MODELOWANIE PROCESÓW ANALIZY RYZYKA UTRATY CIĄGŁOŚCI FUNKCJONOWANIA ORGANIZACJI

Łukasz Tomaszewski, Piotr Zaskórski

Wojskowa Akademia Techniczna

Streszczenie. W artykule podjęto problem zapewniania ciągłości funkcjonowania organizacji. Mówiąc o ciągłości działania, należy mieć świadomość zagrożeń i możliwości przeciwdziałania w wymiarze taktycznym, operacyjnym oraz strategicznym. Organizacje dążą do eliminacji lub ograniczenia skutków zaistnienia sytuacji, która przyczynia się do spadku sprawności i efektywności ich działania. W artykule skoncentrowano się na zapewnianiu ciągłości działania poprzez potwierdzenie zdolności organizacji do utrzymywania w stabilności zaplanowanych procesów funkcjonowania i takiego reagowania na zakłócenia warunków normalnej działalności, aby tam, gdzie to możliwe, nastąpiło przywrócenie normalnych warunków działania lub możliwa była realizacja zadań w trybie działania zastępczego. O tym wszystkim decyduje jednak rzetelne szacowanie i monitorowanie ryzyka.

1. Wstęp

Mówiąc o ciągłości działania, organizacje powinny umiejętnie wydzielać ze swojej struktury te zadania, które zagrożone są największą podatnością na niepowodzenie. Możliwe jest to tylko przy właściwej znajomości własnych procesów, odpowiednio prowadzonej analizie zagrażających czynników, jak również optymalnej konfiguracji działań w zakresie taktycznym, operacyjnym oraz strategicznym. Rosnące znaczenie informacji oraz zintegrowanych systemów informatycznych zarządzania sprawia, że coraz trudniej jest zapewnić ciągłość wykorzystywanych przez przedsiębiorstwo zasobów. Dotyczy to nie tylko kwestii ich pozyskiwania, lecz także właściwego zagospodarowania w celu wytworzenia planowanych rezultatów. To z kolei przekłada się na pozytywne postrzeganie przedsiębiorstwa przez klientów oraz wielkość generowanych zysków. Organizacje dążą zatem, aby nie dopuścić do zaistnienia sytuacji, która przyczyni się do spadku skuteczności i efektywności ich działania. Odnosi się to nie tylko do umiejętności postępowania z zaistniałym ryzykiem, lecz także do zdolności minimalizowania jego skutków. Dla tych potrzeb tworzone są plany ryzyka, utożsamiane współcześnie również z planami ciągłości funkcjonowania organizacji.

Wprowadzając do problematyki podejmowanej w artykule, należy zaznaczyć, że „zapewnienie ciągłości działania to, po pierwsze, zdolność organizacji do utrzymywania w stabilności zaplanowanych procesów funkcjonowania, a po drugie, zdolność takiego reagowania na zakłócenia warunków normalnej działalności, aby tam, gdzie to możliwe, szybko przywrócić normalne warunki

działania, a tam gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań"[1].

2. Zarządzanie ciągłością funkcjonowania organizacji

Organizacje gospodarcze, będące elementem systemu gospodarczego państwa, działają współcześnie przy konieczności sprostania wyzwaniom płynącym z otoczenia. Jest to zarówno otoczenie bliższe (konkurenci, klienci, dostawcy, strategiczni sojusznicy) jak i dalsze (techniczne, polityczno-prawne, ekonomiczne, społeczno-kulturowe, międzynarodowe)[2]. Na tej podstawie można powiedzieć, że przedsiębiorstwa są pewnym systemem działania, w którym realizowany jest szereg procesów. Procesy te wymagają zużycia określonych zasobów (kapitał, ludzie, infrastruktura, technologia, materiały, surowce, zasoby informacyjne oraz energetyczne), które przetwarzane są w systemie organizacyjnym w elementy wyjściowe w postaci produktu (wyrób, usługa, projekt). Pozwala to na rozpatrywanie przedsiębiorstwa w kategoriach systemowych, odnosząc je do sposobów osiągania celów organizacji (wskaźniki jakościowe, niezawodnościowe, ekonomiczne), wykonywanych poprzez spełnianie szeregu kryteriów (m.in. użyteczność, funkcjonalność, niezawodność, efektywność, ryzyko oraz jakość).

Taka interpretacja organizacji pozwala na wnioskowanie, że sam proces zarządzania należy traktować wieloaspektowo, biorąc pod uwagę różne kryteria. W rzeczywistości istnieje bowiem wiele czynników będących w stanie zaburzyć tak rozpatrywany system. Dotyczy to nie tylko kwestii zasobowej, dotyka również problemu sposobu realizacji celu. W tym aspekcie, aby temu zapobiec, konieczna staje się optymalna synchronizacja działań w oparciu o właściwie prowadzony proces zarządzania. W myśl klasycznej definicji jest to „zestaw działań (obejmujący planowanie i podejmowanie decyzji, organizowanie, przewodzenie, tj. kierowanie ludźmi i kontrolowanie), skierowanych na zasoby organizacji (ludzkie, finansowe, rzeczowe i informacyjne) i wykonywanych z zamiarem osiągnięcia celów organizacji w sposób sprawny i skuteczny"[3]. Biorąc pod uwagę ciągłość działania, współcześnie nie można mówić o profesjonalnym zarządzaniu złożonym przedsięwzięciem jedynie przy wykorzystaniu wskazanych działań. Wraz z rozwojem nauki o organizacji ewoluowały również funkcje zarządcze, które wskazują na działania ukierunkowane na zapewnienie płynności w sferze sprawozdawczości przedsiębiorstwa, na którą w szczególności składa się: raportowanie, normowanie oraz ewidencjonowanie[4].

[1] J. Zawiła-Niedźwiedzki, *Ciągłość działania organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008, s. 5.
[2] R.W. Griffin, *Podstawy zarządzania organizacjami,* PWN, Warszawa 2007, s. 76.
[3] Ibidem, s. 6.
[4] P. Zaskórski, *Wykłady z zarządzania procesami*, WAT, Warszawa 2010.

Dopiero takie zorientowanie może stanowić odzwierciedlenie tzw. „pełnego cyklu zarządzania". Ciągłość funkcjonowania organizacji postrzega się zazwyczaj wieloaspektowo, gdyż może ona dotyczyć m.in. wymiaru informacyjnego, technicznego i technologicznego, zasobowego oraz personalnego. Często utożsamia się z samym procesem zarządzania ryzykiem, co zostało uwidocznione w tabeli 1.

Tabela 1

Charakterystyka zarządzania ryzykiem oraz ciągłością działania

Charakterystyka	Zarządzanie ryzykiem	Zarządzanie ciągłością działania
Metoda	analiza ryzyka	analiza ciężaru strat
Parametry	zdarzenie i prawdopodobieństwo jego wystąpienia	zdarzenie oraz czas jego wystąpienia i trwania
Rodzaj zdarzenia	wszystkie typy – jednak możliwe do sklasyfikowania i nie zawsze wyraźnie wpływające na działalność	różne rodzaje zdarzeń istotnie wpływające na zachwianie równowagi przedsiębiorstwa
Waga i rozmiar zdarzeń	różne rozmiary – jednak koszty możliwe do oszacowania	strategia zaplanowana do pokonania każdej trudności niezależnie od wagi zdarzenia
Zakres	skupienie na ryzykach odnoszących się głównie do podstawowej działalności przedsiębiorstwa	skupienie głównie na wydarzeniach mających potencjalny lub realny wpływ na biznes
Siła i sposób oddziaływania	od problemów narastających do nagłych incydentów	głównie nagłe i szybkie wydarzenia; kultura utrzymania ciągłości działania pozwalająca pokonać problemy narastające

Źródło: T.T. Kaczmarek, *Ryzyko kryzysu a ciągłość działania*, DIFIN, Warszawa 2009, s. 30

Zagadnienia te, choć modelowo porównywalne, różnią się pod względem kilku zasadniczych parametrów (tabela 1). Zarządzanie ciągłością działania jest nową dziedziną, upodabnianą raczej z cyklem klasycznym, jednakże rozpatrywaną w ujęciu interdyscyplinarnym. Obejmuje ona swoim zakresem obszary związane z zarządzaniem ryzykiem, nieruchomościami, łańcuchem dostaw, jakością, BHP, wiedzą, bezpieczeństwem, komunikacją kryzysową i odtwarzaniem działalności w przypadku wystąpienia niepożądanych zdarzeń, kryzysowe[5]. Na tej podstawie Brytyjski Instytut Ciągłości Działania (BCI) definiuje zarządzanie ciągłością działania jako „holistyczny proces zarządzania, który ma na celu określenie potencjalnego wpływu zakłóceń na organizację i stworzenie warunków budowania odporności na nie oraz zdolności skutecznej reakcji w zakresie kluczowych interesów właścicieli, reputacji i marki organizacji, a także wartości osiąganych w jej dotychczasowej działalności"[6].

