra Inżynierii Oprogramowania

doi:10.15199/48.2015.11.45

Nowe podejścia w zarządzaniu ryzykiem dla systemów informacyjnych organizacji

Streszczenie. *W artykule przedstawiono nowe podejście do zarządzania ryzykiem w systemach informacyjnych zgodne z wymaganiami norm ISO/IEC. Proponowane podejście ma na celu zautomatyzowanie procesu podejmowania decyzji w sytuacjach, gdy oszacowanie ryzyka nie spełnia przyjętych przez organizację kryteriów tzw. postępowania z ryzykiem. W artykule zaproponowano także mechanizm wdrażania głównych procedur postępowania z ryzykiem (unikanie, ograniczenie, przeniesienie czy akceptowanie ryzyka) będący podprocesu zarządzania ryzykiem.*

Abstract*. The paper presents a new approach to risk management information systems compliant with the requirements of ISO/IEC. The proposed approach is designed to automate the decision-making process in situations where the risk assessment does not meet the criteria of so called risk treatment adopted by the organization. The paper also proposes a mechanism for the implementation of the main procedures of risk (avoidance, reduction, transfer or acceptance of risk) which is the sub-process of risk management (**New approach to risk management for an organization's information systems**)*.

Słowa kluczowe: analiza ryzyka, postępowania z ryzykiem, zarządzania ryzykiem.
Keywords: risk analysis, risk treatment, risk management.

Wstęp

Ciągłe innowacje technologiczne i konkurencja pomiędzy różnymi organizacjami umożliwiają klientom dostęp do coraz szerszego wachlarza usług i produktów dostarczanych przez systemy teleinformatyczne [1-3]. Szybki rozwój systemów teleinformatycznych, w tym Internetu jako medium dystrybucji produktów i usług, niesie za sobą zarówno korzyści jak również ryzyka [4,5]. Szczególne ryzyko rodzi możliwość bezprawnego ujawnienia, modyfikacji lub kradzieży informacji mających istotnych znaczenie dla organizacji [6,7,8]. Obecnie, szczególnej uwagi wymaga zapewnienie bezpiecznego dostępu do usług i informacji zawartych w tego typu systemach [9,10].

Wybór metod zapewnienia bezpieczeństwa systemów teleinformatycznych w konkretnej organizacji powinien być adekwatny do rodzaju ryzyka. Przejrzyste i aktywne podejście do analizy i zarządzania ryzykiem może nie tylko minimalizować ryzyko, lecz również kreować przewagę konkurencyjną organizacji [11,12]. Niestety minimalizacja ryzyka pociąga za sobą zawsze określone wydatki, które nie każda organizacja jest w stanie udźwignąć. W tej sytuacji dobre zdefiniowanie procesu postępowania z ryzykiem może być alternatywą dla organizacji, która chce zminimalizować ryzyka przy ograniczonym budżecie przeznaczonym na zapewnienie bezpieczeństwa swoich systemów informacyjnych.

Większość dostępnych obecnie i wdrażanych w organizacjach metod analizy i zarządzania ryzykiem takich jak MEHARI [13], NIST [14], BSI [15] z nienależytą powagą traktuje proces postępowania z ryzykiem. Wyjątkiem jest metoda CRAMM [16], która wprawdzie spełnia wymania procesu postępowania z ryzykiem, jednakże tylko w odniesieniu do dwóch z czterech podprocesów (unikanie i/lub ograniczenie ryzyka). Jest to zestaw gotowych zaleceń i rekomendacji podzielonych na 70 grup zabezpieczeń przeciwdziałających zidentyfikowanym zagrożeniom mającym wpływ na informacje, infrastrukturę fizyczną i logiczną. CRAMM pomimo spełnienia dwóch z czterech podprocesów postępowania z ryzykiem jest jednak dedykowany organizacjom, które nie mają ograniczeń budżetowych.

W niniejszym artykule przedstawiono algorytm pozwalający na wybór rozwiązania minimalizującego ryzyko dla każdego oszacowanego scenariusza ryzyka uwzględniając wszystkie podprocesy związanych z postępowaniem z ryzykiem (unikanie i/lub ograniczenie, akceptacje oraz transfer ryzyka).

