

Jerzy Stanik, Maciej Kiedrowicz

Wojskowa Akademia Techniczna

Wydział Cybernetyki

e-mail: jstanik@wat.edu.pl, mkiedrowicz@wat.edu.pl

Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych

Kody JEL: D81, G31

Słowa kluczowe: proces biznesowy, ryzyko procesu, metodyka, strategia

Streszczenie. Proponowana w artykule metodyka stanowi propozycję podejścia do analizy i zarządzania ryzykiem procesów biznesowych, biorącego pod uwagę różne kategorie czynników ryzyka z różnych obszarów działalności organizacji. Przedstawiona w niniejszej pracy metodyka podzielona jest na metodę analizy ryzyka procesów biznesowych oraz metodę zarządzania tym ryzykiem. Poziom ryzyka procesu biznesowego szacowany za pomocą proponowanej tu metody analizy ryzyka stanowi wielkość wejściową metody zarządzania ryzykiem procesów biznesowych oraz służy do opracowania strategii zarządzania ciągłością działania i strategii zapobiegania i redukcji ryzyka.

Wprowadzenie

Nowoczesna organizacja nie konkuruje już tylko ceną i jakością dostarczanych dóbr i usług, jak w organizacji klasycznej, ale także jakością i bezpieczeństwem procesów biznesowych przebiegających w jej wnętrzu. Umożliwia to dostarczenie klientom wartości, której oczekują. Dzieje się to dzięki szybkiemu reagowaniu na incydenty oraz minimalizacji przebiegów decyzyjnych.

Analizując różne podejścia do szacowania poziomu ryzyka, powstaje pytanie czy istnieje możliwość stworzenia kompletnej i spójnej metodyki analizy procesów biznesowych, uwzględniającej różne kategorie czynników ryzyka i wiążącej je w sposób pozwalający na możliwie pełne i jednoznaczne wyznaczenie poziomu ryzyka procesów biznesowych, przy jednoczesnym zachowaniu praktycznej użyteczności proponowanego podejścia. Niniejszy artykuł stanowi próbę odpowiedzi na tak postawione pytanie, pre-

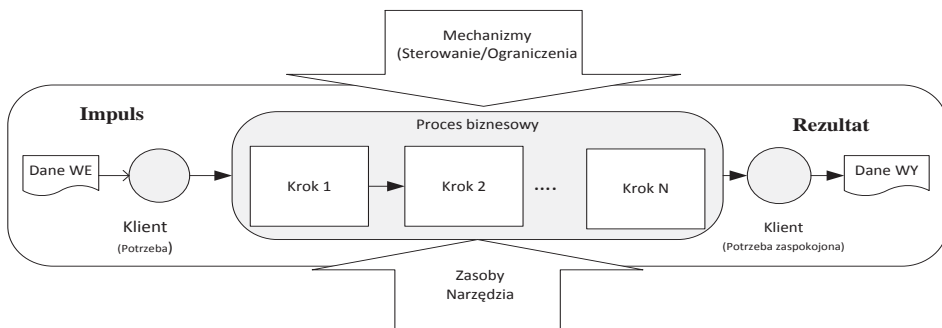
zentując opis metodyki analizy ryzyka procesów biznesowych, która jest zdaniem autorów kompletną i spójną metodyką. Koncepcję metodyki zaprezentowano w rozdziale 2. W rozdziale 3 – *Charakterystyka wyróżnionych składowych metodyki*, uszczegółowiono tę koncepcję. Elementem proponowanej metodyki jest formalizm matematyczny pozwalający na jednoznaczne wyznaczenie poziomu ryzyka procesów biznesowych. Formalizm ten wprowadzono w punktach 3.5.2 – 3.5.4.

1. Podstawowe definicje i określenia

Na potrzeby dalszych rozważań przyjmijmy poniższe definicje i określenia.

Metodyka – to zbiór wytycznych oraz dobrych praktyk dotyczących sposobów postępowania w zakresie działań, metod, technik i narzędzi, które należy stosować przy określonej pracy lub dla osiągnięcia określonego celu.

Proces biznesowy – jest uporządkowanym ciągiem czynności służącym zaspokojeniu potrzeby klienta procesu. Podstawowe elementy składowe procesu przedstawiono na rysunku 1 – jest to zespół czynności lub działań, których celem jest osiągnięcie oczekiwanego rezultatu. Rezultat ten jest osiągany przez przetworzenie stanu wejścia procesu w stan wyjściowy. Przetworzenie to sterowane jest za pomocą z góry ustalonych reguł. Do osiągnięcia tak określonego rezultatu wymagane są określone zasoby. Definicja ta określana jest terminem ICOM (*Input, Control, Output, Mechanism*).



Rysunek 1. Proces biznesowy i jego elementy

Źródło: opracowanie własne.

Organizacja O – nazywamy celowo stworzony zespół zasobów ludzkich, kapitałowych, ideowych oraz działań biznesowych i procesów biznesowych powiązanych ze sobą dla realizacji określonych celów.

Zbiór procesów biznesowych organizacji – $P(O)$ – nazywamy skończony i przeliczalny zbiór procesów biznesowych $P(O) = \{P_1, P_2, \dots, P_i, \dots, P_N\}$, gdzie: N – jest liczbą procesów biznesowych organizacji O . Organizację definiuje się również jako „zbiór zmiennych procesów biznesowych pozostających ze sobą w różnych relacjach wzajem-

nej zależności. Organizacja staje się przestrzenią, w ramach której dokonują się procesy integrowania ludzi wokół zadań i problemów do rozwiązania. Stąd też wynika potrzeba łączenia różnych treści pracy, komponowania zadań w procesy oraz tworzenia struktury organizacyjnej według tychże procesów, a nie według ośrodków władzy lub specjalizacji funkcjonalnej (Sikorski, 1998).