[5] http://www.atm-si.com.pl/uslugi/zarzadzanie_ciagloscia_dzialania

[6] J. Monkiewicz, L. Gąsiorkiewicz (red.), *Zarządzanie ryzykiem działalności organizacji,* C.H. Beck, Warszawa 2010, s. 195.

Rys. 1. Zarządzanie ciągłością działania wg BCI (Business Continuity Management)
Źródło: http://www.atm-si.com.pl/uslugi/zarzadzanie_ciagloscia_dzialania

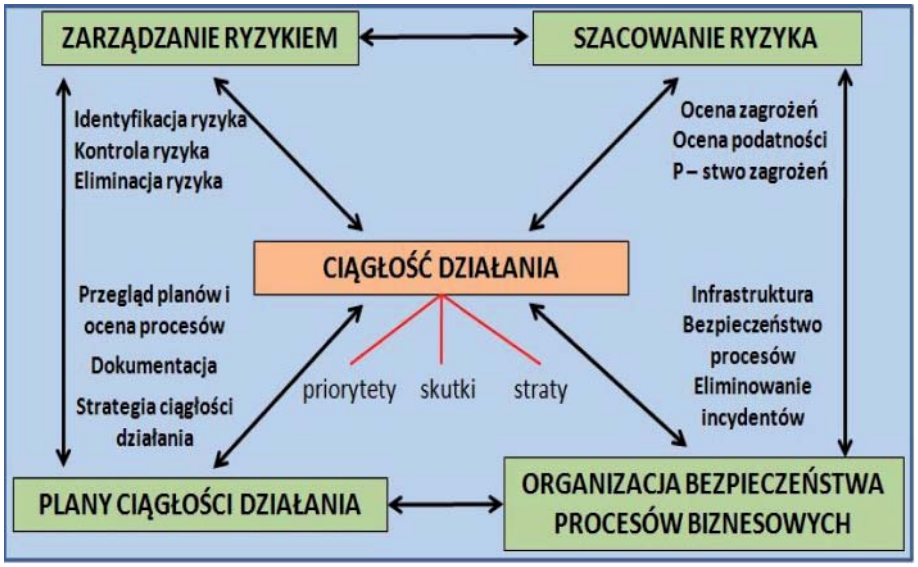
Analiza literatury przedmiotu nakazuje wyodrębniać kluczowe aspekty, które stanowią fundament omawianej dziedziny. Zalicza się do nich w szczególności [15]:

- zdefiniowanie ryzyka, na jakie narażona jest działalność organizacji poprzez specyfikację procesów podatnych na zakłócenia,
- określenie skutków i prawdopodobieństw ryzyka → identyfikowanie działań zapobiegawczych i planowanie reakcji na ryzyko,
- oszacowanie wpływu przerw w realizacji procesów na wynik działalności biznesowej przedsiębiorstwa,
- opracowanie strategii reagowania na zaburzenie ciągłości działania, jak również systematyczne testowanie i weryfikowanie realizowanych funkcji,
- wkomponowanie procesu zapewnienia ciągłości działania w strukturę organizacji,
- rozwijanie aspektu związanego z zapewnieniem ciągłości działania poprzez identyfikację sposobów zabezpieczenia strategicznych zasobów przedsiębiorstwa.

Z punktu widzenia problemu zapewniania ciągłości działania należy proces ten traktować jako „ciąg planowanych działań, zmierzających do zapobieżenia zakłóceniom, lub usuwanie przyczyn i skutków zaistnienia zakłócenia, albo wprowadzenia zastępczych warunków działania do czasu usunięcia skutków zakłócenia”[7]. Należy zatem zwrócić szczególną uwagę na komponenty będące mechanizmem

[7] J. Zawiła-Niedźwiedzki, op. cit., s. 7.

napędzającym optymalne zarządzanie organizacją w aspekcie jej bezpieczeństwa. Dotyczy to nie tylko szacowania i zarządzania ryzykiem, lecz także właściwego planowania i organizacji bezpieczeństwa procesów biznesowych (rys. 2). Na tej podstawie można wnioskować, że zarządzanie ciągłością działania to zapewnienie na drodze ustanowienia procesu i organizacji działania, że pewien uznawany za minimalny niezbędny poziom działania operacyjnego zostanie zachowany nawet w warunkach krytycznego zakłócenia [16].



Rys. 2. Aspekty zarządzania zapewnianiem ciągłości działania
Źródło: J. Zawiła-Niedźwiedzki, op. cit., s. 55

W istocie cykl utrzymania ciągłości działania rozpoczyna się w momencie rozpoznania specyfiki własnych procesów. Tworzy się w tym celu odpowiednie drzewa (struktura statyczna), sieci powiązań, a następnie określa mierniki, dzięki którym możliwe staje się zorientowanie w kwestiach bezpieczeństwa jego realizacji [4]. Faza ta charakteryzuje się równoległym wsparciem procesu oceny i kontroli ryzyka, jak również analizą ciężaru strat. Ramy właściwej korelacji działań wykonywanych w przyszłości stanowi konstruowana strategia utrzymania ciągłości działania. Uwzględnia się w niej wszystkie te czynniki, które mogą mieć decydujący (również negatywny) wpływ na przebieg procesu, przy jednoczesnym jego odniesieniu do kategorii jakościowych produktu. Ponadto strategia wyszczególnia ścieżkę postępowania w przypadku zaistnienia niepożądanych zdarzeń. Zakłócenia te odnoszą się zazwyczaj do błędów kierowania oraz innych nieprzewidzianych w trakcie działalności czynników. Warto przy tym zaznaczyć, że utrzymanie ciągłości działania

(UCD) jest procesem nieprzerwanym i powinno się angażować w niego wszystkich pracowników organizacji, budując swego rodzaju kulturę skierowaną na UCD. Pracownik powinien być zorientowany na ciągłe doskonalenie, jak również szkolony z zakresu reagowania w sytuacjach kryzysowych.

3. Identyfikacja zagrożeń organizacji

Istotnym z punktu widzenia polityki bezpieczeństwa elementem wejściowym do przeprowadzania analizy ryzyka jest identyfikacja zagrożeń organizacyjnych (logistycznych). W zależności od charakteru działalności, przedsiębiorstwa narażone są na występowanie różnego typu niepożądanych zdarzeń. Przykładowo firma, która zajmuje się działalnością usługową w zakresie przewozu materiałów, do zagrożeń swojej działalności będzie zaliczać nadmierny wzrost paliw, długotrwałe uszkodzenia eksploatowanej bazy samochodowej lub też brak umów z klientami zewnętrznymi. Natomiast biorąc pod uwagę przedsiębiorstwo produkcyjne, będzie ono uznawało np. przerwy w dostawie surowców za czynnik zaburzający ciągłość działania. Pojawia się zatem pytanie, jak radzić sobie z powstawaniem szeregu zdarzeń warunkujących płynność bytu przedsiębiorstw? Odpowiedzi na to pytanie można poszukiwać, dążąc do zrozumienia istoty ryzyka, jak również w efektywnie prowadzonym procesie monitorowania i kontroli działalności [14]. Wyróżnia się zatem kilka zasadniczych grup zagrożeń, które zostały zaprezentowane w tabeli 2.

