PAMIĘĆ PRZYSZŁOŚCI

Analiza ryzyka dla zarządzania kryzysowego

Redaktor naukowy
Grzegorz Abgarowicz

Wydawnictwo CNBOP-PIB

Zakres, w jakim uda się nam ograniczyć własną niepewność oraz osiągnąć oczekiwany poziom bezpieczeństwa, jest wprost proporcjonalny do pracy, jaką włożymy w proces planowania i przygotowania. Niemniej sam wysiłek nie gwarantuje jeszcze powodzenia realizowanych przedsięwzięć. Czynnikiem decydującym jest wiedza i umiejętności tych, którym przyjdzie zmierzyć się z problemem zarządzania ryzykiem. Czy są to jednak wystarczające predyspozycje, by podjąć trud zmierzenia się z zarządzaniem ryzykiem?

Albert Einstein zapytany o przyczyny naukowych osiągnięć zwykł mawiać:

Gdy przyglądam się sobie i moim metodom rozumowania, dochodzę do wniosku, że wyobraźnia odgrywa w moim życiu większą rolę niż talent do przyswajania wiedzy obiektywnej.

W obszarach nauki, które posiłkują się metodami antycypacyjnymi, to wyobraźnia zaczyna odgrywać dziś decydującą rolę. Nauka coraz częściej bazuje na tzw. pamięci przyszłości (*memories of the future*) – czyli wskazaniu prawdopodobnych zdarzeń i przygotowaniu już dziś różnych przyszłości.

Ze wstępu

PAMIĘĆ PRZYSZŁOŚCI

Analiza ryzyka dla zarządzania kryzysowego

PAMIĘĆ PRZYSZŁOŚCI

Analiza ryzyka dla zarządzania kryzysowego

Zbyszkowi Piątkowi

Redakcja naukowa:
Grzegorz Abgarowicz

PAMIĘĆ PRZYSZŁOŚCI

Analiza ryzyka dla zarządzania kryzysowego

(praca zbiorowa)

Autorzy:
dr Grzegorz Abgarowicz
dr Krzysztof Cebul
mgr Inga Abgarowicz
mgr Monika Wachnik
mgr Tomasz Plasota
mgr Bartłomiej Połeć
mgr inż. Maciej Napiórkowski

WYDAWNICTWO CNBOP – PIB
Józefów 2015

Redaktor naukowy:
dr Grzegorz Abgarowicz

Recenzenci naukowi:
prof. dr hab. Ryszard Jakubczak
dr hab. inż. Jarosław Prońko

Projekt okładki i strony tytułowej:
Julia Pinkiewicz

Korekta, redakcja techniczna:
Małgorzata Boruta

Korekta rysunków, wykresów i tabel:
Natalia Grądzka

Grafika na okładce:
www.vecteezy.com/vector-art/zhaolifang, www.freepik.com

Publikacja finansowana przez NCBiR w ramach projektu *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP* Nr DOBR/0077/R/lD3/2013/03

ISBN 978-83-61520-30-6
DOI: 10.17381/2015.3

Wydawca:
Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego
Państwowy Instytut Badawczy
05-420 Józefów ul. Nadwiślańska 213

Przygotowanie do druku i druk:
RC Model Sp. z o.o.

Nakład:
650 egzemplarzy

Spis treści

Spis oznaczeń

ABW	Agencja Bezpieczeństwa Wewnętrznego
AHRA	Proces Oceny Ryzyka (All Hazards Risk Assessment)
BIA	Analiza Wpływu na Biznes (Business Impact Analysis)
CZK	Centrum Zarządzania Kryzysowego
CzK	Czas Krytyczny
CzO	Czas Odtworzenia
DRP	Plan Działań na Wypadek Katastrofy (Disaster Recovery Plan)
EML	Szacunkowa Maksymalna Strata (Estimated Maximum Loss)
ETA	Analiza Drzewa Zdarzeń (Event Tree Analysis)
FGŚP	Fundusz Gwarantowanych Świadczeń Pracowniczych
FMEA	Analiza Rodzajów i Skutków Możliwych Błędów (Failure Mode and Effect Analysis)
FTA	Analiza Drzewa Błędów (Fault Tree Analysis)
HAZOP	Analiza Zagrożeń i Zdolności Operacyjnych (Hazard and Operability Study)
HRA	Analiza Niezawodności Człowieka (Human Reliability Analysis)
IK	Infrastruktura Krytyczna
KPZK	Krajowy Plan Zarządzania Kryzysowego
KSI SIMIK	Krajowy System Informatyczny/System Informatyczny Monitoringu i Kontroli
MAiC	Ministerstwo Administracji i Cyfryzacji
MCL	Maksymalna Realna Strata (Maximum Credible Loss)
MFL	Maksymalna Przewidywalna Strata (Maximum Foreseeable Loss)
MPL	Maksymalna Możliwa Strata (Maximum Possible Loss)
MPL	Maksymalna Prawdopodobna Strata (Maximum Probable Loss)
NPOIK	Narodowy Program Ochrony Infrastruktury Krytycznej
NRA	Narodowa Analiza Zagrożeń i Oceny ich Ryzyka (National Risk Assessment)
NRR	Krajowy Rejestr Ryzyk (National Risk Register)
NSRA	Ocena Ryzyka na potrzeby Bezpieczeństwa Narodowego (National Security Risk Assessment)
PDCA	Cykl Deminga (Plan-Do-Check-Act)
PESTLE	Analiza Środowiska Makroekonomicznego Organizacji (Political, Economic, Social, Technological, Legal and Environmental)
PML	Możliwa Maksymalna Strata (Possible Maximum Loss)
PML	Prawdopodobna Maksymalna Strata (Probable Maximum Loss)
QRA	Jakościowe metody oceny ryzyka (Qualitative Risk Assessment)
RCB	Rządowe Centrum Bezpieczeństwa
RoZBN	Raport o zagrożeniach bezpieczeństwa narodowego