Ryzyko procesów biznesowych – na potrzeby metodyki prezentowanej w niniejszym artykule, ryzyko procesów biznesowych definiowane jest jako zagrożenie, podatność lub luka (np.: informacyjna, bezpieczeństwa), że różnego typu technologie, np.: informatyczna, projektowa, produkcyjna, stosowane w danej organizacji (niezależnie od jej rodzaju i skali działalności) nie spełniają wymogów biznesowych, nie zapewniają odpowiedniej jakości, bezpieczeństwa, integralności i dostępności lub ciągłości działania procesów biznesowych, nie zostały odpowiednio wdrożone i nie działają zgodnie z założeniami lub wymaganiami przyjętych polityk. W związku z powyższym, ryzyko procesów biznesowych rozpatrywane jest w podziale na różne kategorie (PN-ISO 31000, 2012): bezpieczeństwo, jakość, ciągłość działania oraz architektura procesu biznesowego.

2. Koncepcja metodyki analizy ryzyka procesów biznesowych

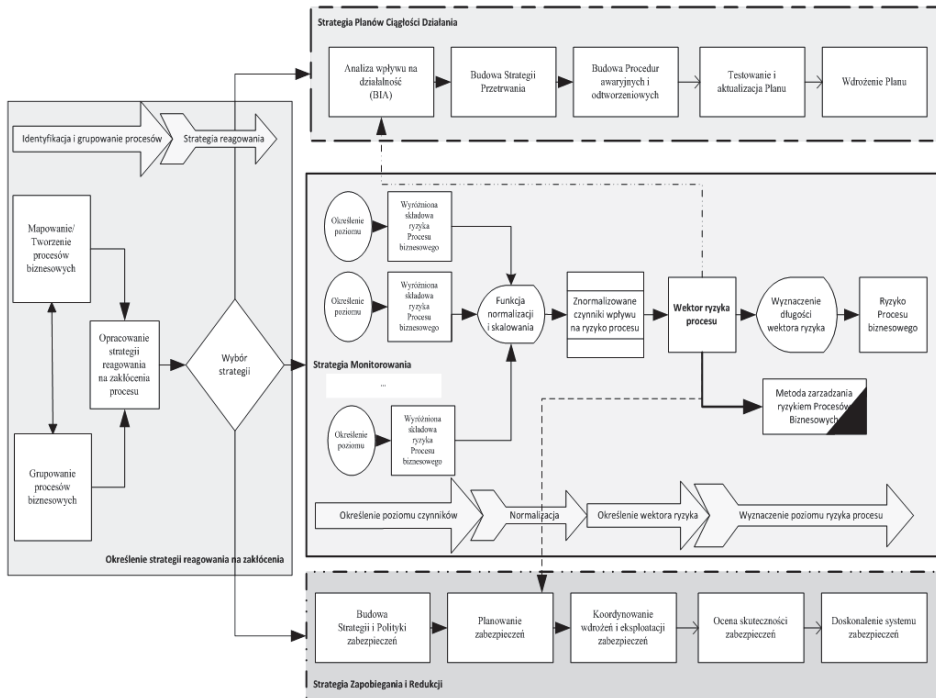
2.1. Założenia

W przedstawionej tu metodyce wzięto pod uwagę możliwość wyboru dowolnego podzbioru (np. kluczowych, podstawowych, pomocniczych lub zarządczych) procesów biznesowych danej organizacji, dlatego wyróżniono w niej etap polegający na wyborze tylko tych procesów biznesowych, które będą objęte analizą ryzyka i późniejszym zarządzaniem tym ryzykiem. Pozwala to na elastyczną i stosunkowo obiektywną analizę ryzyka procesów biznesowych całej organizacji. Oczywiście nic nie stoi na przeszkodzie zastosować proponowaną metodykę we wszystkich procesach biznesowych organizacji.

Dodatkowo, proponowana w niniejszym artykule metodyka zakłada, że każda zmiana w procesie biznesowym, powodująca zmianę jego poziomu ryzyka, wpływa wyłącznie na ten proces i nie przenosi się na inne procesy biznesowe organizacji. Z założenia tego wynika, że jeden wektor zmiany ryzyka procesu biznesowego dotyczyć może wyłącznie jednego procesu biznesowego.

2.2. Koncepcja metodyki

Ogólny schemat działania proponowanej metodyki zaprezentowano na rysunku 2.



Rysunek 2. Wyróżnione składowe ryzyka procesów biznesowych

Źródło: opracowanie własne.

Elementami składowymi przedstawionej metodyki są:

1. Mapowanie/tworzenie procesów biznesowych, obejmujące identyfikację i grupowanie procesów biznesowych, opisane w rozdziale 3.1. *Mapowanie procesów biznesowych*.
2. Opracowanie strategii reagowania na zakłócenia procesu i dokonanie wyboru postępowania z incydentem, opisane w rozdziale 3.2. *Opracowanie i wybór strategii reagowania na zakłócenia procesu biznesowego*.
3. Strategia planów ciągłości działania procesów biznesowych, opisana w rozdziale 3.3. *Strategia planów ciągłości działania procesów biznesowych*.
4. Strategia Zapobiegania i Redukcji, opisana w rozdziale 3.4. *Strategia Zapobiegania i Redukcji*.
5. Strategia monitorowania obejmująca metodę oceny ryzyka procesów biznesowych oraz metodę zarządzania tym ryzykiem, opisana w rozdziale 3.5. *Metoda oceny ryzyka procesów biznesowych*.

