METODA TSM-BCP PROJEKTOWANIA ROZWIĄZAŃ ZAPEWNIANIA CIĄGŁOŚCI DZIAŁANIA ORGANIZACJI

(tekst oparty na referacie przygotowanym na konferencję AGH „Zarządzanie przedsiębiorstwem. Teoria i praktyka" 22-23.11.2007)

dr inż. Janusz ZAWIŁA-NIEDŹWIECKI

Instytut Organizacji Systemów Produkcyjnych Politechniki Warszawskiej

Streszczenie: Bardzo długo w historii teorii zarządzania kwestia reagowania na zakłócenia w działaniu organizacji należała do rutynowych obowiązków menedżera i zależała od jego indywidualnych umiejętności. Tym samym problematyka ciągłości działania należała do zadań zarządzania operacyjnego. Od kilkunastu lat widać trend ku potraktowaniu jej jako zadania zarządzania strategicznego, docenianego przez najwyższe kierownictwo organizacji. W sektorze gospodarczym instrumentów finansowych jest to już obowiązek nakładany przez dyrektywy UE. Zaprezentowana metoda TSM-BCP, datowana na 2003 rok, sprawdzona w kilku dużych wdrożeniach, jest propozycją kompleksowego podejścia organizatorskiego w tym względzie.

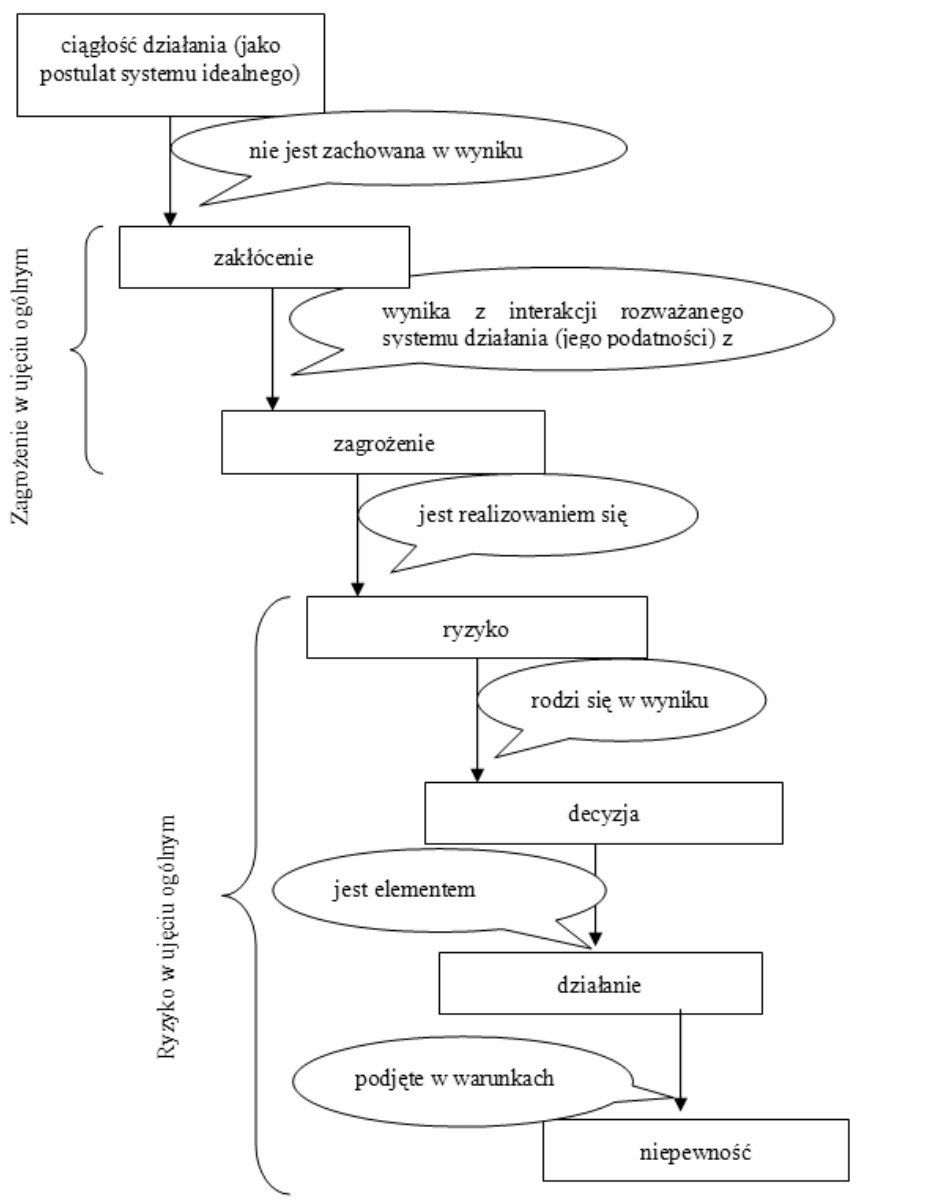
Słowa kluczowe: ciągłość działania, ryzyko operacyjne, zintegrowane bezpieczeństwo, zagrożenie