Zarządzania ryzykiem w systemach informacyjnych

Zarządzania ryzykiem jest klasycznym procesem składającym się z szeregu logicznych kroków powszechnie znanych z dostępnych w literaturze norm i metod [14-19]. Rysunek 1 przedstawia proces zarządzania ryzykiem. Proces ten składa się z ustanowienia kontekstu organizacji, oceny ryzyka, postępowania z ryzykiem, akceptacji ryzyka, komunikacji ryzyka oraz monitorowania i przeglądu ryzyka. Jak widać na rysunku proces ten jest procesem iteracyjnym.

Proces zarzadzania ryzykiem w systemach informacyjnych powinien być integralną częścią wszystkich działań związanych z zarządzaniem bezpieczeństwem informacji, który analizuje na bieżąco to, co może się zdarzyć i jakie mogą być możliwe następstwa tych zdarzeń, a następnie decyduje, co i kiedy należy wykonać, aby zredukować ryzyka do akceptowalnego poziomu. Proces zarządzania ryzykiem należy monitorować i regularnie przeglądać. Każda zmiana w zarządzaniu, w kontekście czy w systemie informacyjnym organizacji może powodować zmiany dotyczące ryzyka i/lub jego poziomu. Proces ten może być zastosowany do organizacji jako całości, dowolnej części organizacji, dowolnego systemu informacyjnego, istniejących zabezpieczeń, ich planów lub wybranych aspektów (np. planowanie ciągłości działania).

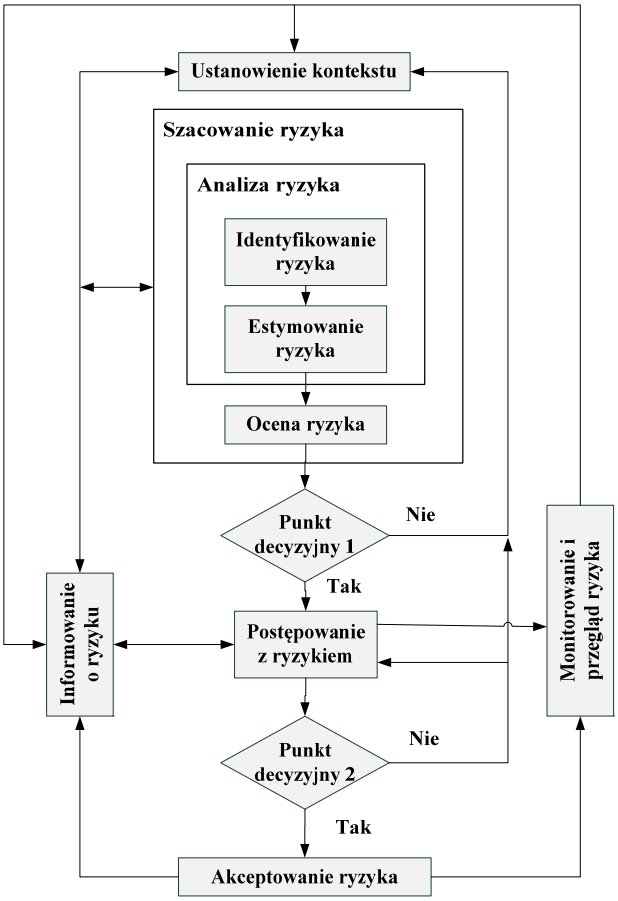
Formalny model szacowania ryzyka

Większość metod analizy i zarządzania ryzykiem oparte są na rozwiązaniach know-how opracowanych przez niezależne lub rządowe organizacje różnych krajów i przeznaczonych do zastosowania w systemach rządowych i organizacjach użytku publicznego [20]. Metody te nie bazują na formalnych modelach matematycznych, a jedynie są zbiorami dobrych praktyk z zakresu IT Governance [21].