3. Charakterystyka wyróżnionych składowych metodyki

3.1. Mapowanie procesów biznesowych

Aby możliwe było monitorowanie procesów biznesowych, konieczna jest ich identyfikacja, analiza i modelowanie. Prace te niejednokrotnie noszą nazwę mapowania procesów. Mapowanie procesów to graficzne przedstawienie przepływu wartości z perspektywy klienta w procesach biznesowych przedsiębiorstwa. Celem mapowania jest identyfikacja miejsc występowania marnotrawstwa oraz, przez dokonanie wielu analiz, stworzenie wizji stanu przyszłego, eliminując lub redukując marnotrawstwo. Budowanie mapy nie może być celem samym w sobie. Celem jest zaprojektowanie i wdrożenie takiego przepływu, w którym skupiamy się na dodawaniu wartości. Ich wynikiem są tzw. graficzne mapy procesów biznesowych. W zależności od przyjętej koncepcji mapy procesów mogą obejmować wszystkie obszary zarządzania bądź tylko wybrany obszar funkcjonalny przedsiębiorstwa.

Mapowanie procesów przebiega w dwóch zasadniczych etapach. Pierwszym z nich jest identyfikacja procesów. Identyfikacji tej można dokonać dwoma metodami – metodą odgórną (*top-down*), gdzie w pierwszej kolejności określa się ogólną działalność organizacji wraz z jej celami, a następnie przechodzi się do uszczegółowienia wskazanych elementów. Metodą oddolną (*bottom-up*), bardziej czasochłonną, jednak dokładniejszą, która polega na analizie wykonywanych w organizacji czynności i na podstawie nich formułowanie przebiegających procesów. Po dokładnej identyfikacji procesów należy przejść do ich klasyfikacji lub pogrupowania. Najczęściej stosuje się grupowanie na:

- procesy zarządzania związane z misją, celami, strategią i pozycją na rynku,
- procesy główne związane z tworzeniem rezultatów organizacji,
- procesy wspomagające związane z klientem wewnętrznym, np. rekrutacja, zaopatrzenie, zarządzanie infrastrukturą.

W literaturze przedmiotu można znaleźć wiele różnych opisów metod procesów, które służą do opracowania modeli zgodnych z koncepcjami BPMS. Do najważniejszych narzędzi stosowanych w modelowaniu procesów biznesowych można zaliczyć: diagramy aktywności i diagramy stanów (Bruegge, Dutoit, 2011), notacje IDEF3 oraz IDEF0 (Nowosielski, 2009), notacja i diagramy EPC (Nowicki, Marczak, 2009) czy język i notacja BPMN (Piotrowski, 2009). Cechy modeli EPC oraz BPMN powodują, że notacje te są bardzo często wykorzystywane w identyfikacji i modelowaniu procesów biznesowych.

3.2. Opracowanie i wybór strategii reagowania na zakłócenia procesu biznesowego

W zależności od wielkości wpływu zakłócenia (incydentu) na organizację lub proces biznesowy i prawdopodobieństwa wystąpienia zakłócenia wyróżniamy cztery podstawowe strategie reagowania na zagrożenia (Zawiła-Nadźwiecki, 2003):

1. Strategia tolerowania (T) – powinna być stosowana w przypadku zakłóceń zewnętrznych nieinwazyjnych i niedestrukcyjnych, rzadko występujących, mających mały wpływ na organizację/proces biznesowy, przemijających samoistnie i niepowodujących trwałych szkód.
2. Strategia monitorowania (M) – dotyczy postępowania z zakłóceniami drobnymi, niedestrukcyjnymi, ale często występującymi, o dostatecznej informacji o zakłóceniach do uruchomienia mechanizmów kompensacji.
3. Strategia zapobiegania (Z) – nazywana strategią prewencji jest stosowana w przypadkach dużego prawdopodobieństwa wystąpienia zakłóceń istotnych elementów działalności, a w szczególności wrażliwych elementów infrastruktury technicznej, których stopień destrukcji jest nieakceptowany.
4. Strategia Planów Ciągłości (P) – dotyczy postępowania z zakłóceniami istotnymi, destrukcyjnymi o bardzo małym prawdopodobieństwie wystąpienia. Ze względu na niskie potencjalne prawdopodobieństwo wystąpienia katastrof mogących spowodować kryzys, ekonomicznie uzasadniona jest rezygnacja ze Strategii (Z) i uprzednie przygotowanie planu postępowania w sytuacjach kryzysowych.

W przedstawionej metodyce wzięto pod uwagę wszystkie wyżej wymienione strategie.

Główny nacisk położono przede wszystkim na strategię zapobiegania i tolerowania, co pozwala na jednoznaczne wyznaczenie poziomu ryzyka procesów biznesowych i zarządzanie nim.

3.3. Strategia planów ciągłości działania procesów biznesowych

Strategia planów ciągłości działania procesów biznesowych składa się z następujących faz:

1. Identyfikacja kluczowych procesów i ich zasobów; Analiza ryzyka.
2. Analiza wpływu zdarzenia na przedsiębiorstwo (*Business Impact Analysis* BIA).
3. Budowa Strategii Przetrwania:
 - Budowa Minimalnej Akceptowalnej Konfiguracji,
 - Analiza dostępnych i brakujących rozwiązań,
 - Opracowanie Strategii Przetrwania (rozwiązania, harmonogram, budżet).
4. Budowa procedur awaryjnych i odtworzeniowych.

5. Testowanie i aktualizacja Planu.
6. Wdrożenie Planu (budowa świadomości pracowników, program szkoleń).

Celem nadrzędnym realizacji analizy BIA jest określenie krytyczności ocenianych procesów, co pozwala na oszacowanie ważności zasobów organizacji, realizowanych w ramach tych procesów: tzn. zasobów IT (systemów informatycznych, infrastruktury informatycznej), lokalizacji oraz krytycznych (co do ilości i umiejętności) zasobów ludzkich. W praktyce analiza BIA powinna prowadzić do utworzenia:

- listy procesów krytycznych wraz z informacją określającą jak długo (maksymalnie) proces może nie być dostępny,
- listy zasobów realizujących te procesy krytyczne (tzn. zasobów IT, lokalizacji oraz kluczowych pracowników),
- listy kluczowych produktów organizacji (czyli produktów, które są realizowane przez procesy wskazane przez organizację jako krytyczne).