RPO	Docelowy Punkt Wznowienia Działalności (Recovery Point Objective)
RTO	Docelowy Czas Wznowienia Działalności (Recovery Time Objective)
STI	System Teleinformatyczny
SWOT	Technika analityczna służąca do porządkowania informacji (Strengths, Weaknesses, Opportunities and Threats)
SZCD	System Zarządzania Ciągłością Działania
WIOŚ	Wojewódzki Inspektorat Ochrony Środowiska
ZZK	Zespół Zarządzania Kryzysowego

Wstęp

Reinhard Mohn, długoletni właściciel Bartelsmann AG, podczas jednego ze swoich wystąpień powiedział: *najpoważniejszym ryzykiem dla organizacji jest zapomnienie o ryzyku*. To właśnie zdolność właściwego postrzegania zagrożeń oraz świadome i konsekwentne przygotowanie się na nie pozwala na zwiększenie pola wiedzy i pewności w sytuacjach, których głównym wrogiem stają się niepewność i chaos. Czy zarządzanie ryzykiem gwarantuje bezpieczeństwo? Odpowiedź może być tylko jedna – nie. Zarządzanie ryzykiem pozwala jedynie na zwiększenie szans na to, że kryzys nie dotknie organizacji, albo że jego skutki zostaną ograniczone na tyle, by organizacja potrafiła je zaakceptować. Jednym z zarzutów, które stawia się *grze w ryzyko,* jest jej antycypacyjny charakter. Próba przewidywania przyszłości – bo przecież do tego sprowadza się zarządzanie ryzykiem – zawsze obarczona jest prawdopodobnym błędem. Niemniej obecnie dysponujemy dużym i sprawdzonym, co najważniejsze, katalogiem naukowo potwierdzonej wiedzy i doświadczenia. To, co trzeba zrobić, to po prostu po nie sięgnąć. Prezentacja pola dyskursu nad ryzykiem to jeden z celów, jaki przyświecał autorom niniejszej pracy. Drugi to wskazanie możliwych do przyjęcia rozwiązań, których zastosowanie zwiększy zdolność planowania cywilnego administracji publicznej. Trzecim i najważniejszym celem jest otworzenie drzwi do jakże interesującego świata zarządzania ryzykiem i zachęcenie czytelników do rozpoczęcia własnej z nim przygody. Zamieszczona na końcu pracy bibliografia powinna zachęcić osoby, które chcą poszerzyć swoją wiedzę. Ciągłe uczenie się i doskonalenie to we współczesnym, szybko zmieniającym się świecie nie tyle chęć poszerzenia własnych możliwości, ale przede wszystkim wymóg i konieczność. Pewność siebie i niedostateczna wiedza są groźniejsze niż jej brak.

Zakres, w jakim uda się nam ograniczyć własną niepewność i osiągnąć oczekiwany poziom bezpieczeństwa, jest wprost proporcjonalny do pracy, jaką włożymy w proces planowania i przygotowania. Niemniej sam wysiłek nie gwarantuje jeszcze powodzenia realizowanych przedsięwzięć. Jak wspomniano już wcześniej, czynnikiem decydującym jest wiedza i umiejętności tych, którym przyjdzie zmierzyć się z problemem zarządzania ryzykiem. Czy są to jednak wystarczające predyspozycje, by podjąć trud zmierzenia się z nim? Einstein, zapytany o przyczyny naukowych osiągnięć, zwykł mawiać: *Gdy przyglądam się sobie i moim metodom rozumowania, dochodzę do wniosku, że wyobraźnia odgrywa w moim życiu większą rolę niż talent do przyswajania wiedzy obiektywnej*. W obszarach nauki, które posiłkują się metodami antycypacyjnymi, to wyobraźnia zaczyna odgrywać dziś decydującą rolę. Nauka coraz częściej bazuje na tzw. *pamięci przyszłości* (*memories of the future*) – czyli

wskazaniu prawdopodobnych zdarzeń i przygotowaniu już dziś *różnych przyszłości*. Magruk za Inayatullahem przytacza, że *nastąpiło przejście z metod prognostycznych poprzez tzw. metody „uczenia się przez działanie" (action learning/research) w kierunku antycypacyjnych metod uczących się (anticipatory action learning). Antycypacja przyszłości implikuje trzy sposoby postępowania:*
1) nie jest robione absolutnie nic na jej podstawie,
2) czynione są przygotowania do wzięcia odpowiedzialności za przewidywany rozwój,
3) podejmowane są czynności w celu wpłynięcia na przyszły bieg wydarzeń[1].

