2
Determinanty funkcjonowania zarządzania bezpieczeństwem systemu logistycznego

2.1. Bezpieczeństwo systemu logistycznego i zarządzanie nim

Najogólniej ujmując, „bezpieczeństwo" we współczesnych poglądach, zarówno teoretyków, jak i praktyków życia codziennego w jego różnych wymiarach kształtowania, coraz częściej ujmowane jest w kategoriach: zagrożeń wartości chronionych (czyli sposób określania celu) oraz przeciwdziałań zmierzających do redukcji zagrożeń lub ograniczenia skutków destrukcyjnych oddziaływań (czyli odpowiednich działań i nakładów zapewniających pożądany stan). Stąd też można powiedzieć, że zagrożenia są nieodłącznym elementem zarówno negatywnej, jak i pozytywnej interpretacji bezpieczeństwa, a stan bezpieczeństwa jest zawsze albo wypadków, albo kompromisem pomiędzy potrzebami związanymi z kształtowaniem pożądanego stanu a możliwościami ich zaspokojenia.

Definicje słownikowe określają „bezpieczeństwo" jako „stan niezagrożenia, spokoju, pewności"[30] oraz zagrożeń, czyli bycia niebezpiecznym dla kogoś lub czegoś[31]. Takie podejście do bezpieczeństwa uwypukla dwa główne jego aspekty postrzegania tzn.[32]: brak zagrożenia oraz poczucie pewności albo ochronę przed nim.

---

[30] *Słownik języka polskiego*, red. M. Szymczak, PWN, Warszawa 1978, t. 1, s. 147.

[31] Tamże, t. 3, s. 907.

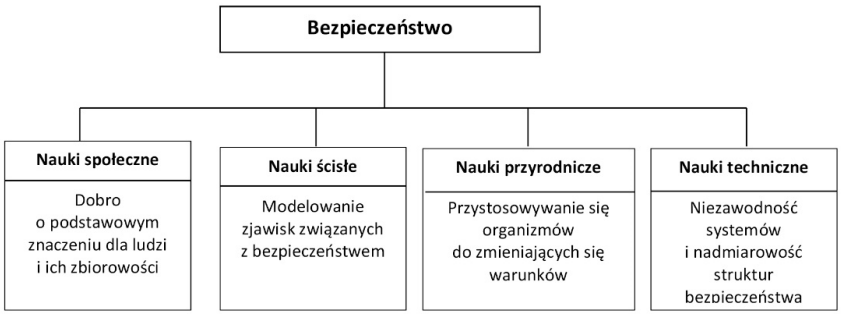
[32] W najbardziej dosłownym znaczeniu bezpieczeństwo jest rzeczywiście identyczne z pewnością (*safety*) i oznacza brak zagrożenia (*danger*) fizycznego albo ochronę przed nim (*A Dictionary of the Social Sciences*, London 1964, s. 629).

Dla pełnego zrozumienia i dogłębnej analizy istoty bezpieczeństwa celowe jest dodanie przymiotników obu tym kategoriom, co sprawia, że stają się one bardziej skonkretyzowane i zawężone przez wskazanie, kogo lub czego dotyczą (wskazanie podmiotu lub przedmiotu).

Dla przykładu, wskazując podmiot, można wyróżnić np. bezpieczeństwo osobiste, bezpieczeństwo przedsiębiorstwa, bezpieczeństwo środowiska.

Odnosząc zaś bezpieczeństwo do ujęcia przedmiotowego, wypada wspomnieć np. o bezpieczeństwie technicznym, logistycznym itd. Oczywiste jest także, że bezpieczeństwo może być też konkretyzowane poprzez zagrożenia (przedmiot oddziaływań i cechy źródeł zagrożeń)[33]. Powstaje dzięki temu szereg nowych (szczegółowych) grup (kategorii, topologii) bezpieczeństwa[34].

Rozumienie bezpieczeństwa zmienia się także w zależności od charakteru nauki wyznaczającej perspektywy badawcze. Najbardziej przydatnymi, z punktu widzenia rozważanych w pracy problemów, są spojrzenia na bezpieczeństwo przez pryzmat obszaru wiedzy nauk społecznych, ścisłych, przyrodniczych i technicznych – rys. 2.1.



Rysunek 2.1. Bezpieczeństwo w kontekście obszaru wiedzy nauk społecznych, ścisłych, przyrodniczych, technicznych

Źródło: opracowanie własne.

Nauki społeczne, dające całościowe spojrzenie na rzeczywistość pokazują bezpieczeństwo w jego złożoności i wielopłaszczyznowej zależności. Bezpieczeństwo traktowane jest jako dobro o podstawowym znaczeniu dla ludzi i ich zbiorowości.

[33] Zob. P. Sienkiewicz, *Teoria i inżynieria bezpieczeństwa systemów*, [w:] Inżynieria systemów bezpieczeństwa, red. nauk. P. Sienkiewicz, PWE, Warszawa 2015, s. 10, 11.

[34] Szerzej zostało opisane w podrozdziale 2.3.

Nauki ścisłe pozwalają precyzyjne definiować, opisywać, przeprowadzać naukowe eksperymenty, symulacje, modelować zjawiska związane z bezpieczeństwem. W tym celu wykorzystuje się przede wszystkim statystykę, probabilistykę, informatykę.

Nauki przyrodnicze zajmują się badaniem różnych aspektów świata materialnego, ożywionego i nieożywionego. W postrzeganiu bezpieczeństwa eksponują kwestie przystosowywania się organizmów do zmieniających się warunków i zmianę formy istnienia, czyli skoków jakościowych pozwalających uzyskać inną, lepszą formę istnienia (bezpieczeństwa) lub dających przewagę nad innymi w środowisku[35].

Nauki techniczne badają zjawiska i ustalają prawidłowości, jakie zachodzą w świecie wytworów i procesów powstałych w wyniku technicznej działalności człowieka. Przy postrzeganiu bezpieczeństwa kładzie się nacisk na kwestie niezawodności systemów i nadmiarowość struktur bezpieczeństwa[36].

Zapewnienie bezpieczeństwa dowolnego podmiotu indywidualnego lub zbiorowego nie jest możliwe bez konieczności użycia wydzielonych, odpowiednio wyszkolonych i wyposażonych sił oraz środków zapewniających przetrwanie i realizację interesów danego podmiotu. Liczba wydzielonych sił i środków na potrzeby bezpieczeństwa zależy od wielkości zagrożeń zewnętrznych pochodzących z otoczenia systemu, a także zagrożeń wewnętrznych, które są „skumulowane" w nim samym. Ponadto zależy od odporności systemu na zagrożenia (jego niezawodności[37]) oraz od dysponowanego potencjału wykonawczego i informacyjno-decyzyjnego. Wydzielone zasoby stanowią element systemu bezpieczeństwa w ramach podsystemu kierowania i wykonawczego, w którym jedną z kluczowych funkcji pełni logistyka.

W literaturze przedmiotu logistyka ta nazywana jest „logistyką bezpieczeństwa" lub „logistyką w bezpieczeństwie" i obejmuje wiedzę oraz umiejętności potrzebne do kształtowania racjonalnych strumieni rzeczowych i związanych z nimi strumieni informacji oraz projektowania (kształtowania) struktur i procesów w celu zaspokojenia potrzeb „określonych" podmiotów (instytucji) występujących w systemie bezpieczeństwa narodowego (w tym gospodarczego) pod warunkiem racjonalności nakładów i kosztów.

Logistyka systemów bezpieczeństwa, jak każda współczesna organizacja, funkcjonuje w środowisku turbulentnym i trudno przewidywalnym. Te uwarunkowania

---

[35] Por. J. Świniarski, *O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych*, Wyd. ULMAK, Warszawa-Pruszków 1997, s. 122–128.

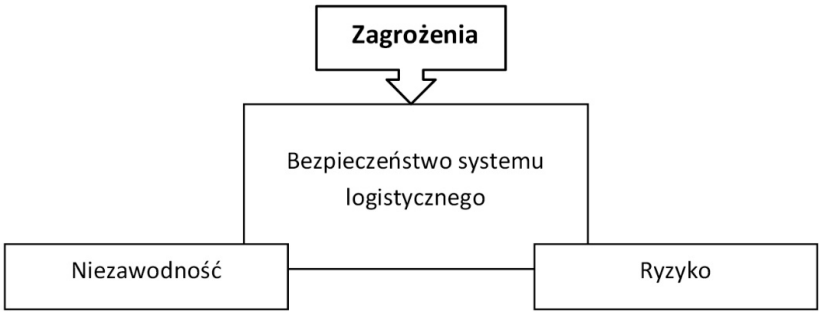
[36] Por. I. Jaźwiński, K. Ważyńskia-Fiok, *Bezpieczeństwo systemów*, PWN, Warszawa 1993.

