Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 298 · 2016

Współczesne Finanse 7

Elżbieta I. Szczepankiewicz

Uniwersytet Ekonomiczny w Poznaniu
Wydział Zarządzania
Katedra Rachunkowości
elzbieta.szczepankiewicz@ue.poznan.pl

WYKORZYSTANIE PUNKTOWEJ METODY OSZACOWANIA RYZYKA OPERACYJNEGO W INSTYTUCJACH FINANSOWYCH*

Streszczenie: Celem artykułu jest przedstawienie możliwości wykorzystania metody punktowej do oceny ryzyka operacyjnego w instytucjach finansowych na przykładzie ryzyka wdrożenia nowego rozwiązania informatycznego. Punktowa metoda oceny ryzyka jest metodą uniwersalną, bowiem może być stosowana w działalności każdej jednostki, niezależnie od sektora czy branży. Efektem aplikacyjnym opracowania jest zaprezentowanie warunków stosowania tej metody, interpretacji wyników, narzędzi wspomagających analizę oraz efektów, jakie przynosi ona w zarządzaniu instytucją finansową.

Słowa kluczowe: ryzyko, analiza ryzyka, oszacowanie ryzyka, metody zarządzania ryzykiem.

Wprowadzenie

Ryzyko w działalności każdej jednostki, niezależnie od sektora lub branży, jest zjawiskiem powszechnym, trwałym i obiektywnym. W literaturze często podkreśla się wieloaspektowy i wieloznaczny charakter ryzyka. Próbę zdefiniowania ryzyka podejmowano w różnych dziedzinach oraz dyscyplinach nauki. Ryzyko stało się przedmiotem zainteresowania m.in. w ekonomii, naukach o zarządzaniu, naukach behawioralnych i naukach prawnych. Powstała teoria ryzyka

* Artykuł powstał w ramach projektu nr 51109-XX4 *Doskonalenie procesów zarządzania ryzykiem w jednostkach sektora publicznego i jednostkach sektora finansowego. Metody, techniki, narzędzia*, realizowanego w Uniwersytecie Ekonomicznym w Poznaniu.

oparta na rachunku prawdopodobieństwa, statystyce matematycznej i teorii procesów stochastycznych.

W literaturze, zdaniem autorki niniejszego szkicu, nadal nie ma jednoznacznej definicji ryzyka. Ogólna definicja zawarta w słowniku języka polskiego [Szymczak (red.), 1995] stwierdza, że ryzyko to możliwość, prawdopodobieństwo, że coś się nie uda, przedsięwzięcie, którego wynik jest nieznany, niepewny, problematyczny. Zatem jest to termin bardzo szeroki i trudny do precyzyjnego zdefiniowania, a prezentowane przez różnych autorów definicje często zależą od kontekstu prowadzonych przez nich badań.

W praktyce działalności jednostek ryzyko, w tym ryzyko operacyjne, najczęściej utożsamiane jest z zagrożeniami, których skutkiem jest możliwość poniesienia straty. Ryzyko może być też możliwością wystąpienia efektu działania niezgodnego z oczekiwaniami decydenta. Efekt ten może być lepszy niż się spodziewano lub gorszy od oczekiwań. Zatem ryzyko w pewnych sytuacjach realnie będzie zagrożeniem, a w innych może być szansą dla jednostki [Tarczyński, Mojsiewicz, 2001, s. 15; Nahotko, 2001, s. 38].

W przeciwieństwie do niepewności ryzyko jest w dużej mierze rozpoznawalne. W praktyce szacuje się prawdopodobieństwo wystąpienia wielu zjawisk i stanów zarówno o charakterze losowym, jak i operacyjnym. Z tego względu skuteczne zarządzanie ryzykiem operacyjnym wymaga, aby było ono identyfikowane i monitorowane w każdym z obszarów funkcjonowania instytucji finansowej oraz każdym procesie. Systematyczna i możliwie dokładna identyfikacja charakteru oraz zakresu potencjalnych czynników i obszarów ryzyka w instytucji pozwala na podjęcie we właściwym czasie odpowiedniej metody jego ograniczenia. Może to być metoda zmniejszająca prawdopodobieństwo wystąpienia szkodliwych czynności, zdarzeń, zagrożeń lub zaniechania działań bądź też minimalizująca ich wpływ i skutki, gdy one zaistnieją. Dla instytucji finansowych nie tylko finansowe skutki zmaterializowania się ryzyka mogą być dotkliwe. Niezwykle ważne są również skutki o charakterze prawnym i wizerunkowym.

Celem artykułu jest przedstawienie możliwości wykorzystania punktowej metody oceny ryzyka do oceny ryzyka operacyjnego w instytucjach finansowych[1] na przykładzie ryzyka wdrożenia nowego rozwiązania informatycznego. Właściwe oraz terminowe wdrożenie nowego rozwiązania IT, zgodnego z przyjętymi wymogami bezpieczeństwa i funkcjonalności, ma kluczowe znaczenie dla zapewnienia ciągłości działalności instytucji finansowej.

[1] Autorka proponuje zastosowanie prezentowanej metody w takich instytucjach finansowych, jak: towarzystwa funduszy inwestycyjnych i zarządzanych przez nie funduszach, powszechnych towarzystwach emerytalnych i OFE, zakładach ubezpieczeń, bankach.

1. Ryzyko operacyjne w klasyfikacji ryzyka działalności

W literaturze spotyka się wiele kryteriów podziału ryzyka związanego z prowadzeniem działalności gospodarczej, realizacją projektów inwestycyjnych, specyficzną działalnością instytucji finansowych (ryzyko bankowe, ubezpieczeniowe), ryzykiem prawnym itp.