Dziś nie prognoza przyszłości, ale jej antycypacja staje się wyzwaniem, przed którym stoi także system bezpieczeństwa narodowego. Aby z niej skorzystać, potrzebna jest jednak świadomość ryzyka i wiara w zdolności analityków zajmujących się zarządzaniem nim u osób podejmujących decyzje polityczne. Z przeszło sześcioletniego doświadczenia wynikającego z obowiązywania przepisów w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego wynika jasno, że dokument ten pomimo jego unikatowości i istotności w żaden sposób nie wpłynął na postrzeganie przez decydentów zagrożeń państwa i nie przełożył się na jakiekolwiek strategiczne decyzje.

Prezentowana Państwu publikacja składa się z siedmiu powiązanych ze sobą rozdziałów. Pierwszy określa *źródła* zarządzania ryzykiem w Polsce. Źródła rozumiane jako różnego rodzaju formalne zobowiązania administracji w tym zakresie. Obowiązek sporządzenia Raportu (…), kontrola zarządcza czy wynikające z konieczności implementacji zapisów Dyrektywy powodziowej przepisy Prawa wodnego formułują konieczność przeprowadzania cyklicznych ocen ryzyka, implikując niejako obowiązek podjęcia przez organy władzy kwestii zarządzania ryzykiem.

Drugi z rozdziałów przedstawia zakres odpowiedzialności administracji publicznej – jej zadania – w odniesieniu do potrzeb zapewnienia bezpieczeństwa oraz sposobu postrzegania przez nią problematyki zarządzania ryzykiem. Wskazuje także, jak w trakcie identyfikacji zagrożeń istotny jest namysł i zwrócenie uwagi na krytyczność wykonywanych przez nią procesów oraz konsekwencje, jakie niesie ze sobą ich przerwanie.

Trzeci rozdział stanowi przegląd norm, które porządkują sposób podejścia do zarządzania ryzykiem oraz wskazują obszary, w których jego wykorzystanie wpływa na poprawę bezpieczeństwa w organizacji. Pierwsze trzy, jak już wskazano, sięgają do praktyki zarządzania ryzykiem, a ich charakterystyka przybliża wynikające z nich zasady, procesy, metody i techniki. Normami tymi są:
- PN-ISO 31000 *Zarządzanie ryzykiem – Zasady i wytyczne,*
- PKN-ISO Guide 73 *Zarządzanie ryzykiem – Terminologia,*
- IEC/FDIS 31010 *Risk management – Risk assessment techniques.*

Kolejny standard, ISO 22301 *Bezpieczeństwo Powszechne – Systemy Zarządzania Ciągłością Działania*, nie odwołuje się bezpośrednio do sposobu zarządzania ryzy-

[1] A. Magruk, *Słabe Sygnały i Dzikie Karty – Innowacyjne Metody Antycypacyjne,* Economy and Management – 4/2010, s. 126-136.

kiem, ile do wykorzystania samej jego analizy do utrzymania ciągłości działania. Nawiązuje przy tym do metod definiowania zagrożeń poprzez identyfikację procesów kluczowych (patrz rozdział drugi) i sposobów ich utrzymania lub odtworzenia. Ostatni omawiany w tym rozdziale standard: BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki* to nowa wydana przez *British Standards Institution* w 2014 r. norma wskazująca sposób wykorzystania wyników zarządzania ryzykiem w specyficznym procesie, jakim jest zarządzanie kryzysowe.

Czwarta część publikacji zawiera charakterystyki metodyk przygotowanych i wykorzystywanych w: Szwecji, Niemczech, Irlandii, Kanadzie, Holandii oraz Wielkiej Brytanii. Stanowi ona punkt wyjścia do dyskusji nad sposobami identyfikacji, oceny, prezentacji ryzyka oraz metodami jego obniżania. O ile dwa pierwsze rozdziały ukazują obligatoryjne rozwiązania stanowiące obowiązek prawny organów, o tyle trzeci i czwarty są propozycjami metod, które można zastosować, starając się z tych obowiązków wywiązać.

