ZAWIŁA-NIEDŹWIECKI Janusz[1]

Analogie zarządzania kryzysowego z zarządzaniem ryzykiem operacyjnym przedsiębiorstwa

WSTĘP

Zarządzanie kryzysowe odnosi się do ryzyka, które przez konkretne zagrożenia może oddziaływać zakłócająco na funkcjonowanie określonej społeczności, np. gminy, miasta, regionu czy kraju. Rozważyć wobec tego warto stopień analogii pomiędzy zarządzaniem kryzysowym a zarządzaniem operacyjnym w przedsiębiorstwie, które po pierwsze też może być postrzegane jako specyficzna społeczność, a po drugie może być administratorem jednego z systemów infrastruktury krytycznej państwa i odpowiadać za jego zawodność w ujęciu Ustawy o zarządzaniu kryzysowym [10; 13].

Z kolei ryzyko operacyjne to ryzyko strat materialnych i reputacyjnych oraz odpowiedzialności prawnej, wynikających z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych [16, s. 62]. Wyartykułowane w tej definicji czynniki ryzyka sugerują intencje, które w świetle teorii organizacji i zarządzania można ująć następująco:

- możliwe są określone zdarzenia wewnętrzne i zewnętrzne zakłócające działanie organizacji, tzn. naruszające prowadzenie procesów,
- procesy są w określonym stopniu i zakresie podatne na zdarzenia zakłócające,
- określone zasoby są newralgiczne dla utrzymania procesów,
- organizacja może ponosić prawną odpowiedzialność za konsekwencje naruszenia procesów lub zasobów.

Do takich samych aspektów ryzyka odwołuje się zarządzanie kryzysowe. Dalej przedstawiono syntetyczną charakterystykę przesłanek tej analogii.

1. TRIADA RYZYKA OPERACYJNEGO

Na triadę tę składają się [16, s. 55-57]: samo ryzyko operacyjne, zapewnianie bezpieczeństwa w odniesieniu do zagrożeń wyrażających to ryzyko w określonym kontekście społecznym i organizacyjnym oraz zapewnianie ciągłości działania w sytuacjach spełniania się zagrożeń czyli materializowania się ryzyka. Kluczowym aspektem jest postulat zapewniania ciągłości działania. Ryzyko operacyjne w tym aspekcie jest związane z kwestią horyzontu czasowego, w jakim rozważa się planowane działanie oraz towarzyszące mu ryzyko i wynikające z tego zagrożenia. Sprawa ta jest istotna z tytułu pytania – na gruncie jakiej dyscypliny naukowej rozważa się naturę ryzyka oraz zapewniania bezpieczeństwa i ciągłości działania. Inaczej bowiem należy to czynić, jeśli przyjmuje się perspektywę odległego horyzontu czasowego - wtedy jest to kwestia z zakresu dyscypliny ekonomia, dla której w kontekście zapewniania ciągłości działania ważne są takie zagadnienia jak: cykl koniunktury, wzrost (rozwój) i jego wysycanie oraz ewentualne osiąganie granicy wzrostu. Natomiast, jeśli przyjmuje się perspektywę bliskiego horyzontu czasowego, jest to kwestia z zakresu dyscypliny nauk o zarządzaniu, a ryzyko operacyjne jest rozważane jako ryzyko niedostatecznej skuteczności działania z perspektywy celu operacyjnego (bieżącego) tego działania. W tym ujęciu ryzyko operacyjne polega na możliwości niespełnienia oczekiwań technicznych, efektywności lub kwalifikacji, a także umyślnego popełnienia szkody. Stanowi więc ono o tym, na ile wewnętrzne

[1] dr hab. n. ekon. inż., Politechnika Warszawska, Wydział Zarządzania, ul. Narbutta 85, 02-524 Warszawa, j.zawila-niedzwiecki@wz.pw.edu.pl

procesy organizacyjne są dość skuteczne, w tym odporne na zakłócenia, aby organizacja mogła realizować swe cele.

Logiczną konsekwencją uświadomienia, zidentyfikowania i oceny ryzyka jest poszukiwanie rozwiązań zabezpieczających i naprawczych. W szczególności wart jest podkreślenia synergiczny związek zagadnień zapewniania bezpieczeństwa i zapewniania ciągłości działania. Z perspektywy zadań stawianych zapewnianiu ciągłości działania wszelkie poczynania na rzecz bezpieczeństwa mają charakter prewencji. Z kolei z perspektywy zapewniania bezpieczeństwa, rozwiązania ciągłości działania są reakcją naprawczą wobec nieskutecznej ochrony. Wynika z tego także rola racjonalnego (tam, gdzie nie działa obowiązek prawny, a istotna jest tylko gra czynników biznesowych) przypisywania znaczenia z jednej strony zapewnianiu bezpieczeństwa (gdy lepiej nie dopuszczać do zakłóceń), a z drugiej poszukiwaniu zastępczych warunków ciągłości działania (gdy ochrona jest nieracjonalna ekonomicznie lub nieskuteczna). Oba te elementy, osadzone w rozwiązaniach jakościowego stałego doskonalenia, zapewniają organizacji elastyczność wobec ryzyka, które w warunkach rosnącej konkurencji na rynku także rośnie.

W gruncie rzeczy używając pojęcia zarządzanie ryzykiem operacyjnym obejmuje się nim panowanie nad triadą zagadnień Ryzyko-Bezpieczeństwo-Ciągłość. Z aktualnej teorii i praktyki tak pojmowanego zarządzania ryzykiem operacyjnym wynika też szereg sugestii pod adresem zarządzania kryzysowego. Poniższe rozważania mają to uświadomić.