[37] Niezawodność systemu logistycznego to zespół właściwości, które opisują jego gotowość do ciągłego zachowania stanu zdolności podczas wykonywania procesów logistycznych, na określonym poziomie.

powodują, że struktura, kompetencje, zarządzanie logistyką bezpieczeństwa itp. są nierozerwalnie związane i zależne od współczesnych paradygmatów bezpieczeństwa, do których zalicza się[38]: wyzwania (sytuacje problemowe generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw bezpieczeństwa); zagrożenia (pośrednie lub bezpośrednie destrukcyjne oddziaływania na podmiot); szanse (niezależne od woli podmiotu okoliczności sprzyjające realizacji interesów oraz osiąganiu celów podmiotu w dziedzinie bezpieczeństwa); ryzyka (możliwości wystąpienia negatywnych dla danego podmiotu skutków własnego działania w sferze bezpieczeństwa).

Należy podkreślić, że ze względu na zagrożenia nie wystarczy posiadać dobrze zorganizowaną logistykę dla podmiotów bezpieczeństwa. Trzeba jeszcze mieć na uwadze sprawnie i skutecznie zorganizowane **bezpieczeństwo w logistyce (bezpieczeństwo systemu logistycznego)** w sensie morfologicznym, funkcjonalnym i informacyjnym. To pozwoli realizować procesy logistyczne na poziomie akceptowalnym dla podmiotu bezpieczeństwa. Mówimy wtedy o bezpieczeństwie logistyki (systemu logistycznego).

Należy uwzględnić, że w ujęciu systemowym bezpieczeństwo systemu logistycznego dowolnego podmiotu bezpieczeństwa jest związane z zagrożeniami, niezawodnością[39] oraz ryzykiem (rys. 2.2.)[40]. Do oceny tych wielkości stosujemy miary ilościowe lub jakościowe, pamiętając o jednolitym podejściu dla określonego systemu logistycznego.



Rysunek 2.2. Składowe bezpieczeństwa systemu logistycznego

Źródło: opracowanie własne.

[38] Por. J. Gryz, *Kształtowanie strategicznego zarządzania bezpieczeństwem narodowym*, [w:] Strategia bezpieczeństwa narodowego Polski, red. nauk. J. Gryz, PWE, Warszawa 2013, s. 96.

[39] Por. P. Sienkiewicz, *Teoria i inżynieria systemów*, [w:] Inżynieria… dz. cyt., s. 11.

[40] Szerzej na temat zagrożeń – podrozdział 1.3, a ryzyka w podrozdziale 2.4.

Liczne autorskie artykuły i monografie[41] dotyczące logistyki bezpieczeństwa prowadzą do następujących wniosków:

1. Logistykę bezpieczeństwa, bez względu na jej miejsce funkcjonowania, należy traktować jako system działania, który powinien być ujmowany w określonych kategoriach i zależnościach holistyczno-systemowych. Systemy logistyczne powinny działać zgodnie z jego zasadami organizacyjnymi i funkcjonalnymi.

   Podstawowym zadaniem podsystemów logistycznych w logistyce bezpieczeństwa (PLwLB) jest zaspokojenie potrzeb podmiotu gospodarczego, tak by on mógł realizować swoje żywotne interesy (dotyczące jego istnienia) i wymagania (np. związane z jakością istnienia, trwania).
2. System logistyczny w logistyce bezpieczeństwa, niezależnie od miejsca funkcjonowania, jest przeznaczony do zaspokojenia potrzeb podmiotu bezpieczeństwa, tworzą go: podsystem kierowania, materiałowy, transportu, medyczny, infrastruktury.

   Relacje łączące elementy systemu logistycznego wynikają z podległości służbowej i funkcjonalnej. Występują ponadto procesy współdziałania i informacyjne wynikające z potrzeby komunikowania.
3. System logistyczny bezpieczeństwa możemy również traktować jako zbiór organów kierowania oraz wykonawczych sprzężonych relacjami informacyjnymi i zasileniowymi, przeznaczonych do utrzymania ciągłości procesów logistycznych.

   Stan bezpieczeństwa nie jest stabilny – nie jest dobrem danym systemowi gospodarczemu raz na zawsze. W świecie realnym występują ciągłe zagrożenia spowodowane zarówno siłami natury, jak i niezamierzoną oraz zamierzoną działalnością człowieka.

Każdy logistyczny system musi zatem czynić starania o zapewnienie sobie stabilnego stanu bezpieczeństwa. Każdy logistyczny system gospodarczy winien wykształcić w swej działalności możliwość szybkiego reagowania na wszelkie zmiany w otoczeniu wewnętrznym i zewnętrznym, w tym również możliwość współpracy w ramach systemu bezpieczeństwa z innymi podmiotami.

Stwierdzenie to nie jest niczym nowym, jako że już w połowie ubiegłego wieku ojciec współczesnego zarządzania P. Drucker, proponując kryteria wyboru oraz projektowania organizacji, stwierdził, że przedsiębiorstwo powinno posiadać

---

[41] Najważniejsze z nich to: *Organizacja i funkcjonowanie systemów logistycznych*, Difin, Warszawa 2011, *Logistyka w bezpieczeństwie* (wyd. 1 i 2), Difin, Warszawa 2010 i 2011; *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*, Difin, Warszawa 2015; *Logistyka w bezpieczeństwie i bezpieczeństwo w logistyce,* [w:] Logistyka, 2/2011; *Logistyka w sytuacjach kryzysowych*, [w:] Logistyka, 3/2011; *Bezpieczeństwo systemów logistycznych*, [w:] Gospodarka materiałowa i logistyka, 5/2014.

trwałość końcową do przetrwania w okresie zamieszania i umiejętność dostosowania się do nowych warunków.

Przyjęta strategia funkcjonowania logistycznego systemu gospodarczego nie powinna być nakierowana tylko na realizację procesów logistycznych i obniżanie kosztów, ale również winna uwzględniać problematykę współczesnych zagrożeń.

System bezpieczeństwa logistycznego danego podmiotu powinien być dostosowany do jego potencjalnych zagrożeń oraz pożądanego poziomu bezpieczeństwa, jaki musi być mu zapewniony. Zatem ilość oraz jakość środków, niezbędnych do zapewnienia danemu podmiotowi pożądanego poziomu bezpieczeństwa w obszarze działań logistycznych, ich organizacja oraz sposób prowadzenia działań (a ściślej, procesów) po wyzwoleniu zagrożenia (zajściu zdarzenia) zależą od jego rodzaju i skali oraz prognozy możliwości wystąpienia również zagrożeń innych rodzajów.

Bezpieczeństwo systemu logistycznego to stan, który daje poczucie pewności i gwarancję: przepływu dóbr rzeczowych i usług, a w konsekwencji zaspokojenie materialnych potrzeb uczestników łańcucha dostaw zgodnie z regułą 7W[42]; przepływu informacji dla potrzeb planowania i zarządzania procesami logistycznymi; ochrony i przetrwania w okresie sytuacji niebezpiecznych (zagrożeń); dostosowania się do nowych warunków (podatność na nieplanowe sytuacje).

Poziom bezpieczeństwa systemu logistycznego dowolnego podmiotu gospodarczego zależy od niego samego oraz od otoczenia bliższego (np. bezpośrednich dostawców i odbiorców), a także dalszego, które jest uwarunkowane odpornością na zakłócenia współpracujących uczestników sieci gospodarczych w wymiarze lokalnym i globalnym.

Bezpieczeństwo logistycznego systemu gospodarczego związane jest z: poziomem przygotowania – i odpornością – systemu do przeciwdziałania sytuacjom nadzwyczajnym (główna uwaga koncentruje się na rozpoznawaniu, monitorowaniu, analizowaniu danych i trafnym podejmowaniu decyzji w obszarze działań logistycznych); jakością stworzonego i funkcjonującego systemu bezpieczeństwa – rozumianego jako zespół sił oraz środków zapewniających akceptowalny przez system logistyczny stan bezpieczeństwa.

Określony poziom bezpieczeństwa logistycznego systemu gospodarczego można uzyskać na wiele sposobów – nie tylko poprzez zapewnienie określonej skuteczności bezpośredniego przeciwdziałania zaistniałym zdarzeniom.

Wielkościami sterowalnymi w tym przypadku są parametry charakteryzujące się czynnikami wpływającymi na poziom bezpieczeństwa systemu, czyli związane

---

[42] 7R – *right product* (właściwy produkt), *right quantity* (właściwa ilość), *right condition* (właściwy stan), *right place* (właściwe miejsce), *right time* (właściwy czas), *right customer* (właściwy klient), *right price* (właściwa cena).

z[43]: zapobieganiem możliwym zagrożeniom bezpieczeństwa; przygotowaniem systemu logistycznego na wypadek uaktywnienia tych zagrożeń; zasobami przeciwdziałającymi tym zagrożeniom; usuwaniem następstw danego zdarzenia.