Kolejne dwa rozdziały przedstawiają metody i techniki, które można wykorzystać podczas analizy ryzyka. Rozdział piąty jest rozwinięciem i uszczegółowieniem IEC/FDIS 31010 *Risk management – Risk assessment techniques*. Zostały w nim opisane i scharakteryzowane poszczególne techniki analityczne wymienione nie tylko w przywołanym standardzie, ale także te, które zdaniem autorów zasługują na uwagę podczas przeprowadzania analizy ryzyka na potrzeby bezpieczeństwa narodowego. Część z metod IEC/FDIS 31010 została w tym rozdziale pominięta, ponieważ zostały one opisane szczegółowo w rozdziale trzecim. Natomiast rozdział szósty stara się odpowiedzieć na pytanie, na ile metoda foresight może dostarczyć rzetelnej wiedzy w zakresie identyfikacji zagrożeń. Przedstawia założenia i sposób przeprowadzenia pełnej analizy, w tym jej zdolności do eksploracji ryzyka. Skąd położenie akcentu właśnie na problem diagnozy i identyfikacji? Biorąc pod uwagę cel zarządzenia ryzykiem, a więc podniesienia poziomu bezpieczeństwa, musimy zgodzić się z zasadą GIGO (*Garbage In, Garbage Out*), która wskazuje, że *wyniki przetwarzania błędnych danych będą błędne nawet wtedy, gdy procedura przetwarzania była poprawna*. Jeśli więc zidentyfikujemy niewłaściwe i *pozorne ryzyka* nieoddające rzeczywistych problemów organizacji (w tym przypadku państwa), wyniki zawsze będą błędne, a skutki zarządzania nimi nie przyczynią się do poprawy bezpieczeństwa.

Ostatni zamykający monografię rozdział prezentuje przygotowaną na potrzeby systemu zarządzania kryzysowego metodykę zarządzania ryzykiem. Powstała ona w wyniku współpracy autorów publikacji, pracowników Rządowego Centrum Bezpieczeństwa oraz specjalistów *British Standards Institution.* Jej przygotowanie poprzedził cykl szkoleń i warsztatów, długie godziny dyskusji i spierania się nawet o każdy szczegół oraz kompromis. Metodyka jest przykładem i propozycją innego spojrzenia na rozwiązanie problemu pomiaru i zarządzania ryzykiem. Opiera się na założeniu, że to cele poszczególnych organów władzy powinny być podstawą do identyfikacji ryzyka, a w wyniku ich dekompozycji można wskazać i opisać procesy na tyle szczegółowo, aby można było wyodrębnić te kluczowe z punktu widzenia systemu bezpieczeństwa narodowego.

Peter Bernstein w *Przeciw bogom* pisze: *Idea zarządzania ryzykiem zyskuje znaczenie dopiero wtedy, gdy ludzie zaczynają wierzyć, że mogą co najmniej w pewnym stopniu decydować o swoim losie*. Czy ta publikacja daje nadzieję na to, że zaproponowane w niej rozwiązania mogą zwiększyć zdolność wpływania na przyszły los? Że potrafimy w oparciu o metody naukowe trafnie przewidywać? Że w oparciu o te przewidywania potrafimy właściwie się przygotować i ograniczać zdarzenia niekorzystne lub ich skutki? To są pytania, na które odpowiedzi musi znaleźć sam czytelnik. Autorzy wyrażają jedynie nadzieję, że książka ta choć w części rozwiąże problemy, z którymi borykamy się, stając naprzeciw losowi w grze, w której prawdopodobieństwo wygranej jest, jak twierdzą sceptycy, tylko odrobinę większe niż w grze w kości.

Zespół autorski chciałby podziękować wszystkim tym, bez których pomocy i zaangażowania nie byłaby możliwa publikacja książki, którą trzymacie Państwo w rękach. Na szczególne podziękowania zasługuje zespół pracowników Rządowego Centrum Bezpieczeństwa, których doświadczenie i determinacja wpłynęły na ostateczny kształt większości rozdziałów. Dziękujemy więc: Dorocie Leduchowskiej, Anecie Dobruk-Serkowskiej, Witoldowi Skomrze, Maćkowi Pyznarowi, Tomkowi Szewczykowi, Michałowi Grzybowskiemu i Emilowi Wróblowi. Za pomoc w dostępie do norm, długie i żarliwe dyskusje oraz cierpliwość osobom związanym z *British Standards Institution:* Joannie Bańkowskiej, Krzysztofowi Gaweckiemu, Robertowi Olejniczakowi i Kamilowi Galickiemu. Dziękujemy także wszystkim, którzy brali udział w projekcie *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP:* szefom, pracownikom i współpracownikom: Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego Państwowego Instytutu Badawczego, Szkoły Głównej Służby Pożarniczej, Akademii Obrony Narodowej, Politechniki Warszawskiej oraz firmie Medcore.