1. WPROWADZENIE

Współczesne przedsiębiorstwo staje wobec rosnących wyzwań gospodarczych, związanych z globalizacją konkurencji rynkowej, oraz wobec wyzwań cywilizacyjnych, związanych z tempem zmian kulturowych, tworzeniem się społeczeństwa informacyjnego, czy niestety nowoczesnym terroryzmem. Zjawiska te wymuszają wyrafinowaną organizację działania oraz korzystanie z wyrafinowanych rozwiązań technicznych. Tym samym, z uwagi na kurczenie się marginesu naturalnej elastyczności, rośnie podatność przedsiębiorstwa na różnorodne zagrożenia. Odpowiedzią powinno być specjalne przygotowanie organizacji wewnętrznej i rozwiązań służących radzeniu sobie z możliwymi zagrożeniami. W tym zakresie istnieje bogata oferta usług proponowanych przez firmy doradcze. Bazują one na doświadczeniu kumulowanym wraz z kolejnymi projektami. Rzadko jednak ich podejście wynika z solidnej analizy podstaw teoretycznych samych zjawisk zakłócania funkcjonowania organizacji oraz sposobu reagowania na nie.

2. KONTEKST PROBLEMOWY „CIĄGŁOŚCI DZIAŁANIA"

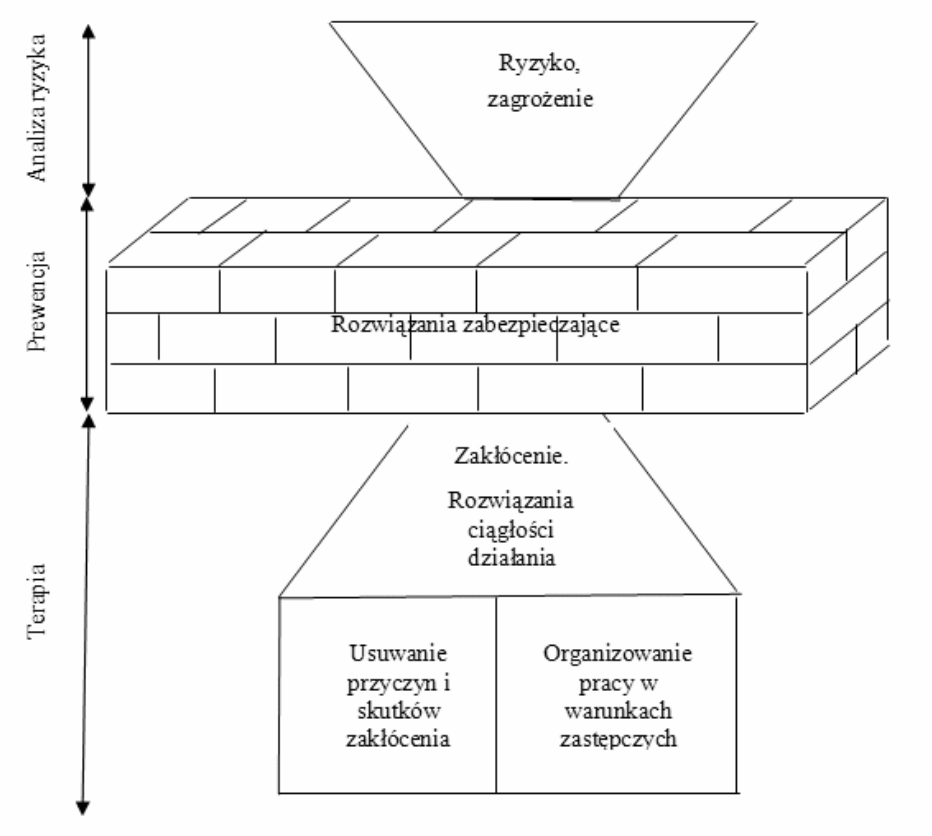
Można sobie postawić pytania: co powoduje, że ciągłość działania zostaje naruszona?, jaki jest ciąg przyczynowo-skutkowy takiego mechanizmu naruszenia? Ustalenia ujmuje rysunek 1, zaś obszerną analizę zawiera praca [1].



Rys. 1. Mechanizm logiczny naruszenia ciągłości działania (źródło: opracowanie własne)

Konkluzją z tej analizy jest ustalenie, że w ramach świadomego zarządzania ryzykiem, jako prewencja wobec zagrożeń, prowadzona jest polityka zrównoważonego zapewniania bezpieczeństwa, a na wypadek gdy rozwiązania bezpieczeństwa są nieskuteczne lub nie

sensowne (np. zbyt drogie), prowadzona jest polityka zapewniania ciągłości działania (rys.2).