Zgodnie z ogólnoświatowym podziałem dotyczącym ryzyka prowadzenia działalności gospodarczej przez jednostkę, niezależnie od sektora lub branży, wyodrębnia trzy grupy ryzyk: zewnętrzne i wewnętrzne (w tym: strategiczne, finansowe i operacyjne) oraz losowe.

Ryzyka zewnętrzne są związane m.in. ze zmianami politycznymi, społecznymi, demograficznymi oraz zmianami prawa i regulacji, ekonomicznymi trendami, konkurencją, dostępnością do rynków, obejmowaniem nowych rynków lub segmentów rynków, postępem technologicznym, decyzjami akcjonariuszy, uzależnieniem od kluczowych kontrahentów, niestabilnymi wykonawcami/podwykonawcami prowadzonych inwestycji.

Wewnętrzne ryzyko strategiczne dotyczy m.in. niepowodzenia utrzymania udziału w rynku, w identyfikacji potrzeb klientów, realizacji strategii wejścia na rynek, nieskutecznych aliansów, fuzji, alokacji działalności, nieskutecznych przywództw wewnątrz organizacji, długookresowych planowań zasobów intelektualnych, niedostosowania do potrzeb strukturą organizacyjną, a także możliwości utraty wizerunku na skutek zaniedbania lub niewłaściwego zachowania.

Wewnętrzne ryzyko finansowe jest związane m.in. z planowaniem finansowym, dostępem do źródeł finansowania, kredytami, walutami, płatnościami, utrzymaniem płynności, inwestycjami finansowymi i rzeczowymi, stopą procentową, inflacją, płaceniem kar umownych, stratami pieniężnymi, np. w przypadku kradzieży, oszustwa.

Kategoria ryzyka operacyjnego jest bardzo szeroka i obejmuje kilka podkategorii. W literaturze jest wiele jego definicji. Niektórzy autorzy definiują je jako rezultat niewystarczającej kontroli wewnętrznej, błędów ludzkich lub awarii systemów informatycznych. Jako główne kategorie w dziedzinie błędów ludzkich wymieniają niedoświadczenie, niekompetencję oraz korupcję [Chong, Brown, 2001]. Inni definiują je jako ryzyko poniesienia pośrednich lub bezpośrednich strat, związanych z niewłaściwie prowadzonymi lub błędnymi wewnętrznymi procesami, osobami czy systemami, albo wiążących się ze zdarzeniami zewnętrznymi (np. losowymi, realizacją umów z podmiotami zewnętrznymi) [Analysing IT Infrastructure Risk, 2001; Griffiths, 2005; Reich, 2004]. Zatem można mówić o wielu obszarach ryzyka operacyjnego, które są związane z: ochroną

zasobów i bezpieczeństwem informacji, prowadzeniem działalności zgodnie z regulacjami, zarządzaniem procesami wewnętrznym, skuteczną kontrolą wewnętrzną, personelem, interakcjami z klientami i kontrahentami. Klasyfikację obszarów oraz czynników ryzyka operacyjnego zawiera tab. 1.

Tabela 1. Klasyfikacja obszarów i czynników ryzyka operacyjnego w działalności

Obszary ryzyka	Zagrożenia, zdarzenia i czynności lub zaniechanie działań związanych z:
Konkurencyjność	pozyskaniem nowych i utrzymaniem obecnych klientów, satysfakcją klientów, zyskownością klientów, czasem operacji, rozwojem produktów, utratą wartości marki
Kontrakty	zawieraniem umów (ryzyko prawne, dodatkowych kosztów, nieprzestrzegania harmonogramu prac, niepełne specyfikacje), niedotrzymanie warunków umów, zaniechanie czynności podczas trwania inwestycji lub końcowego odbioru robót
Zarządzanie procesami wewnętrznymi	realizacją dostawami, utrzymywaniem zapasów, logistyką i dystrybucją, efektywnością i jakością procesów, wyceną produktów, błędami serwisu, realizacją projektów i inwestycji
Prowadzenie działalności zgodnie z regulacjami	niestosowaniem się do przepisów prawa, standardów, regulacji dotyczących danej instytucji, wypełnianie norm sektorowych, branżowych, środowiskowych i innych balansowanie z wykorzystaniem luk prawnych,
Ochrona zasobów i bezpieczeństwo informacji	zniszczeniem, utratą, nieuprawnionym wykorzystaniem zasobów rzeczowych, zarządzaniem licencjami, innowacjami i środowiskiem IT, ciągłością działania systemów informatycznych, awariami infrastruktury IT
Kontrola wewnętrzna	adekwatnością wewnętrznych regulacji i procedur, prowadzeniem dokumentacji, wiarygodną sprawozdawczością, podziałem uprawnień i odpowiedzialnością, ochroną przed defraudacjami i aktami przestępczymi
Ludzki	czynnikami wpływającymi na zdrowie i bezpieczeństwo pracowników i klientów, utrata kluczowych specjalistów lub kompetencyjnej kadry kierowniczej

Ryzyka losowe są związane z wystąpieniem niezależnych od instytucji zdarzeń zewnętrznych, takich jak: pożar, powódź, zalanie, katastrofa budowlana itp., a także ryzyka te mogą być wywołane przez czynniki wewnętrzne, wynikające z niedopełnienia przepisów, wewnętrznych procedur lub niedbałości personelu.