Tabela 2

Identyfikacja zagrożeń przedsiębiorstwa

GRUPA	ZAGROŻENIA
Katastrofy naturalne	trzęsienia ziemi, skażenie środowiska naturalnego, powódź, huragan, wyładowania atmosferyczne i inne
Terroryzm	szantaż, zamach i inne
Zakłócenia fizyczne	brak dostępu do siedziby, uszkodzenie budynku, za niska/ wysoka temperatura powietrza, za duża wilgotność powietrza, pożar, zasilanie i inne
Zakłócenia funkcjonalne	strajk, sabotaż, niedostępność pracowników, wypadek i inne
Zakłócenia techniczne	wyczerpanie zapasów materiałowych, brak zasilania, awaria klimatyzacji i inne
Zakłócenia informatyczne	dotyczące: infrastruktury technicznej, oprogramowania, wirusów, informacji oraz danych
Zakłócenia wynikające z braku zasobów	brak zasobów osobowych, finansowych, materiałowych, brak usług zewnętrznych i inne

Źródło: J. Zawiła-Niedźwiedzki, op. cit., s. 77-78

Skutki tak sklasyfikowanych zagrożeń mogą być różnorakie. Najczęściej, wg zaleceń ISA–TR99.00.02, zalicza się do nich obrażenia u ludzi, straty finansowe, szkody w otoczeniu, przerwy w działalności operacyjnej oraz negatywny wpływ na wizerunek publiczny firmy[8]. Dla potrzeb zapewnienia ciągłości działania najczęściej tworzy się scenariusze powstałych zdarzeń oraz tzw. „drzewa użyteczności". Pozwalają one w sposób kompleksowy odzwierciedlić istotę zakłóceń oraz proponować możliwe do podjęcia działania zapobiegawcze.

4. Model podsystemu zarządzania ryzykiem – metody i narzędzia

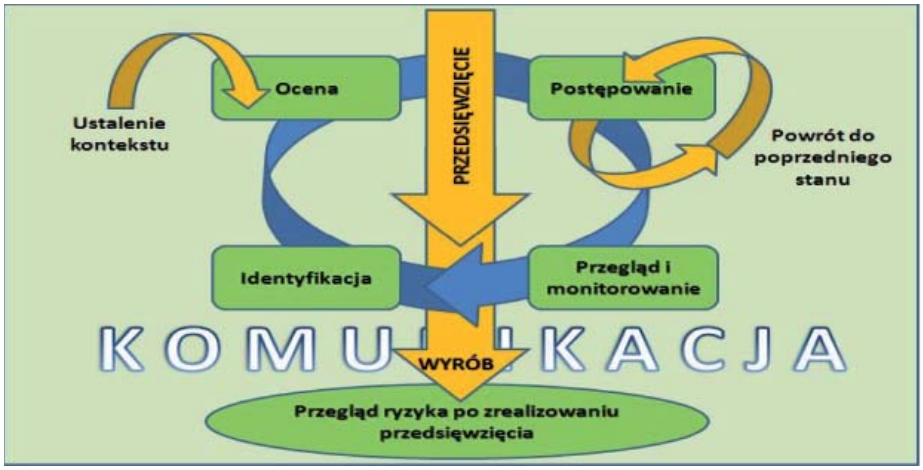
Funkcjonowanie organizacji, niezależnie od charakteru działalności, związane jest z dokonywaniem wyborów spośród ustalonych w fazie planowania opcji. Najczęściej, ze względu na ograniczoność zasobów, podejmowanie decyzji odbywa się w warunkach pewności (kiedy zapewnione są wszystkie niezbędne zasoby do jej podjęcia) oraz niepewności (gdy kierownictwo nie jest w stanie wnioskować o przyszłych stanach przedsięwzięcia) [6]. Z tego też względu, mówiąc o niepewności, należy rozpatrywać ją jako długookresowy stan towarzyszący funkcjonowaniu podmiotów gospodarczych na rynku, wynikający z ograniczonej przewidywalności i wieloznaczności zachowań podmiotów gospodarczych oraz zawodności procesów realnych i informacyjnych. Z kolei niepewność w krótkim czasie określana jest mianem ryzyka. Z systemowego punktu widzenia traktowane jest ono jako obraz niepożądanych zdarzeń oraz ich skutków. O procesie charakteryzującym się dużym poziomem zakłóceń mówimy, że jest on obarczony zwiększonym poziomem ryzyka, a co za tym idzie trudniejsze staje się sfinalizowanie podejmowanych w nim działań. Nie zawsze jednak taka interpretacja ma zastosowanie. Współcześnie „ryzyko to możliwość sukcesu, ale również niepowodzenia, porażki, straty. To także przedsięwzięcie, którego wynik jest niepewny, wątpliwy. Ryzyko to również możliwość powstania szkody"[9]. Zgodnie z wytycznymi normy PN–IEC 62198 pod pojęciem zarządzania ryzykiem kryje się zatem „systematyczne stosowanie polityki, procedur i praktyki zarządzania do zadań ustalania kontekstu ryzyka, jego identyfikowania, analizowania, wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka"[10]. Interpretacja ta jest z kolei odzwierciedleniem klasycznie rozumianego ogólnego modelu zarządzania ryzykiem w przedsiębiorstwie (rys. 3).

---

[8] P. Zaskórski (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, WAT, Warszawa 2011, s. 100.

[9] J. Zawiła-Niedźwiedzki, I. Staniec (red.), *Zarządzanie ryzykiem operacyjnym*, C.H. Beck, Warszawa 2008, s. 14.

[10] PN–IEC 62198:2005, *Zarządzanie ryzykiem przedsięwzięcia. Wytyczne stosowania*, pkt 3.



Rys. 3. Koncepcja zarządzania ryzykiem przedsięwzięcia
Źródło: PN–IEC 62198:2005, *Zarządzanie ryzykiem przedsięwzięcia. Wytyczne stosowania*, pkt 4.2

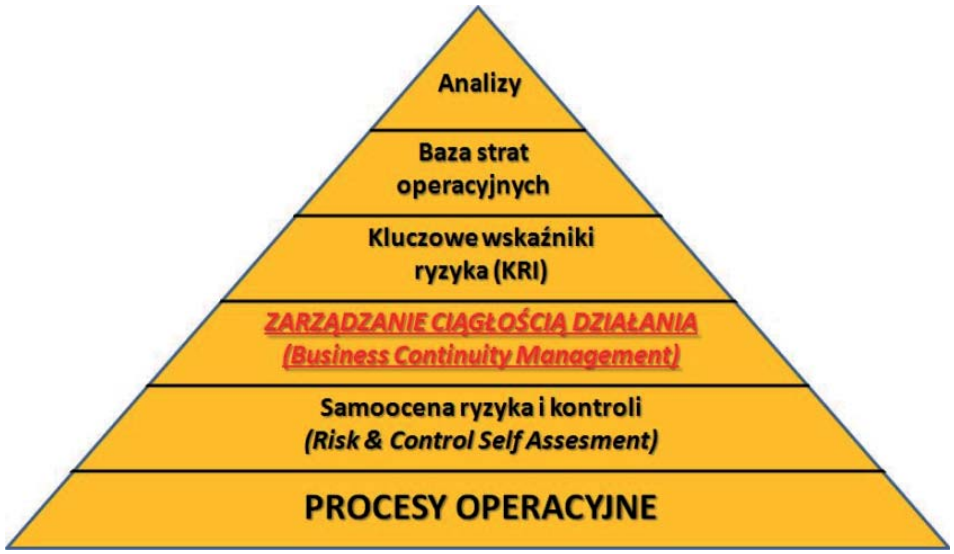
Najczęściej, analizując model funkcjonowania przedsiębiorstwa w aspekcie systemu zarządzania ryzykiem, w przedsięwzięciu mówi się o występowaniu tzw. ryzyka operacyjnego. „Jest to ryzyko poniesienia bezpośrednich lub pośrednich strat związanych z niewłaściwie prowadzonymi lub błędnymi wewnętrznymi procesami, osobami lub systemami albo związanych ze zdarzeniami zewnętrznymi”[11]. Z kolei na tle ryzyka operacyjnego poszukuje się wpływu na całokształt przedsięwzięcia właściwie konfigurowanego procesu zarządzania ciągłością działania.