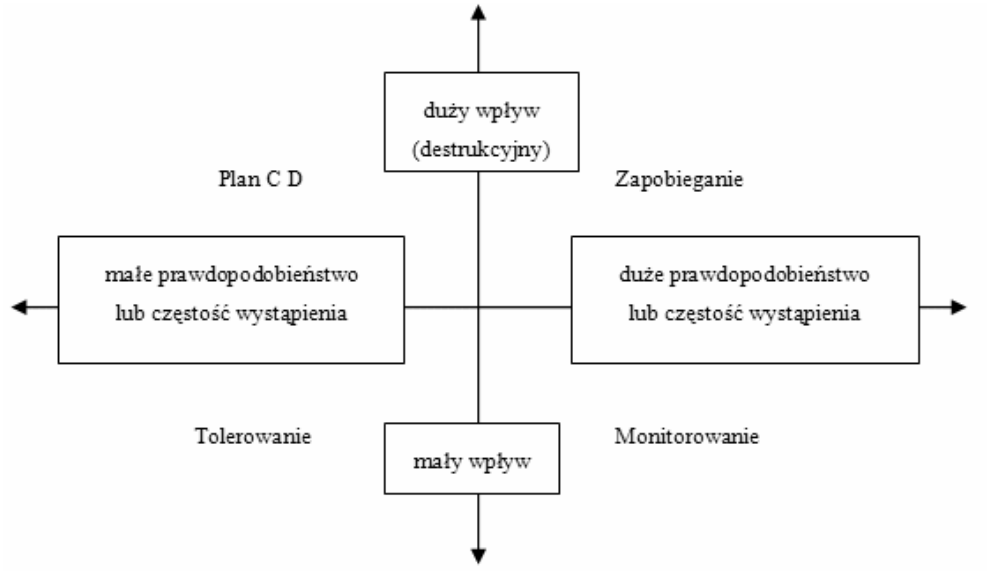
Rys. 2. Relacje „bezpieczeństwa" i „ciągłości działania" w zarządzaniu ryzykiem (źródło: opracowanie własne)

3. MODEL POLITYKI CIĄGŁOŚCI DZIAŁANIA

Zadania zapewniania ciągłości działania, jako wynikające z wydarzeń będących efektem spełniania się ryzyka, można analizować w kontekście dwu podstawowych czynników ryzyka, jeśli odwołać się do elementarnego wzoru:

$$\mathbf{R = P \cdot W}$$

gdzie R to ryzyko, P to prawdopodobieństwo wystąpienia zdarzenia krytycznego, a W to wielkość wpływu (np. strat) zdarzenia krytycznego na normalną działalność organizacji. Ideę takiego spojrzenia analitycznego ilustruje rysunek 3.



Rys. 3. Modelowe postępowanie z zagrożeniami (źródło: opracowanie własne)

Pokazany na nim podział przestrzeni problemowej na cztery pola należy rozumieć jako obraz kompleksowego zarządzania ciągłością działania. Każda z czterech części ograniczonych osiami odpowiada innemu modelowemu podejściu do reagowania na analizowane zdarzenia krytyczne. Trzeba to rozumieć w ten sposób, że każde z wyobrażanych zdarzeń krytycznych (a poprzez nie zidentyfikowanych zagrożeń dla normalnej działalności) jest docelowo traktowane w sposób właściwy dla jego oceny, w sensie prawdopodobieństwa wystąpienia i szacowanych możliwych skutków.

Tolerowanie oznacza pogodzenie się z przejściowymi niedogodnościami. Monitorowanie oznacza, że wiedza o zakłóceniu jest dostateczna do uruchomienia mechanizmu oczywistej kompensacji. Zapobieganie oznacza działania w celu zapobieżenia negatywnym skutkom zakłócenia. Plan Ciągłości Działania jest zestawem scenariuszy przewidywanego materializowania się zagrożeń oraz działań zaplanowanych na taką okoliczność.

Podejście Tolerowania powinno być przypisywane do postępowania z zakłóceniami w swej naturze zewnętrznymi wobec danej organizacji, a tylko wtórnie jej dotyczącymi, w szczególności nie inwazyjnymi, a zwłaszcza nie destrukcyjnymi. Przykład: firma transportowa rozwożąca prasę – przeczekanie mgły porannej i późniejsze rozwiezienie gazet.

Podejście Monitorowania powinno być przypisywane do postępowania z zakłóceniami w swej naturze drobnymi, choć częstymi (przez co należy zakładać ich incydentalnie większy wpływ przez kumulację zdarzeń w krótkim czasie), ale wyraźnie nie destrukcyjnymi. Z tej strategii ma wynikać obowiązek szczegółowego rozwiązania przez posunięcia organizacyjne oraz nawet drobiazgowe regulacje wewnętrzne reakcji na

wszelkie typowe zakłócenia. Istotą jest nikły lub wręcz żaden wzrost kosztu z tytułu rozwiązań reagowania, bowiem mają one przede wszystkim organizacyjny charakter. Przykład: nieobecności chorobowe pracowników – obowiązek zawiadamiania zawczasu zakładu pracy oraz opracowane zasady organizowania zastępstw.