Istnieje kilka metod bazujących na formalnych modelach [26,30]. Większość tych metod jest oparta na przedstawionym poniżej pięciofazowym modelu analizy ryzyka [22, 23]:

- Faza 1 - identyfikacja i klasyfikacja zasobów,
- Faza 2 - identyfikacja zagrożeń wraz z ich źródłem, motywem itp.
- Faza 3 - ocena ryzyka,

- Faza 4 - identyfikacja, wybór oraz implementacja zabezpieczeń – wskazane zostają zabezpieczenia pod kątem ich opłacalności, kosztochłonności oraz pilności ich wprowadzenia w organizacji.



Rys.1. Proces zarządzania ryzykiem w bezpieczeństwie informacji

- Faza 5 - implementacja systemu zabezpieczeń – nowo wybrane zabezpieczenia powinny być rozpatrywane pod kątem założonego poziomu ryzyka.

Poniżej przedstawiono podstawowe struktury matematyczne formalnego modelu analizy ryzyka o nazwie FoMRA [23] uzupełnione parametry, które pozwalają na dokładnie szacowanie (analizę i ocenę) istniejącego ryzyka w organizacji dla każdego identyfikowanego scenariusza ryzyka, który negatywne może wpływać na bezpieczeństwo organizacji.

(1) $A = \{ a_i : i = 1, ..., n_A \}$ - zbiór zasobów

(2) $V = \{ v_j : j = 1, ..., n_V \}$ - zbiór podatność

(3) $O = \{ o_k : k = 1, ..., n_O \}$ - zbiór uwarunkowań wewnętrznych i zewnętrznych wpływających na podatność zasobu,

(4) $T = \{ t_m : m = 1, ..., n_T \}$ - zbiór zagrożeń zasobów

(5) $P = \{ p_l : l = 1, ..., n_P \}$ - zbiór aktorów (źródeł zagrożeń)

(6) $S = \{ s_n : n = 1, ..., n_S \}$ - zbiór scenariusze zagrożeń

(7) $DP = \{ dp_s : s = 1, ..., n_{DP} \}$ - zbiór środki redukujące przyczyny powstania zagrożeń

(8) $DI = \{ di_t : t = 1, ..., n_{DI} \}$ - zbiór środki redukujące skutki zagrożeń

Powyższe struktury określają odpowiednio klasy podatności zasobów systemu oraz uwarunkowań wewnętrznych i zewnętrznych wpływających na podatność zasobów, klasy zagrożenia zasobów oraz źródeł tych zagrożeń, scenariusze zagrożeń, środki redukujące przyczyny powstania zagrożeń oraz środki redukujące skutki zagrożeń wynikające z utraty zasobów.

Założono również, że dany jest n-elementowy uporządkowany zbiór $\Re$ wartości dla argumentów systemu informacyjnego (SI), odpowiadających zbiorom *A, V, O, T, P, S, DP, DI oraz M, W gdzie: M i W są macierzami i wagami redukującymi* przyczyny powstania zagrożeń, skutki zagrożeń oraz ryzyka.

W zbiorze $\Re = [r_{\min}, r_{\max}] \subset N$, gdzie *N* jest zbiorem liczb naturalnych, zdefiniowano następujące pomocnicze funkcje:

- $value_A : A \to \Re^* \times \Re^* \times \Re^*$ - przypisuje danemu zasobowi $a \in A$ wartości trzech podstawowych parametrów bezpieczeństwa: *CIA* (*Confidentiality, Integrity, Availability*)
- $value_V : V \to \Re^* \times \Re^* \times \Re^*$ - przypisuje danej podatności $v \in V$ wartości trzech parametrów *AEV* (*Accident, Error, Voluntary*).

  Dla $value_A$, $value_V$ zbiór $\Re^* = \Re + \{null\}$, gdzie $null \in \Re^*$ jest wartością neutralną, która oznacza, że ze względu na to, iż określony argument funkcji nie posiada określonej cechy, to nie można mu przypisać żadnej wartości.
- $value_T : T \to \Re$ - przypisuje dane zagrożenie $t \in T$ wartości t
- $value_{DP} : DP \times S \times N \to \Re$ - przypisuje dany środek redukujący przyczyny powstania zagrożenia $d_p \in DP$ wartości d_p
- $value_{DI} : DI \times S \times N \to \Re$ - przypisuje dany środek redukujący skutek powstania zagrożenia $d_i \in DI$ wartości d_i