W rzeczywistości podstawą struktury zarządzania ryzykiem są procesy operacyjne realizowane wewnątrz danej organizacji. Na ich podstawie dokonywana jest samoocena ryzyka, przy jednoczesnej kontroli wykonywanych działań. Pozwala to nie tylko na ustalenie odchyleń od wcześniej udokumentowanego planu, lecz także na szybką reakcję w przypadku wystąpienia w systemie zagrożeń powodujących jego organizacyjne zachwianie [12]. To z kolei wskazuje na ważność procedur monitorowania procesów. Samoocena ryzyka jest szczególnie przydatna w aspekcie zapewnienia prawidłowego przebiegu cyklu zarządzania ciągłością działania. Dzięki temu możliwe staje się określenie kamieni milowych przedsięwzięcia, a co za tym idzie ustalenie, jakie rodzaje ryzyka mają na nie największy wpływ [7]. W tym celu tworzy się zestaw tzw. wskaźników ryzyka, będących parametrami realizowanego procesu biznesowego pod względem występujących w nim zakłóceń. W efekcie uruchamiana jest baza danych o niepożądanych zdarzeniach, wspierana zestawem narzędzi informatycznych, na podstawie których wnioskuje się wpływ poszczególnych rodzajów ryzyka na proces [7]. Raporty, będące podstawą struktury zarządzania ryzykiem operacyjnym, pozwalają

[11] A. Korczowski, op. cit., s. 17.

na zorientowanie się w przyszłości, jak wyglądał przebieg przeszłych zdarzeń, po to, aby ograniczyć rozmiar przewidywanych strat.

Zarządzanie ciągłością działania zajmuje kluczowe miejsce w strukturze ryzyka operacyjnego, gdyż pozwala na konfigurowanie funkcji realizowanych w ramach całego systemu, jakim jest organizacja. Zostało to zaprezentowane na rys. 4.



Rys. 4. Miejsce zarządzania ciągłością działania w strukturze zarządzania ryzykiem operacyjnym
Źródło: J. Monkiewicz, L. Gąsiorkiewicz, op. cit., s. 194

Szczególną rolę w cyklu zarządzania ryzykiem przypisuje się procesowi **planowania**. Efektem działań w tym zakresie jest stworzenie planu postępowania ze zidentyfikowanym ryzykiem z wyszczególnieniem metod, jakie mają służyć jego zapobieganiu. Plan powinien również uwzględniać role i obowiązki realizatorów przedsięwzięcia, zakresy tolerancji niepożądanych zdarzeń oraz skategoryzowane poziomy ryzyka określone na podstawie przyjętych prawdopodobieństw [1]. Tematykę związaną z tym obszarem systemowo definiuje standard PMI (*Project Management Institute*), uwzględniając komponenty wejściowe i wyjściowe oraz stosowane narzędzia i techniki. W tym kontekście, do wkładów procesu planowania zalicza się [1]:

- deklarację zakresu przedsięwzięcia (informacje o rodzajach realizowanych procesów, ich przebiegu oraz planowanych rezultatach),
- plan zarządzania kosztami (pozwala dokonać reakcji na ryzyko w przypadku przekroczenia budżetu przeznaczonego na przedsięwzięcie),
- plan zarządzania harmonogramem (określający umiejscowienie w czasie realizowanych operacji cząstkowych),

- plan zarządzania komunikacją (pozwala na planowanie: kto, kiedy i w jaki sposób będzie podejmował działania w przypadku wykrycia zakłóceń w systemie),
- czynniki środowiskowe prowadzonej działalności (determinują zwiększenie niepewności działania → ich uwzględnienie jest konieczne z punktu widzenia bezpieczeństwa przedsięwzięcia) oraz aktywa procesów organizacyjnych.

Na etapie planowania nie odnotowuje się ilościowych i jakościowych narzędzi wspierających, gdyż odbywa się on w formie zebrań oraz analiz planistycznych wymienionych powyżej elementów wejściowych. W efekcie tego powstaje plan zarządzania ryzykiem uwzględniający w szczególności [1]:

- metodykę (określa sposób postępowania z zakłóceniami, stosowane narzędzia i techniki oraz proponowane podejścia do rozwiązywania problemów),
- role i obowiązki (specyfikacja osób zaangażowanych bezpośrednio w działania prewencyjne i minimalizujące powstałe ryzyko),
- budżetowanie (oszacowanie przewidywanych kosztów wystąpienia ryzyka),
- wyznaczenie terminów (określenie, kiedy należy dokonywać gruntownych pomiarów w celu specyfikacji aktualnej sytuacji przedsiębiorstwa),
- kategorie ryzyk (identyfikowanie, jakie ryzyka i w jakim przedziale będą do zaakceptowania, a w przypadku jakich konieczne jest podejmowanie natychmiastowych działań korygujących),
- i inne, takie jak: sposób raportowania czy specyfikacje prawdopodobieństw i skutków wystąpienia ryzyka.

W istocie proces planowania pozwala odpowiedzieć na pytanie: gdzie szukać ryzyka? Potencjalnych czynników może być wiele, dlatego też wskazuje się na konieczność wykrywania zakłóceń źródłowych, stanowiących praprzyczyny możliwych przyszłych problemów. To z kolei stanowi istotę etapu **identyfikacji i analizy ryzyka**. W tym celu tworzy się tzw. katalog ryzyka, sporządzony w oparciu o szczegółową analizę struktury organizacyjnej i realizowanych procesów. Pozwala on na orientację, gdzie w procesie będą występowały tzw. „słabe ogniwa", które zadecydują o formie wytwarzanego rezultatu. Tak sporządzona lista powinna obejmować wszystkie możliwe do zaistnienia nieścisłości (źródła ryzyka) systemu (organizacji), do których zalicza się przede wszystkim [7]:

- zmiany w założeniach lub zmiany wymagań i zakresu przedsięwzięcia,
- błędy wykonania, niezrozumienie lub pominięcie istotnych elementów na etapie projektowania,
- źle definiowane lub zrozumiane role i odpowiedzialności,
- złe oszacowania, niekompetencja lub brak doświadczenia zespołu,
- zależność od zdarzeń i zespołów zewnętrznych.

Identyfikacja ryzyka zatem to „proces określania, jakie ryzyka mogą wpływać na przedsięwzięcie oraz udokumentowania cech charakterystycznych tych

ryzyk"[12]. Szczególną uwagę zwraca się w nim na rozpoznanie kamieni milowych przedsięwzięcia, uwarunkowanych różnorodnością i dostępnością wykorzystywanych zasobów. Do tego celu należy posługiwać się zestawem metod i narzędzi, m.in. takich jak metoda delficka, burza mózgów, wywiady, analizy przyczyn źródłowych, techniki oparte na diagramach (schematy blokowe systemu, diagramy przyczynowo-skutkowe oraz diagramy wpływów), analiza SWOT czy też analizy ekspertów [1]. W normach i literaturze przedmiotu metod tych wymienia się dużo więcej, lecz najbardziej rozpowszechnione zostały zaprezentowane w tabeli 3.

Tabela 3

Wybrane metody identyfikacji i analizy ryzyka w organizacji

Rodzaj	Określenie metody	Opis i komentarze
Metoda burzy mózgów	Katalog ryzyk	Sporządzenie listy zagrożeń lub sytuacji niebezpiecznych związanych z daną czynnością, urządzeniem lub systemem.
	HAZOP	Systematyczna analiza działania układu dla wykrycia i określenia zagrożeń, w szczególności odchyleń od założonego przebiegu procesu, którym mogą towarzyszyć bardzo duże konsekwencje.
	FMEA	Systematyczna analiza działania układu dla wykrycia i określenia zagrożeń, ustalenia przyczyn powstawania oraz skutków ich występowania.
Metoda rankingu ryzyka	Względny ranking	Metoda, w której uwzględnia się zarówno ilościowe, jak i jakościowe metody identyfikacji ryzyka, których celem jest ustalenie zagrożeń związanych ze stosowanymi materiałami, warunkami pracy i ustaleniu ich kolejności według poziomu ryzyka.
Metody drzew logicznych	Analiza drzewa niezdatności	Celem modeli logicznych jest identyfikacja specyficznych związków pomiędzy przyczynami a kombinacją zdarzeń, które mogą mieć wpływ na powstawanie zagrożenia. Metody drzew logicznych wymagają szeregu szczegółowych informacji i pozwalają na prowadzenie drobiazgowej analizy. Każdą z tych metod można stosować do analizy zidentyfikowanego ryzyka.
	Analiza drzew zdarzeń	
	Analiza niezawodności człowieka	

Źródło: [2]

Analizę ryzyka prowadzi się zazwyczaj w formie ilościowej oraz jakościowej. Jakościowa analiza to „proces hierarchizacji ryzyka poprzedzający ich dalszą analizę lub działania z nimi związane i realizowany poprzez ocenę i odniesienie do siebie

[12] *A Guide to the Project Management Body of Knowledge*, Fourth Edition, MT&DC, Warszawa 2009, s. 296.

ich prawdopodobieństw oraz skutków wystąpienia”[13]. Z kolei ocena ilościowa jest „procesem liczbowej analizy wpływu rozpoznanych ryzyk na całościowe cele przedsięwzięcia (…). Przeprowadza się ją w odniesieniu do ryzyka, które w wyniku analizy jakościowej uznano za zdolne do wywarcia znaczącego wpływu na trudne do pogodzenia cele organizacji”[14]. Najczęściej dla potrzeb analizy ryzyka stosuje się miarę punktową, pozwalającą szacować ryzyko z następującej zależności:

$$VaR=PxS, \tag{1}$$

gdzie: VaR – wartość ryzyka; P – poziom częstości występowania ryzyka; S – poziom strat.