2.2. Zarządzanie progresywne

W zarządzaniu kryzysowym mamy do czynienia z systemem otwartym, a wśród cech otoczenia wpływających na jego strukturę można wymienić[44]:

- złożoność otoczenia oznaczającą świadomość, z jak wielu i jak zróżnicowanych składa się ono elementów;
- niepewność otoczenia, która jest bezpośrednio związana z dynamiką oraz niestabilnością, przy czym można wymienić cztery typy źródeł niepewności charakteryzujących każdy system gospodarczy:
  - niepewność wynikająca z niewiedzy i braku umiejętności rozwiązywania problemów, a tym bardziej tych; które pojawiają się niespodziewanie,
  - niepewność w stosunkach organizacja – otoczenie, ze względu na trudną rozpoznawalność zjawisk i zdarzeń pojawiających się w zasadzie w sposób niezależny od poszkodowanych,
  - niepewność związana z brakiem zgodności między siecią zadań i siecią informacyjną, np. na skutek złych lub niepełnych danych z miejsca zdarzenia,
  - niepewność związana z wieloznacznością przepisów, w tym resortowych, rządowych, samorządowych.

Zarządzanie takim systemem wymaga informacji, która powinna charakteryzować się poprawnością, użytecznością, selektywnością, kompletnością, aktualnością, terminowością, komunikatywnością, dyspozycyjnością. Każdy menedżer, podejmując decyzję ma określone potrzeby informacyjne, które są kształtowane przez dwa podstawowe czynniki[45]: rodzaj rozwiązywanego zadania *Q*; wiedzę i doświadczenie człowieka (użytkownika *U*).

Do potrzeb informacyjnych zaliczamy między innymi opinie, prognozy, diagnozy, dane faktograficzne itp., które są niezbędne dla użytkownika w związku

---

[43] Por. E. Kołodziński, *Istota inżynierii systemów zarządzania bezpieczeństwem,* [w:] http://www.uwm.edu.pl, 10.08.2016.

[44] Por. A. Koźmiński, W. Piotrkowski, *Zarządzanie. Teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa 1996, s. 658.

[45] *Wstęp do informatyki gospodarczej*, red. A. Rokicka-Broniatowska, SGH, Warszawa 2006, s. 149.

z jego określonym celem działania, a także ze względu na przewidywania co do zaistniałych okoliczności towarzyszących temu dzianiu.

Potrzeby informacyjne mogą być zarówno indywidualne, czyli dotyczące danej jednostki, jak i grupowe. Powinny być one poddawane procedurze obiektywizacji, czyli trzeba mieć na uwadze rzeczywiste wymagania użytkowników.

Potrzeby te można podzielić na dwa podzbiory:

- *Iu* – informacji potrzebnych do rozwiązania *Q*, lecz już dostępnych użytkownikowi;
- *L* – takich informacji, które są potrzebne i nie są bezpośrednio dostępne.

Kształtowanie się potrzeb informacyjnych można zilustrować za pomocą schematu[46]:

$$< U, Q, M > \Rightarrow I \Rightarrow Iu \cup L$$

gdzie:

U – użytkownik poszukiwanej informacji,
Q – zadanie (problem) rozwiązywane przez *U*,
M – oznacza metody, które *U* zamierza zastosować do rozwiązania *Q*,
I – informacje potrzebne dla *U* do rozwiązania *Q* przy stosowaniu metody *M*,
L – informacje (zwane luką informacyjną) potrzebne do rozwiązania *Q* i których *U* nie ma.

L powstaje pomiędzy ilością informacji pożądanych a dostępnych. Luka powiększa się wraz ze wzrostem złożoności problemu (a z takimi mamy do czynienia w sytuacjach kryzysowych) i ilością informacji.

Należy również pamiętać, że elementarną ilość informacji *I* związaną ze zdarzeniem x_i ($i = <1,N>$) zachodzącym z pewnym prawdopodobieństwem $p(x_i)$ można wyrazić wzorem[47]:

$$I(x_i) = \log \frac{1}{p(x_i)} = -\log p(x_i)$$

Stąd nasuwają się wnioski:

- im mniejsze prawdopodobieństwo wystąpienia danego zdarzenia elementarnego, tym większa ilość informacji musi być z nim związana;
- jeżeli x_i jest określone, tzn. $p(x_i) = 1$, wówczas $I(x_i) = 0$;
- mając dwa zdarzenia niezależne x_i i x_j o łącznym prawdopodobieństwie $p(x_i, x_j)$, to $I(x_i, x_j) = p(x_i) + p(x_i)$.

Opisane prawidłowości zachodzą pod warunkiem, że ilość informacji związana jest z niepewnością co do wyniku danego doświadczenia, każda z wiadomości

[46] Tamże, s. 150.
[47] Por. tamże, s. 64–67.

elementarnych niesie pewną informację oraz z każdym ze zdarzeń x_i można skojarzyć odpowiadające mu prawdopodobieństwo $p(x_i) = p_i$.

Zbiór L ma określone cechy, do których zaliczamy[48]: luka jest zawsze „czyjąś" luką; jest luką ze względu na zadanie Q; zmienność w czasie; rozmytość granic; wymaga różnorodnych informacji; zawsze występuje ze względu na niewyczerpalność informacji.

Zarządzanie w sytuacjach kryzysowych wymaga nie tylko dobrej użytecznej informacji. Należy uwzględnić[49]: presję czasu; fakt, że zdarzenia rozwijają się szybciej niż reagowanie na nie; występowanie ograniczenia dostępu do informacji wraz ze wzrostem zapotrzebowania na nią ze strony organów zarządzających, jak i całego społeczeństwa; poczucie kierownictwa, że nie jest w stanie podołać zmianom, które mają miejsce (może pojawić się panika); występowanie wyraźnego konfliktu zainteresowanych stron; decydującego znaczenia nabiera dostosowanie wcześniej opracowanych scenariuszy działania do konkretnej sytuacji; zjawisko, że decyzje podejmowane są w warunkach stresu, ograniczonej informacji i podwyższonego poziomu ryzyka; występowanie ograniczenia kolegialnych reguł wypracowania decyzji.

Tak złożony system wymaga specyficznego, indywidualnego i twórczego podejścia w zarządzaniu, które może przybrać charakter progresywny, konserwatywny.

Określenie „progresja" oznacza stopniowe wzrastanie, stopniowe podwyższanie, posuwanie się naprzód; robienie postępu[50].

Progresywne działania to takie, które wyróżniają i charakteryzują się[51]:

- skłonnością do samodzielnego i spontanicznego rozwiązywania problemów, najczęściej przez zastosowanie metody prób i błędów[52],
- tendencją do wyznawania i głoszenia idei postępu oraz zdolnością wprowadzania ich w życie,
- odchodzeniem od stereotypów, schematów i analogiczności.

Progresywność stanowi przeciwieństwo nienowoczesności, zacofania, schematyzmu, konserwatyzmu, zachowawczości i tradycjonalizmu[53].

---

[48] A. Szymonik, *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu,* Difin, Warszawa 2015, s. 74.

[49] Tamże.

[50] *Słownik języka polskiego*, [w:] http://sjp.pl, 08.01.2015.

[51] A. Szymonik, *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Difin, Warszawa 2011, s. 76.

[52] Metoda prób i błędów – spontaniczny, oparty na intuicji sposób rozwiązywania zadań i problemów, polegający na wykonywaniu pozornie chaotycznych czynności tak długo, aż uzyska się pożądany rezultat (w różnych dziedzinach nauki i działalności praktycznej metoda prób i błędów jest podstawą wielu innych metod prowadzących do odkryć i rozwiązywania problemów – w matematyce nazywa się ją metodą kolejnych przybliżeń); wg *Prób i błędów metod*, [w:] http://portalwiedzy.onet.pl, 25.09.2016.

[53] Por. *Słownik synonimów i antonimów*, [w:] http://leksykony.interia.pl/, 04.08.2016.

Można by się pokusić o twierdzenie, że idealne zarządzanie progresywne to takie, które przewiduje powstanie sytuacji kryzysowej i próbuje ją wyeliminować rzeczywistymi działaniami, zanim takowa miałaby szansę zaistnieć. A głównym mottem takiego modelu jest: „Zawsze lepiej jest zapobiegać, niż usuwać skutki zaistniałego problemu, i to zarówno ze względu ekonomicznego, jak i społecznego".

Ten rodzaj zarządzania jest najbardziej pożądany w fazie przedkryzysowej. To w niej poza ciągłym monitorowaniem sytuacji główny wysiłek skupiony jest na działaniach przygotowawczych i zabezpieczających, które w konsekwencji powinny prowadzić do wyeliminowania (neutralizacji), a przynajmniej do zmniejszenia, złagodzenia przebiegu i zminimalizowania skutków kryzysu. Czas trwania fazy przedkryzysowej zależy od tego, czy kryzys można było przewidzieć, czy nie (sytuacje kryzysowe przewidywalne i nieprzewidywalne)[54]. I właśnie na tym etapie powinniśmy poszukiwać nowych rozwiązań w technikach, technologiach i sposobach zarządzania w sytuacjach kryzysowych, co najbardziej odpowiada działaniu progresywnemu.

Menedżerowi progresywnemu podejmującemu decyzję towarzyszy ryzyko. To on musi zdobyć się na odwagę podejmowania niepewnych działań, które mogą być niezgodne z opiniami innych ludzi czy ogólnie przyjętymi zasadami.