2. RYZYKO W UJĘCIU PRZYCZYN, PODATNOŚCI I SKUTKÓW

Co do istoty kwestii ryzyka, to dla wszystkich podmiotów gospodarczych, a szerzej wszystkich organizacji, o stopniu znaczenia ryzyka w ich działalności decydują takie aspekty, jak [1]:

- horyzont czasowy planowania działalności – im jest on dalszy, tym bardziej rośnie stopień nieprzewidywalności wiązany z ryzykiem,
- doświadczenie jako wiedza o konkretnych przejawach ryzyka – im większe, tym bardziej możliwe jest stosowanie narzędzi analizy statystycznej do określania ryzyka,
- niestabilność otoczenia, pojmowana w wielu wymiarach, od geograficznego (np. tereny szczególnie narażone na katastrofy naturalne) przez ekonomiczne, prawne, po polityczne,
- obiekt oddziaływania jednych rodzajów ryzyka, które bywają zarazem źródłem innych jego rodzajów.

Wpływanie na ryzyko operacyjne, podobnie jak i na inne rodzaje ryzyka, odbywa się w myśl następujących tzw. strategii szczegółowych zarządzania ryzykiem [7, t. 1, s. 42-52]:

- transfer ryzyka – przeniesienie bezpośrednich skutków wystąpienia szkody lub konsekwencji finansowych na inny podmiot, który przejmuje to ryzyko na siebie (np. ubezpieczyciel, ale i partner biznesowy typu kooperant);
- retencja ryzyka – stworzenie zawczasu własnego zabezpieczenia na wypadek zaistnienia szkody (np. fundusz rezerwowy), ale łatwej do przewidzenia i oszacowania, mało kosztownej w relacji do środków własnych organizacji, mało prawdopodobnej do kumulacji z innymi szkodami;
- nieświadoma retencja ryzyka – zaniechanie przeciwdziałania ryzyku z powodu braku świadomości jego istnienia;
- redukcja ryzyka – wprowadzenie zabezpieczeń dobranych do rodzajów zagrożeń, wielkości ryzyka, rozmiarów jego skutków;
- podział ryzyka – ryzyko określonego rodzaju jest dekomponowane na rodzaje ryzyka mniejszych kategorii i dla każdego z nich dobierane są działania mitygujące;
- akceptacja ryzyka – przekonanie, że rozmiar potencjalnych szkód nie przekracza granic tolerowania, a zabezpieczanie się przed ryzykiem jest zbyt kosztowne; w tej kategorii mieszczą się działania na rzecz zapewniania ciągłości działania w formie planów awaryjnych.

Prawidłowa analiza i ocena ryzyka powinna uwzględniać jego dynamiczną strukturę i to w dwóch aspektach. Pierwszym jest ciąg logiczny biegnący od przyczyn zdarzeń krytycznych, przez mechanizm ich spełniania się, po ostateczne spełnienie czyli skutki. Ryzyko w gruncie rzeczy dostrzega się bowiem przez [16]:

– zagrożenia, które stanowią o przyczynowym obrazie ryzyka,
– interakcję tych zagrożeń z podatnościami podmiotu, który doświadcza ryzyka, co stanowi istotę mechanizmu spełniania się ryzyka,
– skutki spełniania się ryzyka.

Drugim aspektem jest integrowanie różnych podziałów ryzyka na jego rodzaje, przeprowadzanych z perspektywy poszczególnych dziedzin aktywności społecznej i podmiotów działających w ich obszarze. Podziały takie powinny być dokonywane odrębnie w ujęciu przyczynowym, a odrębnie w ujęciu skutkowym.

Do tej pory koncepcja ujęcia problematyki ryzyka zaproponowana w 1921 roku przez Knighta nie została właściwie zakwestionowana. Niemniej nie udało się zadowalająco doprecyzować tego pojęcia. Dzieje się tak przede wszystkim dlatego, że postrzeganie ryzyka silnie zależy od perspektywy strony nim dotkniętej. Równocześnie nie są to wszystkie przesłanki relatywizacji spojrzenia na ryzyko. W ujęciu przyczynowym bardziej niż w ujęciu skutkowym można mówić o obiektywnym definiowaniu ryzyka, albowiem w tym ujęciu jest badany mechanizm jego powstawania i można precyzyjnie opisać jego cechy. Natomiast od strony skutków ryzyko postrzegane jest już wyraźnie subiektywnie, niezależnie od tego, czy obserwator jest osobą fizyczną, czy prawną, gdyż to samo zdarzenie może rodzić skutki o różnych konsekwencjach dla dwu podmiotów o nawet podobnym profilu działalności i umiejscowieniu.

Wpływanie na ryzyko operacyjne, tj. reagowanie organizacji na zidentyfikowane ryzyko, może polegać na wpływaniu na jego przyczyny, mechanizm spełniania się go lub jego skutki. Działanie takie odbywa się w kontekście istoty samego ryzyka i możliwości oddziaływania na nie oraz w kontekście zdolności organizacji do podjęcia się takiego oddziaływania, czy to w znaczeniu dysponowania właściwymi środkami/narzędziami, czy posiadania odpowiednich umiejętności. Sytuacja taka na ogół jest pozytywnie dynamiczna, tzn. coraz lepsze poznawanie ryzyka oraz praktykowanie oddziaływania na nie daje organizacji doświadczenie, które zwiększa skuteczność ograniczania ryzyka. Oczywiście prawidłowość ta dotyczy tylko rodzajów ryzyka o źródłach będących w zasięgu oddziaływania organizacji oraz o intensywności i skali tego oddziaływania współmiernych do możliwości reagowania organizacji.