W niniejszym opracowaniu przyjęto, że ryzykiem operacyjnym w instytucji finansowej określa się prawdopodobieństwo wystąpienia pewnych czynności, zdarzeń, zagrożeń o charakterze operacyjnym lub losowym wewnętrznym bądź też zaniechanie wymaganych działań, których skutkiem mogą być straty finansowe, a także szkody o skutkach prawnych lub wizerunkowych. Skutki te stanowią przeszkodę w realizacji wyznaczonych celów instytucji.

2. Istota procesu identyfikacji i oceny ryzyka

Zarządzanie ryzykiem operacyjnym w instytucji finansowej powinno być ciągłym procesem, obejmującym wszystkich uczestników, wszystkie poziomy

i procesy. Wdrożenie procesu zarządzania ryzykiem w sposób uporządkowany powinno polegać na [Szczepankiewicz, 2011a, 2011b]:

- ustaleniu celów strategicznych instytucji i celów operacyjnych dla poszczególnych komórek organizacyjnych,
- opisaniu procesów biznesowych i wskazaniu ich właścicieli;
- identyfikacji czynników oraz obszarów ryzyka w odniesieniu do procesów, systemów i jednostek organizacyjnych,
- analizie i oszacowaniu ryzyka w powyższych obszarach (określenie przyczyn, częstotliwości i siły wpływu skutków na instytucję),
- określeniu poziomu ryzyka akceptowanego przez kierownictwo,
- segregacji i hierarchizacji ryzyka według istotności,
- określeniu strategii postępowania z ryzykiem w obszarach,
- zastosowaniu ustalonych narzędzi redukcji i kontroli ryzyka,
- monitorowaniu poziomu ryzyka i efektywności redukcji ryzyka,
- raportowaniu wyników o skuteczności zarządzania ryzykiem,
- ocenie skuteczności i wprowadzaniu działań korygujących.

W praktyce korzysta się z różnych metod i technik analizy ryzyka – od technik jakościowej analizy problemu przez odpowiednie metody ilościowe, w tym także statystyczne, aż po narzędzia informatyczne, wspomagające wykorzystanie metod ilościowych i jakościowych [szerzej: Szczepankiewicz, Dudek 2005, 2007; Szczepankiewicz, 2012]. Szacowanie ryzyka polega na ocenie prawdopodobieństwa wystąpienia zdarzenia i ustaleniu potencjalnej wartości skutków jego wystąpienia. Wielkość potencjalnego ryzyka obliczana jest według następującej formuły:

$$\mathbf{R = P \times S}$$

gdzie:

R – wielkość oczekiwanej straty związanej z danym ryzykiem,

P – prawdopodobieństwo wystąpienia rozpatrywanego zdarzenia (częstotliwość strat),

S – skutek (oddziaływanie), gdy wystąpi rozpatrywane zdarzenie (poziom strat).

Prawdopodobieństwo (P) może być wymierne lub tylko odczuwalne przez decydenta[2]. W niektórych analizach, np. dotyczących zasobów IT, może stanowić złożenie dwóch czynników: częstości występowania zagrożenia i podatności

[2] Na prawdopodobieństwo wystąpienia zagrożenia, w tym powodowanego rozmyślnie przez ludzi, mają wpływ takie czynniki, jak: atrakcyjność zasobu, łatwość przekształcenia zasobu w nagrodę, techniczne możliwości wprowadzenia czynnika zagrożenia i łatwość wykorzystania podatności zasobu na zagrożenie [ISO/IEC TR 13335-3, s. 61].

danego zasobu na zagrożenie [szerzej: Szczepankiewicz, Szczepankiewicz, 2006a, 2006b, 2006c]. Strata w wyniku wystąpienia niekorzystnego zdarzenia (S) może mieć charakter finansowy, wywoływać skutek prawny lub utratę wizerunku, a także ich kombinacje albo wszystkie jednocześnie[3]. Dla prawdopodobieństwa oraz skutku przyjmuje się odpowiednią skalę, np. 1-3, 1-5, 1-10. W wyniku kombinacji tych dwóch zmiennych można stworzyć podstawową 3-stopniową macierz ryzyka (rys. 1).

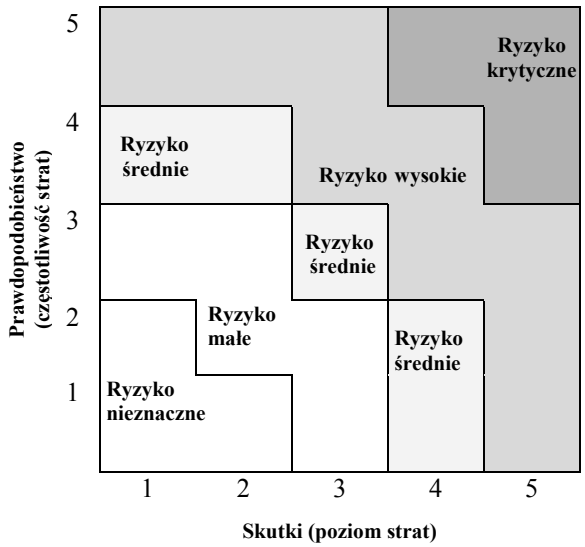
Prawdopodobieństwo (częstotliwość strat)	Skutki (poziom strat)		
	Niskie	**Średnie**	**Wysokie**
Wysokie	Ryzyko bardzo często występujące i powodujące względnie niskie straty	Ryzyko bardzo często występujące i powodujące dość wysokie straty	Ryzyko krytyczne, występujące z dużą częstotliwością i powodujące wysokie straty - zagraża osiągnięciu celów
Średnie	Ryzyko dość systematycznie występujące i powodujące niskie straty	Ryzyko dość systematycznie występujące i powodujące dość wysokie straty	Ryzyko dość systematycznie występujące i powodujące wysokie straty
Niskie	Ryzyko rzadko występujące i powodujące niskie straty	Ryzyko rzadko występujące ale powodujące dość wysokie straty	Ryzyko rzadko występujące, ale powodujące wysokie straty