Dodatkowo, w celu określenia wag ryzyka $W^{s,a}$ dla każdego scenariusza zagrożeń *s* przyporządkowanego zasobowi *a* predefiniowano poniższe macierze:

- macierz redukcji przyczyny $M^s_{pot\ n\times n\times n}$, która uzależnia deklarowaną wagę środków redukujących przyczyny powstania zagrożenia $W^s_{pot}[i,j,k] \in \Re$ od $CM_{s,j}$ (dla określonego *j=dp₁, ..., $dp_{n_{DP}}$*) oraz wartości podatności $value_V(v)$,
- macierz redukcji skutku $M^s_{imp\ n\times n\times n}$, która uzależnia deklarowaną wagę środków redukujących skutki zagrożenia $W^s_{imp}[i,j,k] \in \Re$ od $CM_{s,j}$ (dla określonego *j=di₁, ..., $di_{n_{DI}}$*) oraz wartości zasobu $value_A(a)$,
- macierz ryzyka $M^{s,a}{}_{n\times n}$, która uzależnia deklarowaną wagę ryzyka $W^{s,a}[i,j] \in \Re$ od wagi W^s_{pot} wyznaczonej z macierzy $M^s_{pot\ n\times n\times n}$ oraz od wagi W^s_{imp} wyznaczonej z macierzy $M^s_{imp\ n\times n\times n}$.

$CM_{s,j} \in \Re$ jest ważoną wartością środka redukującego przyczyny powstania zagrożenia lub redukującego skutki tego zagrożenia. Poniższe równanie przedstawia sposób obliczania $CM_{s,j}$:

(9)

$$CM_{s,j} = \left\lfloor (r_{\max} - r_{\min}) \cdot \frac{\sum R_i \times P_i}{\sum P_i} + r_{\min} + 0.5 \right\rfloor$$

gdzie: $j \in DP \cup DI$ – zastosowany środek zaradczy, $\lfloor x \rfloor$ - oznacza operację zaokrąglania wyniku *x* w dół do liczby należącej do zbioru $\Re$ (do kresu dolnego liczby *x* w tym zbiorze), R_i–odpowiedź na zadane pytanie audytowe (wartość 1 lub 0), $P_i = value_X(j, s, no(R_i))$ – wartość przypisana i-temu pytaniu, przy czym *X* = *DP* lub *DI*; wartość ta zależy od określonego typu środka zaradczego *j*, scenariusza *s* oraz numeru pytania $no(R_i)$ powiązanego z odpowiedzią R_i.

Wagi zdefiniowanych macierzy M^s_{pot}, M^s_{imp} i $M^{s,a}$ uzależniono od krytyczności procesów biznesowych w danej organizacji. Krytyczność procesu zależeć będzie od wartości podatności $value_V(v)$, zasobów $value_A(a)$ oraz skuteczności implementowanych środków redukujących przyczyny powstania zagrożenia *DP* ($dp_s : s = 1,...,n_{DP}$) i jego skutek *DI* ($dp_t : t = 1,...,n_{DI}$).

Dla tak określonych macierzy wyznaczano dodatkowo także poniższe zbiory macierzy:

(10) $$M_{pot} = \bigcup_{s\,:\,\exists_{dp \in DP}(s,dp) \in \overline{DP}} \{M^s_{pot}\}$$

(11) $$M_{imp} = \bigcup_{s\,:\,\exists_{di \in DI}(s,di) \in \overline{DI}} \{M^s_{imp}\}.$$

(12) $$M = \bigcup_{(a,s) \in \overline{A \times S}} \{M^{s,a}\}.$$

Przedstawiony powyżej skrócony opis modelu nazywany jako FoMRA(1) uwzględnia podstawowe wymagania ISO/IEC 27005:2014 - Zarządzania ryzykiem w bezpieczeństwie informacji. Model FoMRA(1) umożliwia w pełni szacować ryzyka.