Wbrew pozorom nie zakłada się automatycznej wyższości działań prewencyjnych nad naprawczymi. Ocena i dobór działań dokonywane są przy wykorzystaniu kryteriów ekonomicznych - niekiedy racjonalnym podejściem do ryzyka jest naprawiać jego skutki, a nie im zapobiegać. Pierwszy rodzaj oddziaływania określa się mianem zapewniania bezpieczeństwa operacyjnego, drugi zaś zapewnianiem ciągłości działania. Oddziaływania obu rodzajów bazują na analizie ryzyka, jego przyczyn i skutków, ale także na analizie istoty działania organizacji, związanego z danym przejawem ryzyka. Ryzyko przejawia się bowiem za pośrednictwem zjawisk o określonym charakterze, których wpływ na organizację jest możliwy dopiero wtedy, gdy takie zjawisko natrafi na podatność organizacji dotyczącą jednego lub kilku procesów w niej realizowanych, albo w znaczeniu niedoskonałości organizacyjnej takiego procesu, albo słabości w zakresie doboru zasobów wykorzystywanych przez proces. W praktyce każde zdarzenie krytyczne (spełnienie się ryzyka) polega na naruszeniu zasobu (zasobów) warunkującego realizację procesu. Analiza ryzyka polega więc na ustaleniu i ocenie:
– procesów, które decydują o realizacji zadań organizacji,
– zestawu zjawisk zakłócających i prawdopodobieństw ich wystąpienia,
– podatności zasobów, mierzonej wielkością potencjalnego wpływu zjawiska zakłócającego na działalność organizacji.

Takie wnikliwe dekomponowanie zagadnienia ryzyka prowadzi do poszukiwań sklasyfikowania jego rodzajów [16, s. 40-42 oraz 63-68]. Zasadnicza tego trudność wynika z konieczności uwzględnienia równocześnie przyczyn, sposobu i procesu spełniania oraz przejawów materializowania się. Główny problem stanowią skomplikowane relacje organizacji z jej otoczeniem, z czego wynika potrzeba przypisania tak przyczyn, jak i skutków do otoczenia lub do samej organizacji (jej działalności). Możliwe są bowiem wszystkie z następujących kombinacji (z tym, że dwie pierwsze najczęściej):

– przyczyna w otoczeniu, a skutek wewnątrz organizacji – np. obniżenie rentowności produkcji z powodu wzrostu wartości waluty narodowej,
– przyczyna i skutek wewnątrz organizacji – np. przestój spowodowany błędem pracownika,
– przyczyna wewnątrz organizacji, a skutek w otoczeniu – np. ujawnienie się wady wyrobu w okresie użytkowania go przez nabywcę,
– przyczyna i skutek w otoczeniu (choć oczywiście istnieje tu mechanizm wpływu skutku ryzyka na organizację i jej działalność) – np. uszczuplenie rynku zbytu w następstwie odległej geograficznie katastrofy naturalnej.

Pozostałe znaczące cechy poszczególnych rodzajów ryzyka, które należałoby wziąć pod uwagę, rozważając generalną klasyfikację ryzyka, to:
– czas od wystąpienia przyczyny do zaistnienia skutku,
– rozmiar potencjalnej lub już zaszłej szkody,
– dolegliwość szkody (zakłócenia) rozumiana znów w kilku aspektach, takich jak: wartość strat, czas potrzebny na przywrócenie stanu pierwotnego (jeśli to w ogóle możliwe), charakter konsekwencji (fizyczny, geograficzny, społeczny, organizacyjny itp.),
– powtarzalność (częstość spełniania się) tego rodzaju ryzyka i wynikających z niego szkód,
– przewidywalność ryzyka (znajomość statystycznej prawidłowości występowania, katalog możliwych scenariuszy realizowania się oraz możliwych skutków).

3. ZAPEWNIANIE BEZPIECZEŃSTWA ZASOBOWEGO JAKO PREWENCJA WOBEC RYZYKA

Na praktykę zarządzania ryzykiem operacyjnym istotny wpływ ma silny związek tego ryzyka z zasobami organizacji. Ich niedostatek, zbyt mała dostępność lub niska jakość są w praktyce działania organizacji postrzegane jako zagrożenia, natomiast pewność dysponowania tymi zasobami na odpowiednim poziomie i o odpowiedniej jakości jest postrzegana jako przejaw bezpieczeństwa. W intuicyjnym odbiorze bezpieczeństwo to jest kojarzone z rodzajem zasobu i fakt ten często znajduje odzwierciedlenie organizacyjne - zarządzanie ryzykiem operacyjnym jest dzielone na dwie kategorie, tj. klasyczne i nowoczesne obszary zarządzania działalnością pomocniczą (zasobami) w organizacji [16, s. 84-91]. Pierwszą kategorię stanowią: ochrona fizyczna (i techniczna) oraz bezpieczeństwo osobowe. Są to zagadnienia od dawna badane przez teorię organizacji. Dla tych obszarów w pełni uzasadnione jest mówienie o rekomendowanych dobrych praktykach. Przy tym spojrzenie na ochronę fizyczną i techniczną jest naznaczone specyfiką branży, w jakiej działa dany podmiot, podczas gdy bezpieczeństwo osobowe, jako skutkujące pewną polityką personalną, jest zagadnieniem uniwersalnym, podobnym w każdej organizacji. Drugą kategorię stanowią: bezpieczeństwo informacji i systemów informatycznych oraz zapewnianie ciągłości działania. W tym wypadku, z racji nowości problematyki, można spotkać się z różnymi spojrzeniami na zagadnienie i wynikającymi z tego koncepcjami analizy zagrożeń i poszukiwania rozwiązań.