Rys. 1. Macierz ryzyka w skali trzystopniowej

Można przyjąć, że ryzyka o stopniu najniższym nie będą wymagać żadnych dodatkowych przeciwdziałań, ryzyka średnie należy obniżyć i systematycznie monitorować, a ryzyka o stopniu największym wymagają podjęcia szybkich działań interwencyjnych. Bardziej rozbudowana skala może mieć wpływ na dokładniejszy pomiar i proces zarządzania ryzykiem.

Na rysunku 2 przedstawiono macierz ryzyka w skali pięciostopniowej.

[3] Skutek określa się na podstawie dostępnych danych historycznych tworzonych w instytucji w wyniku monitoringu i prowadzenia wewnętrznych statystyk, z zewnętrznych statystyk firm tworzących bazy takich danych oraz na podstawie danych planowanych.



Legenda:
- ryzyko nieznaczne – pola o wartości 1, 2;
- ryzyko małe – pola o wartości 3, 4, 6;
- ryzyko średnie – pola o wartości 4, 8, 9;
- ryzyko wysokie – pola o wartości 5, 10, 12, 15, 16;
- ryzyko bardzo wysokie (krytyczne) – pola o wartości 20, 25.

Rys. 2. Macierz ryzyka w skali 5-stopniowej

Interpretację prawdopodobieństwa wystąpienia ryzyka w instytucji finansowej mierzonego w skali 5-stopniowej i procentowo zawiera tab. 2.

Tabela 2. Interpretacja prawdopodobieństwa ryzyka w skali 5-stopniowej

Punkty w skali 1-5	Wartość % dla skali 1-5	Opis prawdopodobieństwa	Przykładowa interpretacja prawdopodobieństwa ryzyka
1	1-19%	małe	Prawdopodobieństwo małe, jeśli istnieje mała szansa na wystąpienie ryzyka lub w ostatnich pięciu latach ono nie występowało
2	20-39%	umiarkowane	Prawdopodobieństwo umiarkowane, jeśli ryzyko występuje rzadko, np. raz na trzy lata
3	40-59%	wysokie	Prawdopodobieństwo wysokie, jeśli ryzyko pojawia dość się często np. raz na dwa lata
4	60-79 %	bardzo wysokie	Prawdopodobieństwo bardzo wysokie, jeśli ryzyko występuje często, średnio co rok
5	80-100%	krytyczne	Prawdopodobieństwo krytyczne, jeśli ryzyko występuje częściej niż raz na rok

W tabeli 3 przedstawiono interpretację znaczenia poziomu strat w instytucji finansowej również w skali 5-stopniowej i procentowo.

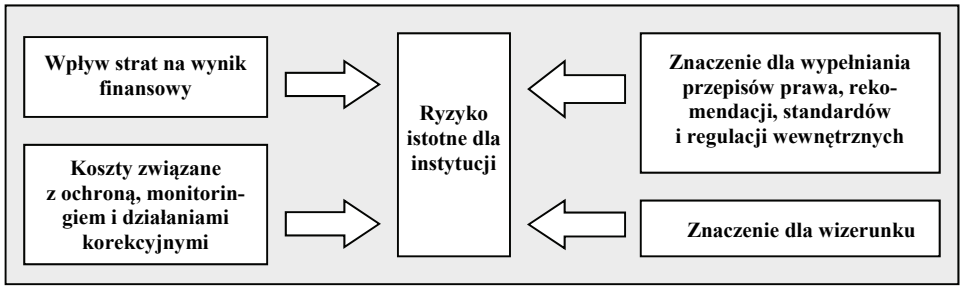
Tabela 3. Interpretacja skutków ryzyka w skali pięciostopniowej

Punkty w skali 1-5	Wartość % dla skali 1-5	Opis skutków (poziomu strat)	Przykładowa interpretacja skutków ryzyka
1	1-19%	małe	Skutki nie wymagają nakładu czynności, nie wywołują trwałej szkody oraz nie mają istotnego wpływu na finanse instytucji
2	20-39%	znaczące	Skutki są widoczne, wymagają czasu do rozwiązania i niewielkiego nakładu czynności, mogą być zagrożone zasoby finansowe
3	40-59%	poważne	Skutki mogą powodować brak realizacji celu, wymagają nakładu pracy przez kierownictwo, mają większy wpływ na wynik finansowy
4	60-79 %	bardzo duże	Skutki mogą być trudne do usunięcia, wymagają czasu, mają bardzo duży wpływ na finanse, możliwe, że zadanie nie będzie zrealizowane
5	80-100%	krytyczne	Skutki mogą nie zostać usunięte, wymaga to bardzo dużo czasu i zasobów, skutki mogą stać się wydarzeniem publicznym

Identyfikacja ryzyka polega na określeniu możliwych czynników (zagrożeń, zdarzeń), które mogą wystąpić jako przeszkody w realizacji celów instytucji finansowej w analizowanym obszarze działalności. Nadrzędnym celem procesu identyfikacji ryzyka jest podział ryzyka na istotne i nieistotne. Wobec ryzyk istotnych należy podjąć natychmiastowe działania. Podczas ustalenia istotności ryzyka należy brać po uwagę takie czynniki, jak:

- znaczenie finansowe strat, czyli ich wpływ na wynik finansowy,
- znaczenie skutków ryzyka dla wizerunku, czyli ich wpływ na obniżenie konkurencyjności i spadek zaufania wśród klientów,
- znaczenie dla wypełniania przepisów prawa, rekomendacji, standardów i regulacji wewnętrznych,
- poziom kosztów związanych z wprowadzeniem środków ochrony i zabezpieczeń, monitoringiem oraz działaniami korekcyjnymi.