Skutkiem tego może być odniesiony sukces lub totalna porażka, wiążąca się np. ze zdrowiem i życiem człowieka. Niejednokrotnie decyzje podejmowane przez menedżera progresywnego, zarządzającego w sytuacjach kryzysowych, można przyrównać do decyzji podejmowanych przez kardiochirurga[55].

Menedżer, wybierając w sposób nielosowy jeden z możliwych wariantów, podejmuje ryzykowne decyzje, często pod presją czasu, w celu „uleczenia" systemu, firmy czy likwidacji olbrzymiego zagrożenia wywołanego np. skażeniem emisji substancji promieniotwórczych do atmosfery.

Podejmowaniu decyzji muszą towarzyszyć: kreatywność, pewność w postępowaniu i nieugięte dążenie do zamierzonego celu. Jest to duża odpowiedzialność nie tylko za siebie, ale również za całość np. zespołu uruchamiającego system chłodzenia reaktora w warunkach wysokiego promieniowania, grożącego utratą zdrowia czy nawet życia.

Często decyzja jest przedmiotem krytyki, przyczyną obaw, utraty pozycji, autorytetu, pracy – może towarzyszyć jej niezadowolenie wśród np. społeczeństwa trącącego zaufanie nie tylko do władz lokalnych, lecz nawet do rządu.

---

[54] A. Skarżyński, *Próba ogólnej systematyki sytuacji kryzysowych oraz wybranych towarzyszących im działań techniczno-organizacyjnych,* materiały z XI Międzynarodowej Konferencji Naukowo-Technicznej Inżynierii Wojskowej, t. 1, *Zarządzanie i organizacja działań w sytuacjach kryzysowych. Ratownictwo i ochrona ludności*, Warszawa 2000, s. 45-46.

[55] A. Szymonik, *Organizacja i funkcjonowanie*… dz. cyt., s. 77.

Ważne jest, by nie postępować pochopnie, decyzje muszą być przemyślane, uwzględniające skutki i rezultaty przyszłych działań. Tylko tak jak w pracy kardiochirurga niejednokrotnie pod presją czasu menedżer, wykorzystując dostępne dane, prognozy, symulacje, musi się opierać na osobistej wiedzy, doświadczeniu, a także intuicji, by wybrać wariant, do tej pory niesprawdzonego w praktyce, określonego działania i monitorować jego skutki.

Jak sama nazwa wskazuje, sytuacja kryzysowa jest to taki stan, który wymaga natychmiastowych działań, jeżeli nie zrobimy czegoś w danym momencie, za chwilę może być już za późno, a – jak wiadomo – poprawianie błędów wiąże się z dużymi kosztami, nie tylko finansowymi, ale również społecznymi, które niejednokrotnie związane są z tym, co najcenniejsze, a więc zdrowiem i życiem ludzkim.

Sytuacja kryzysowa wymaga od nas zdecydowania i determinacji. Nie ma w niej miejsca dla tzw. populistów, którzy obiecują rezultaty zgodne z oczekiwaniami większości społeczeństwa w celu uzyskania jego poparcia i zdobycia wpływów lub władzy, a nie mają żadnego zaplecza, programu poprawy.

Z drugiej strony menedżerowi nie można dać wolnej ręki, jego działania muszą podlegać kontroli, by nie doszło do nadużycia i nieodwracalnych, negatywnych skutków jego postępowania. W naszych rozważaniach kardiochirurg może zaszkodzić jednemu pacjentowi w przeciwieństwie do osoby zarządzającej reagowaniem na sytuacje kryzysowe, od której zależy życie i zdrowie czasami wielu osób, jak np. w sytuacji awarii technicznych czy klęsk żywiołowych.

Zarządzanie progresywne powinno dotyczyć przede wszystkim przewidywania powstawania sytuacji kryzysowych i stosowania narzędzi oraz instrumentów, które by im zapobiegały, a przynajmniej ograniczały skutki.

Nowatorskie rozwiązania winny być rezultatem badań i priorytetowych technologii (tabela 2.1.), a później tematem praktycznych szkoleń i treningów.

Tabela 2.1. Obszary badawcze i związane z nimi priorytetowe technologie

Obszar badawczy	Priorytetowe technologie
Technologie informacyjne	Techniki łączenia danych, zbierania i klasyfikacji danych, technologie przetwarzania obrazu, technologie zarządzania informacjami i danymi
Sztuczna inteligencja i wspieranie procesu decyzyjnego	Przeszukiwanie informacji i danych, zarządzanie wiedzą, modelowanie i symulacja, optymalizacja i technologie wspomagania decyzji
Urządzenia komunikacyjne	Komunikacja rekonfigurowana, bezpieczna komunikacja mobilna, zarządzanie sieciami komunikacyjnymi, szerokopasmowe łącza przesyłu danych

Ochrona informacji	Technologie szyfrowania, przeszukiwanie danych, kontrola dostępu
Technologie komputerowe	Techniki bezpiecznego przetwarzania, przetwarzanie wysokowydajne
Systemy informatyczne	Infrastruktura wspierająca zarządzanie i rozpowszechnianie informacji, systemy optymalizacji i planowania procesu decyzyjnego
Scenariusze i symulacje decyzji	Tworzenie zaawansowanych modeli i symulacja zachowań ludzi, symulacje dla procesu decyzyjnego, przewidywanie podatności struktur, techniki zarządzania ewakuacją i skutkami, symulacja emisji
Zintegrowane platformy	Platformy bezzałogowe (lądowe, morskie i lotnicze, satelity obserwacyjne i nawigacyjne)
Sprzęt oparty na czujnikach	Kamery, czujniki, w tym technologie wykrywania szczególnych zagrożeń chemicznych i biologicznych, urządzenia pasywne z czujnikami na podczerwień (IR)
Czujniki	Czujniki wielowidmowe, przetwarzanie sygnałów wielowidmowych
Nawigacja, prowadzenie, kontrola i śledzenie	Oznaczenia RFID (elektroniczne oznakowanie produktu), śledzenie, technologie GPS, radionawigacja, śledzenie oparte na kodach kreskowych
Elektroniczne uwierzytelnianie	Systemy elektronicznego oznaczenia („etykiety"), „inteligentne karty" (*smart cards*)
Symulatory, urządzenia szkolące i sztuczne środowiska	Rzeczywistość wirtualna, systemy szkolenia personelu
Techniki kryminalistyczne – biometria	Rozpoznawanie odcisków palców, rozpoznawanie twarzy, rozpoznawanie, tęczówki, siatkówki, głosu, charakteru pisma, podpisu
Biotechnologia	Szybka analiza czynników biologicznych i podatności ludzi na choroby i substancje toksyczne, techniki odkażania, techniki badania i oczyszczania wody, techniki badania i kontroli żywności
Materiały biologiczne, chemiczne i medyczne	Chemiczne i biologiczne techniki wykrywania
Przeżywalność i technologie zwiększające odporność	„Inteligentne" ubrania i urządzenia, materiały przeciwwybuchowe, szczególna architektura krytycznych budowli uwzględniająca skutki wybuchu i wstrząsu
Lekkie i odporne materiały, osłony	Lekkie materiały ochronne dla ludzi, „inteligentne" tkaniny, lekkie materiały ochronne miejsc, technologia ochronnych i odpornych na wybuchy materiałów

Przechowywanie i dystrybucja, wytwarzanie energii	Generatory elektryczne, rozprowadzanie energii
Systemy kosmiczne	Multispektralna obserwacja Ziemi
Nauki socjologiczne	Analiza i opracowanie modeli zachowań ludzi, zachowań populacji, czynników ludzkich w procesach decyzyjnych, zespołach

Źródło: por. Z. Mierczyk, *Nowoczesne technologie w systemach monitorowania bezpieczeństwa*, [w:] Metodologia badań bezpieczeństwa narodowego „Bezpieczeństwo" 2010, t. II, AON, Warszawa 2011, s. 32, 33.

Zarządzanie progresywne powinno wykorzystywać: szeroki dostęp do wewnętrznych i zewnętrznych narzędzi bezpieczeństwa, obejmujących wywiad, policję, sądownictwo, środki ekonomiczne, finansowe, dyplomatyczne; wyniki badań oraz nowoczesne technologie.

Sprawne, nowoczesne i skuteczne zarządzanie progresywne wymaga systemów informacyjnych wspomagających monitorowanie, identyfikację i przeciwdziałanie zagrożeniom bezpieczeństwa obywateli, w tym procesów informacyjno-decyzyjnych oraz zarządzania kryzysowego, a także skutecznego kierowania działaniami i reagowania kryzysowego.

2.3. Zarządzanie konserwatywne

Słowo „konserwatyzm" pochodzi od łacińskiego *conservare,* co znaczy „zachowywać, ocalić"[56]. W *Słowniku języka polskiego*, konserwatyzm określony jest jako: „silne przywiązanie do tradycji i niechęć do zmian"[57]. Antonimy tego słowa[58]: „liberalizm", „postępowość", ale nie „progresja", czyli można założyć, że te dwa kierunki się nawzajem uzupełniają.