Postępowania z ryzykiem

Kolejną modyfikacją modelu FoMRA(1), zapewniającą jego nową funkcjonalność jest zgodność z wymaganiami ISO/IEC 27005 (postępowanie z ryzykiem) [18]. Szacowanie ryzyka odbywa się według standardowego procesu opisanego wyżej i polega na porównaniu szacunkowej wielkości ryzyka z przyjętymi przez organizację kryteriami. Określają one, czy i na ile dane ryzyko jest dla organizacji istotne, czy należy je przyjąć i jakie działania względem niego podjąć.

W przypadku uzyskania wyniku, który nie spełnia (częściowo lub w pełni) kryteriów organizacji mogą być wdrożone poniższe procesy postępowania z ryzykiem:

- ograniczenie ryzyka – podejmowanie działań, które mają na celu zmniejszenie prawdopodobieństwa powstania zagrożenia i/lub skutku tej zagrożenia lub obydwu, związanych z ryzykiem (np. zastosowanie odpowiednich zabezpieczeń),
- akceptowanie ryzyka – przyjęcie powstałych strat wynikających z określonego ryzyka (np. zaakceptować ryzyka takiego, jakie jest, ponieważ jego prawdopodobieństwo i konsekwencje są wystarczająco niskie lub średnio niskie),
- unikanie ryzyka – niedopuszczanie do działań, które mogłyby spowodować wystąpienie ryzyka,
- przeniesienie ryzyka – dzielenie strat z tytułu powstałego ryzyka ze trzecią stroną (np. ubezpieczenie przed konsekwencjami ryzyka).

Decyzja o wyborze określonej czynności (wdrożenia określonego procesu) jest na ogół oparta na szacowaniu kosztów między ryzykiem a postępowaniem z ryzykiem.

W proponowanym rozwiązaniu możemy ograniczyć ryzyko na kilka różnych sposobów (według oceny możliwości organizacji w kontekście ich zasobów i aktywów):

- wybór scenariuszy *S*, które podlegają ograniczeniu w odniesieniu do zabezpieczeń przyporządkowanych do nich (zabezpieczenia te są podzbiorami świadczonych usług w postaci środków $CM_{s,j}$ (dla określonego $j=dp_1, ..., dp_{n_{DP}}$ – redukujących przyczyny (np. zniechęcających czy zapobiegawczych), i/lub $j=di_1, ..., di_{n_{DI}}$ – redukującego skutku (ochronnych czy łagodzących)). Ograniczenie takie będzie związane z wdrożeniem nowych zabezpieczeń w miejscu tych zabezpieczeń, które są nieskuteczne lub ich brak, i które są niezbędne dla działania organizacji,
- wybór wszystkich działań, które charakteryzują się największym skutkiem w danym scenariuszu i tylko one podlegają ograniczeniu (wdrażamy tylko te zabezpieczenia, które mogą nam generować największe straty w sytuacji ich braku),
- wybór działań posiadających zabezpieczenia według możliwych ponoszonych kosztów (od najmniejszych do największych), jeśli organizacja podejmie się ich unikania, ograniczenia lub np. ich transferu (zabezpieczenia proceduralno-prawne (CS – *Control Security*), zabezpieczenia personalno-komunikacyjne (PS – *Personel security*), zabezpieczenia sprzętowo-programowe (SHS – *Software-Hardware Security*).

Powyższe sposoby ograniczenia ryzyka oraz innych możliwych sposobów, w tym akceptacji, i transferu ryzyka zostały zamodelowane poniższej (patrz rozdz. 3).

Warunki tworzenia algorytmu postępowania z ryzykiem oraz wyniki eksperymentu

Podobnie jak w przypadku innych systemów obliczeniowych, systemy zarządzania ryzykiem poddawane są nieustannym modyfikacjom lub udoskonaleniom. Zmiany te można podzielić na dwie grupy. Pierwsza z nich to różnego rodzaju optymalizacje obliczeń, w tym zmiany koncepcyjne stosowanych algorytmów lub ich optymalizacje, czy wręcz praktyczne zastosowanie różnych metod opracowanych dla rozwiązania dowolnego zadania obliczeniowego. Druga to zwiększanie funkcjonalności systemu o dodatkowe opcje lub wprowadzenie całkiem nowych możliwości. Poniżej przedstawiono algorytm, który pozwala na taką optymalizację obliczeń, aby uzyskać odpowiedni stań zabezpieczeń zasobów bez wpływu na działalność organizacji (np. niezakłócone świadczenie usług):