Ważnym etapem BIA jest wyznaczenie parametrów RTO i RPO dla każdego z analizowanych procesów: *Recovery Time Objective* – to czas potrzebny, aby wznowić proces przerwany w wyniku awarii; *Recovery Point Objective* – określa akceptowalny poziom utraty danych wyrażony w czasie. Przy założeniu, że dla danego procesu nie dopuszcza się utraty żadnych danych, przyjmuje się $RPO = 0$.

Zarządzanie ciągłością biznesową oparte na Strategii Planów Ciągłości (P), nie powinno być działalnością wyizolowaną w ramach organizacji. Bardzo ważne jest, aby zapewnienie możliwości ciągłego działania w naturalny sposób wynikało z celów organizacji, strategii ich osiągnięcia oraz potencjalnego wpływu zakłóceń na procesy biznesowe.

3.4. Strategia Zapobiegania i Redukcji

Strategia Zapobiegania i Redukcji składa się z następujących faz:

- Budowa Strategii i Polityki zabezpieczeń, Planowanie zabezpieczeń,
- Koordynowanie wdrożeń i eksploatacji zabezpieczeń,
- Ocena skuteczności zabezpieczeń, Doskonalenie systemu zabezpieczeń.

Polityka zabezpieczeń powinna zawierać:

- definicję celów zabezpieczenia procesu biznesowego,
- strukturę organizacyjną oraz zdefiniowanie odpowiedzialności za wszystkie aspekty zabezpieczenia,
- opis strategii zarządzania ryzykiem,
- określenie wymagań dotyczących zabezpieczenia procesu biznesowego, a w szczególności: zdefiniowanie klas poufności informacji, określenie obszarów zabezpieczenia procesu, zdefiniowanie oraz wdrożenie procedur i regulaminów postępowania, zapewniających osiągnięcie i utrzymanie stanu bezpieczeństwa procesu biznesowego,
- opis wybranych mechanizmów zabezpieczeń,
- sposób akredytacji zabezpieczenia procesu biznesowego.

Do realizacji polityki i planu zabezpieczeń konieczny jest wybór właściwych środków zabezpieczeń. Jest to proces złożony, który powinien uwzględniać następujące aspekty: technologię, procedury, kadry oraz organizacyjne i techniczne zabezpieczenia. Ważne jest zrozumienie, w jaki sposób każdy z tych środków oddziałuje na proces biznesowy i organizację. Pamiętając zatem o tzw. dobrych praktykach oraz wytycznych (PN-ISO/IEC 27005, 2013) zaleca się, aby:

- wybór zabezpieczeń był właściwy i uzasadniony oraz pozwolił spełnić wymagania zidentyfikowane w procesie szacowania i postępowania z ryzykiem,
- wybór ten uwzględniał zarówno kryteria akceptowania ryzyka, jak i wymagania wynikające z przepisów prawa, regulacji oraz zobowiązań kontraktowych,
- wybór ten uwzględniał koszt i czas wdrożenia zabezpieczeń lub aspekty techniczne, środowiskowe i kulturowe funkcjonowania procesu biznesowego.

Często jest możliwe obniżenie całkowitych kosztów użytkowania procesu biznesowego poprzez właściwy wybór zabezpieczeń związanych z bezpieczeństwem informacji.

3.5. Metoda oceny ryzyka procesów biznesowych

Ocena poziomu ryzyka, dla każdego z procesów biznesowych organizacji przebiega zgodnie z następującymi krokami.

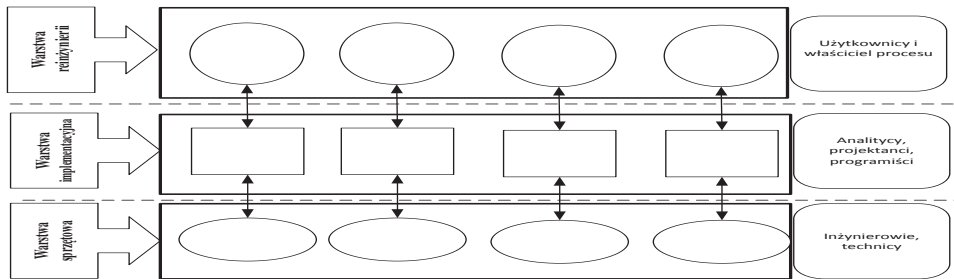
- określenie poziomu czynników wpływających na ryzyko,
- normalizacja wyznaczonych wartości czynników wpływających na ryzyko,
- określenie wektora ryzyka na podstawie znormalizowanych wielkości składowych ryzyka,
- wyznaczenie ostatecznego poziomu ryzyka dla danego procesu biznesowego.
-

3.5.1. Określenie poziomu czynników wpływających na ryzyko

W metodzie bierze się pod uwagę dowolną liczbę grup czynników, które zdaniem autorów pozwalają na stosunkowo obiektywną i dokładną ocenę poziomu ryzyka procesów biznesowych. Przykładową listą grup czynników przedstawiono poniżej:

1. W obszarze bezpieczeństwa informacji następujące atrybuty: Dostępność procesu biznesowego, Poufność przetwarzanych danych przez proces, Integralność procesu, Spełnienie wymagań bezpieczeństwa zawartych w polityce bezpieczeństwa, Straty procesu rozumiane jako koszty poniesione w wyniku utraty przypisanych atrybutów bezpieczeństwa.
2. W obszarze ciągłości działania następujące atrybuty: Spełnienie wymagań zawartych w polityce bezpieczeństwa z zakresu ciągłości działania procesów, Skutki finansowe wstrzymania/przerwania realizacji procesu, Skutki pozafinansowe wstrzymania/przerwania realizacji procesu, Koszty i czas niedostępności procesu.