Grzegorz Abgarowicz

1. Determinanty zarządzania ryzykiem w Polsce

Zarządzanie ryzykiem wykorzystywane jest w wielu dziedzinach aktywności państwa, w odniesieniu do różnego rodzaju jego sektorów, w tym między innymi: finansów publicznych, bezpieczeństwa informacji, czy zarządzania bezpieczeństwem. Nieodłączną część systemu zarządzania bezpieczeństwem stanowi system zarządzania kryzysowego. W Polsce został on utworzony na mocy ustawy o zarządzaniu kryzysowym z 26 kwietnia 2007 r. Zgodnie z ustawową definicją działalność ta składa się z czterech faz: zapobiegania, przygotowania, reagowania i odbudowy. Istotę drugiej z nich stanowi planowanie na wypadek wystąpienia sytuacji kryzysowych, zdefiniowane jako planowanie cywilne. Ze względu na realizację jednego z zadań z tego zakresu, tj. obowiązku opracowania dokumentów planistycznych przez organy zarządzania kryzysowego na poszczególnych szczeblach podziału terytorialnego, zaimplementowano do polskiego prawa wybrane elementy procesu zarządzania ryzykiem, w tym ocenę ryzyka. Na potrzeby sporządzania dokumentów, takich jak Raport o Zagrożeniach Bezpieczeństwa Narodowego, plany zarządzania kryzysowego, plany ochrony infrastruktury krytycznej oraz Narodowy Program Ochrony Infrastruktury Krytycznej opracowano wytyczne i zalecenia odnoszące się do wykorzystania oceny ryzyka w ramach planowania cywilnego.

1.1. System zarządzania kryzysowego

Zapisy odnoszące się do wykorzystania oceny ryzyka na potrzeby systemu zarządzania kryzysowego zostały wprowadzone do polskiego porządku prawnego ustawą z 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Ich brzmienie ewaluowało od pierwotnej wersji ustawy, poprzez jej kolejne nowelizacje (z 2009 i 2010 r.), które ukształtowały obecny stan przepisów. Niezależnie od kolejnych zmian legislacyjnych związanych z problematyką oceny ryzyka, proces ten zawsze łączono z obszarem planowania cywilnego oraz ochroną infrastruktury krytycznej, a ściślej rzecz ujmując z obowiązkiem przygotowania dokumentów planistycznych w tym zakresie. Już w pierwotnej wersji ustawy ocenę ryzyka wystąpienia zagrożeń ujęto jako element struktury ówczesnych planów reagowania kryzysowego oraz planów ochrony infrastruktury krytycznej. Zapisy te przetrwały do dzisiaj.

Zgodnie z art. 5 ust. 2 pkt 1a obowiązującej ustawy elementem planów zarządzania kryzysowego jest *charakterystyka zagrożeń oraz ocena ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej, oraz mapy ryzyka i mapy zagrożeń.* Usta-

wodawca wskazał także na obowiązek opracowania planów ochrony infrastruktury krytycznej przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Niemniej jednak zapis obligujący wykonawców przedmiotowych planów do uwzględnienia w nich oceny ryzyka dla infrastruktury krytycznej został zniesiony, znalazł się bowiem w stosownym rozporządzeniu Rady Ministrów dedykowanym tylko i wyłącznie opracowaniu tychże dokumentów planistycznych[1]. Ponadto uchylono zapis zobowiązujący organy administracji publicznej do opracowania ww. dokumentów na szczeblu krajowym oraz wojewódzkim.

Znaczące zmiany w przepisach wniosła nowelizacja ustawy z 17 lipca 2009 r.[2]. Wprowadzono termin mapy ryzyka rozumianej jako *mapa lub opis przedstawiający potencjalne negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę*[3]. Zdefiniowano również mapę zagrożeń jako *mapę przedstawiającą obszar geograficzny objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń*. Co więcej, proces planowania cywilnego uzupełniono o dwa dokumenty strategiczne, uwzględniające konieczność dokonywania oceny ryzyka zagrożeń: Raport o zagrożeniach bezpieczeństwa narodowego oraz Narodowy Programu Ochrony Infrastruktury Krytycznej.

Podczas kolejnej nowelizacji ustawy z 29 października 2010 r. uwzględniono zobowiązania unijne w zakresie europejskiej ochrony infrastruktury krytycznej, w tym związane z zagadnieniem ryzyka[4]. Zgodnie z nimi Dyrektor RCB, we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy IK, na bieżąco rozpoznaje potencjalną europejską infrastrukturę krytyczną, badając, czy spełnia określone wymogi. Ponadto przekazuje również Komisji Europejskiej co dwa lata sprawozdanie zawierające ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów stwierdzonych w każdym z systemów, w których została wyznaczona europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej[5].

Zapisy ustawy odwołują się więc wielokrotnie do oceny ryzyka w kontekście procesu planowania. Niemniej jednak nie zawierają one podstawowej terminologii związanej z zarządzaniem ryzykiem, to znaczy takich pojęć, jak: *ryzyko*, *analiza ryzyka*, czy też *ocena ryzyka*, co wydaje się wadą obecnie przyjętych uregulowań prawnych.

Wśród dokumentów planistycznych obejmujących ocenę ryzyka zagrożeń, których przygotowanie jest obowiązkiem wynikającym z zapisów ustawowych, naczelną rolę pełni Raport o zagrożeniach bezpieczeństwa narodowego. Ze względu na swój

---

1 Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. 2010 nr 83, poz. 542).