Podejście Zapobiegania powinno być przypisywane do postępowania z zakłóceniami istotnymi, destrukcyjnymi i potencjalnie często występującymi. Jest to strategia prewencji,, jej naturalnymi konsekwencjami są inwestycje i rozwiązania ograniczające ryzyko zagrożenia. Typowe posunięcia to dublowanie rozwiązań technicznych. Przykład: częste wyłączenia zasilania – instalacja podtrzymywaczy napięcia lub generatorów energii.

Podejście Planu Ciągłości Działania powinno być przypisywane do postępowania z zakłóceniami istotnymi, destrukcyjnymi, lecz potencjalnie rzadko występującymi, co uzasadnia decyzje o rezygnacji ze podejścia Zapobiegania i świadome podejmowanie ryzyka zagrożeń. Przykład: Giełda – światowe statystyki mówią, że zawieszenie notowań z powodu niesprawności systemu komputerowego zdarza się nie częściej niż raz na 3 lata i trwa nie dłużej niż jeden dzień, uzasadnione jest więc, poleganie na scenariuszu zastępczego funkcjonowania w trakcie usuwania tak rzadko zdarzającej się, poważnej awarii.

Polityka Ciągłości w zakresie Tolerowania (T) powinna określać podstawowe zasady przystępowania organizacji do stanu pogodzenia z zaistniałym zakłóceniem, badania przesłanek jego utrzymywania się, stwierdzania jego ustąpienia oraz powrotu do rutynowego funkcjonowania. Dokumentowi Polityki T powinny towarzyszyć procedury/instrukcje szczegółowo określające konieczne działania komórek organizacji w sytuacjach zakłóceń zakwalifikowanych do poddania ich tej polityce. Przykład: mimo że reakcja organizacji na zakłócenie może krańcowo polegać na zawieszeniu wypełniania statutowych funkcji, to być może należy poinformować o tym partnerów handlowych lub opinię publiczną, skierować pracowników do prac zastępczych nie poddających się działaniu zakłócenia, uruchomić rozwiązania śledzące stopień intensywności zakłócenia. W momencie zaś ustąpienia zakłócenia należy dokonać weryfikacji czy jest możliwe podjęcie zawieszonych dotąd czynności/funkcji.

Polityka Ciągłości w zakresie Monitorowania (M) powinna określać podstawowe zasady reagowania organizacji na zakłócenia, co do których świadomość ich zaistnienia w połączeniu z istniejącymi regułami zachowań (ewentualnie spisanymi w postaci procedur i instrukcji) powinna w dostatecznym stopniu uruchamiać organizacyjne mechanizmy kompensacji zakłócenia. Dokumentowi Polityki M powinny towarzyszyć procedury/instrukcje szczegółowo określające konieczne działania komórek organizacji w sytuacjach zakłóceń zakwalifikowanych do poddania ich tej polityce. Przykład: w banku, pracowników bezpośredniej obsługi klientów obowiązuje procedura uprzedzania o nieobecnościach spowodowanych np. chorobą, zaś określona liczba pracowników zaplecza jest przeszkolona do obsługi klientów na zasadzie zastępstw, przy czym każdego dnia określona ich liczba ma być gotowa do podjęcia takiej zastępczej pracy na wypadek absencji nadzwyczajnej, o której pracownik nie uprzedził zawczasu.

Polityka Ciągłości w zakresie Zapobiegania (Z) powinna określać plany organizacji dotyczące działań prewencyjnych, które w odniesieniu do szczególnie istotnych elementów

działalności organizacji, a zwłaszcza szczególnie wrażliwych elementów jej infrastruktury technicznej, mają zniwelować destrukcyjny wpływ zakłóceń. Typowymi działaniami podejmowanymi w tym celu są: tworzenie rozwiązań zapasowych, nadmiarowych, zwielokrotnionych w stosunku do przeciętnych zapotrzebowań. Dokumentowi Polityki Z powinny towarzyszyć analizy szczegółowo określające stopień i zakres wrażliwości rozwiązań istniejących, plany rozwiązań zmniejszających zagrożenia, procedury/instrukcje szczegółowo określające organizację i zasady działania bieżącego oraz specjalnych interwencji specjalistycznych zespołów do zwalczania specyficznych zagrożeń (pożar, atak hakerski, awaria informatyczna). Przykład: zapasowy ośrodek komputerowy, dublowane linie komunikacyjne prowadzone fizycznie różnymi drogami i/lub z wykorzystaniem odmiennych mediów transmisji. Także dyżury specjalnych ekip interwencyjnych o stosownych kwalifikacjach.

Równocześnie należy podkreślić, że każda z par obiekt – zagrożenie ujęta w Polityce Z, a więc w planie działań prewencyjnych, o ile polegają one na inwestycjach zmniejszających zagrożenie, to do czasu ich zakończenia powinny być ujęte także w jednej z pozostałych Polityk (zaleca się, aby w Polityce P) celem zapewnienia stosownej reakcji na zagrożenie.