3. W obszarze jakości procesu biznesowego następujące atrybuty: Elastyczność procesu, Znaczenie dla Organizacji i Klienta, Spełnienie wymagań zawartych w polityce jakości, Koszty oraz długość realizacji procesu.
4. W pozostałych obszarach: Efektywność zarządzania zmianami, Niezawodność.



Rysunek 3. Warstwowy model procesu biznesowego w organizacji na potrzeby analizy ryzyka

Źródło: opracowanie własne.

Poziom szczegółowości wyróżnionych składowych ryzyka powinien wynikać z zależności pomiędzy analizą ryzyka a architekturą procesów biznesowych organizacji. Warstwowy model architektury procesu biznesowego w organizacji na potrzeby analizy ryzyka przedstawiono na rysunku 3.

3.5.2. Normalizacja

Ze względu na to, że składowe ryzyka procesów biznesowych należą z reguły do różnych zbiorów wartości, konieczne jest wprowadzenie funkcji lub zbioru funkcji jednoznacznie odwzorowujących te składowe na jednolity przedział wartości $[1, \dots, N]$. Przyjęcie przedziału wartości $[1, \dots, N]$ wynika z dążenia do jak najprostszego kształtu funkcji odwzorowujących składowe prezentowanego modelu na jednolity przedział wartości, przy jednoczesnym zapewnieniu czytelności wyników analizy ryzyka. Wykluczenie z tego przedziału wartości mniejszych od 1, a w szczególności wartości 0, wiąże się koncepcją ryzyka szczątkowego (*residual risk*) (Hash, 2002), w myśl której nie istnieje możliwość całkowitego wyeliminowania ryzyka, a zatem żadna ze składowych ryzyka prezentowanej w niniejszej pracy metody analizy ryzyka procesów biznesowych również nie może być wielkością zerową. W celu odwzorowania wielkości poszczególnych składowych ryzyka procesów biznesowych na jednolity przedział wartości, wprowadzamy pojęcie funkcji normalizacji. Funkcją normalizacji nazywamy rodzinę funkcji $\xi: X \rightarrow [1, 2, \dots, N]$ określoną dla wyróżnionych składowych ryzyka procesów biznesowych. Przykładowo dla składowej dostępności procesu biznesowego – λ_{P_i} i poufności danych przetwarzanych przez ten proces – α_{P_i} , funkcje ξ_λ, ξ_α ; przy czym: $P_i \in P(O)$, $\xi \in \Xi$ oraz przedział wartości $[1, \dots, 8]$, $\lambda \in \Lambda$ – zbiór klas dostępności, $\alpha \in A$ – zbiór klas poufności, określone na mogą być następująco:

$$\xi_\lambda(\lambda_{P_i}) = \begin{cases} 1, & \text{gdy } \lambda_{P_i} = VI \\ 2, & \text{gdy } \lambda_{P_i} = V \\ 3, & \text{gdy } \lambda_{P_i} = IV \\ 4, & \text{gdy } \lambda_{P_i} = III \\ 5, & \text{gdy } \lambda_{P_i} = II \\ 7, & \text{gdy } \lambda_{P_i} = I \end{cases}; \quad \xi_\alpha(\alpha_{P_i}) = \begin{cases} 1, & \text{gdy } \alpha_{P_i} = F \\ 2, & \text{gdy } \alpha_{P_i} = E \\ 3, & \text{gdy } \alpha_{P_i} = D \\ 4, & \text{gdy } \alpha_{P_i} = C \\ 6, & \text{gdy } \alpha_{P_i} = B \\ 8, & \text{gdy } \alpha_{P_i} = A \end{cases} \quad (1)$$

Wzory dla pozostałych składowych, wymienionych w rozdziale 3.5.2. Czynniki mające wpływ na ryzyko procesu biznesowego, można znaleźć w publikacji J. Stanika (w druku).

Postacie funkcji normalizacji z rodziny Ξ określone powinny być w taki sposób, aby odwzorować ich wartości na przedział $[1, \dots, N]$, oraz aby zachować właściwe proporcje ich wpływu na ryzyko procesów biznesowych. Dodatkowym ograniczeniem jest, aby liczba M wyróżnionych funkcji normalizacji z rodziny Ξ powinna dać się wyrazić w postaci iloczynu dwóch liczb naturalnych większych od 1, czyli $\|\Xi\| = M = m \times n$, $m > 1, n > 1$. Ponadto należy dążyć, aby iloczyn $M \times N \cong 100$, wtedy wyliczoną długość wektora ryzyka procesu biznesowego można mierzyć w skali procentowej i łatwo interpretować.

3.5.3. Wektor ryzyka procesu biznesowego i jego wielkość

Mając określoną bazę przestrzeni wektorowej $(M_{m \times n}, \mathbf{R}, +, \cdot)$ w algebrze $(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes)$, można wprowadzić pojęcie wektora ryzyka procesu biznesowego. Wektorem ryzyka procesu biznesowego P_i w algebrze $(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes)$ nazywamy wektor $\vec{R}_{P_i} \in M^{m \times n}$ będący kombinacją liniową elementów ryzyka systemu P_i w bazie przestrzeni liniowej $(M_{m \times n}, \mathbf{R}, +, \cdot)$:

$$\vec{R}_{P_i} = \xi_{\alpha^1}(\alpha_{P_i}^1) \cdot \vec{\alpha}^1 + \xi_{\alpha^2}(\alpha_{P_i}^2) \cdot \vec{\alpha}^2 + \dots + \xi_{\alpha^M}(\alpha_{P_i}^M) \cdot \vec{\alpha}^M \quad (2)$$