Jako, że zapewnianie bezpieczeństwa organizacji odnoszone jest do poszczególnych rodzajów zasobów, to mówi się też o bezpieczeństwie osobowym, bezpieczeństwie fizycznym i technicznym, bezpieczeństwie finansowym oraz bezpieczeństwie informacji i informatycznym. Jak łatwo zauważyć poszczególne kategorie pozostają w ścisłym związku, a po części też nakładają się na siebie. Mówi się więc np. o bezpieczeństwie fizycznym osób, o bezpieczeństwie danych osobowych, bezpieczeństwie fizycznym walorów finansowych itd.

Zapewnianie bezpieczeństwa fizycznego i technicznego wywodzi się z następujących kluczowych przesłanek [11, s. 229-259]:
– potrzeby precyzyjnego zakreślenia granic lokalizacji organizacji oraz stref wykonywania poszczególnych funkcji i usług na rzecz klientów, a także przez pracowników organizacji oraz na ich rzecz;
– potrzeby wyobrażenia sobie i zdefiniowania potencjalnych zagrożeń oraz możliwych scenariuszy ich realizowania się jako zakłóceń normalnej pracy organizacji;

– potrzeby zorganizowania procesów wykonywania funkcji organizacji, zapewniania ochrony fizycznej oraz dobierania i stosowania rozwiązań ochrony, w tym także technicznych.

Zapewnianie bezpieczeństwa osobowego wywodzi się z następujących kluczowych przesłanek [11, s. 159-177]:
– potrzeby doboru i zatrudniania pracowników odznaczających się wysokim poziomem morale i odpowiedzialności (tzw. reguła prawości);
– wymogu adekwatności umiejętności zawodowych pracowników do wykonywanych zadań oraz potencjalnej zdolności do adaptowania się do zmieniających się wymagań, co może być pochodną rozwoju organizacyjnego i biznesowego podmiotu lub konkurencyjnego rozwoju rynku (tzw. reguła fachowości);
– potrzeby doboru pracowników oraz organizacji pracy, które z dwu stron współprzyczyniają się do stworzenia atmosfery i warunków dla identyfikacji powodzenia zawodowego pracownika z sukcesem pracodawcy (tzw. reguła lojalności).

Zapewnianie bezpieczeństwa informacji wywodzi się z następujących kluczowych przesłanek [15, s. 18-37]:
– zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym (tzw. reguła poufności);
– zapewnienia zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania (tzw. reguła integralności);
– zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. reguła dostępności).

Odnośnie do rozwiązań ściśle informatycznych zachodzi potrzeba zadbania o ochronę informacji w zakresie trzech podstawowych kryteriów[2]:
– bezpieczeństwa informacji,
– bezpieczeństwa świadczenia usług,
– autentyczności i rozliczalności danych oraz podmiotów.

W projektowaniu rozwiązań bezpieczeństwa stosuje się następujące ogólne zasady, odnoszone do poszczególnych rodzajów zasobów, jakimi posługuje się w swej działalności organizacja, w tym przede wszystkim do ludzi jako głównego źródła niebezpieczeństwa i obiektu zagrożenia [16, s. 90-91]:
– zasada uprawnionego dostępu – każdy pracownik przeszedł szkolenie z zasad bezpieczeństwa i ochrony oraz spełnia kryteria dopuszczenia do pracy i informacji (tajemnic służbowych);
– zasada przywilejów koniecznych – każdy pracownik ma prawo dostępu do pracy i informacji, ograniczone do tych, które są konieczne do wykonywania powierzonych mu zadań;
– zasada wiedzy koniecznej – każdy pracownik ma wiedzę o pracy, do której ma dostęp, co najmniej taką, jaka jest konieczna do realizacji powierzonych mu zadań;
– zasada usług koniecznych – organizacja świadczy tylko takie usługi jakich wymaga klient;
– zasada asekuracji – każdy mechanizm zabezpieczający musi być zabezpieczony innym (podobnym), a w przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie;
– zasada świadomości zbiorowej – wszyscy pracownicy są świadomi konieczności ochrony zasobów organizacji i aktywnie uczestniczą w tym procesie;
– zasada indywidualnej odpowiedzialności – za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby;
– zasada obecności koniecznej – prawo przebywania w określonych miejscach mają tylko osoby upoważnione;
– zasada stałej gotowości – organizacja jest przygotowana na wszelkie zagrożenia, niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;
– zasada najsłabszego ogniwa – poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element;

[2] Por. normy ISO12207, ISO13355, ISO15408, seria ISO 27001÷6 oraz zasady dobrych praktyk ITIL.

– zasada kompletności – zabezpieczenie jest tylko wtedy skuteczne, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu pracy;
– zasada ewolucji – każda organizacja musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych;
– zasada odpowiedniości – używane mechanizmy muszą być adekwatne do sytuacji;
– zasada akceptowanej równowagi – podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji (szczególnie zaleca się tu miary kosztowe co do nakładów, efektów i potencjalnych strat).