2 Ustawa z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. 2009 nr 131, poz. 1076).

3 Art. 3 ust. 10 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2013, poz. 1166).

4 Tamże, art. 6a.

5 Tamże, art. 6c.

strategiczny charakter stanowi bowiem podstawę procesu planowania cywilnego. Zgodnie z ustawą Raport sporządzany jest przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów na potrzeby Krajowego Planu Zarządzania Kryzysowego. Wskazani wykonawcy opracowują raporty cząstkowe do Raportu zgodnie z przyjętą procedurą[6]. Koordynację przygotowania dokumentu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, a w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef ABW.

Ponadto kierunki działania wynikające z wniosków z Raportu, stanowiące element KPZK, są również uwzględniane planach zarządzania kryzysowego na niższych szczeblach. W założeniu ma więc on stanowić dokument wyjściowy do planowania kryzysowego.

Zgodnie z art. 5 ust. 3 ustawy dokument ten obejmuje następujące elementy:

- wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka,
- określenie celów strategicznych,
- określenie priorytetów w reagowaniu na określone zagrożenia,
- wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych,
- programowanie zadań w zakresie poprawy bezpieczeństwa przez uwzględnianie regionalnych i lokalnych inicjatyw,
- wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych.

Celem Raportu jest zatem identyfikacja najważniejszych zagrożeń na szczeblu krajowym, określenie ryzyka ich wystąpienia, jak również wskazanie działań zapobiegawczych oraz przygotowawczych pozwalających na zmniejszenie prawdopodobieństwa wystąpienia zagrożeń oraz ograniczenia ich skutków[7].

Integralną część pierwszego elementu Raportu stanowi mapa ryzyka. O ile w ustawie zawiera się jej definicję, to zakres oraz formę jej wykonania określa Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego. Zgodnie z rozporządzeniem mapę ryzyka sporządza się w formie:

- mapy topograficznej, a w postaci elektronicznej – mapy wektorowej lub rastrowej, przedstawiającej zasięg geograficzny zagrożeń z przypisanym prawdopodobieństwem wystąpienia i oceną skutków wystąpienia dla ludności, gospodarki lub środowiska,
- tabeli opisującej parametry zagrożeń oraz ich prognozowane skutki,
- opisowej, jeżeli charakter zagrożenia uniemożliwia przedstawienie informacji w formie mapy lub tabeli[8].

---

[6] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2010.

[7] Ocena ryzyka na potrzeby zarządzania kryzysowego, Raport o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

[8] § 5 ust. 1 Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.U. 2010 nr 83, poz. 540).

Opis parametrów zagrożeń i możliwych skutków ich wystąpienia w formie tabelarycznej lub opisowej uważa się za bardzo istotny dla procesu planowania element Raportu. Pozwala on bowiem skupić się na przygotowaniu do reagowania na najbardziej istotne zagrożenia według stopniowania prawdopodobieństwa ich wystąpienia, jak również dotkliwości skutków dla ludności i infrastruktury, przy występującym deficycie sił i środków[9].

Przepisy rozporządzenia wskazują również, jakie kategorie zagrożeń obejmuje tak rozumiana mapa ryzyka. Należą do nich zagrożenia:

1) o istotnym wpływie na funkcjonowanie i rozwój państwa, a w szczególności mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego,
2) których skutki mogą:
   - godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, zwłaszcza w suwerenność, niepodległość i nienaruszalność terytorium,
   - zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach,
   - oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa,
   - dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie,
3) występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych,
4) o charakterze terrorystycznym mogące doprowadzić do sytuacji kryzysowej[10].

Wskazany katalog obejmuje więc nie tylko zagrożenia prowadzące do sytuacji kryzysowej w myśl definicji ustawowej, tj. (…) *wpływającej negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych obszarach lub środowiska (…)*, ale również te o charakterze globalnym, które wpływają na rozwój całego państwa w kontekście środowiska międzynarodowego.

Rozwinięciem przepisów prawnych w zakresie oceny ryzyka na potrzeby omawianego dokumentu jest Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego przygotowana przez Rządowe Centrum Bezpieczeństwa[11]. Wskazuje ona sposób wykonania jego poszczególnych części. Uwzględnia również przyjętą na potrzeby opracowania dokumentu metodykę oceny ryzyka.

Zgodnie z procedurą sporządzenie raportu cząstkowego polega na wypełnieniu przez wykonawców formularza w wersji elektronicznej (z rozszerzeniem

---

[9] W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, wyd. PRESSCOM, Wrocław 2010, s. 69.

[10] § 4 pkt 1 Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.U. 2010 nr 83, poz. 540).

[11] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2010, s. 18.

*xls) dostarczonego przez Rządowe Centrum Bezpieczeństwa. Został on stworzony w programie Microsoft Excel. Formularz zawiera siedem arkuszy kalkulacyjnych: zagrożenia, zapobieganie, przygotowanie, reagowanie, dane historyczne, wykazy oraz wnioski[12]. Pierwszy z nich odnosi się do przyjętej metodyki oceny ryzyka. Zgodnie z procedurą proces ten złożony jest z czterech następujących kroków:

1. Identyfikacja zagrożeń (zgodnie z działami administracji rządowej).
2. Opisanie scenariuszy (wskazania m.in. potencjalnych miejsc wystąpienia, przyczyn wystąpienia zagrożenia oraz jego typu).
3. Analiza skutków (dla ludności, gospodarki, mienia, infrastruktury, środowiska oraz wpływu na infrastrukturę krytyczną).
4. Ocena ryzyka (określenia prawdopodobieństwa, skutków, wartości ryzyka oraz poziomu jego akceptacji)[13].