Często zależność (1) uzupełnia się dodatkowo o takie parametry jak wskaźnik podatności czy współczynnik ekspozycji. Pierwszy z nich określa, w jakim stopniu możliwe jest minimalizowanie ryzyka w danym procesie, natomiast drugi podkreśla znaczenie ryzyka z punktu widzenia wpływu na realizację celów przedsięwzięcia. Rozwinięta postać miary punktowej przedstawia się następująco:

$$VaR=P\bullet S\bullet Exp\bullet P_d, \tag{2}$$

gdzie: P – poziom częstości występowania ryzyka; S – poziom strat; Exp – współczynnik ekspozycji; P_d – wskaźnik podatności na ryzyko.

W wyniku takiego oszacowania wartości ryzyka zestawia się na matrycy wyznaczającej zakresy jego akceptowalności. Pozwala to na wyróżnienie ryzyka „mało istotnego (akceptowalne)”, „umiarkowanie istotnego (dopuszczalne)” oraz „bardzo istotnego (niedopuszczalne)” i z reguły matryca ta jest opracowywana na etapie planowania zarządzania ryzykiem (tabela 4).

Prowadzenie ilościowej analizy ryzyka opiera się również na wykorzystaniu innych technik, takich jak diagramy drzewa decyzyjnego (podstawa tzw. analizy oczekiwanej wartości pieniężnej), analiza wrażliwości, modelowanie i symulacje przebiegu procesów [1]. W tym aspekcie, odnosząc się do ciągłości funkcjonowania organizacji, konieczne staje się opracowanie odpowiednich scenariuszy przebiegu zdarzeń zakłócających jej działanie. Z pewnością zastosowanie znajduje tutaj technika FTA (*Fault Tree Analysis*) oraz PHA (*Preliminary Hazard Analysis*).

Modelowanie procesów analizy ryzyka metodą FTA polega na usystematyzowanym rozkładzie danego zdarzenia na czynniki pierwsze w celu identyfikacji zakłóceń inicjujących. Można ją prowadzić dla zdarzeń szczytowych o charakterze pozytywnym bądź negatywnym, co w konsekwencji pozwala na łatwe zrozumienie

[13] Ibidem, s. 303.
[14] Ibidem, s. 309.

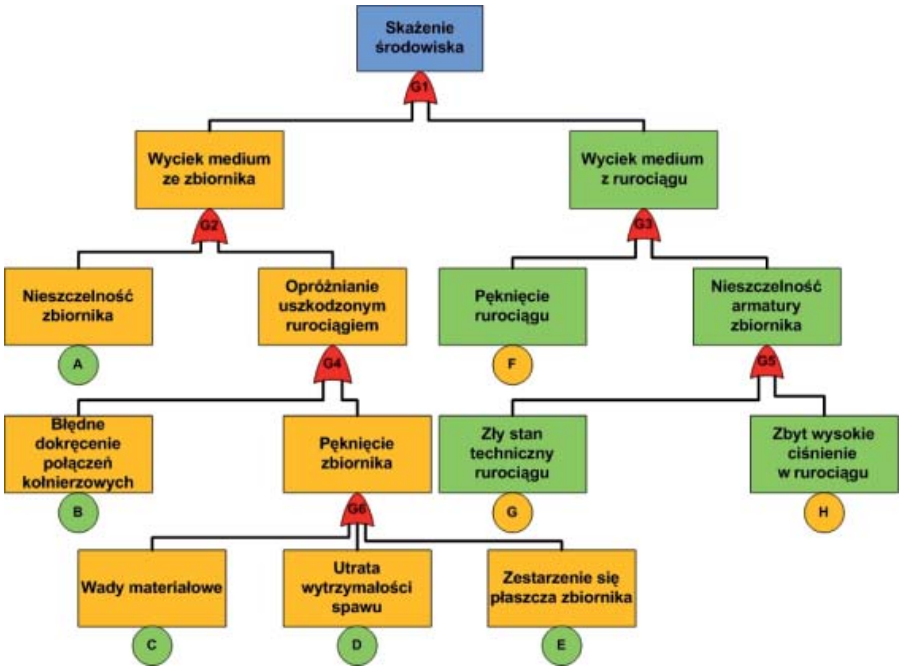
zachowania się systemu. W związku z tym, że drzewa te często mają duży zakres, ich przetwarzanie może wymagać stosowania technik komputerowych. Cecha ta powoduje niekiedy trudności w jego weryfikacji. Wykorzystanie omawianej techniki zaprezentowano na przykładzie zagrożenia związanego z eksploatacją infrastruktury technicznej bazy paliw płynnych (rys. 5).

Tabela 4

Macierz prawdopodobieństwa i skutków wystąpienia ryzyka

P - stwo	ZAGROŻENIA					SZANSE				
0,90	0,05	0,09	0,18	0,36	0,72	0,72	0,36	0,18	0,09	0,5
0,70	0,04	0,07	0,14	0,28	0,56	0,56	0,28	0,14	0,07	0,04
0,50	0,03	0,05	0,10	0,20	0,40	0,40	0,20	0,10	0,05	0,03
0,30	0,02	0,03	0,06	0,12	0,24	0,24	0,12	0,06	0,03	0,01
0,10	0,01	0,01	0,02	0,04	0,08	0,08	0,04	0,02	0,01	0,01
	0,05	0,10	0,20	0,40	0,80	0,80	0,40	0,20	0,10	0,05
	RYZYKO NIEDOPUSZCZALNE			RYZYKO DOPUSZCZALNE				RYZYKO AKCEPTOWALNE		

Źródło: *A Guide to the Project Management Body of Knowledge*, s. 306



Rys. 5. Analiza zdarzenia szczytowego „skażenie środowiska" metodą FTA
Źródło: opracowanie własne

Z kolei metoda PHA jest narzędziem, za pomocą którego możliwe staje się identyfikowanie wszystkich faz życia określonego systemu działania w sposób jakościowy. Analizę ryzyka przeprowadza się dla potrzeb określenia skutków wystąpienia niepożądanych zdarzeń, jak również środków zapobiegawczych, jakie należy podjąć, aby je minimalizować. Wykorzystuje się przy tym [2]:

- informacje stanowiące zestawienie znanych zagrożeń występujących w obrębie obiektu (stanowisko pracy, proces, obiekt użytkowy, produkcyjny i inne),
- wyniki analizy właściwej, dotyczącej potencjalnej możliwości oddziaływania obiektu lub procesu na otoczenie.

W metodzie wyszczególnia się następujące komponenty:

1) rodzaj zagrożenia,
2) zdarzenie powodujące sytuację zagrożenia,
3) sytuację zagrożenia,
4) zdarzenie prowadzące do potencjalnego wypadku,
5) potencjalny wypadek,
6) skutki,
7) działania zapobiegawcze.

Poniżej zaprezentowano sposób przeprowadzania metody dla dziesięciu zagrożeń, jakie mogą wystąpić podczas użytkowania i obsługiwania obiektu bazy paliw płynnych (tabela 5).