Dane wejściowe algorytmu są zgodne z danymi wejściowymi modelu FoMRA(1) z następującymi modyfikacjami:

- zbiór zasobów *A* jest uporządkowany w sposób następujący: zasoby są kolejno indeksowane liczbami naturalnymi większymi od zera zgodnie z kryteriami bezpieczeństwa poufności, integralności oraz dostępności,
- zbiory działań skutkowych przyporządkowanych odpowiednim scenariuszom oraz zasobom są uporządkowane według dwóch hierarchii, najpierw

według kryteriów bezpieczeństwa zasobów: poufności, integralności oraz dostępności, a następnie zgodnie z kryteriami: działania ochronne i działania łagodzące (jako działania generujące skutek dla organizacji),

- zbiór działań przyczynowych jest uporządkowany w sposób następujący: działania są kolejno indeksowane liczbami naturalnymi większymi od zera zgodnie z kryteriami: działania zniechęcające i zapobiegające. W tych kategoriach stosuje się ponadto następującą hierarchię: działania celowe, awarie oraz błędy.

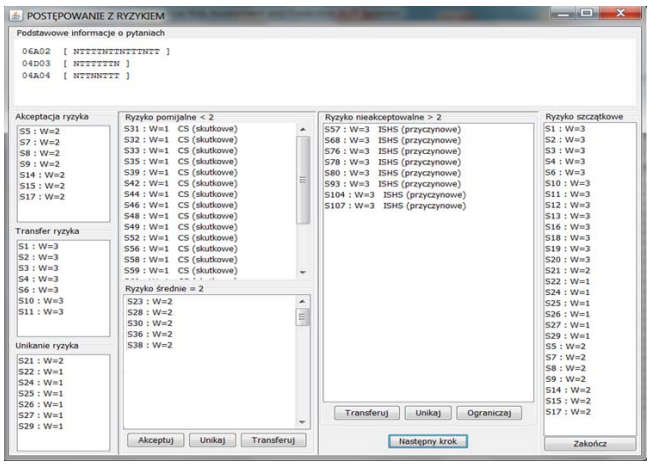
Zaprojektowany algorytm wykonuje się w dwunastu następujących fazach: najpierw rozważane są zabezpieczenia typu CS, potem PS, następnie ISHS (wybrane ważniejsze obiekty typu SHS mające przyporządkowaną wartość Max wymagające spełnienia warunku opisanego w $CM_{s,j}$, a na końcu pozostałe SHS (przynależność zmiennych $CM_{s,j}$ *(dp)* oraz $CM_{s,j}$ *(di)*). W każdym z tych przypadków występują trzy fazy obliczeń: kolejno dla akceptowanego parametru zabezpieczeń 4, 3 oraz 2 (wartość zmiennej *W[i,o]*). Wszystkie kroki algorytmu mogą być przerwane na żądania (w każdej chwili możemy transferować, akceptować czy podjąć dalsze czynności mające na celu ograniczenie i/lub unikanie ryzyka).