Polityka Planu Ciągłości Działania (P) powinna określać plany organizacji dotyczące działań koniecznych w przypadku zmaterializowania zagrożenia w postaci konkretnego zakłócenia. Plany powinny obejmować rozwiązania organizacyjne dotyczące prowadzenia samej Polityki oraz scenariusze przypadków zakłóceń i zakładanych wobec nich działań, mających na celu zapewnienie kontynuacji przynajmniej podstawowej aktywności biznesowej organizacji. Ponadto Polityka P powinna określać zasady reagowania *ad hoc* na zdarzenia, których niestety nie udało się przewidzieć w scenariuszach (w ogóle lub co do skali). Dokumentowi Polityki P powinny towarzyszyć procedury/instrukcje szczegółowo określające organizację służb prowadzących plany ciągłości działania, podstawowe reguły komunikowania się w warunkach awarii, zasady reagowania na typowe zagrożenia, scenariusze przewidywanych rozległych zakłóceń i reagowania na nie, zasady uwzględniania w nowych wersjach planów awaryjnych doświadczeń ze zwalczania świeżo zaszłych zakłóceń.

Podział na cztery podejścia odzwierciedla też potrzebę racjonalności w zarządzaniu ciągłością działania, z uwzględnieniem nakładów i zastosowanych środków. Prowadzi to do wzbogacenia intuicyjnego pojmowania rozwiązań ciągłości działania jako planów reagowania na zakłócenia, a więc działań ex-post w stosunku do zaistnienia zdarzenia krytycznego, o postępowanie prewencyjne (ex-ante) w stosunku do istoty mechanizmu spodziewanego zdarzenia krytycznego. Tym samym zapewnianie ciągłości działania staje się też częścią zintegrowanego zarządzania ryzykiem [2, str. 20], zwłaszcza w zakresie manipulowania ryzykiem. Logiczną bowiem konsekwencją uświadomienia, zidentyfikowania i oceny ryzyka jest poszukiwanie rozwiązań zabezpieczających i naprawczych. W szczególności wart podkreślenia jest synergiczny związek zagadnień zapewniania bezpieczeństwa i zagadnień 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 na fakt nieskutecznej ochrony.

Wynika z tego także znaczenie racjonalnego (tam, gdzie nie działa obowiązek prawny, a tylko gra czynników biznesowych) podziału przypisywania prymatu pomiędzy zapewnianie bezpieczeństwa (gdy wolimy nie dopuszczać do zakłóceń) a poszukiwanie zastępczych warunków ciągłości (gdy ochrona jest nieracjonalna ekonomicznie).

To przenikanie się zagadnień wskazuje też na potrzebę integrowania zadań i struktur organizacyjnych obarczonych tym zadaniami, w zakresie zarządzania ryzykiem, bezpieczeństwem i ciągłością działania. Ryzyko takie określane jest dodatkowo terminem „operacyjne" (taka terminologia pochodzi z rynku finansowego [3]), choć z uwagi na przedmiot odniesienia powinno raczej nosić miano „ryzyka organizacyjnego". Co gorsza w obliczu przesłanek zasygnalizowanych we Wprowadzeniu, uważa się, że zagadnienie zarządzania tym ryzykiem powinno należeć do zadań zarządzania strategicznego współczesną organizacją [4], co zaprzecza klasycznemu używaniu w teorii organizacji przymiotnika „operacyjny" w opozycji do określeń „strategiczny", czy „taktyczny". Do zupełnego już pomieszania pojęć dochodzi niestety w terminologii angielskiej, gdzie pojęcie „operational risk management" oznacza zarówno „operacyjne zarządzanie ryzykiem", jak i „zarządzanie ryzykiem operacyjnym".

4. PODSTAWY METODYCZNE

Z rygorystycznie naukowego punktu widzenia mówienie o metodach w odniesieniu do dotychczasowej praktyki projektowania rozwiązań zarządzania ciągłością działania może być uznane za pewną przesadę. Tym niemniej warto podkreślić, że doświadczenie w tym zakresie wykroczyło znacznie poza spontaniczne formy opracowywania planów awaryjnych, jak kiedyś to określano, dobrze tym samym oddając ówczesny ograniczony charakter powstających rozwiązań. Można już wskazać trzy nurty porządkowania doświadczeń, które mogą służyć systematyzacji wiedzy, a nawet, jak to bywa podnoszone w USA, sformułowaniu teorii Business Continuity Management [5]. Są to:

- rekomendacje sektorów: bankowego i ubezpieczeniowego, poparte dyrektywami MiFID (Market in Financial Instruments Directives) Komisji i Parlamentu Europejskiego[6],
- normy ISO i normy narodowe dotyczące przede wszystkim bezpieczeństwa informacji (seria norm ISO-27000, ISO-17799, BS-25999),
- metody projektowania firm doradczych (zwłaszcza publicznie dostępna metoda DRII [8]).