Rysunek 3 prezentuje czynniki wpływające na ustalenie istotności ryzyk.



Rys. 3. Czynniki wpływające na ustalenie istotności ryzyk

Przykładowe podejście, wykorzystujące metodę punktową do oceny istotności ryzyka operacyjnego w instytucji finansowej, prezentuje tab. 4.

Tabela 4. Ocena punktowa ryzyka i istotność ryzyka

Prawdopodobieństwo wystąpienia ryzyka (P)		Skutki (oddziaływanie) ryzyka na instytucję (S)		Ocena punktowa ryzyka (wartość ryzyka) R= PxS	Istotność ryzyka	
Punkty w skali 1-5	Opis częstotliwości strat	Punkty w skali 1-5	Opis poziomu strat		Opis ryzyka	Klasyfikacja istotności
1	małe	1	małe	1 pkt	nieznaczne	nieistotne
1	małe	2	znaczące	2 pkt	nieznaczne	
1	małe	3	poważne	3 pkt	małe	
1	małe	4	bardzo duże	**4 pkt**	**średnie**	ostrożność w klasyfikacji
1	małe	5	krytyczne	**5 pkt**	**wysokie**	
2	umiarkowane	1	małe	2 pkt	nieznaczne	nieistotne
2	umiarkowane	2	znaczące	4 pkt	małe	
2	umiarkowane	3	poważne	**6 pkt**	małe	**istotne**
2	umiarkowane	4	bardzo duże	**8 pkt**	**średnie**	
2	umiarkowane	5	krytyczne	**10 pkt**	**wysokie**	
3	wysokie	1	małe	3 pkt	małe	nieistotne
3	wysokie	2	znaczące	**6 pkt**	małe	**istotne**
3	wysokie	3	poważne	**9 pkt**	**średnie**	
3	wysokie	4	bardzo duże	**12 pkt**	**wysokie**	
3	wysokie	5	krytyczne	**15 pkt**	**wysokie**	
4	bardzo wysokie	1	małe	**4 pkt**	**średnie**	nieistotne
4	bardzo wysokie	2	znaczące	**8 pkt**	**średnie**	**istotne**
4	bardzo wysokie	3	poważne	**12 pkt**	**wysokie**	
4	bardzo wysokie	4	bardzo duże	**16 pkt**	**wysokie**	
4	bardzo wysokie	5	krytyczne	**20 pkt**	**krytyczne**	
5	krytyczne	1	małe	**5 pkt**	**wysokie**	nieistotne
5	krytyczne	2	znaczące	**10 pkt**	**wysokie**	**istotne**
5	krytyczne	3	poważne	**15 pkt**	**wysokie**	
5	krytyczne	4	bardzo duże	**20 pkt**	**krytyczne**	
5	krytyczne	5	krytyczne	**25 pkt**	**krytyczne**	

Oszacowanie ryzyka[4] daje podstawę do podejmowania decyzji o postępowaniu z ryzykiem oraz stanowi podstawę projektowania odpowiednich procedur kontrolnych. Ma to podstawowe znaczenie dla skutecznego i efektywnego zarządzania działalnością instytucji.

3. Strategie postępowania z ryzykiem

Zarówno skutki, jak i prawdopodobieństwo wystąpienia szkodliwych zdarzeń, stają się kluczowymi czynnikami wyboru danej metody ograniczenia ryzyka. Przy realizacji projektów IT stosuje się strategie postępowania z ryzykiem, które scharakteryzowano w tab. 5.

[4] W procesie szacowania ryzyka może wystąpić zagrożenie analityczne, prowadzące do wyciągania fałszywych wniosków przy opisie ryzyk istotnych. Należy ostrożnie szacować zdarzenia, których prawdopodobieństwo jest bardzo małe, a straty będą bardzo duże lub krytyczne – wówczas skutki zmaterializowania się ryzyka będą ogromne. W tabeli 4 obszary te oznaczono opisem „ostrożność w klasyfikacji".