4. ZAPEWNIANIE CIĄGŁOŚCI DZIAŁANIA JAKO ZABEZPIECZENIE PRZED RYZYKIEM

Oczekiwanie bezpieczeństwa implikuje rozwiązania, których zasadniczym celem jest prewencja polegająca na dostrzeganiu czynników zagrożeń, monitorowaniu charakterystycznych i typowych symptomów ich aktywizowania się oraz zapobieganiu ich interakcji z systemem działania organizacji lub z jej otoczeniem. Jeśli te posunięcia zawodzą i dochodzi do zakłócenia działalności organizacji, to przychodzi czas na zaplanowaną i zorganizowaną aktywność naprawczą jako zdolność do utrzymywania ciągłości działania [16, s. 91-92].

Ryzyko, jakiemu podlega organizacja, jest bezpośrednią konsekwencją prowadzonego działania, którego konieczność i sens wynikają ze świadomej decyzji co do potrzeby i kierunku takiego działania. Dopiero ono ma charakter ryzykowny. Zagrożenia, jako formy przejawiania się ryzyka, są przedmiotem analizy pod kątem ich ewentualnego wpływu na organizację i są potencjalnymi zjawiskami, na które nakierowane są: obserwacja przesłanek zaistnienia zakłóceń oraz działania prewencyjne dokonywane w celu zapobieżenia interakcji zagrożenia z systemem działania organizacji (jej podatnościami). Z kolei to zakłócenia (spełnienie się zagrożeń) są faktycznym obiektem działań określanych mianem szeroko rozumianej polityki zapewniania ciągłości działania. Gdy dane zagrożenie oddziałuje na system działania organizacji lub jego otoczenie, a system staje się podatny na to oddziaływanie, ma się do czynienia z zakłóceniem. Wobec tego postępowanie służące zapewnianiu ciągłości działania jest podobne do postępowania służącego zabezpieczaniu przed zagrożeniami. Różni je relacja czasowa i charakter oddziaływania wobec zagrożenia, któremu mają przeciwdziałać zabezpieczenia i które ma być ograniczane w wyniku postępowania zapewniania ciągłości działania. Oba uzupełniają się, aby zapewnić organizacji oczekiwaną odporność na różne okoliczności naruszania normalnej działalności.

5. RYZYKO OPERACYJNE W ŚWIETLE DYSCYPLIN NAUKOWYCH – EKONOMIA ORAZ FINANSE

Z istoty ryzyka operacyjnego wynika, że leży ono w zakresie zainteresowania wszystkich dyscyplin wiedzy związanych z funkcjonowaniem organizacji, a w szczególności ekonomii, finansów oraz zarządzania. Stopień tego zainteresowania, a co za tym idzie stan wiedzy w ujęciu poszczególnych dyscyplin, są różne. Przeważnie ryzyko jest jednak kojarzone z dyscypliną nauk o finansach. Tymczasem sektorowi finansowemu wprawdzie zawdzięcza się zaawansowanie w rozpatrywaniu problematyki ryzyka, natomiast jej naturalny zakres obejmuje kwestie właściwe trzem wspomnianym dyscyplinom dziedziny nauk ekonomicznych, a dodatkowo sięgające szeregu innych dyscyplin z dziedzin nauk społecznych i nauk technicznych.

Od dawna praktykowana i rozwijana od strony teoretycznej [2], a konieczna w praktyce gospodarczej, jest analiza ciągłości działania z perspektywy rachunkowości (finanse). W tym ujęciu ciągłość jest analizowana przez badanie procesów gospodarczych na podstawie zdarzeń gospodarczych i systemu rachunkowości finansowej. Kluczową kwestią jest badanie danych ekonomicznych przez przedsiębiorstwo [14]. Zapewnienie ciągłości finansowej osiąga się przez analizę i wybór sposobów prawidłowego zarządzania płynnością finansową, a zapewnienie ciągłości operacyjnej przez analizę i wybór sposobów zarządzania konkurencyjnością, zmianami popytu i zmianami w pozyskiwaniu wszystkich trzech niezbędnych czynników produkcji [9].

Na gruncie nauk o finansach wypracowuje się głównie metody ustalania poziomu niezbędnej adekwatności kapitałowej (rezerw zdolnych kompensować straty), natomiast istotę spełniania się ryzyka operacyjnego (swoistego mechanizmu, który prowadzi od przyczyn do skutków) można określić, i w konsekwencji wpływać na jego poziom, na gruncie działania będącego przedmiotem badania innych nauk niż finanse [16, s. 17]. Szczególnie istotne dla wyrażenia umiejętności kontrolowania poziomu ryzyka jest utrzymywanie zdolności do zachowania ciągłości działania. Po pierwsze, jest to postulatem doskonałości systemu działania, jakim jest każda organizacja. W tym sensie zapewnianie ciągłości działania jest przedmiotem zarządzania strategicznego, wyraża cel nadrzędny sprawności organizacji i obejmuje prymat w obszarze zarządzania ryzykiem operacyjnym. W perspektywie strategicznej pozostaje zagadnieniem z pogranicza dyscyplin: ekonomii i nauk o zarządzaniu [12]. Po drugie, ciągłość działania jest rozumiana jako postępowanie organizatorskie tworzące zdolność organizacji do skutecznego reagowania w sytuacji zaistnienia zakłócenia będącego wynikiem swoistej interakcji przejawów zagrożenia z wewnętrzną podatnością organizacji, jej infrastruktury, zasobów lub rozwiązań zorganizowania.