Wszystkie one są zasadniczo rodzajami list kontrolnych podających bądź bardzo ogólnie sformułowane zasady ostrożnościowe, bądź wykaz typowych zagadnień składających się na bezpieczeństwo i które wobec tego należy uwzględnić w tworzeniu rozwiązań bezpieczeństwa i ciągłości działania. W przypadku firm doradczych opis stosowanych metod jest bardzo skąpy, co deklaratywnie jest wyjaśniane ochroną firmowego „know-how". Jedynym wyjątkiem jest metoda DRII, opracowana właśnie jako produkt handlowy, z cieszącą się popularnością ofertą szkoleń i certyfikowania projektantów.

Na podstawie przebadanych przez autora około 50 projektów wyłania się podział na projekty prowadzone na zasadzie scenariusza jak największego zdarzenia krytycznego oraz projekty wykreowania doskonalącego się mechanizmu organizacyjnego ukierunkowanego na budowanie zdolności do reagowania na zdarzenia krytyczne i ich przesłanki. Pierwsze podejście opiera się na argumentacji, że w ramach większego rozwiązania powstają gotowe recepty i umiejętności do reagowania na mniejsze zdarzenia krytyczne. Wydaje się jednak, że poza stosunkowo szybkim przygotowaniem rozwiązania, na którym zostaje skupiony projekt, podejście to ma szereg słabości, które można ująć w jednej podstawowej – słabo się zakorzenia w kulturze organizacji.

Podejście oparte na zasadzie stałego doskonalenia przede wszystkim odwołuje się do kultury danej organizacji, wyrasta z niej, odzwierciedla bieżący stan wiedzy (świadomości) w organizacji i dzięki temu nie forsuje rozwiązań przekraczających bieżące zdolności wykonawcze. Dominującą zasadą jest stałe doskonalenie oraz odwołanie się do motywacji, determinacji i elastyczności pracowników, którzy w sytuacji krytycznej często stają się najważniejszym zasobem, jaki ma posłużyć opanowaniu nietypowego i często szczególnie agresywnego oddziaływania czynnika krytycznego.
Kwestie jakie przychodzi rozwiązać to:

- jak organizacyjnie zapewnić zarządzanie ryzykiem, bezpieczeństwem i ciągłością działania,
- jak identyfikować i oceniać ryzyko,
- jak poszukiwać rozwiązań zabezpieczających przed przejawami ryzyka,
- jak oceniać racjonalność podziału oczekiwań i zadań pomiędzy zarządzanie bezpieczeństwem a zarządzanie ciągłością działania,
- jak wymusić stałe doskonalenie poczynań zmierzających do panowania nad ryzykiem i zapewniających właściwy poziom, bezpieczeństwo i ciągłość działania (także w sensie spełnienia wymogów prawa w tym zakresie).

5. STRUKTURA METODY TSM-BCP

Przedstawiona tu metoda została opracowana w roku 2003 i od tej pory doskonalona w toku projektów dla 9 dużych podmiotów gospodarczych (finanse, przemysł, usługi komunalne). Każdy z projektów trwał od 6 do 18 miesięcy. Z kolei w roku 2006 pod takim kątem przeprowadzono badania polskiego sektora ubezpieczeń (wzięło w nim udział 46 na 66 istniejących zakładów ubezpieczeń).
Na metodę składają się działania w trzech przestrzeniach projektowych, prowadzące do kształtowania:

- struktury organizacyjnej dedykowanej do zagadnienia zapewniania ciągłości działania (lub szerzej ryzyka, bezpieczeństwa i ciągłości),
- mechanizmu spirali działań organizatorskich służących realizacji celu projektowania,
- form utrwalania wiedzy o problemie i rozwiązaniach.

5.1. STRUKTURA ORGANIZACYJNA

W modelowym układzie dedykowaną strukturę tworzą: Komitet Ciągłości Działania, Koordynator Ciągłości Działania, wszystkie komórki organizacyjne oraz Sztab Kryzysowy. Jest to struktura o charakterze sztabowym w stosunku do Kierownictwa organizacji, związana z zadaniem wiodącym. Zadanie to może być pojmowane węziej (taka optyka wynika zazwyczaj z decyzji organizacji, która wdraża metodę) tj. ograniczone do zagadnienia ciągłości. Korzystniej jest jednak, gdy tworzony jest Komitet ds. Ryzyka tzn. jego obszarem zadań jest zarządzanie ryzykiem organizacyjnym, a dopiero w konsekwencji także zarządzanie bezpieczeństwem i ciągłością. Komitet działa oczywiście tylko okresowo, w formie spotkań, na których rozliczane są dotychczasowe oraz nakładane nowe zadania. Wykonawcami tych zadań są wszystkie komórki organizacyjne, których dotyczą różne aspekty oddziaływania ryzyka lub działania mające tym ryzykiem manipulować. Celem bieżącej koordynacji tych prac wskazywany jest Koordynator, którym może być wybrana spośród istniejących komórek organizacyjnych, która od tej chwili część swego czasu poświęca tym zadaniom, korzystając z autorytetu formalnego Komitetu.