A zatem konserwatywny sposób zarządzania wyróżnia się akceptacją ogólnego stanu, systemu wartości, powolnym wprowadzaniem nowych zasad, a także przywiązaniem do istniejącego, sprawdzonego systemu. Realizowany proces planowania, organizowania, przewodzenia, kontrolowania organów kierujących i wykonawczych odbywa się w sposób już opracowany, sprawdzony i zatwierdzony, zarówno przez naczelne ogniwa, jak i instytucje opiniotwórcze.

[56] *Konserwatyzm,* [w:] http://www.wosna5.pl/, 03.04.2015.
[57] *Słownik języka polskiego*, [w:] http://sjp.pwn.pl/slownik, 03.04.2015.
[58] *Słownik synonimów i antonimów*, [w:] http://megaslownik.pl/, 03.04.2015.

Ten typ zarządzania najbardziej przydatny jest w fazie:

- kryzysowej, w której zagrożenie może mieć charakter jednorazowy lub charakter ciągły, o wydłużonym czasie działania (czas trwania sytuacji kryzysowej będzie zależał od charakteru kryzysu i od podjętych działań);
- pokryzysowej, która wymaga określonych działań, sił i środków do usunięcia lub przezwyciężenia skutków sytuacji kryzysowej; można wymienić trzy przykładowe grupy przedsięwzięć[59]:
  - działania w zakresie organizacji, planowania, logistyki, doboru kadr, zabezpieczenia miejsc, łączności itp.,
  - pozyskanie środków finansowych (źródła finansowania), np. budżet, pomoc międzynarodowa, sponsorzy, środki własne,
  - pozyskanie sił i środków technicznych, np. wykwalifikowane zespoły, materiały i sprzęt techniczny, sprzęt i środki medyczne, możliwość wykorzystania infrastruktury (drogi, rampy, lotniska, mosty, szpitale).

Wywód na temat przydatności zarządzania konserwatywnego w fazie kryzysowej oraz pokryzysowej oparty jest na sprawdzonej życiowej maksymie, że eksperymentowanie, a także wprowadzenie nowych metod, a tym bardziej innowacyjnych, na żywym organizmie jest czasami bardzo ryzykowne i kosztowne.

Dokonując analizy systemowej zarządzania konserwatywnego i progresywnego, można przedstawić kilka wniosków[60]:

Pierwszy wniosek wiąże się ze stwierdzeniem, że idealne działanie w sytuacji kryzysowej powinno być połączeniem zarządzania konserwatywnego i progresywnego. Znalezienie kompromisu pomiędzy tymi odmiennymi stylami zarządzania jest idealnym sposobem podejmowania decyzji w sytuacji kryzysowej. Każda decyzja powinna zostać przemyślana i poddana obiektywnej opinii osób, w których otoczeniu dana kwestia ma być wdrożona. Decyzje podjęte pod presją czasu wielokrotnie okazują się porażką.

Czasu nie da się cofnąć, a skutki mogą się okazać nieprzewidywalne. Zarówno posiadana wiedza, jak i doświadczenie pomagają nam w „głębszym myśleniu", tzn. pozwalają nam bardziej trafnie oceniać sytuację oraz wybrać wariant działania najbardziej przydatny, a także zadawalający.

Drugie spostrzeżenie wiąże się z tym, że konserwatywny sposób kierowania wyróżnia się akceptacją ogólnego stanu, systemu wartości, powolnym wprowadzaniem nowych zasad, a także przywiązaniem do istniejącego systemu; cały czas opiera się na tym, co jest bardzo zachowawcze i sprawdzone. Zachowanie progresywne jest bardzo odważne, nowatorskie, nowoczesne.

---

[59] Zob. A. Szymonik, *Organizacja i funkcjonowanie*…, dz. cyt., s. 81.

[60] Zob. tamże.

Trzeci wniosek związany jest z tym, że zarządzanie kryzysowe to działalność organów będąca elementem kierowania bezpieczeństwem, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury. To nic innego jak odpowiedź na stan kryzysu występującego w przedsiębiorstwie czy też innej organizacji zarówno na skutek działania sił przyrody, jak i działania człowieka.

Chcąc tę sytuację rozwiązać, należy sobie zawsze postawić pytanie: jak logicznie w sposób uporządkowany zmierzyć się z problemem? Zidentyfikowanie sytuacji kryzysowej ze względu na jej złożoność nie jest możliwa między innymi z powodu niepełnych informacji, których pozyskanie jest utrudnione. W związku z tym całkowita ocena sytuacji musi uwzględniać interakcję między różnymi systemami (m.in. technologicznymi i ludzkimi).

W rozwiązaniu sytuacji kryzysowej najczęściej mamy do czynienia z konserwatywnymi decyzjami, czyli robieniem tego, co już było wielokrotnie realizowane. Uzyskujemy wtedy efekt uczenia się, czyli im częściej coś robimy, to wykonujemy to szybciej i lepiej. Zarządzanie konserwatywne to jakby mechanizm zapewniający pewne poczucie komfortu, ponieważ poprzez jego racjonalną realizację często (choć nie zawsze) udowadniamy sobie prawidłowość postępowania (tzw. efekt przewidywalności).

Czwarty wniosek nawiązuje to faktu, że w sytuacjach kryzysowych konserwatyści będą stosować utarte schematy oparte na „tradycji", na zasadach. Co jednak, jeśli to nie przyniesie oczekiwanych rezultatów? Sięgną do nowych rozwiązań i tak powstanie grupa ludzi o progresywnym nastawieniu.

Jedni i drudzy mają swoje dobre i złe „strony", a wtedy najlepiej pójść na kompromis – wybrać najlepsze cechy. Częściej wybieramy te sprawdzone, konserwatywne sposoby działania w sytuacjach kryzysowych. Ale bez progresu nie ma rozwoju (albo jest powolny) i mamy żmudne realizowanie tego, „co powinno się robić natychmiast". Nie istnieją stricte oddzielne zarządzania – progresywne i konserwatywne.

Wszędzie, chcemy czy nie chcemy, aby sprostać rzeczywistości, muszą być zastosowane elementy każdego z postępowań.

Piąty wniosek wiąże się z tym, że zarządzając sytuacją kryzysową, należy wykorzystać zespół interdyscyplinarnych, profesjonalnych, celowych i skoordynowanych oddziaływań, dzięki czemu łatwiej uzyskać cel. Interdyscyplinarność oddziaływań wynika z charakteru doświadczenia kryzysowego, a szczególnie ze zjawiska jakby „rozlewania się" kryzysu na otoczenie – bliższe i dalsze. To właśnie powoduje, że w zarządzaniu kryzysowym oprócz rutyny, doświadczenia,

wykorzystania sprawdzonych metod (postępowanie konserwatywne) istotne jest to, co przynoszą nauka, badania i jej rozwiania (działanie progresywne).

Spostrzeżenie szóste, pokazuje, że w zarządzaniu konserwatywnym stosowane procedury, metody działania na ogół są sprawdzone i przetestowane. Natomiast wszelkiego rodzaju innowacje (zarządzanie progresywne) w rozwiązywaniu trudności są jak najbardziej wskazane, pozwalają spojrzeć na problem z wielu perspektyw i znajdować coraz to inne rozwiązania, ale wymaga to na pewno większych kosztów oraz niesie ryzyko wystąpienia innych nieprzewidzianych konsekwencji, które mogą być wynikiem podjętej decyzji.

Dobrym podejściem do zarządzania kryzysowego jest modyfikacja zasad klasycznych poprzez wprowadzenie pewnych zmian uwzględniających zaistniałą sytuację w sposób dynamiczny, co pozwala na dostosowanie się i wprowadzenie korekt do podejmowanych decyzji, przyczyniając się do uproszczania procesów oraz eliminowania niektórych jego etapów. Jednak nie zawsze podejmowane decyzje są słuszne i dlatego należy dynamicznie dostosowywać zmiany w decyzjach w zależności od sytuacji krytycznych; trzeba być przygotowanym na niepowodzenia i być świadomym odpowiedzialności za podejmowane decyzje.

Współczesne zarządzanie w systemach gospodarczych opiera się na informacji, ale nie pod względem jej ilości, tylko jakości. W zarządzaniu kryzysowym należy porzucić paradygmat wielkości, a wykorzystywać to, co pozwoli na szybką reakcję, i uprzedzić wszelkie niekorzystne działania wynikające z zagrożeń. Można to określić, jako „przeciwzaskoczenie" wszystkiemu, co jest niekorzystne dla człowieka i środowiska.

2.4. Zarządzanie ryzykiem w systemach logistycznych

Zrozumienie oraz wyjaśnienie roli i miejsca ryzyka w systemach logistycznych wymaga przytoczenia i przeanalizowania trzech definicji: ryzyka, systemu logistycznego, ryzyka w systemach logistycznych.

Pochodzenie wyrazu „ryzyko" nie jest jednoznacznie zdefiniowane. W języku arabskim *risq* oznacza los, dopust boży, w hiszpańskim *ar-risco* oznacza odwagę i niebezpieczeństwo, w angielskim oznacza sytuację powodującą niebezpieczeństwo lub możliwość, że zdarzy się coś złego.