Ciekawa też jest kwestia wiedzy o samej problematyce zarządzania zapewnianiem ciągłości działania. I tu możliwe są trzy generalne perspektywy naukowe – dyscypliny ekonomia, dyscypliny finanse oraz dyscypliny zarządzanie. Z perspektywy ekonomii podstawowym zamierzeniem jest zapewnienie ciągłości działalności operacyjnej oraz zapewnienie ciągłości (zdolności) finansowej. Wiąże się to z działaniami makro (zjawiska globalne i regionalne) i mikroekonomicznymi na poziomie podmiotów gospodarczych. Zapewnianie ciągłości ekonomicznej powinno następować przez identyfikację stopnia nieokreśloności perspektyw zjawisk gospodarczych i dobieranie działań o akceptowanym poziomie ryzyka. Każdą z perspektyw charakteryzują podstawowe kategorie i procesy, między którymi zachodzą zależności determinujące ciągłość działania. Dominują kategorie makro, np. inflacja nie tylko wpływa na inne kategorie i procesy makroekonomiczne, ale również oddziałuje na ciągłość operacyjną i finansową, a w następnej kolejności na procesy mikroekonomiczne. Dodatkowo występują kategorie wspólne, np. produkcja makro, operacyjna i mikro [11].

6. RYZYKO OPERACYJNE W ŚWIETLE DYSCYPLINY – NAUKI O ZARZĄDZANIU

Konkluzją z dotychczasowych rozważań jest to, że w opracowaniach nt. ryzyka dominuje perspektywa finansowa oceny ryzyka. W efekcie utrwala się wyraźna luka w wiedzy o innych możliwościach oddziaływania na ryzyko operacyjne niż tworzenie rezerw finansowych. Innych, tzn. środkami o charakterze prawnym, organizacyjnym i technicznym. Dopiero takie poszerzone spojrzenie pozwala w pełni wykorzystywać dorobek nauk o organizacji i zarządzaniu w celu ograniczania ryzyka. Co jeszcze ważniejsze, tylko takie podejście uświadamia, że akurat ten rodzaj ryzyka odnosi się do zjawisk i problemów z dziedziny zarządzania, które – choć wcześniej nieprzypisywane do ryzyka operacyjnego – są od dawna znane i mogą służyć sprawdzonymi koncepcjami, metodami oraz technikami organizatorskimi i zarządczymi. Perspektywa ryzyka (a właściwie trzech zintegrowanych perspektyw: Ryzyka–Bezpieczeństwa–Ciągłości działania) może stać się kluczem do interpretacji współczesnych wyzwań zarządzania. Przesłanki takiego stanowiska są następujące:

- przez analizowanie ryzyka najpełniej wyjaśnia się powody ograniczonej przewidywalności dowolnego działania,
- przez wyznaczanie kierunków zabezpieczania najpełniej wskazuje się sposób zwiększania takiej przewidywalności,
- zapewnianie ciągłości działania najpełniej wyraża ludzkie dążenie do pełnej zaradności wobec utrudnień w powziętych działaniach,
- triada Ryzyko-Bezpieczeństwo-Ciągłość oznacza panowanie nad ryzykiem polegające na racjonalnym rozłożeniu akcentów pomiędzy prewencję wobec zagrożeń dla działania organizacji a zaprojektowane reagowanie na występowanie zakłóceń.

Ryzyko operacyjne jest bowiem zawsze obecne w zarządzaniu organizacją według dowolnej z koncepcji zarządzania. Natomiast w odwrotnym ujęciu, tj. odpowiedzi na pytanie – która z koncepcji zarządzania szczególnie dobrze służy wyjaśnianiu istoty ryzyka operacyjnego – wypada wskazać podejście procesowe, podejście zasobowe i podejście organizacji uczącej się. Podejście procesowe jest podstawą ustalania najbardziej newralgicznej części działalności organizacji widzianej jako zbiór procesów krytycznych [3]. Analiza ich wrażliwości pozwala zidentyfikować zbiór zasobów krytycznych, tzn. najbardziej podatnych na zagrożenia, a zarazem kluczowych dla możliwości utrzymania ciągłości procesów krytycznych. W ostatnich latach notuje się specyficzny renesans podejścia zasobowego [6]. Jest ono podstawowe dla zagadnienia ryzyka operacyjnego z uwagi na fakt, że organizacyjne naruszenie ciągłości działania zawsze polega na bezpośredniej utracie zasobów lub utracie kontroli nad zasobami. Wyznacza to tryb podejścia analitycznego w zapewnianiu bezpieczeństwa i ciągłości działania. Kolejną kwestią jest aspekt kultury organizacyjnej, który powinien polegać na stałym doskonaleniu zdolności zapewniania bezpieczeństwa i ciągłości działania, tak w zakresie analizy ryzyka, jak i reagowania na symptomy spełniania się ryzyka, a więc polegać na systematycznym pogłębianiu wiedzy o ryzyku, zagrożeniach i dostępnych metodach oraz technikach reagowania [4].

Z kolei przez nauki o zarządzaniu zagadnienie zapewniania ciągłości działania w swoistej dla tej nauki interpretacji jest jak dotąd podejmowane tylko szczątkowo, np. [5; 8], mimo że stabilność działania czy trwałość procedur i struktur organizacji są motywami teorii organizacji od samego jej początku. Można ją wyinterpretować z pierwszych koncepcji F. Taylora, prawa harmonii K. Adamieckiego czy postulatu bezpiecznej organizacji H. Fayola. Niemniej jednak jako ważne praktyczne wyzwanie zaczęło być formułowane dopiero od czasu rewolucji informatycznej przełomu lat 70. i 80. XX w. Wtedy to pierwsze instytucje osiągnęły na tyle wysoki poziom informatyzacji działalności, że zaczęły odczuwać uzależnienie swego wizerunku w oczach klientów i swych wyników ekonomicznych od niezakłóconego działania systemów teleinformatycznych. Takie źródło współczesnego postrzegania problemu zapewniania ciągłości działania jako nieprzerwanego świadczenia usług przyczyniło się do rozwoju oferty firm doradczych w tym zakresie oraz do ukształtowania się kilku znaczących ośrodków pracujących nad rekomendacjami dobrych praktyk zapewniania ciągłości działania. Najbardziej znane to: amerykański Disaster Recovery Institute International, brytyjski Business Continuity Institute, azjatycka sieć Business Continuity Management Institute. Drugim nurtem rozwoju koncepcji zarządzania zapewnianiem ciągłości działania są prace komitetów normalizacyjnych, zwłaszcza Australii i Nowej Zelandii, Singapuru, USA oraz Wielkiej Brytanii [15].