Tabela 5. Strategie postępowania z ryzykiem w instytucji finansowej

Strategia	Charakterystyka strategii
Redukcja i monitorowanie ryzyka	zapobieganie wystąpieniu ryzyka lub zmniejszenie jego skutków poprzez zastosowanie takich mechanizmów jak: systematyczna ocena i monitorowanie ryzyka, stosowanie technicznych i organizacyjnych środków ochrony zasobów, wdrożenie procedur kontrolnych, szkolenie personelu, wprowadzenie systemów jakości, ocena dostawców usług zewnętrznych, zabezpieczenia prawne wykonania umów i inne mechanizmy zapobiegawcze, nakazowe, korygujące, wykrywające
Akceptowanie określonego poziomu ryzyka (ryzyko akceptowalne)	to decyzja o braku reakcji na ryzyko lub o jego tolerowaniu; dotyczy to przypadków, gdy zarządzający akceptuje ryzyko: o niskim prawdopodobieństwie i skutkach jego wystąpienia (ryzyko nieznaczne); dana działalność niesie za sobą potencjalnie wyższą wartość dodaną niż koszt stosowanych środków ochrony; powstało ryzyko rezydualne (pozostałe), którego nie można całkowicie wyeliminować środkami ochrony; tworzy się plany awaryjne, które stanowią zabezpieczenie w momencie wzrostu ryzyka, ryzyko jest monitorowane
Dywersyfikacja ryzyka	poprzez rozproszenie ryzyka, np. outsourcing obsługi działań, w których brakuje kompetencji w instytucji, a także: zmniejszenie koncentracji ryzyka IT związanego z kluczowymi dostawcami sprzętu, zabezpieczeń, usług serwisowych itp.
Transfer ryzyka	poprzez przeniesienie na inne podmioty poprzez np. ubezpieczenie: od zdarzeń losowych, baz danych, sprzętu informatycznego, projektu
Unikanie ryzyka	poprzez rezygnację z procesu lub redefinicję procesu w taki sposób, aby wyeliminować lub zmniejszyć ryzyko nieodzowne w działalności, metodami organizacyjnymi (np. podział uprawnień użytkowników systemów informatycznych), lub metodami technicznymi (np. zakup dobrej jakości sprzętu i systemów, zabezpieczenie techniczne serwerowi), lub rezygnacja z prowadzenia projektu narażonego na duże ryzyko niepowodzenia

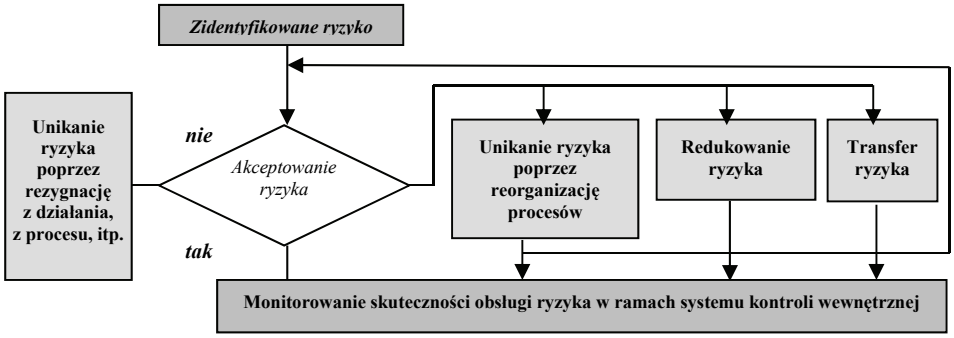
Źródło: Na podstawie: [Szczepankiewicz, Szczepankiewicz, 2006d, 2006e].

Przyjmując dwa omawiane kryteria oceny ryzyka – prawdopodobieństwo i jego skutki – można również uszeregować typy strategii zarządzania ryzykiem w postaci macierzy (rys. 4).

Prawdopodobieństwo ryzyka				
	Wysokie	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka i transfer ryzyka pozostałego	Ciągłe monitorowanie i weryfikacja ryzyka, unikanie ryzyka poprzez reorganizację lub transfer ryzyka (ubezpieczenie, reasekuracja, outsourcing)	Unikanie ryzyka poprzez rezygnację z procesu lub działania, zapobieganie ryzyku u źródła
	Średnie	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka i akceptacja ryzyka pozostałego	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka lub transfer ryzyka	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka i transfer ryzyka pozostałego (ubezpieczenie, reasekuracja, outsourcing)
	Niskie	Brak reakcji na ryzyko, akceptacja, tolerowanie ryzyka na określonym poziomie, minimalne monitorowanie i okresowa weryfikacja	Ciągłe monitorowanie ryzyka i okresowa weryfikacja, akceptacja ryzyka lub tolerowanie ryzyka na określonym poziomie	
		Niskie	**Średnie**	**Wysokie**
		Skutki ryzyka		

Rys. 4. Macierz strategii postępowania z ryzykiem

Rysunek 5 prezentuje cały cykl postępowania z ryzykiem w instytucji finansowej.



Rys. 5. Cykl postępowania ze zidentyfikowanym ryzykiem

Podsumowując, należy podkreślić, że w następstwie wdrożenia danej strategii zarządzania ryzykiem operacyjnym bardzo ważnym elementem tego procesu jest monitorowanie skutecznej realizacji strategii. Monitorowanie skuteczności obsługi ryzyka w instytucjach finansowych powinno się odbywać w ramach funkcjonujących w nich obligatoryjnych systemów kontroli wewnętrznej.

4. Przykład oszacowania ryzyka projektu informatycznego

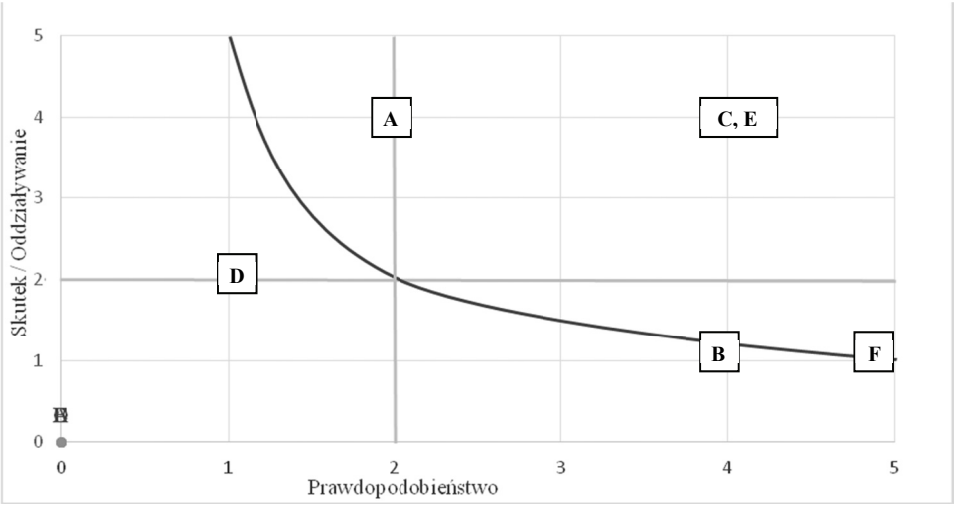
Przed wykorzystaniem metody punktowej do oceny ryzyka dla nowo wdrażanego rozwiązania IT należy opracować jednolitą definicję prawdopodobieństwa (P) oraz skutków (S) oddziaływania na instytucję finansową. W tabeli 6 zawarto przykładowy sposób analizy ryzyka, w tym czynników operacyjnych, dla wdrażanego rozwiązania IT.