W odniesieniu do tej części raportu cząstkowego w Procedurze zawarto następujące wytyczne dla wykonawców:

- konieczność identyfikacji zagrożeń odpowiadających kryteriom raportu cząstkowego, tj. takich, które można przyporządkować do jednej ze wskazanych wyżej kategorii zagrożeń, biorąc pod uwagę zarówno doświadczenia historyczne, jak i zmiany demograficzne, klimatyczne czy też postęp technologiczny,
- konieczność wykorzystania wszelkich możliwych źródeł informacji niezbędnych do identyfikacji zagrożeń, tj. m.in. analizy danych historycznych, szacowania eksperckiego, modelowania matematycznego, czy też badania przypadków (*case study*),
- konieczność przygotowania opisu wszystkich scenariuszy zdarzeń w ramach danego zagrożenia przy uwzględnieniu elementów wskazanych powyżej (krok 2 procesu oceny ryzyka), biorąc pod uwagę możliwość rozprzestrzeniania się zagrożeń, wraz z określeniem, czy dany scenariusz został ujęty we właściwym planie zarządzania kryzysowego, oraz czy powinien znaleźć się w Krajowym Planie Zarządzania Kryzysowego,
- konieczność zastosowania opisanych parametrów, będących podstawą do szacowania prawdopodobieństwa wystąpienia zagrożeń, ich skutków, wartości ryzyka oraz poziomu jego akceptacji, jak również narzędzia obrazującego wyniki analizy ryzyka, tj. matrycy ryzyka.

Na potrzeby opracowania raportu cząstkowego stosuje się 5-stopniową metodę oceny ryzyka, której istotą jest prawidłowe określenie kategorii prawdopodobieństw i kategorii potencjalnych strat w stosunku do skali analizowanych scenariuszy dla zagrożeń. Wykorzystuje ona dwa podstawowe czynniki wpływające na wartość określanego ryzyka:

- prawdopodobieństwo wystąpienia zagrożenia (konkretnego scenariusza),
- skutki (konsekwencje) takiego zagrożenia (konkretnego scenariusza)[14].

[12] Tamże, s. 7.
[13] Tamże, s. 6.
[14] Tamże.

Skalę jakościową prawdopodobieństwa opisuje tabela 1.1.

Tabela 1.1. Jakościowy opis skali prawdopodobieństwa

Skala	Prawdopodobieństwo	Opis
1	bardzo rzadkie	Może wystąpić tylko wyjątkowych okolicznościach. Może wystąpić raz na pięćset lub więcej lat.
2	rzadkie	Nie oczekuje się, że się może zdarzyć i/lub nie jest w ogóle udokumentowana, nie istnieje w przekazach ludzi i/lub zdarzenia, nie wystąpiły w podobnych organizacjach, urządzeniach, społecznościach i/lub istnieje mała szansa, powód, czy też inne okoliczności aby zdarzenia mogły wystąpić. Mogą one wystąpić raz na sto lat.
3	możliwe	Może zdarzyć się w określonym czasie i/lub mało, rzadko przypadkowo zdarzenia, że są udokumentowanen lub cząstkowo przekazywane w formie ustnej i/lub bardzo mało zdarzeń i/lub jest powodujące, że zdarzenie może wystąpić. Może zdarzyć się raz na dwadzieścia lat.
4	prawdopodobne	Jest prawdopodobne, że wystąpi w większości okoliczności i/lub zdarzenia są systematycznie dokumentowane i przekazywane są w formie ustnej i/lub występuje znaczna szansa, powód, lub urządzenia pozwalające na jego wystąpienie. Może zdarzyć się raz na pięć lat.

Źródło: Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2010

Skala skutków zbudowana jest w sposób analogiczny. Jednakże rozpatruje się je oddzielnie dla trzech kategorii: Z – życie i zdrowie, M – mienie wraz z infrastrukturą oraz S – środowisko. Skalę jakościową obrazuje tabela 1.2.

Tabela 1.2. Klasyfikacja skutków i ich charakterystyka

Skala	Skutki	Kat.	Opis (Z - życie i zdrowie, M - mienie, S - środowisko)
A	nieistotne	**Z**	Nie ma ofiar śmiertelnych i rannych. Nikt lub mała liczba ludzi została przemieszczona na krótki okres czasu (do 2 godzin). Nikt lub niewielka liczba osób wymaga pomocy (nie finansowanej lub materialnej).
		M	Praktycznie bez zniszczeń. Brak wpływu lub bardzo niewielki na społeczność lokalną. Brak lub niewielkie straty finansowe.
		S	Niemierzalny efekt w środowisku naturalnym.