Poniżej na rysunku 2 przedstawiono pseudokod algorytmu dla fazy CS z poziomem czwartym. Pozostałe fazy są analogiczne. Celem jest uzyskanie jak najlepszego stanu bezpieczeństwa opisywanego systemu. W konsekwencji po zakończeniu wszystkich tych faz uzyskujemy ryzyko szczątkowe (ryzyko szczątkowe jest ostateczne wynikiem uzyskanym po podjęciu wszystkich decyzji odnośnie ostatecznej oceny stanu ryzyka oraz postępowania z ryzykiem (akceptacje, transfer, ograniczenia/unikania).

```
1.  for i=1 to nA do
2.    for o=1 to nS do
3.      cond[i,o]← true;
4.      while cond[i,o] do
5.        if W[i,o]=4 then
6.          if WI[i,o]=4 and DI(i,o)=∅ then
7.            if DP[i,o]=∅ then cond[i,o]← false
8.            else
9.              if WP[i,o]=4 then
10.               X ← DP(i,o);
11.               while X≠∅ do
12.                 if dp∈X then
13.                   if val(CM(dp))=0 and CM(dp)∈CS then
14.                     val(CM(dp))← 1;
15.                     comp(WP[i,o]);
16.                     if WP[i,o]=4then goto 22
17.                     else
18.                       comp(W[i,o]);
19                        cond[i,o]← false
20.                     endif;
21.                   endif;
22.               X← X\{dp};
23.             endwhile
24            else
25.             if WP[i,o]∈{2,3} then goto 10
26.           endif;
27.           if WP[i,o]=1 then comp W[i,o]
28.           endif;
29.         endif;
30.       endif;
31.     endif;
32.     if WI[i,o]=4 and DI(i,o)≠∅ then
33.       X ← DI(i,o);
34.       while X≠∅ do
35.         if di∈X then
36.           if val(CM(di))=0 and CM(di)∈CS then
37.             val(CM)← 1;
38.             comp(WI[i,o]);
39.             if WI[i,o]> 3 then goto 5;
40.             endif;
41.             if WI[i,o]< 3 then comp(W[i,o]);
42.             endif;
43.             if W[i,o]< 4 then goto 3;
44.             endif;
45.         endif;
46.       X← X\{di};
47.     endwhile
48.   endif;
49.   endif;
50.  endif;
51.  endwhile;
52.  endfor;
53. endfor.
```

Rys. 2. Algorytm postępowania z ryzykiem dla fazy z CM(dp), CM(di)∈CS oraz W[i,o]=4

Powyższy algorytm spełnia wymagania wytycznych normy ISO/IEC 27005 odnośnie postępowania z ryzykiem. Uzupełniony o algorytm postępowania z ryzykiem model FoMRA(1) spełnia w pełni wymagania normy odnośnie szacowania i postępowania z ryzykiem. Poniżej (patrz rysunek 3) przedstawiono graficzny przykład zastosowania algorytmu prezentowanego powyżej.



Rys. 3. Graficzne realizacja algorytmu postępowania z ryzykiem

Wprowadzone modyfikacje formalnej metody szacowania i postępowania z ryzykiem FoMRA(1) wyraźnie pokazały, że istnieje możliwość wprowadzania nowych funkcjonalności, które są istotne z punktu widzenia praktyki audytora bezpieczeństwa w branży IT i pozwalają na pełne zautomatyzowanie procesu postępowania z ryzykiem. Najważniejszym osiągnięciem wynikającym z przeprowadzonych modyfikacji, pozwalających na nową funkcjonalność jest zgodność FoMRA(1) z wymaganiami ISO/IEC 27005. Rozwiązanie to na dzień dzisiejszy jest unikatowe, gdyż żadna z obecnych metod nie charakteryzuje się automatyzacją działania procesów ograniczając się tylko do ręcznego sterowania tymi procesami.

Wnioski

Na podstawie wyników badań dotyczących postępowania z ryzykiem wykazano, że istnieje możliwość redukcji ryzyka poprzez stworzenie bazy wiedzy o wszystkich rodzajach zabezpieczeń, umożliwiającej audytorowi podejmowania decyzji związanych z unikaniem/ograniczeniem ryzyka, jego akceptacją lub transferem ryzyka według kryteriów zdefiniowanych przez organizację (nienarzuconych jak w większości modeli

biznesowych). Otrzymane wyniki potwierdzają prawidłowość przejętych założeń teoretycznych. Kierunkiem dalszych badań jest przede wszystkim rozwój FoMRA(1) umożliwiający unikania koszto- i czasochłonnych analiz, które muszą być wykonane po wprowadzeniu dowolnych zmian w systemie

LITERATURA

[1] Datta, A.: Information Technology Capability, Knowledge Assets and Firm Innovation: A Theoretical Framework for Conceptualizing the Role of Information Technology in Firm Innovation. International Journal of Strategic Information Technology and Applications. 2(2011) 9-26