Kolejnym etapem w podsystemie zarządzania ryzykiem jest **proces monitorowania i kontroli**. Polega on na realizacji działań związanych z urzeczywistnianiem planów reakcji (również awaryjnych) na ryzyko, ich śledzeniem, monitorowaniem ryzyka rezydualnego oraz rozpoznawaniem nowego ryzyka w odniesieniu do oceny skuteczności przedsięwzięcia [1]. Niezależnie od zastosowanej strategii działania, podstawę monitorowania i kontroli ryzyka stanowi sprawozdawczość przedsiębiorstwa (raportowanie i ewidencjonowanie). Pozwala to nie tylko na podejmowanie natychmiastowych działań korygujących (zapobiegawczych), lecz także przyczynia się do aktualizacji zdefiniowanej na etapie identyfikacji listy potencjalnych zakłóceń ładu organizacyjnego. Do najbardziej rozpowszechnionych technik i narzędzi warunkujących powodzenie tego etapu należy analiza rezerw, odchyleń i trendów, audyty ryzyka, wyniki pomiaru wykonania technicznego oraz zebrania specjalistów poświęcone analizowaniu przebiegu równolegle wykonywanych procesów organizacji [1].

Tabela 5

Wykorzystanie metody PHA na przykładzie procesu magazynowania paliw płynnych

1	2	3	4	5	6	7
Nieszczelność tacy zbiornika	Erozja/korozja betonu; obsunięcia terenu	Rozszczelnienie zbiornika magazynującego	Tworzenie rozlewiska w tacy magazynowanego paliwa	Przeciek substancji do gleby	Skażenie środowiska wodno--gruntowego	Stosowanie piezometrów; badania procesu starzenia betonu i potencjalnych pęknięć
Rozszczelnienie autocysterny	Podłączanie ramienia nalewczego do zaworu oddolnego załadunku cysterny	Niedokładne podłączenie ramienia nalewczego; zużycie elementów (uszczelek, podłączeń)	Uszkodzenie ramienia nalewczego; wyciek przetłaczanego medium	Wyrwanie ramienia nalewczego; wyciek przetłaczanego medium	Zranienie personelu; skażenie środowiska	Kontrola stanu technicznego wszystkich elementów podłączenia
Brak dostaw mediów	Pęknięcie wodociągu; przerwanie linii energetycznej	Brak dostaw prądu, wody	Błędne funkcjonowanie elementów zbiornika i jego instalacji	Przegrzanie zbiornika; brak funkcjonowania urządzeń elektrycznych	Pożar; wybuch; brak możliwości przyjęcia i dystrybucji magazynowanej cieczy	Zainstalowanie zasilania awaryjnego; podpięcie do sieci z dwóch niezależnych źródeł
Przepełnienie cysterny	Zły stan techniczny przepływomierzy masowych Coriolisa	Niepoprawne wskazanie ilości magazynowanej cieczy	Przekroczenie maksymalnej ilości przetoczonej cieczy do cysterny	Wyciek paliwa; przekroczenie dopuszczalnej ilości paliwa umożliwiającej bezpieczny transport	Zanieczyszczenie środowiska; powstanie pożaru lub wybuchu; zatrucie lub zranienie pracowników	Okresowe badania przepływomierzy

Terroryzm	Przedostanie się na teren bazy osób postronnych	Wniesienie na teren bazy ładunku wybuchowego	Detonacja materiału wybuchowego	Eksplozja zbiornika; zniszczenie rurociągów przesyłowych	Pożar, zranienia, uszkodzenia infrastruktury, skażenie środowiska	Kontrola osób i pojazdów wjeżdżających na teren bazy paliw; monitoring; przepustki wejściowe
Korozja zbiornika	Zawartość zbiornika stalowego zanieczyszczona parą wodną	Powstanie rdzy wewnątrz zbiornika	Ciśnienie robocze	Rozszczelnienie zbiornika ciśnieniowego	Skażenie środowiska; pożar lub wybuch; zranienie personelu	Stosowanie stali nierdzewnej; stosowanie ochrony katodowej
Elektryczność statyczna	Przeładunek magazynowanej cieczy	Skumulowanie się ładunku elektrycznego	Powstanie iskry	Zapłon lub wybuch magazynowanej cieczy	Zniszczenie zbiornika, rurociągów technologicznych i instalacji	Stosowanie uziemienia elementów metalowych
Błędy personelu	Nieostrożność osób prowadzących załadunek cysterny; zły stan techniczny cysterny	Nagłe rozszczelnienie napełnianej cysterny	Zrzut załadowanego paliwa na tacę załadowczą	Zanieczyszczenie infrastruktury terminalu	Zanieczyszczenie sieci kanalizacyjnej produktami ropopochodnymi; stworzenie atmosfery wybuchowej; zatrucia	Zainstalowanie zbiorników slopowych; utrzymywanie wymaganego stanu instalacji i obiektów technicznych

Rozszczelnienie rurociągu technologicznego	Rozwinięte powierzchnie korozyjne; zmęczenie materiału; złe założenia konstrukcyjne	Przeładunek medium	Przekroczenie dopuszczalnego ciśnienia	Wyciek przetłaczanego medium; rozerwanie rurociągu	Skażenie środowiska; zranienie personelu; zatrzymanie czynności związanych z przeładunkiem	Kontrola stanu technicznego rurociągów; stosowanie przyrządów pomiarowych wykrywających spadki ciśnienia
„EFEKT DOMINA”	Pożar zbiornika magazynującego	Niekontrolowany wzrost temperatury i powierzchni pożaru	Eksplozja zbiornika	Przedostanie się pożaru na inny zbiornik magazynujący	Pożar kolejnego zbiornika magazynującego	Zachowanie odpowiednich odległości między zbiornikami; stosowanie kurtyn wodnych i barier zabezpieczających

Źródło: opracowanie własne

Podsumowując, analiza ryzyka zajmuje kluczowe miejsce w podsystemie zarządzania ryzykiem i należy traktować ją jako „proces identyfikacji ryzyka, określania jego wielkości i identyfikowania obszarów wymagających zabezpieczeń”[15], stosowanych dla potrzeb zapewnienia integralności systemu[16], jakim jest organizacja.

5. Ryzyko utraty ciągłości funkcjonowania organizacji

5.1. Wymiar informacyjny

Bardzo ważne, z punktu widzenia realizacji celów strategicznych przedsiębiorstwa, jest zapewnienie ciągłości działania w zakresie wykorzystywania zasobów informacyjnych. Dzieje się tak, ponieważ rosnące znaczenie nowoczesnych koncepcji zarządzania oraz zintegrowanych systemów informatycznych nakłada na przedsiębiorstwa warunki właściwej współpracy z otoczeniem zewnętrznym. Od efektów tej współpracy zależy z kolei bezpieczeństwo danych transferowanych z organizacji. Na tej podstawie, mówiąc o ryzyku w odniesieniu do informacji, można powiedzieć, że występuje ono w przypadku złamania podstawowych zasad bezpieczeństwa. Informacja, traktowana jako „element wiedzy, komunikowany, przekazywany komuś za pomocą języka lub innego kodu oraz także to, co w danej sytuacji może dostarczyć jakiejś wiedzy, bądź też wiadomość, komunikat, wskazówka”[17], powinna cechować się dostępnością, poufnością, integralnością, niezawodnością, autentycznością, tajnością oraz rozliczalnością [14]. Wskazuje się przy tym na ważność właściwie opracowanego systemu bezpieczeństwa informacji traktowanego jako „część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji”[18]. Ryzyko informacji powodowane jest zatem występowaniem szeregu zagrożeń związanych z eksploatacją i bezpieczeństwem systemu teleinformatycznego. Zalicza się do nich[19]:

- działania człowieka powodujące utratę tajności, integralności lub dostępności informacji,
- działania sił wyższych powodujące utratę tajności, integralności lub dostępności informacji,

[15] Norma PN-I-13335-1:1999, *Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele systemów informatycznych*, pkt 3.15.

[16] Wg PN-I-13335-1:1999, *Integralność systemu – właściwość polegająca na tym, że system realizuje swoje zamierzone funkcje w nienaruszony sposób (…)*.

[17] J. Zawiła-Niedźwiedzki, I. Staniec (red.), op. cit., s. 179.

[18] Ibidem.

[19] P. Zaskórski (red.), *Zarządzanie organizacją…*, op. cit., s. 77-78.