Z powyższego przeglądu wynika potrzeba podkreślenia różnicy w postrzeganiu ryzyka z perspektywy dyscyplin naukowych ekonomii i finansów a dyscypliny zarządzania. W ujęciu ekonomiczno-finansowym chodzi przede wszystkim o określenie odpowiedniego poziomu zasobów niezbędnych do sfinansowania skutków spełnienia się ryzyka. Zasoby te nie mogą być za małe, ale też nieracjonalnie byłoby gdyby ich poziom był zbyt wysoki, dlatego badania skupiają się na metodach możliwie trafnego modelowania tego poziomu. W ujęciu teorii zarządzania w większym stopniu chodzi o aspekt zdecydowanie bardziej organizacyjny. Po pierwsze, chodzi o niedopuszczanie do spełniania się ryzyka, a po drugie o zaplanowanie reagowania organizacyjnego na wypadek jednak spełnienia się go. Oznacza to, że potrzebna jest dokładna znajomość jego istoty w znaczeniu mechanizmu zagrożenia oraz kontekstu jego występowania związanego z zasobowo-organizacyjnymi uwarunkowaniami działania danej organizacji i jej otoczenia. Oczywiście oba ujęcia – ekonomiczno-finansowe i zarządzania – uzupełniają się w poszukiwaniu jak najlepszego rozumienia natury ryzyka i jego spełniania się oraz doboru sposobów reagowania. W odniesieniu do reagowania podejście finansowe ma jednak charakter statyczny, podczas gdy rozwiązania organizacyjne zapewniania ciągłości działania cechuje dynamika i elastyczność dostosowywania się do konkretnej sytuacji zdarzenia będącego konsekwencją spełnienia ryzyka.

WNIOSKI

Istnieje wyraźna analogia pomiędzy zarządzaniem kryzysowym (odnoszonym do społeczności funkcjonującej w ramach pewnego obszaru administracyjnego z jego organami władzy publicznej odpowiedzialnej za to zarządzanie) a zarządzaniem ryzykiem operacyjnym w ramach pojedynczego przedsiębiorstwa. Źródłem tej analogii są koncepcje zarządzania, w świetle których przedsiębiorstwo jest zawsze odzwierciedleniem struktur i mechanizmów społecznych, ponieważ jest powołane i uformowane przez ludzi oraz działa dla ludzi. Dlatego też dobre praktyki środowiska podmiotów gospodarczych, dotyczące poszczególnych elementów triady Ryzyko-Bezpieczeństwo-Ciągłość, powinny być rozważane i uwzględniane na potrzeby opracowania dokumentów planistycznych związanych z systemami zarządzania kryzysowego i relacji między tymi systemami. Różnica między tymi rodzajami zarządzania polega tylko na tym, że pojedyncza organizacja (przedsiębiorstwo), w przypadku ryzyka operacyjnego, jest środowiskiem dużo bardziej jednorodnym niż społeczność, którą chroni się przed kryzysami. Natomiast charakteryzowanie ryzyka (w ujęciu przyczynowym, podatności i skutkowym), jego ocena oraz tok postępowania prewencyjnego i naprawczego są co do zasad tożsame. Podobne też są reguły zarządzania i tworzenia struktur organizacyjnych odpowiedzialnych za panowanie nad ryzykiem. Szczególnie istotny w analizie ryzyka jest podział na perspektywę przyczyn i podatności oraz perspektywę skutków. Ujęcie przyczynowe pozwala na systematyczne wprowadzanie zabezpieczeń przed ryzykiem i doskonalenie praktyki bieżącego działania uwzględniającego istnienie ryzyka. Ujęcie skutkowe zaś pozwala na systematyczne przygotowywanie sposobów i zasobów postępowania naprawczego na wypadek zaistnienia sytuacji kryzysowych. W szczególności zaś w zarządzaniu kryzysowym warto poszukiwać analogii do zarządzania ryzykiem operacyjnym co do następujących ustaleń [17, s. 133-136]:

1. Zarządzanie ryzykiem operacyjnym rozumiane jako triada „Ryzyko operacyjne – Bezpieczeństwo – Ciągłość działania" jest kwintesencją zarządzania podejmując w samej swej istocie kwestie skuteczności, sprawności i efektywności działania organizatorskiego.
2. Zarządzanie zapewnianiem ciągłości działania jest częścią nauki o zarządzaniu o docelowej roli i wartości analogicznej do znaczenia teorii niezawodności w dziedzinie nauk technicznych.
3. Z perspektywy społecznej zarządzanie zapewnianiem ciągłości działania, odnoszone do pojedynczej organizacji, uzupełnia teorię zarządzania kryzysowego przypisaną do skali regionalnej lub krajowej.
4. Zarządzanie zapewnianiem ciągłości działania jest równocześnie przeciwdziałaniem ryzyku operacyjnemu. Pozostaje przy tym w związku z pozostałymi obszarami takiego przeciwdziałania, tj. zarządzaniem zapewnianiem bezpieczeństwem i zarządzaniem jakością. Ponieważ ryzyko operacyjne jest wyrazem niedoskonałości organizacji, to zarządzanie zapewnianiem ciągłości działania jest jedną z dróg doskonalenia organizacji i w tym sensie wpisuje się w szerokie rozumienie zarządzania przez jakość.
5. Modelowe reagowanie na możliwość zaistnienia zakłóceń sprowadza się do czterech postaw reagowania zwanych: tolerowaniem, monitorowaniem, zapobieganiem i planowaniem [17, s. 96-104].
6. Zarządzanie zapewnianiem ciągłości działania jest procesem, który wymaga przypisania dedykowanej struktury organizacyjnej, określenia zasad działania, zadań i odpowiedzialności oraz przydzielenia zasobów.
7. Zarządzanie zapewnianiem ciągłości działania wymaga stałego doskonalenia rozwiązań, czego powodem jest zmienność wewnętrzna organizacji, jej procesów i zasobów, oraz zmienność otoczenia zewnętrznego i jego oddziaływania na organizację. Ważnym elementem tego doskonalenia jest systematyczne gromadzenie uporządkowanej wiedzy o zjawiskach zagrożeń, o zaistniałych zakłóceniach, a w tym kontekście ocena stosowanych dotąd i dostępnych w przyszłości rozwiązań zaradczych. Podobnie istotne jest ćwiczenie (testowanie) sprawności organizacji w rozwiązywaniu sytuacji krytycznych na drodze symulowania sytuacji pojawienia się zakłóceń.

Streszczenie

Zarządzanie kryzysowe może w pełni korzystać z dorobku nauk o zarządzaniu w zakresie zarządzania ryzykiem operacyjnym. Różni je właściwie tylko środowisko oddziaływania ryzyka. Pojedyncza organizacja (przedsiębiorstwo), w przypadku ryzyka operacyjnego, jest środowiskiem dużo bardziej jednorodnym niż społeczność, którą chroni się przed kryzysami. Natomiast charakteryzowanie ryzyka (w ujęciu przyczynowym, podatności i skutkowym), jego ocena oraz tok postępowania prewencyjnego i naprawczego są co do zasad tożsame. Podobne też są reguły zarządzania i tworzenia struktur organizacyjnych odpowiedzialnych za panowanie nad ryzykiem. Szczególnie istotny w analizie ryzyka jest podział na perspektywę przyczyn i podatności oraz perspektywę skutków. Ujęcie przyczynowe pozwala na systematyczne wprowadzanie zabezpieczeń przed ryzkiem i doskonalenie praktyki bieżącego działania uwzględniającego istnienie ryzyka. Ujęcie skutkowe zaś pozwala na systematyczne przygotowywanie sposobów i zasobów postępowania naprawczego na wypadek zaistnienia sytuacji kryzysowych.

Analogies crisis management of operational risk management

Abstract

Crisis management can fully benefit from the achievements of management sciences in the field of operational risk management. They differ only actually impact the risk environment. Single organization (enterprise), in the case of operational risk, is much more homogeneous than the community that protects against crises. In contrast, the risk characterization (in terms of causal, compliance and effect relationship), its evaluation and process of conduct preventive and corrective what the rules are the same. Similar rules are also managing and creating organizational structures responsible for the management of risks. Particularly important in the analysis of risk is the division of the perspective of the causes and perspective of the consequences. Shot causal allow systematic introduction of risk protection and improvement of the practice of the current action taking into account the existence of risk. Shot-effect allows for systematic preparation methods and resource recovery proceedings for responding to emergencies.

BIBLIOGRAFIA

1. Jajuga K. (red.), *Zarządzanie ryzykiem*. PWN, Warszawa 2007.
2. Kaczmarek T., Ćwiek G., *Ryzyko kryzysu a ciągłość działania*. Difin, Warszawa 2009.
3. Kaszubski R., Romańczuk D. (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*. Związek Banków Polskich, Warszawa 2012.
4. Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie. Zarządzanie bezpieczeństwem*. Difin, Warszawa 2012.
5. Koźmiński A., *Zarządzanie w warunkach niepewności*. WN PWN, Warszawa 2004.
6. Krupski R., *Rozwój szkoły zasobów zarządzania strategicznego*, „Przegląd Organizacji" nr 4/2012.
7. Monkiewicz J. (red.), *Podstawy ubezpieczeń*. Poltext, Warszawa 2004.
8. Obłój K., *Pasja i dyscyplina strategii*. Poltext, Warszawa 2010.
9. Sierpińska M., Jachna T., *Metody podejmowania decyzji finansowych*, PWN, Warszawa 2007.
10. Skomra W., *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*. Presscom, Wrocław 2010.
11. Staniec I., Zawiła-Niedźwiecki J. (red.), *Zarządzanie ryzykiem operacyjnym*. C.H.Beck, Warszawa 2008.
12. Sudoł S., *Przedsiębiorstwo, podstawy nauki o przedsiębiorstwie, zarządzanie przedsiębiorstwem*. PWE, Warszawa 2006.
13. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym z późn. zm. (tekst ujednolicony z dnia 02.10.2013.)
14. Wojtyna A. (red.), *Kryzys finansowy i jego skutki dla krajów na średnim poziomie rozwoju*. PWE, Warszawa 2011.
15. Wołowski F., Zawiła-Niedźwiecki J., *Bezpieczeństwo systemów informacyjnych*. Edu-Libri, Kraków 2012.
16. Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*. edu-Libri, Kraków 2013.