Współcześnie ryzyko jest definiowane jako deficyt informacji co do realizacji jednego wyznaczonego celu lub wielu celów[61]; potencjalna niemożliwość osiągnięcia

[61] T. Kaczmarek, *Zarządzanie zdywersyfikowanym ryzykiem w świetle badań interdyscyplinarnych*, WSZiM, Warszawa 2003, s. 7.

celów przedsięwzięcia lub umowy zgodnie z określonymi wymogami dotyczącymi parametrów (charakterystyk) wyrobu, harmonogramu realizacji dostaw lub kosztów[62]; miara niepewności, ilościowa ocena prawdopodobieństwa wystąpienia zdarzeń niekorzystnych (zakłóceń), czyli tego, co postrzegamy jako zagrożenie[63]; zbiór dwóch głównych elementów: prawdopodobieństwo nieosiągnięcia określonego rezultatu oraz konsekwencji i skutku nieosiągnięcia określonego rezultatu[64]; zjawiska towarzyszące decyzjom niedeterministycznym.

W ślad za przywołanymi definicjami w odniesieniu do systemów logistycznych celowe jest określenie ryzyka jako warunków, w których logistyk zna przypuszczalną wielkość prawdopodobieństwa osiągnięcia założonych rezultatów przez celowo zorganizowany i połączony zespół takich elementów (podsystemów) jak np.: zaopatrzenie, produkcja, dystrybucja wraz z relacjami między nimi oraz ich własnościami, warunkującymi przepływ strumieni – rzeczowego i informacji. Zaprezentowana definicja pozwala na sformułowanie następujących wniosków: ryzyko ściśle jest związane z zapewnieniem użyteczności miejsca i czasu strumienia rzeczowego oraz towarzyszących informacji w systemie logistycznym; potencjalna niemożliwość osiągnięcia celu przez system logistyczny jest uzależniona od zdarzeń niekorzystnych występujących w jego podsystemach (np. logistyki zaopatrzenia, produkcji i dystrybucji) oraz w otoczeniu dalszym (np. na rynku dostawców i odbiorców).

Funkcjonowanie systemu logistycznego jest uzależnione między innymi od sprawności i skuteczności zarządzania ryzykiem, które można zdefiniować jako: panowanie nad niepewnością[65]; działanie lub praktyka postępowania z ryzykiem[66]; system metod i działań zmierzających do obniżenia stopnia oddziaływania ryzyka na funkcjonowanie podmiotu gospodarczego i do podejmowania w tym celu optymalnych decyzji[67]; skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka[68].

---

[62] AQAP 2070, *Proces NATO dotyczący wzajemnej realizacji rządowego zapewnienia jakości GQA*, wyd. 1, styczeń 2004, C-4.

[63] J. Komorowski, *Cele przedsiębiorstwa a rozwój gospodarczy. Ujęcie behawioralne*, SGH, Warszawa 2012, s. 191.

[64] AQAP 2070, *Proces NATO…*, dz. cyt., C-5.

[65] *Zarządzanie ryzykiem*, [w:] https://mfiles.pl, 25.01.2016.

[66] AQAP 2070, *Proces NATO…*, dz. cyt., C-5.

[67] Zob. A. Szymonik, M. Bielecki, *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*, Difin, Warszawa 2015, s. 82.

[68] Polska Norma PN-ISO 31000 2012P *Zarządzanie ryzykiem. Zasady i wytyczne*, Polski Komitet Normalizacyjny, marzec 2012.

Zarządzanie ryzyka w systemach logistycznych obejmuje[69]:

- identyfikację, która:
  - jest procesem ciągłym,
  - ustala przyczyny ryzyka, które mogą być: techniczne, np. nowe wymagania branżowe – traceability[70]; organizacyjne, np. nietrafione usługi outsourcingowe[71], czy niedocenienie działań konkurencji; związane z zarządzaniem, np. uchybienia w obszarze planowania, zabezpieczenia zasobów, kontrolowania, koordynacji; zewnętrzne, np. klęski żywiołowe czy zmiany regulacyjne,
  - jest prowadzona na podstawie wspólnego modelu, jednolitej metodologii,
  - stwierdza możliwe następstwa,
  - wskazuje podmioty, procesy mogące być dotknięte ryzykiem;
- analizę ryzyka – sprecyzowanie prawdopodobieństwa nieosiągnięcia określonego rezultatu oraz konsekwencji i skutku jego nieosiągnięcia dla systemu logistycznego (w praktyce ryzyko stanowi iloczyn prawdopodobieństwa wystąpienia zagrożenia i wielkości skutków tych zagrożeń);
- planowanie – proces opracowania i udokumentowania zorganizowanej, wszechstronnej i interaktywnej strategii zarządzania ryzykiem w systemie logistycznym, która uwzględnia wydzielenie odpowiednich zasobów do realizacji tego zadania, odpowiedzialnych oraz czasu realizacji;
- redukowanie – proces wdrażania strategii i metod w celu utrzymania ryzyka na akceptowanym poziomie w odniesieniu do wymagań i celów realizowanych przez system logistyczny;
- monitorowanie – proces, w którym systematycznie obserwuje się i ocenia realizację działań redukowania ryzyka w odniesieniu do określonych wymagań dla systemu logistycznego (proces ten dostarcza koniecznych informacji do sprawnego i skutecznego podejmowania decyzji uprzedzających pojawienie się ryzyka);
- dokumentowanie – proces, w którym zapisuje się, utrzymuje zapisy i przedstawia wyniki różnych działań zarządzania ryzykiem w systemie logistycznym.

Skuteczne zarządzanie ryzykiem nie jest możliwe bez jego oceny, którą można przeprowadzić **metodą jakościową lub ilościową.** To ona pozwoli oszacować

---

[69] T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2006, s. 98.

[70] Traceability – oznacza możliwość śledzenia i podążania za pochodzeniem żywności, pasz, zwierzęcia hodowlanego, substancji przeznaczonej do dodania lub która może być dodana do żywności i pasz na wszystkich etapach produkcji, przetwarzania i dystrybucji.

[71] Zob. J. Foltys, *Outsourcing jako metoda eliminacji barier kulturowych w funkcjonowaniu organizacji*, [w:] Zastosowanie psychologii w zarządzaniu, Wyd. UŚ, Katowice 2010, s. 124, 125.

wielkość prawdopodobieństwa i skutków zaistnienia zidentyfikowanych uprzednio rodzajów ryzyka.

Materiałami wyjściowymi do jakościowej analizy rodzajów ryzyka mogą być np.[72]:

- plan zarządzania ryzykiem;
- lista zidentyfikowanych rodzajów ryzyka wraz z podziałem ich na kategorie uwzględniając procesy logistyczne (w tym etap projektowania, zaopatrywania i obsługi posprzedażnej), systemy logistyczne w wymiarze mikro, makro;
- raport o stanie zaawansowania realizacji wytyczonych celów logistycznych (np. 4W – właściwe miejsce, czas, ilość i jakość, czy 7W – właściwe miejsce, czas, ilość, jakość, cena, produkt, informacja);
- charakterystyka typu stosowanych rozwiązań logistycznych w realizacji działań związanych z typem organizacji produkcji (np. jednostkowa, małoseryjna, seryjna, masowa), organizacją przepływów produkcyjnych (np. rytmiczna i nierytmiczna, elastyczne systemy wytwórcze), lokalizacją i rozkładem poszczególnych urządzeń uczestniczących w procesie wytwarzania (np. przedmiotowe, technologiczne, mieszane, ręczne, maszynowe, zmechanizowane, zautomatyzowane), cechą wyrobu (konstrukcja, struktura, złożoność, stopień przetwarzania, technologia wytwarzania), zasadami zapatrzenia materiałowego (np. wspólne zarządzanie zapasami, zarządzanie zapasami przez dostawcę, wspólne planowanie, prognozowanie i odnawianie zapasów);
- charakterystyka dokładności danych, na których podstawie dokonano identyfikacji i opisu ryzyka (dane te powinny być ocenione pod kątem ich wiarygodności oraz dostępności);
- zestaw przyjętych w firmie skal prawdopodobieństwa i mierników skutków występowania zagrożeń;
- lista założeń, które zostały przyjęte w procesie identyfikacji i oceny źródeł ryzyka.

W każdym procesie zarządczym do zrealizowania wytyczonego celu niezbędny jest prawidłowy dobór narzędzi. Podstawowymi narzędziami i technikami używanymi do jakościowej analizy ryzyka mogą być[73]: lista prawdopodobieństw i skutków ryzyka (dla prawdopodobieństwa korzysta się tu ze skal opisowych, np. bardzo wysokie, umiarkowane, niskie i bardzo niskie, lub liczbowych, a w przypadku

[72] J. Atłachowicz, *Ilościowa i jakościowa ocena ryzyka*, [w:] http://wartowiedziec.org, 25.06.2016.