Odrębnie, na wypadek poważnych zdarzeń krytycznych, tworzy się i przygotowuje, w sensie szkolenia specyficznych umiejętności oraz gromadzenia rezerwowych zasobów, dodatkowy byt organizacyjny – Sztab Kryzysowy. W mniejszych organizacjach Sztab bywa tożsamy ze składem Kierownictwa, uzupełnionym o specjalistów właściwych dla przewidywanych sytuacji krytycznych. W dużych organizacjach, gdzie Kierownictwo zajmuje się tylko zagadnieniami strategii i zarządzania wysokiego poziomu, Sztab, który musi cechować bardzo dobra znajomość działalności operacyjnej, siłą rzeczy może najwyżej korzystać z jakiejś formy przekazywania autorytetu formalnego przez Kierownictwo (np. w formie symbolicznego udziału w składzie Sztabu członka Kierownictwa).

5.2. CYKL ORGANIZATORSKI

Spirala cyklu organizatorskiego, postrzegana najzupełniej klasycznie jako cykl Deminga (PDCA [9]), ma prowadzić od analizy czynników krytycznych do projektowania rozwiązań oraz ich stopniowego doskonalenia. Analiza obejmuje:

- identyfikację procesów biznesowych celem wskazania ich najważniejszych elementów,
- identyfikację zagrożeń i form, w jakich mogą się przejawiać,
- identyfikację podatności jako miejsc, w których organizacja szczególnie mocno wystawiona jest na zagrożenia.

Taka analiza prowadzi do specyfikacji możliwych zakłóceń, a także oceny ich istotności, w tym odniesienia do postulowanego potraktowania zapobiegawczo-naprawczego w ujęciu z rysunku 3.

Od tego momentu rozpoczyna się faza projektowania scenariuszy jako rozwiązań naprawczych (w sensie koncepcji postępowania) oraz jako dokumentacji rozwiązania. Projektowanie obejmuje typowe działania mikrocyklu organizatorskiego: pomysł, wykonanie, kontrola, użycie (często tylko jako test). Projektowanie takie składa się z:

- analizy mechanizmu realizowania się konkretnego zakłócenia,
- określenia modelu reagowania na to zakłócenie zmierzającego do: przywrócenia stanu sprzed zakłócenia oraz na ten czas ustanowienia zastępczego sposobu zorganizowania pracy,
- wyspecyfikowania wszystkich kroków realizacji takiego modelu reagowania i opracowanie niezbędnych rozwiązań cząstkowych (procedur, instrukcji, procesów, działań) i harmonogramu ich opracowania
- realizacji zadań wg harmonogramu oraz ich testowania.

Powstały scenariusz powinien być systematycznie doskonalony w kontekście doświadczeń praktycznych (użycie wobec zdarzeń krytycznych) oraz ewolucji wiedzy o problemie (okresowe przeglądy metodą sztabową).

5.3. UTRWALANIE WIEDZY

Odbywa się ono w aspekcie bezpośrednio organizacyjnym, który stanowią działania szkoleniowe, testy i narady sztabowe inspirowane przez Komitet ds. Ryzyka oraz poszczególne komórki organizacyjne, oraz w aspekcie zintegrowanej dokumentacji, którą stanowią takie kategorie dokumentów jak:

- Polityka Bezpieczeństwa i Ciągłości deklarująca podstawowe zasady,
- Regulamin Bezpieczeństwa i Ciągłości określający prawa i obowiązki w tworzeniu, utrzymywaniu i rozwijaniu rozwiązań
- Plan Ciągłości Działania będący wzorcowym zbiorem dokumentacji dotyczącej ciągłości działania (w tym procedur poszczególnych komórek organizacyjnych),
- scenariusze opisujące przewidywane zakłócenie i zaplanowane postępowanie reaktywne.

Ogromne znaczenie dla skutecznego gromadzenia i utrwalania wiedzy (także w sensie uniezależnienia od absencji i fluktuacji kadr zaangażowanych w prace nad ciągłością działania) ma wprowadzenie kompleksowych zasad prowadzenia dokumentacji i jej wewnętrznego redagowania. Dokumentacja ta ma bowiem posłużyć reagowaniu na wystąpienie sytuacji krytycznej, kiedy często brak czasu na zastanawianie się nad interpretacją zapisu.