Wymiar algebry $(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes)$ (Trajdos, 1993) wynosi:

$$\dim(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes) = M.$$

Z tego, że wymiar algebry $(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes)$ wynosi N wynika, że istnieje N wektorów bazowych przestrzeni wektorowej $(M_{m \times n}, \mathbf{R}, +, \cdot)$ z algebry $(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes)$, zdefiniowanych następująco:

$$\vec{\alpha}^1 = \begin{pmatrix} 1 & \dots & 0^n \\ \vdots & \ddots & \vdots \\ 0^m & \dots & 0^M \end{pmatrix}; \dots; \vec{\alpha}^M = \begin{pmatrix} 0 & \dots & 0^n \\ \vdots & \ddots & \vdots \\ 0^m & \dots & 1 \end{pmatrix} \quad (3)$$

Z kombinacji liniowej powyższego wzoru wynika, że wpływ wszystkich M wymiarów analizy ryzyka procesów biznesowych na uzyskany wektor ryzyka $\vec{R}_{P_i} \in M^{m \times n}$ jest jednakowy. W celu uszczegółowienia oszacowania poziomu ryzyka procesu biznesowego może być dlatego konieczne przypisanie poszczególnym składowym ryzyka wag ich wpływu na końcowy poziom ryzyka procesu biznesowego oraz modyfika-

cja współrzędnych wektora ryzyka $\overrightarrow{R_{P_i}} \in M^{m \times n}$ z wykorzystaniem tych wag wpływu. W niniejszym artykule to zagadnienie pominięto.

3.5.4. Wyznaczenie ostatecznego poziomu ryzyka dla danego procesu biznesowego

Mając zdefiniowane pojęcie wektora ryzyka procesu biznesowego w algebrze $(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes)$, możemy ostatecznie wprowadzić definicję całkowitego ryzyka procesu biznesowego P_i . Ryzykiem procesu biznesowego P_i w algebrze $(M_{m \times n}, \mathbf{R}, +, \cdot, \otimes)$ nazywamy liczbę $R_{P_i} \in \mathcal{R}$ równą długości wektora, będącego wektorem ryzyka procesu biznesowego P_i , czyli:

$$R_{P_i} = \|\overrightarrow{R_{P_i}}\| \quad (4)$$

Przedstawiona wielkość R_{P_i} określa w sposób ilościowy wielkość ryzyka procesu biznesowego P_i , co stanowi wielkość wynikową proponowanej w niniejszej pracy metody analizy ryzyka procesów biznesowych. W celu jakościowego przedstawienia poziomu ryzyka wyznaczonego za pomocą przedstawionej powyżej metody ilościowej, można przyjąć następujące przedziały ryzyka:

$R_{P_i} > 70$ – ryzyko katastroficzne,

$R_{P_i} \in (60, \dots, 70]$ – ryzyko bardzo wysokie,

$R_{P_i} \in (50, \dots, 60]$ – ryzyko wysokie,

$R_{P_i} \in (40, \dots, 50]$ – ryzyko średnie,

$R_{P_i} \in (30, \dots, 40]$ – ryzyko niskie,

$R_{P_i} \in (20, \dots, 30]$ – ryzyko bardzo niskie,

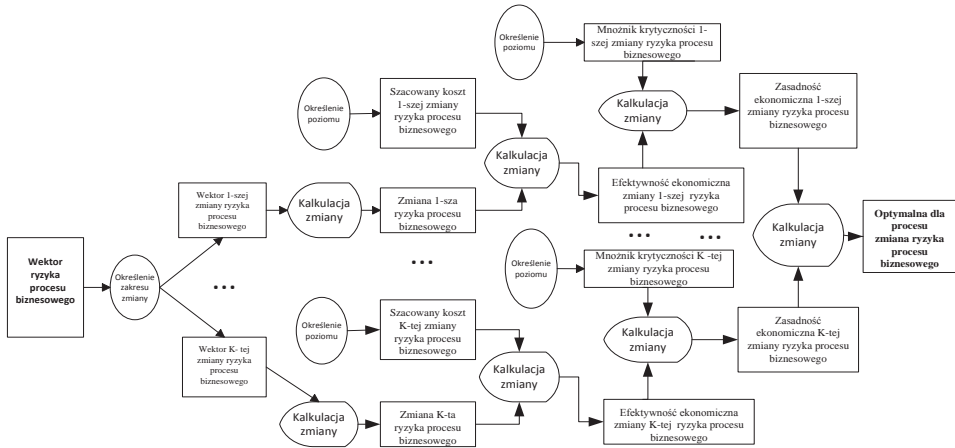
$R_{P_i} < 20$ – ryzyko śladowe.

Powyższe przedziały wartości wyznaczono przy następujących założeniach:

- 12 wymiarów analizy ryzyka procesów ($M = 12$),
- funkcje $\xi \in \Xi$ jednoznacznie odwzorowują te składowe na jednolity przedział wartości $[1, \dots, 8]$.
- na podstawie praktycznego wykorzystania metodyki prezentowanej w niniejszym artykule.

3.6. Metoda zarządzania ryzykiem

Ogólny schemat działania proponowanej metody zarządzania ryzykiem procesów biznesowych zaprezentowano na rysunku 4.



Rysunek 4. Ogólny schemat działania proponowanej metody zarządzania ryzykiem systemów

Źródło: opracowanie własne.