[73] M. Wirkus, H. Roszkowski, E. Dostatni, W. Gierulski, *Zarządzanie projektem*, PWE, Warszawa 2014, s. 162.

skutków ryzyka – np. bardzo dotkliwe, dotkliwe, umiarkowane, łagodne, bardzo łagodne lub według skali liczbowej); macierz ocen prawdopodobieństwa i skutków wystąpienia ryzyka, która pozwala uwzględnić łącznie wymienione wielkości i je ocenić (tabela 2.2.).

Tabela 2.2. Macierz prawdopodobieństwa i skutków wystąpienia zdarzenia

Prawdopodobieństwo						
	0,9	0,05	0,09	0,18	0,36	0,72
	0,7	0,04	0,07	0,14	0,28	0,56
	0,5	0,03	0,05	0,1	0,2	0,4
	0,3	0,02	0,03	0,06	0,12	0,24
	0,1	0,01	0,01	0,02	0,04	0,08
	0	0,05	0,1	0,2	0,4	0,8
			Skutki			

Źródło: M. Wirkus, H. Roszkowski, E. Dostatni, W. Gierulski, *Zarządzanie projektem*, PWE, Warszawa 2014, s. 162.

W jakościowej ocenie analizy ryzyka stosuje się skale liniowe i logarytmiczne. W przypadku prawdopodobieństwa skala rozpoczyna się od 0 – zdarzenie niemożliwe i kończy 1 – zdarzenie pewne (deterministyczne). Całą macierz podzielono na trzy obszary oznaczające ryzyko łagodne (obszar najjaśniejszy), umiarkowane (obszar środkowy), duże (obszar najciemniejszy).

Ilościowa analiza ryzyka często jest poprzedzana badaniami jakościowymi.

Materiałami wyjściowymi do ilościowej analizy ryzyka są: plan zarządzania ryzykiem; lista zidentyfikowanych rodzajów ryzyka; lista hierarchii rodzajów ryzyka; lista rodzajów ryzyka do dalszej analizy; dane historyczne; opinie ekspertów oraz rezultaty innych procesów planowania w danej realizacji.

Narzędzia wykorzystywane do analizy ilościowej różnią się między sobą ze względu na stopień skomplikowania. Do najczęściej używanych należą: ankiety (przeprowadza się je wśród logistyków decydentów i ekspertów w celu wyznaczenia wielkości prawdopodobieństwa i skutków wystąpienia ryzyka); analiza wrażliwości (pozwala na wyznaczenie, które ryzyka mają potencjalnie największy wpływ na przebieg procesu logistycznego lub funkcjonowania systemu logistycznego); analiza drzew decyzyjnych (ustala diagram następstw wraz z określonym ich prawdopodobieństwem i kosztami, zawiera każdą z możliwych logicznych ścieżek zdarzeń mogących pojawić się w trakcie realizacji procesu logistycznego lub po osiągnięciu celu systemu logistycznego funkcjonującego w skali mikro czy makro).

W praktyce do ilościowej analizy ryzyka wykorzystujemy tzw. metodę szacunkową, zwaną również metodą delficką – grupy eksperckiej. Jest to metoda subiektywna, gdyż oparta na własnym osądzie powołanych do badania ekspertów. Wymaga ona dogłębnej znajomości badanych obszarów jednostki. Każdy z członków grupy przypisuje wytypowanym wcześniej obszarom odpowiedni poziom ryzyka. W tej metodzie poziom ryzyka przypisywanego poszczególnym obszarom i zadaniom ma charakter subiektywny. Jest bowiem określany przez oceniającego na podstawie jego osądu. Analiza ryzyka metodą szacunkową realizowana jest w następujących etapach[74]: utworzenie grupy eksperckiej; każdy członek grupy niezależnie, a więc bez porozumienia z innymi, tworzy własną listę rankingową w kolejności wynikającej z oceny nasilenia ryzyka, liczba punktów jest uzależniona od liczby wyodrębnionych zadań; zadanie, które powinno być realizowane, jako pierwsze, otrzymuje najwyższą liczbę punktów, każde kolejne zadanie otrzymuje o 1 punkt mniej – ostatnie zadanie na liście otrzymuje 1 punkt; punkty przypisane poszczególnym zadaniom przez wszystkich ekspertów powołanej grupy są sumowane; hierarchizacja zadań następuje w kolejności malejącej liczby punktów, począwszy od zadania, które otrzymało największą ilość punktów; dla wyrażenia otrzymanego wyniku w procentach dzieli się sumę punktów poszczególnych zadań przez łączną liczbę punktów, które otrzymało zadanie pierwsze na liście, a następnie mnoży przez 100%.

Efektem przeprowadzenia analizy ilościowej ryzyka dla realizacji celów systemu logistycznego, np. centrum dystrybucyjnego czy firmy transportowej, może być analiza probabilistyczna (zawiera prognozy dotyczące kosztów logistycznych i czasów realizacji zadań) wielkości prawdopodobieństwa osiągnięcia celów kosztów logistycznych i czasowych lub określenie trendów charakteryzujących wyniki ilościowej analizy ryzyka (takie informacje można uzyskać na podstawie kilkukrotnego przeprowadzenia analizy ilościowej).

Rezultatem planowanych reakcji na ryzyko jest proces opracowywania wariantów postępowania i czynności zmniejszających zagrożenia, a zwiększających potencjalne korzyści dla sformułowanych procesów i systemów logistycznych.

Plan reakcji na ryzyko to kluczowy etap procesu zarządzania ryzykiem, gdyż opracowuje się w nim metody reagowania na zdarzenia korzystne i niekorzystne. Skuteczność planowania reakcji na ryzyka zadań zagrożonych ma bezpośredni wpływ na wzrost lub spadek ryzyka realizacji procesu czy systemu logistycznego.

Planowane reakcje muszą być proporcjonalne do skutków wystąpienia niekorzystnych zjawisk, likwidować (lub niwelować) wpływy danego zagrożenia w sposób kosztowo efektywny oraz być realizowane terminowo.

---

[74] E. Kulińska, *Metody analizy ryzyka w procesach logistycznych*, [w:] Logistyka, 2/2011, s. 398.

W procesie planowania reakcji na ryzyka powszechnie stosuje się kilka strategii. Do każdego z rodzajów ryzyka należy tak dobrać plan postępowania, by podjęte działania były jak najbardziej skuteczne. Do najpopularniejszych strategii zalicza się[75]:

- Unikanie ryzyka – polega na takiej modyfikacji planów realizacji procesu logistycznego czy modyfikacji systemu logistycznego, by zlikwidować dane ryzyko (niestety, nie można w praktyce wyeliminować wszystkich zdarzeń, z którymi wiążą się niebezpieczeństwa) albo korzystnie zmienić uwarunkowania z nim związane.
- Transfer ryzyka – jest to działanie polegające na przeniesieniu skutków wystąpienia ryzyka na inny podmiot. Działanie to jest bardzo skuteczne w obszarze finansów. Wiąże się ono zazwyczaj z koniecznością wypłacenia premii podmiotowi/osobie przyjmującej ryzyko (np. ubezpieczenie na wypadek zaginięcia ładunku, pożaru czy zmycia ładunku z pokładu).
- Łagodzenie ryzyka – metoda ta jest najpowszechniejszą ze wszystkich strategii reagowania na ryzyko. Proces ten polega na podejmowaniu określonych działań prowadzących do zmniejszenia prawdopodobieństwa lub skutków ryzyka.
- Akceptowanie ryzyka – przyjmuje się je i przygotowuje działania pozwalające na zminimalizowanie wszelkich konsekwencji wynikających z ewentualnego wystąpienia niekorzystnego zjawiska. Jest to świadoma decyzja osób zarządzających ryzykiem, by nie wprowadzać żadnych zmian w planie projektu związanych z wystąpieniem danego niekorzystnego zjawiska. Istnieją dwa podstawowe typy akceptacji ryzyka: aktywna i pasywna.

Pasywna akceptacja polega na przyjęciu ryzyka bez podejmowania jakichkolwiek działań w celu rozwiązania problemów, jakie się z nim wiążą.

Aktywna akceptacja polega na pogodzeniu się z ryzykiem, ale wymaga stworzenia specjalnego planu działania w razie wystąpienia niekorzystnego zdarzenia, a w niektórych przypadkach tzw. planu odwrotu.

Rezultatem właściwego ocenienia i zdefiniowania ryzyka jest plan awaryjny.

Wcześniejsze opracowanie planu awaryjnego może w sposób istotny obniżyć koszty działań podejmowanych w reakcji na wystąpienie danego niekorzystnego zjawiska.

Rezultatami procesu planowania reakcji na ryzyka są[76]:

- plan reakcji na ryzyka,
- ewidencja ryzyk rezydualnych (lista ryzyk, które jeszcze pozostają w systemie logistycznym po wdrożeniu strategii unikania, przenoszenia i łagodzenia ryzyka),

---

[75] Por. J. Atłachowicz, *Ilościowa i jakościowa ocena ryzyka*, [w:] http://wartowiedziec.org, 25.06.2015 i M. Wirkus, H. Roszkowski, E. Dostatni, W. Gierulski, *Zarządzanie* …, dz. cyt., s. 164, 165.