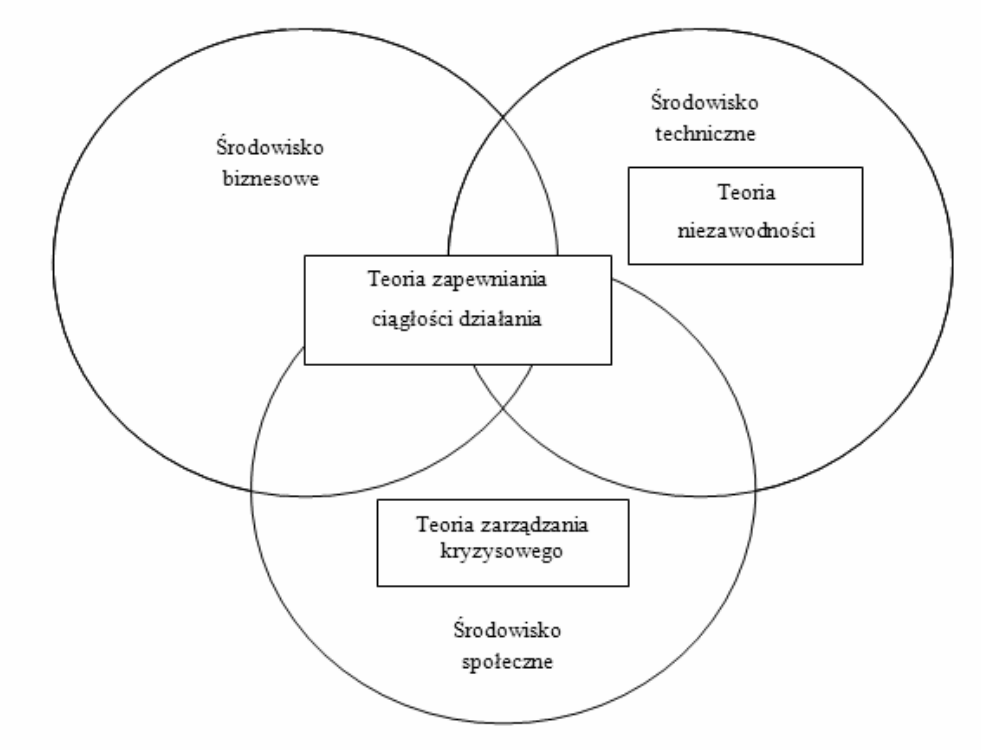
Utrwalanie wiedzy jest bowiem utrwalaniem doświadczenia i wynikającej z niego prawidłowej praktyki działania.

6. PODSUMOWANIE

Zasadniczą ideą metody jest ustalenie wyzwań (analiza procesów, zagrożeń, podatności) i uruchomienie mechanizmu stałego doskonalenia, postrzeganego jako dorastanie umiejętnościami do poziomu wyzwań (i ich dynamiki), jakie sytuacja wewnętrzna oraz otoczenie biznesowe i konkurencyjne stawiają organizacji.

Generalnie zaś zarządzanie ciągłością działania, skutkujące racjonalnymi rozwiązaniami, jest wyrazem odpowiedzialności (w ujęciu teorii etyki biznesu) w zarządzaniu i kreuje nowoczesną kulturę organizacji. Warto przy tym zauważyć, że

przenosi to na szerszy plan społeczny tradycję inżynierskiej świadomości co do zawodności wszelkich wytworów ludzkich, co ilustruje rysunek 4.



Rys. 4. Związki teorii zapewniania ciągłości działania z teorią niezawodności technicznej oraz teorią zarządzania kryzysowego (źródło: opracowanie własne)

7. LITERATURA

[1] Zawiła-Niedźwiecki J. *Ciągłość działania organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2007

[2] Conrow E.H. *Effective Risk Management. Some keys to success*, American Institute of Aeronautics and Astronautics Inc., Reston, 2000

[3] Committee on Banking Supervision. *Sound Practices for the Management and Supervision of Operational Risk*, Bank for International Settlements, Basel, 2003

[4] Bizon-Górecka J. *Strategie zarządzania ryzykiem w organizacji gospodarczej*", Przegląd Organizacji 1/2001

[5] www.thebci.org (the Business Continuity Institute)

[6] Główny Inspektorat Nadzoru Bankowego. *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*, Narodowy Bank Polski, Warszawa 2004

[7] Dyrektywa 2004/39/ EC, Rozporządzenie Komisji nr 1287/2006, Dyrektywa 2006/31/ EC, Dyrektywa 2006/73/ EC
[8] www.drii.org (Disaster Recovery Institute International)
[9] Dahlgaard J.J., Kristensen K., Gopal K.K. *Podstawy zarządzania jakością*, PWN, Warszawa, 2000

TSM-BCP, BUSINESS CONTINUITY SOLUTIONS DESIGN METHOD

Summary: For a very long time in history of management theory the problem of reacting to disturbances in functioning of organisation was treated as routine duty of a manager and depended on ones personal skills. Thus the problem of continuity of operations was considered a task of operational management. For some years there is a trend to reat this as task for strategic managment, considered by top organisations' officers. In financial sector it is even a requirement of EU directives. Presented method TSM-BCP, dating from year 2003, tried in a number of implementations, is a proposal of complex approach to organising those problems.

Keywords business continuity, operational risk, integrated security, business menace