Wyniki przeprowadzonej oceny ryzyka można przedstawić graficznie w postaci mapy ryzyka. Należy nanieść każde mogące wystąpić ryzyko dla poszczególnych czynników ryzyka. Dwoma prostopadłymi liniami (przykładowo na poziomie wartości 2 dla P i S) oznacza się poziom ryzyka akceptowalnego w instytucji. Następnie trzeba określić poziom istotności ryzyka zaznaczony krzywą. Obraz rozkładu ryzyka na mapie uświadamia decydentom ryzyka istotne, które znalazły się ponad nią.

Tabela 6. Przykład kompleksowej oceny ryzyka dla projektu IT

Ryzyko	**Ocena punktowa ryzyka i opisowa R=PxS**	**Proponowana reakcja na ryzyko - przykłady działań**	**Ocena istotności ryzyka po reakcji**	**Obniżenie poziomu ryzyka**
A Losowe (zewnętrzne i wewnętrzne)	2 x 5 = 10 Ryzyko istotne	- zawarcie umów zabezpieczających ewentualne szkody losowe (ubezpieczenie budynków, baz danych i sprzętu komputerowego od zdarzeń losowych)	2 x 2 = 4	60%
B Zewnętrzne	4 x 2 = 8 Ryzyko istotne	- zawarcie umowy w celu bieżącego dostosowania rozwiązania IT do zmian regulacji	3 x 1 = 3	62,5%
C Strategiczne (wewnętrzne)	4 x 5 = 20 Ryzyko istotne	- odpowiedni dobór (konkretne wymogi) wykonawców projektu - dokładnie opracowana specyfikacja wymagań dla rozwiązania - stały monitoring projektu	2 x 4 = 8 Ryzyko istotne	60%
D Finansowe	1 x 3 = 3	- dokładne sprawdzenie warunków umowy - kontrola finansowa rachunków wystawianych przez wykonawcę (zgodność z umową) przez kierownika projektu i głównego księgowego	1 x 2 = 2	33,3%
E Operacyjne (zarządzanie projektem)	4 x 5 = 20 Ryzyko istotne	- odpowiednie szkolenia dla członków komitetu sterującego projektem - zapewnienie pomocy specjalistów zewnętrznych przy pisaniu specyfikacji - zawarcie umowy z zabezpieczeniem kar umownych za opóźnienia w realizacji projektu ze strony wykonawcy	4 x 2 = 8 Ryzyko istotne	60%
F Operacyjne (ubezpieczeń-stwo zasobów IT)	5 x 2 = 10 Ryzyko istotne	- polityka bezpieczeństwa informacji, stosowanie środków ochrony i egzekwowanie reguł ochrony - ochrona fizyczna i techniczna sprzętu komputerowego (w tym mobilnego) - odpowiednie szkolenie pracowników	3 x 2 = 6 Ryzyko istotne	40%

Na rysunku 6 przedstawiono przykładową mapę ryzyka realizacji projektu IT wraz podziałem ryzyka na istotne i nieistotne. Można również sporządzić mapę po reakcji na ryzyko w celu obserwacji efektów obniżenia ryzyka.



Rys. 6. Przykładowa mapa ryzyka dla projektu IT z krzywą graniczną

Prezentowany powyżej przykład został przedstawiony na podstawie autorskiego modelu teoretycznego, którego najważniejsze założenia i determinanty zaprezentowano w punktach 1-3 niniejszego opracowania. Metoda ta została zweryfikowana przez autorkę w praktyce w dużej jednostce sektora publicznego. Zdaniem autorki, metoda jest na tyle uniwersalna, że może być wykorzystana w instytucjach finansowych oraz innych jednostkach, niezależnie od branży lub sektora.

Podsumowanie

Nie można oczekiwać, że ryzyko operacyjne z działalności instytucji finansowej da się całkowicie wyeliminować. Można jedynie próbować doprowadzić go do takiej formy użyteczności, która uczyni z niego zjawisko o niskiej szkodliwości. Ważne są zarówno skutki o charakterze finansowym, jak i prawnym oraz wizerunkowym.

Skuteczne zarządzanie różnymi obszarami ryzyka, w szczególności przy realizacji dużych projektów IT, to bardzo trudne zadanie. Do istotnych czynników skutecznego wdrożenia procesu zarządzania ryzykiem zaliczyć należy: odpowiednie kompetencje zarządu i kierownictwa operacyjnego, przewidzenie wystarczającego czasu na wdrożenie adekwatnych rozwiązań i środków ochrony przed potencjalnymi zagrożeniami oraz poziom wydatków finansowych z tym związanych. Skuteczne zarządzanie ryzykiem wymaga także przekonania pra-

cowników do przestrzegania wprowadzonych procedur wewnętrznych i takiego kształtowania kultury organizacji, aby patrzyli oni na swoje czynności przez pryzmat ryzyka oraz osiągania celów instytucji finansowej.