[76] Tamże, s. 164, 165.

- ewidencja ryzyk wtórnych – są to ryzyka, które powstają w wyniku: wdrożenia strategii reagowania na ryzyko oraz są konsekwencją postanowień kontraktowych (umów wraz zakresami odpowiedzialności, jakie przejmują na siebie inne podmioty współuczestniczące w realizacji procesów logistycznych),
- oszacowanie wielkości niezbędnych kwot rezerw na realizację zadań logistycznych (są to tzw. bufory finansowo-zasobowe zarezerwowane przez menedżerów na wypadek wystąpienia sytuacji niekorzystnych, np. w przypadku rosnących kosztów paliw).

Zarządzanie ryzykiem nie jest procesem jednoznacznym, łatwym. W celu ułatwienia wdrażania i utrzymania procesu zarządzania ryzykiem instytucje międzynarodowe opracowały wiele norm, które precyzują jego strukturę, sposób oceny oraz monitorowania. Do standardów tych zaliczmy[77]: ISO 31000:2009 – dostarcza uniwersalny model dla specjalistów oraz firm wdrażających procesy zarządzania ryzykiem i ma na celu zastąpienie obecnych standardów, metodologii i modeli, które różnią się między sobą w zależności od branży, tematu i regionu; COSO II: 2004 (zarządzanie ryzykiem korporacyjnym) – zintegrowana struktura ramowa, określa podstawowe elementy zarządzania ryzykiem w przedsiębiorstwie, omawia najważniejsze zasady ERM[78] i koncepcje, sugeruje wspólny język i zapewnia wyraźny kierunek i wytyczne dla zarządzania ryzykiem w firmie; *Pomarańczowa Księga Zarządzania Ryzykiem – zasady i koncepcje 2004 r.*, określa sposoby zarządzania ryzykiem, stanowi „zespół procesów wykorzystywanych do identyfikacji, oceny i osądu ryzyka, przypisywania własności, podejmowania działań w celu zmniejszenia lub przewidzenia ryzyka oraz monitorowania przeglądu osiąganych postępów”[79].

Na podstawie materiału uzyskanego z Biura Audytu i Zarządzania Ryzykiem Korporacyjnym w jednym z polskich koncernów można wywnioskować, że ważnymi elementami w zarządzaniu ryzykiem w systemach logistycznych, w wymiarze mikro (przedsiębiorstwa) i makro (wzdłuż całego łańcucha dostaw) są:

- doprecyzowana metodologia oceny, uwzględniająca ryzyka związane z:
  - strategią (np. wyborem kluczowego dostawcy, odbiorcy),
  - finansami w obszarze kosztów logistycznych (np. zmiany kursu walut przy zakupach zagranicznych),
  - procesami biznesowymi (np. ryzyko wynikające z nieodpowiednich lub zawodnych procesów logistycznych, takich jak: zaopatrzenie, magazynowanie, dystrybucja, obsługa klienta i zamówienie, pakowanie),

[77] Więcej w rozdziale 3.
[78] ERM (Enterprise Risk Management) – zarządzanie ryzykiem przedsiębiorstwa.
[79] E. Młodzik, *Zarządzanie ryzykiem operacyjnym w banku*, [w:] http://jmf.wzr.pl/, 25.06.2015.

  - czynnikami zewnętrznymi (ryzyko spowodowane przez działania spoza systemu gospodarczego, związane z zachowaniem odbiorców, konkurencji, usług substytucyjnych, a także zmianami politycznymi, prawnymi, technologicznymi),
  - IT (np. ryzyko wynikające z niewłaściwego zarządzania zasobami teleinformatycznymi przetwarzanymi z wykorzystaniem technologii informatycznej nieaktualnej, przestarzałej),
  - organizacją i zarządzaniem (np. ryzyko związane z relacjami z interesariuszami oraz wynikające z niewłaściwej struktury systemów logistycznych, systemu delegowań uprawnień, niewłaściwe postępowanie pracowników),
  - bezpieczeństwem fizycznym (np. ryzyko związane z ochroną ładunków logistycznych w czasie transportu, magazynowania – pożary, kradzieże, zmycie z pokładu, wypadki);
- opracowane mechanizmy kontrolne dla wszystkich uczestników procesów i systemów logistycznych w celu:
  - zapobiegania ryzykom (kontrola prewencyjna, czyli zapobiegająca),
  - wykrywania materializacji ryzyka i łagodzenia jego wpływu (kontrola detekcyjna, czyli wykrywająca);
- oceny mechanizmów kontrolnych – jednakowe dla wszystkich;
- stworzony jednolity model, który winien uwzględniać: identyfikację ryzyka, ocenę ryzyka, ocenę ryzyka brutto[80], ocenę mechanizmów kontrolnych, ocenę ryzyka netto, opracowanie i wdrożenie planów działań naprawczych, monitorowanie i raportowanie oceny ryzyka;
- ustalone mechanizmy i struktury koordynacji zarządzania ryzykiem;
- zapewnione narzędzia i wsparcie metodologiczne dla uczestników procesu logistycznych;
- plany działań naprawczych, których celem jest zwiększenie efektywności procesu zarządzania poszczególnymi rodzajami ryzyka (poprzez usprawnienie istniejących lub wprowadzonych nowych mechanizmów kontrolnych);
- monitorowane i raportowane oceny ryzyka przez właścicieli ryzyka i procesów;
- wyznaczone osoby (właściciele) odpowiedzialne za ryzyko, które:
  - odpowiadają przed swoim przełożonym lub kompetentną komórką za ocenę poziomu ryzyka,
  - odpowiadają za nadzór (i koordynację) nad działaniami związanymi z opracowaniem, wdrożeniem oraz realizacją działań wobec ryzyka,

[80] Ocena ryzyka brutto – przed wprowadzeniem mechanizmów kontrolnych, ocena ryzyka netto – po wprowadzeniu mechanizmów kontrolnych.

  - identyfikują i oceniają ryzyko, opracowują z właścicielami procesów plany działań naprawczych, zbierają informacje o zdarzeniach świadczących o materializacji ryzyka, monitorują efektywność procesu zarządzania danym ryzykiem;
- wyznaczone osoby (właściciela) procesu/podprocesu, które są odpowiedzialne przed swoim przełożonym lub inną komórką za:
  - koordynację procesu testowania mechanizmów kontrolnych oraz oceny ryzyka w swoich procesach i podprocesach,
  - walidację[81] poziomów ryzyka brutto i netto, które zostały zidentyfikowane w procesie i podprocesach oraz ocenione w ramach prowadzonej samooceny,
  - uzgodnienie z właścicielami ryzyka planów działań naprawczych wobec ryzyka zidentyfikowanego w procesie i podprocesach oraz wdrożenie, a także monitoring realizacji planów;
- wyznaczone osoby sprawujące nadzór nad realizacją działań kontrolnych w procesach, w których uczestniczą, są zobowiązane do pełnej współpracy z właścicielami ryzyka oraz procesu w okresie testowania mechanizmów kontrolnych oraz oceny zidentyfikowanego ryzyka, w tym projektowania nowych mechanizmów kontrolnych (właściciele kontroli są najczęściej pracownikami wskazanymi w planach działań naprawczych jako osoby odpowiedzialne za realizację planu i modyfikację mechanizmów kontrolnych).

Zarządzanie ryzykiem winno być nierozerwalną częścią procesu kierowania, które rozpoczyna się na etapie organizowania systemu logistycznego, i trwać do końca jego funkcjonowania. Należy pamiętać, że nie wystarczy dobra analiza i ocena niekorzystnych zdarzeń i ich skutków bez sprecyzowanych, wcześniej opracowanych sposobów reagowania na ryzyko w postaci planów reakcji.

Ważnym ogniwem w procesie zarządzania ryzykiem w systemach logistycznych jest człowiek – logista, który powinien być przygotowany do zachowania się w czasie wystąpienia niekorzystnych sytuacji poprzez podejmowanie działań neutralizujących skutki zagrożeń. Jego postępowanie powinno być zgodne z wcześniej opracowanymi i zatwierdzonymi procedurami, które z jednej strony ułatwiają eliminowanie skutków zdarzeń, a z drugiej strony chronią go przed nieuzasadnionymi konsekwencjami ze strony przełożonych czy obowiązującego w tym zakresie prawa.

Należy pamiętać, że żyjemy w świecie zdominowanym przez kulturę, w której z reguły nie toleruje się błędów i porażek.

---

[81] Walidacja to potwierdzenie, przez dostarczenie dowodu obiektywnego, że zostały spełnione wymagania odnośnie do konkretnego użycia lub zastosowania (PN-EN ISO 9000:2001). Przyjmuje się, że walidacja to generalnie uzyskanie dowodu, że środki kontroli przyjęte w ramach określonego planu są skuteczne, W. Przytuła, *Walidacja*, http://mfiles.pl/pl/index.php/Walidacja, 15.07.2015.