- awarie elementów sprzętowych różnorodnych systemów teleinformatycznych i/lub przemysłowych zaangażowanych w taki proces
- oraz wady eksploatowanego w nich oprogramowania.

Warto zaznaczyć, że kluczowy wpływ na bezpieczeństwo informacji ma przede wszystkim właściwa **eksploatacja infrastruktury fizycznej**. Mowa tutaj o zasobach technicznych, do których zalicza się w szczególności sprzęt komputerowy (jednostki centralne, komputery przenośne i inne), sieci telekomunikacyjne (komputery, procesory komunikacyjne i inne) oraz nośniki danych. Wymienione komponenty w istocie mogą stanowić poważne źródła ryzyka, przyczyniające się w konsekwencji do utraty informacyjnej ciągłości działania. Odnosi się to zarówno do czynników, na które kierownictwo organizacji nie ma wpływu, jak i takich, które mogą być wywołane niewłaściwym stosowaniem procedur bezpieczeństwa. Można na tej podstawie mówić o zagrożeniach odnoszących się do sposobu obsługiwania zasobów technicznych oraz systemów, w których dane przetwarzane są w informacje (tabela 6).

Tabela 6

Potencjalne zagrożenia danych i informacji w eksploatowanych zasobach technicznych

TYP ZAGROŻENIA	SPECYFIKACJA
Zewnętrzne	zakłócenia w procesach komunikacji, zanieczyszczenie powietrza, kurz, pył, czynniki chemiczne, zakłócenia systemu zasilania, wyładowania atmosferyczne, klęski żywiołowe, niewłaściwa temperatura powietrza lub zbyt duża wilgotność
Wewnętrzne	awarie sprzętu, wady oprogramowania, pomyłki operatorów i zaniedbania użytkowników, błędy w dokumentacji systemu informatycznego
Celowa działalność człowieka	ataki pasywne: śledzenie komunikacji w sieci komputerowej, nielegalne udostępnianie zasobów i niewłaściwa realizacja zadań; śledzenie promieniowania elektromagnetycznego w celu nielegalnego przechwycenia danych
	ataki aktywne: niszczenie dokumentów i nośników danych, kradzieże sprzętu i dokumentacji, sabotaż, wandalizm, terroryzm, wyłudzanie danych i haseł, powielanie i zniekształcanie komunikatów w sieciach komputerowych, modyfikacje i przekierowywanie danych, infiltracja, hakerzy i krakerzy

Źródło: E. Kolbusz, I. Rejer (red.), *Wstęp do informatyki w zarządzaniu*, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2006, s. 287-310

Konsekwencją wystąpienia któregokolwiek z wymienionych zagrożeń jest utrata podstawowych atrybutów informacji. Dlatego też wskazuje się na ważność właściwej realizacji w tym zakresie polityki bezpieczeństwa, obejmującej różne metody ochrony danych, do których zalicza się w szczególności [5]:

- metody organizacyjne i administracyjne (przydziały uprawnień, kontrola dostępu, harmonogram uruchamiania programów, rejestracja dokumentów, właściwa organizacja stanowisk pracy),

- metody techniczne (zamki, systemy elektroniczne, karty magnetyczne, wydzielenie miejsc przechowywania nośników, sejfy, szafy pancerne, sygnalizacja zagrożenia pożarem, generatory prądotwórcze),
- metody programowe (oprogramowanie antywirusowe, macierze dyskowe RAID, *firewall*, identyfikacja i uwierzytelnianie użytkowników, macierzowe sposoby ochrony, narzędzia do wykrywania intruzów),
- szyfrowanie danych (przekształcanie bloku danych za pomocą odpowiedniego – tajnego klucza),
- ochrona prawna (zgodność ze standardami, certyfikaty bezpieczeństwa).

Wśród innych zabezpieczeń informacji w zasobach technicznych wskazuje się na te, które zawarte zostały w normach[20] z zakresu bezpieczeństwa systemów informatycznych. Na uwagę zasługują następujące środki ochrony:

- fizyczna granica obszaru bezpiecznego (bariery, bramki wejściowe),
- fizyczne zabezpieczenie wejścia (dostęp ma tylko autoryzowany personel),
- zabezpieczenie pomieszczeń, biur i urządzeń,
- systemy wspomagające (stosowane w przypadku awarii sprzętu – są to urządzenia o charakterze zastępczym),
- zabezpieczenie okablowania i konserwacja sprzętu.

Podsumowując, odnosząc zapewnienie informacyjnej ciągłości działania do procesu zarządzania ryzykiem, należy podkreślić, że „bezpieczeństwo informacji oznacza stopień uzasadnionego (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufania, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego): ujawnienia, zniszczenia, modyfikacji, uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej oraz przesyłanej w określonym systemie obiegu informacji"[21].

5.2. Wymiar personalny

Wymiar personalny wyznaczany jest zasobami strategicznymi organizacji typu kapitał ludzki, który obejmuje „ogół specyficznych cech i właściwości ucieleśnionych w pracownikach (wiedza, umiejętności, zdolności, zdrowie, motywacja), które mają określoną wartość oraz stanowią źródło przyszłych dochodów zarówno dla pracownika – właściciela kapitału ludzkiego, jak i dla organizacji korzystającej z tegoż kapitału na określonych warunkach"[22]. Korzystanie z tego kapitału wiąże się z występowaniem

[20] PN – EN ISO/IEC 17799:2007, *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.*

[21] P. Zaskórski (red.), *Zarządzanie organizacją…*, op. cit., s. 71.

[22] Ł. Tomaszewski, *Efektywny proces pozyskiwania pracowników źródłem sukcesu organizacji*, (w:) W. Załoga (red.), *Uwarunkowania wewnętrzne organizacji źródeł jej potencjału*, WAT, Warszawa 2011.

pewnych źródeł ryzyka mających wpływ na personalną ciągłość działania organizacji. W tym kontekście należy odnieść się do trzech zasadniczych reguł odzwierciedlających konieczność zapewnienia bezpieczeństwa osobowego [15]:

- **reguła prawości:** pozyskiwanie wyłącznie takich pracowników, którzy zdolni są podejmować role organizacyjne, o wysokim morale i odpowiedzialności,
- **reguła fachowości:** pracownicy powinni cechować się odpowiednią wiedzą, doświadczeniem zawodowym, kwalifikacjami oraz umiejętnie przystosowywać się do kultury organizacji, jej celów oraz przyjętej strategii,
- **reguła lojalności:** wskazuje się na konieczność zatrudniania takich pracowników, których obecność będzie przyczyniała się do propagowania optymalnej atmosfery w pracy.

Współcześnie nie brakuje jednak sytuacji, gdzie zatrudniani są pracownicy o stosunkowo niskich kompetencjach. Początkowe dobre wrażenie, jakie wywierają w procesie ich pozyskiwana, w późniejszym toku działalności może okazać się złudne. Prowadzi to często do rozwoju sytuacji, w których zauważalne jest celowe bądź niezamierzone destrukcyjne działanie człowieka (ryzyko błędu ludzkiego). Do innych rodzajów ryzyka personalnego zalicza się w szczególności [16]:

- brak odpowiedniej ilości pracowników w organizacji,
- problem braku umiejętności wykorzystywania przez kierowników potencjału ucieleśnionego w pracownikach,
- dużą liczbę pracowników o niewłaściwych kwalifikacjach,
- ryzyko związane z bezpieczeństwem informacji wykorzystywanych przez pracowników (problem poufności, tajności, dostępność oraz integralności).

Źródła ryzyka osobowego uzależnione są również od umiejscowienia w otoczeniu systemu organizacyjnego. Mowa tutaj o tzw. źródłach wewnętrznych oraz zewnętrznych, które zaprezentowano na rys. 6.

Można zatem wnioskować, że ryzyko personalne jest sumą kilku składowych czynników, do których zalicza się m.in.: ryzyko niedostosowania podaży i popytu na rynku pracy, selekcyjne, motywacyjne oraz inwestowania w rozwój pracowników [16]. Ryzyko to nie jest do końca przewidywalne. Człowiek zawsze będzie omylny, a jego zamierzenia nigdy nie zostaną do końca poznane, dlatego też dla potrzeb zwiększania poziomu bezpieczeństwa w tym obszarze należy zadbać o rozwój pakietu szkoleniowego oraz inwestowanie w kapitał niematerialny organizacji.