[2] Raduan, C. R., Jegak, U., Haslinda, A., Alimin, I.I.: A Conceptual Framework of the Relationship Between Organizational Resources, Capabilities, Systems, Competitive Advantage and Performance. Research Journal of International Studies. 12(2009) 45-58

[3] Van Kleef, J.A.G., Roome, N.J.: Developing capabilities and competence for sustainable business management as innovation: a research agenda. Journal of Cleaner Production. 15(2007) 38-51

[4] Bhatnagar, A., Ghose, S.: Segmenting consumers based on the benefits and risks of Internet shopping. Journal of Business Research. 57 (2004) 1352–1360

[5] Byeong-Joon, M.: Consumer adoption of the internet as an information search and product purchase channel: some research hypotheses. Int. J. Internet Marketing and Advertising. 1(2004) 104-118

[6] Bumsuk, J., Ingoo, H., Sangjae L.: Security threats to Internet: a Korean multi-industry investigation. Information & Management. 38(2001) 487–498

[7] Posthumus, S., Solms, R.: A framework for the governance of information security. Computers & Security. 23(2004) 638–646

[8] Baker, W. H., Wallace, L.: Is Information Security Under Control?: Investigating Quality in Information Security Management. Security & Privacy, IEEE. 5(2007) 36 – 44

[9] Yeh, Q-J., Chang, A., J-T.: Threats and countermeasures for information system security: A cross-industry study. Information & Management. 44(2007) 480–491

[10] Ezingeard, J. N., Bowen, S. M.: Triggers of change in information security management practices. Journal of General Management. 32(2007) 53-72

[11] Whitman, M. E., Mattord, H.: Principles of Information Security. 3rd ed., course technology, Boston, US (2009)

[12] Mellado, D., Blanco, C., Sánchez, L. E., Medina, E. F.: A systematic review of security requirements engineering. Computer Standards & Interfaces. 32(2010) 153–165

[13] Méthode Harmonisée d'Analyse de Risques (MEHARI): Club de la Sécurité de l'Information Français, France (2010)

[14] G. Stoneburner, A. Goguen, A. Feringa (2002) NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, Gaithersburg, US

[15] Bundesamt für Sicherheit in der Informationstechnik (2008) BSI-Standard 100-2: IT-Grundschutz Methodology, Bonn, Deutsche

[16] Risk Analysis and Management Method (CRAMM): Central Computing and Telecommunications Agency. United Kingdom (1987)

[17] Artur Rot (2008) IT Risk Assessment: Quantitative and Qualitative Approach, Proceeding of the Word Congress on Engineering and Computer Science, WCECS 2008, San Francisco, USA

[18] ISOIEC 27005 (2008) Information technology _ Security techniques _ Information security risk management. International Organization for Standardization, Genève, Suisse

[19] EBIOS (2004) Expression des Besoins et Identification des Objectifs de Securite. DCSSI, France

[20] El Fray, I., Kurkowski, M., Pejaś, J., Mackow, W.: A New Mathematical Model for Analytical Risk Assessment and Prediction in IT Systems. Control and Cybernetics 41(2012) 1-28

[21] Moeller, R.: IT Audit, Control, and Security. John Wiley & Sons, Inc., Hoboken, New Jersey, US (2010)

[22] Risk Analysis and Management Method (CRAMM): Central Computing and Telecommunications Agency. United Kingdom (1987)

[23] El Fray, I., A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems. Computer Information Systems and Industrial Management. Springer Berlin Heidelberg, 428-442

***Autorzy**: dr hab. inż. Imed El Fray, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Katedra Inżynierii Oprogramowania, ul. Żołnierska 52, 71-210 Szczecin e-mail: ielfray@zut.edu.pl; dr hab. inż. Jerzy Pejaś, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Katedra Inżynierii Oprogramowania, ul. Żołnierska 52, 71-210 Szczecin E-mail: jpejas@zut.edu.pl; dr inż. Tomasz Hyla, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Katedra Inżynierii Oprogramowania, ul. Żołnierska 52, 71-210 Szczecin E-mail: thyla@zut.edu.pl.*