Zarząd instytucji finansowej musi ewoluować i doskonalić system zarządzania ryzykiem (w tym oceniać skuteczność departamentu ryzyka, departamentu IT itp.). Musi także systematycznie oceniać skuteczność prowadzenia kontroli zapobiegającej występowaniu niepożądanych nieprawidłowości oraz skuteczności kontroli realizowanych zadań przez kierownictwo operacyjne w poszczególnych pionach organizacyjnych.

Należy pamiętać, że zarządzanie ryzykiem w instytucji finansowej nigdy nie osiąga swojego końca edukacyjnego i dopiero po wielu latach można stwierdzić, że osiągnęło ono pewien poziom wymagalnej dojrzałości.

Literatura

Analysing IT Infrastructure Risk (2001), www.isaca.org.pl (dostęp: 10.12.2006).

Chong Y.Y., Brown E.M. (2001), *Zarządzanie ryzykiem projektu*, Oficyna Ekonomiczna, Kraków.

Griffiths P. (2005), *Risk-Based Auditing*, Gover Publishing Company, UK, Fernham.

ISO/IEC TR 13335-3 (2003), *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*, PKN, Warszawa.

Nahotko S. (2001), *Ryzyko ekonomiczne w działalności gospodarczej*, Oficyna Wydawnicza. Ośrodka Postępu Organizacyjnego Sp. z o.o., Bydgoszcz.

Reich A. (2004), *Nowa Bazylejska Umowa Kapitałowa. Ryzyko Operacyjne*, NBP-GINB, Warszawa.

Szczepankiewicz E.I. (2011a), *Assessment and Communications of Risks for the Purposes of IT Resources Security Management* [w:] J. Bizon-Górecka (red.), *Ryzyko: Zarządzanie ryzykiem w przedsiębiorstwie. Strategie zarządzania ryzykiem w przedsiębiorstwie – komunikacja ryzyka*, TNOIK, Bydgoszcz, s. 403-420.

Szczepankiewicz E.I. (2011b), *Theoretical and Ppractical Aaspect of Rrisk Mmanagement in the Aarea of IT in an Oorganization* [w:] *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, Wydawnictwo WSAiB w Gdyni, Gdynia, s. 392-404.

Szczepankiewicz E.I. (2012), *Theoretical and Practical Aspects of Using Quantitative and Qualitative Risk Assessment Methods in IT Resources Management* [w:] *Theory of Management 6: The Selected Problems for the Development Support of Management Knowledge Base*, University of Zilina, Zilina, Slovac Republic, s. 149-153.

Szczepankiewicz E.I., Dudek M. (2005), *Szacowanie ryzyka w zarządzaniu i audycie – zagadnienia wstępne*, „Monitor Rachunkowości i Finansów", nr 9, s. 29-39.

Szczepankiewicz E.I., Dudek M. (2007), *Oszacowanie ryzyka w środowisku informatycznym aplikacji biznesowych na potrzeby zarządzania i audytu* [w:] *Audyt wewnętrzny w 2007 roku*, Zeszyty Naukowe, nr 475, Prace Katedry Rachunkowości Uniwersytetu Szczecińskiego, nr 29, Uniwersytet Szczeciński, Szczecin, s. 281-294.

Szczepankiewicz E.I., Szczepankiewicz P. (2006a), *Analiza ryzyka w środowisku informatycznym rachunkowości. Część 1 – Zagadnienia wstępne*, „Monitor Rachunkowości i Finansów", nr 1.

Szczepankiewicz E.I., Szczepankiewicz P. (2006b), *Analiza ryzyka w środowisku informatycznym rachunkowości. Część 2 – Wybrane strategie, metody i techniki*, „Monitor Rachunkowości i Finansów", nr 2, s. 29-36.

Szczepankiewicz E.I., Szczepankiewicz P. (2006c), *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym. Część 2 – Etap oszacowania ryzyka*, „Monitor Rachunkowości i Finansów", nr 7, s. 36-46.

Szczepankiewicz E.I., Szczepankiewicz P. (2006d), *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym. Część 3 – Strategie postępowania z ryzykiem operacyjnym*, „Monitor Rachunkowości i Finansów", nr 8.

Szczepankiewicz E.I., Szczepankiewicz P. (2006e), *Zarządzanie ryzykiem informatycznym według międzynarodowych norm i standardów*, „Monitor Rachunkowości i Finansów", nr 11, s. 43-49.

Szymczak M. (red.) (1995), *Słownik języka polskiego*, t. III, PWN, Warszawa.

Tarczyński W., Mojsiewicz M. (2001), *Zarządzanie ryzykiem*, PWE, Warszawa.

THE USE OF POINT METHOD TO ASSESSMENT OPERATIONAL RISK IN FINANCIAL INSTITUTIONS

Summary: The operational risk and risk of losing information in the IT environment is a common phenomenon today and it may affect any financial institution. In recent years, various methods and methodologies of identifying risk factors and assessing risk effects have been developed, both through research and practice. The purpose of the present paper is to discuss the risk management process. It covers both the theoretical issues connected with the execution of this process and the practical aspects of its effective implementation in an financial institutions.

Keywords: risk, risk value assessment, risk management strategies.