Rys. 6. Źródła powstania ryzyka personalnego w organizacji
Źródło: J. Zawiła-Niedźwiedzki, I. Staniec, op. cit., s. 161

5.3. Wymiar fizyczny/techniczny

Działalność każdej organizacji wiąże się z koniecznością eksploatowania urządzeń i obiektów technicznych o stopniu złożoności zależnym od specyfiki prowadzonej działalności. Na tej podstawie (w ujęciu ogólnym) można sądzić, że bezpieczeństwo fizyczne odgrywa szczególną rolę w zapewnianiu ciągłości działania organizacji. Ryzyko, jakie niesie ze sobą użytkowanie infrastruktury fizycznej, jest na tyle duże, że wystarczy okresowe zaniechanie czynności obsługowych, aby doprowadzić do długotrwałego zaprzestania funkcjonowania przedsiębiorstwa. Kluczową rolę przypisuje się przy tym czynnikom zewnętrznym, jak również relacji człowiek–maszyna (inny obiekt techniczny).

Źródeł ryzyka technicznego można poszukiwać w błędach popełnianych wewnątrz organizacji, jak również w trudnych do przewidzenia zakłóceniach płynących z otoczenia. Poszukuje się zatem przesłanek potwierdzających konieczność zapewnienia fizycznej ciągłości działania [16]:

– istnieje potrzeba dokładnego określenia granic systemu, wykonywanych w nim funkcji i procesów dla potrzeb klientów wewnętrznych i zewnętrznych,
– pojawia się konieczność szczegółowej identyfikacji zagrożeń obiektów technicznych, ze względu na ich kluczowe znaczenie w wytwarzaniu oczekiwanych rezultatów,

– obiekty techniczne stanowią wsparcie w realizacji funkcji podstawowych organizacji oraz skutecznego procesu wytwarzania i projektowania.

W tym kontekście można powiedzieć, że zarządzanie ochroną fizyczną „przenika się z pozostałymi obszarami zarządzania ryzykiem operacyjnym i charakteryzuje się włączeniem w swój obszar funkcji pochodnych od bezpieczeństwa środowiskowego i osobowego, ogranicza i kontroluje ruch wszystkich osób na terenie siedzib i działania podmiotu, zajmuje się głównie fizycznym zabezpieczeniem i kontrolą całości terenu podmiotu"[23]. Minimalizacja ryzyka w obiektach odbywa się głównie poprzez zastosowanie szeregu systemów bezpieczeństwa, do których zalicza się systemy sygnalizacji włamania i napadu, sygnalizacji pożaru, telewizji użytkowej (CCTV), kontroli dostępu, ewakuacyjne i antypanikowe, zabezpieczeń mechanicznych, ochrony terenów zewnętrznych, ochrony radioelektronicznej, transmisji i monitoringu sygnałów alarmowych oraz monitoringu zagrożeń środowiskowych i przemysłowych [16].

W zależności od tego, co zabezpiecza dany system, może na niego oddziaływać szereg zakłóceń. Do przewidywanych zagrożeń, jak również podstawowych źródeł ryzyka, zalicza się burze, huragany, tornada, trzęsienia ziemi, pożary, powodzie, wybuchy, strajki, brak zasilania i łączności, brak wody, wymagania prawne, szpiegostwo, oszustwo, sabotaż, wypadek przemysłowy, terroryzm i inne.

6. Podsumowanie

Działalność współczesnych przedsiębiorstw narażona jest na występowanie szeregu zdarzeń determinujących ich właściwe funkcjonowanie. Zarządzanie ciągłością działania, jako nowy nurt nauki, rozpatrywane jest interdyscyplinarnie, włączając w swój zakres takie obszary jak zarządzanie ryzykiem, nieruchomościami, łańcuchem dostaw, BHP, wiedzą, bezpieczeństwem oraz kryzysowe. W związku z tym szczególny nacisk powinien być położony na umiejętne planowanie, identyfikację, analizę oraz monitorowanie i kontrolę możliwych do wystąpienia niesprawności całego systemu organizacyjnego. W tym kontekście ciągłość działania należy rozpatrywać wieloaspektowo, biorąc pod uwagę zarówno wymiar informacyjny, techniczny/fizyczny, technologiczny oraz personalny. Każdy z tych obszarów stanowi grupę innych źródeł ryzyka dla przedsiębiorstwa, których poszukuje się nie tylko w ramach porządku wewnątrzorganizacyjnego, lecz także w uwarunkowaniach zewnętrznych (otoczenie). Dlatego też wskazuje się na zasadność korzystania z szeregu metod i narzędzi w aspekcie identyfikacji możliwych do wystąpienia zagrożeń, a nawet sytuacji kryzysowych.

[23] J. Zawiła-Niedźwiedzki, op. cit., s. 37.

Tak więc godny podkreślenia jest fakt, że zapewnienie i utrzymanie ciągłości jest podstawowym kanonem i priorytetowym obszarem zainteresowań w zakresie bezpieczeństwa i ochrony organizacji. Jednakże we współczesnej gospodarce często spotyka się sytuacje, gdzie podejmowanie ryzyka staje się koniecznością z punktu widzenia osiągnięcia przewagi konkurencyjnej. Zasadne zatem będzie powiedzenie *Commodum eius esse debet curius est periculum*, co oznacza, że „zysk powinien być tego, czyje jest ryzyko".

LITERATURA:

1. *A Guide to the Project Management Body of Knowledge*, Fourth Edition, MT & DC, Warszawa 2009.
2. B. Chrószcz, *Analiza i ocena ryzyka zawodowego osób obsługujących systemy maszynowe transportu pionowego w polskich kopalniach węgla kamiennego*, rozprawa doktorska, Akademia Górniczo-Hutnicza, Kraków 2007.
3. R.W. Griffin, *Podstawy zarządzania organizacjami*, PWN, Warszawa 2007.
4. T.T. Kaczmarek, *Ryzyko kryzysu a ciągłość działania*, DIFIN, Warszawa 2009.
5. E. Kolbusz, I. Rejer (red.), *Wstęp do informatyki w zarządzaniu*, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2006.
6. A. Korczowski, *Zarządzanie ryzykiem w projektach informatycznych: teoria i praktyka*, HELION, Gliwice 2010.
7. J. Monkiewicz, L. Gąsiorkiewicz (red.), *Zarządzanie ryzykiem działalności organizacji*, C.H. Beck, Warszawa 2010.
8. PN–EN ISO/IEC 17799:2007, *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*.
9. PN–I-13335-1:1999, *Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele systemów informatycznych*.
10. PN–IEC 62198:2005, *Zarządzanie ryzykiem przedsięwzięcia. Wytyczne stosowania*.
11. Ł. Tomaszewski, *Efektywny proces pozyskiwania pracowników źródłem sukcesu organizacji*, (w:) W. Załoga, *Uwarunkowania wewnętrzne organizacji źródeł jej potencjału*, WAT, Warszawa 2011.
12. P. Zaskórski, *Strategie informacyjne w zarządzaniu organizacjami gospodarczymi*, WAT, Warszawa 2005.
13. P. Zaskórski, *Zarządzanie procesami*, wykłady WAT, Warszawa 2010.
14. P. Zaskórski (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, WAT, Warszawa 2011.
15. J. Zawiła–Niedźwiedzki, *Ciągłość działania organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008.
16. J. Zawiła–Niedźwiedzki, I. Staniec (red.), *Zarządzanie ryzykiem operacyjnym*, C.H. Beck, Warszawa 2008.

Modeling the processes of risk analysis for losing continuity in functioning of the organization

Abstract. The article describes the issue of maintaining continuity for an organization. Discussing this subject one should be aware of the risks and opportunities of tactical, operational and strategic preventions. Organizations seek to eliminate or mitigate the effects of a situation, which would contribute to a decrease in the efficiency and effectiveness of their actions. In addition, the focus is put on the issue of ensuring business continuity through the specification of organization's ability to maintain stability of the planned processes. In this context, tools and techniques to prevent distortions of previous normal activities are specified. It is reasonable to create such procedures that make it possible to restore proper operating conditions or to accomplish the tasks in the mode of operation of replacement substitute actions. However, all this depends on an accurate assessment and on monitoring of risks.