Wyznaczona w poprzednim rozdziale wielkość ryzyka procesu biznesowego ma wartość informacyjną, określającą ogólny poziom zagrożeń związanych z danym procesem i stanowi punkt wyjścia dla dalszego etapu zarządzania ryzykiem, który powinien prowadzić do wybrania i implementacji efektywnych ekonomicznie mechanizmów i zabezpieczeń ograniczenia ryzyka procesu biznesowego bądź zaakceptowania jego bieżącego poziomu. Wykonanie operacji „Wprowadzenie zabezpieczeń dotyczących procesu biznesowego”, dążącej do zmiany poziomu ryzyka tego procesu, prowadzi do wyznaczenia nowych współrzędnych wektora opisującego stan ryzyka procesu biznesowego. Zmianę współrzędnych wektora ryzyka, w prezentowanym modelu, odzwierciedla wektor zmiany ryzyka systemu informatycznego:

$$\overrightarrow{\Delta R_{P_i}^k} = \overrightarrow{R_{P_i}^k} - \overrightarrow{R_{P_i}} \quad (5)$$

gdzie: $k \in \{1, \dots, K_{P_i}\}$; K_{P_i} – jest liczbą fizycznie wykonalnych rozważnych zmian w procesie P_i wpływających na wielkość ryzyka procesu biznesowego P_i . Ponieważ możliwe jest przejście z jednego poziomu ryzyka procesu P_i , pisanego wektorem $\overrightarrow{R_{P_i}}$ do wielu różnych poziomów ryzyka, to na etapie analizy fizycznie wykonalnych operacji mogących wpłynąć na ryzyko procesu, poszczególne wektory zmian ryzyka procesu oznaczane są indeksem $k \in \{1, \dots, K_{P_i}\}$. Zatem $\overrightarrow{\Delta R_{P_i}^k}$ określa wielkość zmiany ryzyka procesu P_i , wynikającej z k -tej zmiany w ryzyka w procesie P_i , wpływającej na wielkość ryzyka tego procesu biznesowego.

Każda zmiana wielkości ryzyka wiąże się z wykonaniem pewnych modyfikacji w procesie biznesowym, a te z kolei wiążą się z poniesieniem określonych kosztów, dlatego oceniając dostępne modyfikacje w procesie biznesowym, prowadzące do zmniejszenia poziomu ich ryzyka, należy uwzględnić czynnik ekonomiczny tych zmian.

Należy mieć na uwadze, że większość zmian zmierzających do ograniczenia ryzyka systemów informatycznych będzie rozciągnięta w czasie, zatem do prawidłowego oszacowania realnego kosztu ich wprowadzenia należy wykorzystać metodę kalkulacji kosztów uwzględniającą zmianę wartości pieniądza w czasie.

Mając określone pojęcie zmiany ryzyka procesu (wzór 5) oraz pojęcie kosztu tej zmiany wyrażonego wzorem (6):

$$\mathcal{B}_{\Delta R_{P_i}^k} = \sum_{l=0}^L \frac{O_{P_i}^{k,l} - I_{P_i}^{k,l} - W_{P_i}^{k,l} - \Delta \eta_{P_i}^k}{(1+r)^l} \quad (6)$$

można określić termin efektywności ekonomicznej zmiany ryzyka systemu informatycznego, zgodnie z poniższym wzorem (Ryba, 2004):

$$\mathcal{A}(\overrightarrow{\Delta R_{P_i}^k}) = \frac{\Delta R_{P_i}^k}{\mathcal{B}_{\Delta R_{P_i}^k}} \quad (7)$$

gdzie:

L – długość okresu, na jaki planowana jest eksploatacja procesu P_i , (w latach),

$O_{P_i}^{k,l}$ – oszczędności w l -tym roku wynikające z opisanej wektorem,

$\overrightarrow{\Delta R_{P_i}^k}$ – zmiany ryzyka procesu P_i , np. w postaci obniżonych składek ubezpieczeniowych,

$I_{P_i}^{k,l}$ – wydatki inwestycyjne w l -tym roku na proces P_i , związane z wdrożeniem opisanej wektorem $\overrightarrow{\Delta R_{P_i}^k}$ zmiany ryzyka procesu P_i ,

$W_{P_i}^{k,l}$ – wydatki w l -tym roku związane z utrzymaniem mechanizmów w proces P_i , związane z wdrożeniem opisanej wektorem $\overrightarrow{\Delta R_{P_i}^k}$ zmiany ryzyka procesu P_i ,

r – stopa dyskontowa w okresie planowanej eksploatacji procesu P_i ,

$\Delta \eta_{P_i}^k$ – zmiana wielkości oczekiwanej rocznej straty dla procesu P_i ,

$\Delta R_{P_i}^k$ – zmiana ryzyka procesu P_i ,

$\mathcal{B}_{\Delta R_{P_i}^k} \neq 0$ - szacowany koszt opisanej wektorem $\overrightarrow{\Delta R_{P_i}^k}$ zmiany ryzyka procesu biznesowego P_i .

Rozpatrując możliwe zmiany w procesach biznesowych organizacji, należy wziąć pod uwagę to, że część z nich może wynikać z nowych wymogów ustawodawstwa, inne są odpowiedzią na zmieniającą się sytuację gospodarczą, a niektóre wynikają wyłącznie z dążenia organizacji do minimalizacji zidentyfikowanych zagrożeń.

W celu dokonania ostatecznego wyboru optymalnej zmiany ryzyka, w pro ponowanej metodzie, należy wprowadzić i odpowiednio wykorzystać:

- mnożnik istotności zmiany ryzyka procesu biznesowego, np. zdefiniowanego następująco:

$$\varphi_{P_i}^k = \begin{cases} 2, & \text{gdy wprowadzenie zmiany opisanej wektorem } \overrightarrow{R_{P_i}^k} \\ & \text{są wymogiem prawnym} \\ 1, & \text{gdy wprowadzenie zmiany opisanej wektorem } \overrightarrow{R_{P_i}^k} \\ & \text{są kluczowe dla prawidłowego funkcjonowania procesu} \\ 0, & \text{w pozostałych przypadkach} \end{cases} \quad (8)$$

- wskaźnik zasadności ekonomicznej zmiany ryzyka procesu biznesowego, np. zdefiniowanego następująco:

$$\lambda_{P_i}^k = 2^{\varphi_{P_i}^k} \times \mathcal{A}(\overrightarrow{\Delta R_{P_i}^k}). \quad (9)$$

Uwzględnienie mnożnika istotności zmiany $\varphi_{P_i}^k$ pozwala na określenie dodatkowych priorytetów możliwych zmian ryzyka. Przedstawione wzorem (9) pojęcie zasadności ekonomicznej określa zmodyfikowaną o czynniki regulacyjno-prawne racjonalność zmiany poziomu ryzyka procesu biznesowego. Wykorzystując wzory (8) i (9), można zdefiniować pojęcie optymalnej¹ dla procesu zmiany ryzyka procesu biznesowego P_i .

Podsumowanie

Przedstawiona w niniejszym artykule metodyka analizy i zarządzania ryzykiem procesów biznesowych, charakteryzuje się wysoką złożonością, wynikającą z zastosowania aparatu matematycznego. Spowodowane to jest uwzględnieniem wielu czynników wpływających na poziom ryzyka procesów biznesowych, praktycznie uniemożliwia prawidłowe oraz efektywne czasowo i kosztowo wyznaczanie ryzyka procesu biznesowego oraz zarządzanie tym ryzykiem w sposób tradycyjny, bez zastosowania rozwiązań informatycznych lub technik komputerowych.

Z uwagi na różnorodność czynników i szerokie spektrum ich oddziaływań na procesy biznesowe, zastosowanie analizy ryzyka powinno być nieodłącznym elementem procesu podejmowania decyzji i planowania wariantów funkcjonowania każdej organizacji. Wiedza o ryzyku występującym w procesie biznesowym, pozwala na odpowiednie kształtowanie tego procesu, tak aby poziom bezpieczeństwa w nim osiągnął akceptowalny poziom. Analizując źródła i kategorie ryzyka w procesach biznesowych, należy przede wszystkim brać pod uwagę ich charakterystykę, architekturę procesu oraz jego cykl życia. Ta wiedza, w połączeniu ze statystykami dotyczącymi jakości, bezpieczeństwa oraz architektury procesu, wydaje się być kluczem do minimalizacji ryzyka, we wszystkich jego aspektach – ludzkim, środowiskowym, bezpieczeństwa, jakości i ekonomicznym.

¹ Mając na uwadze subiektywizm definiowania wskaźnika istotności zmiany ryzyka procesu, wskaźnika zasadności ekonomicznej oraz wskaźnika aprobaty dla zwiększenia poziomu ryzyka procesu oraz ograniczenie liczności stron artykułu, koncepcja sposobu wyznaczenia optymalnej zmiany ryzyka procesu biznesowego została w niniejszym artykule pominięta.

Rozważania zawarte w niniejszym artykule mają przede wszystkim znaczenie poznawcze, dlatego pominięto formalny opis niektórych zagadnień. Zamiarem było pokazanie koncepcji, innego niż tradycyjne, spojrzenia na problemy kwantyfikacji zagrożenia.

Publikacja zrealizowana w ramach projektu naukowo-badawczego pt. „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości”, nr umowy z Narodowym Centrum Badań i Rozwoju: DOBR-BIO4/006/13143/2013.

Bibliografia

- Bruegge, B., Dutoit, A. (2011). *Inżynieria oprogramowania w ujęciu obiektowym. UML, wzorce projektowe i Java*. Gliwice: Helion.
- Hash, J. (2002). *Risk Management Guidance For Information Technology Systems*. ITL Bulletin, National Institute of Standards and Technology, Gaithersburg MD.
- Nowicki, T., Marczak, M. (2009). The modeling analysis and simulation of transport company functioning. W: M. Fertsch, K. Grzybowska, A. Stachowiak (red.), *Modeling of modern enterprises logistics*. Poznań: Wydawnictwo Politechniki Poznańskiej.
- Nowosielski, S. (2009). Modelowanie procesów gospodarczych w literaturze i praktyce. W: S. Nowosielski (red.), *Podejście procesowe w organizacjach*. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego.
- Piotrowski, M. (2007). *Notacja modelowania procesów biznesowych*. Warszawa: Wydawnictwo BTC.
- PN-ISO/IEC 27005 (2013). *Technika informatyczna, Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji*. PKN.
- PN-ISO 31000:2012 (2012). *Zarządzanie ryzykiem – Zasady i wytyczne*. PKN.
- Ryba, M. (2004). *Pomiar efektywności monitorowania bezpieczeństwa IT*. Materiały konferencyjne Kontrola'2004, Bielsko-Biała.
- Sikorski, C. (1998). *Ludzie nowej organizacji. Wzory kultury organizacyjnej wysokiej tolerancji niepewności*. Łódź: Wydawnictwo Uniwersytetu Łódzkiego, s. 23.
- Stanik, J. (w druku). *Model ryzyka procesów biznesowych*.
- Trajdos, T. (1993). *Matematyka*. Warszawa: Wydawnictwa Naukowo-Techniczne.
- Zawiła-Nadźwiecki, J. (2003). *Metoda TISM-BCP – Total Security Management, Business Continuity Planning*. Warszawa: European Network Security Institute.

MULTIFACETED METHODOLOGY ANALYSIS AND BUSINESS PROCESSES RISK MANAGEMENT

Keywords: business process, process risk, methodology, strategy

Summary. Presented in this paper the methodology constitutes a proposal of approach to risk analysis and management of business processes, taking into account the different categories of risk factors with different areas of activities of an organization. Proposed in this study the methodology is divided into the method of risk analysis of business processes and the method of management of this risk. The level of risk in the business processes estimated by using the proposed method of risk analysis is an input value for the risk management of business processes as well as to develop strategies for business continuity management and risk prevention and reduction.

Translated by Jerzy Stanik

Cytowanie

Stanik, J., Kiedrowicz, M. (2017). Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych. *Ekonomiczne Problemy Usług, 1* (126/1), 339–354. DOI: 10.18276/epu.2017.126/1-33.