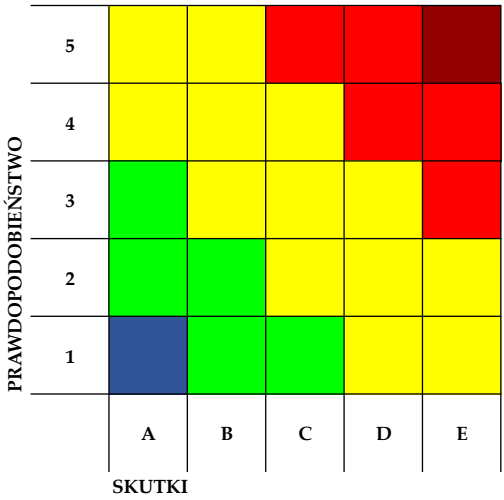
Skala	Skutki	Kat.	Opis (Z - życie i zdrowie, M - mienie, S - środowisko)
B	małe	Z	Mała liczba rannych, lecz bez ofiar śmiertelnych. Wymagana pierwsza pomoc. Konieczne przemieszczenia ludzi (mniej niż na 24 godziny). Część ludzi potrzebuje pomocy.
		M	Występują pewne zniszczenia. Występują pewne utrudnienia (nie dłużej niż 24 godziny). Nie wymagane dodatkowe środki.
		S	Niewielki wpływ na środowisko naturalne o krótkotrwałym efekcie.
C	średnie	Z	Potrzebna pomoc medyczna, lecz bez ofiar śmiertelnych. Niektórzy wymagają hospitalizacji. Potrzebne dodatkowe miejsca w szpitalach oraz dodatkowy personel medyczny. Przebywanie ewakuowanych ludzi w wyznaczonych miejscach z możliwością powrotu w ciągu 24 godzin.
		M	Ustalenie miejsc zniszczeń, które wymagają rutynowej naprawy. Normalne funkcjonowanie społeczności z niewielkimi niewygodami. Spore straty finansowe.
		S	Pewne skutki w środowisku naturalnym, lecz krótkotrwałe lub małe skutki o długotrwałym efekcie.
D	duże	Z	Mocno poranieni, dużo osób hospitalizowanych, duża liczba osób przemieszczonych (więcej niż na 24 godziny). Ofiary śmiertelne. Potrzeba szczególnych zasobów do pomocy ludziom i do usuwania zniszczeń.
		M	Społeczność częściowo nie funkcjonująca, niektóre służby są nieosiągalne. Duże straty finansowe. Potrzebna pomoc z zewnątrz.
		S	Długotrwałe efekty w środowisku naturalnym.
E	katastrofalne	Z	Duża liczba poważnie rannych. Duża liczba hospitalizowanych. Ogólne i długotrwałe przemieszczenie ludności. Duża liczba ofiar śmiertelnych. Wymagana duża pomoc dla dużej liczby ludzi.
		M	Rozległe zniszczenia. Niemożność funkcjonowania społeczności bez istotnej zewnętrznej pomocy.
		S	Duży wpływ na środowisko naturalne i/ lub stałe zniszczenia.

Źródło: Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2010

Kolejnym krokiem po określeniu czynników prawdopodobieństwa i skutków jest pokazanie zależności pomiędzy nimi, tj. wskazanie wartości ryzyka. Elementem niezbędnym do jej wyznaczenia jest matryca ryzyka[15] (rys. 1.1). Poszczególne wartości ryzyka zaznaczono następującymi kolorami:

[15] Tamże, s. 17.

- minimalne (kolor niebieski),
- małe (kolor zielony),
- średnie (kolor żółty),
- duże (kolor czerwony),
- ekstremalne (kolor brunatny).



Rysunek 1.1. Matryca ryzyka na potrzeby Raportu o zagrożeniach bezpieczeństwa narodowego

Źródło: Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego; s. 17

Ostatnim elementem procesu oceny ryzyka jest określenie tzw. akceptacji ryzyka, czyli poziomu ryzyka akceptowalnego dla scenariusza w ramach określonego obszaru zadaniowego podległego odpowiedniemu ministrowi kierującemu działami administracji rządowej, kierownikowi urzędu centralnego lub wojewodzie. W zależności od tego na ile akceptowalne są aktualne rozwiązania oraz przypisane im siły i środki, oraz czy wymagane jest wprowadzenie dodatkowych środków bezpieczeństwa, wyróżnia się:

- ryzyko akceptowane (A),
- ryzyko tolerowane (T),
- ryzyko warunkowo tolerowane (WT),
- ryzyko nieakceptowane (N)[16].

Każdy z wykonawców po określeniu jednej z czterech kategorii akceptacji ryzyka dla danego scenariusza ma obowiązek jej uzasadnienia. Wskazanie jej poziomu stanowi bowiem subiektywną ocenę osób opracowujących raport cząstkowy[17].

Powyżej wymienione wytyczne stanowią podstawę dla wykonawców raportów cząstkowych do wypełnienia poszczególnych komórek arkusza *Zagrożenia*.

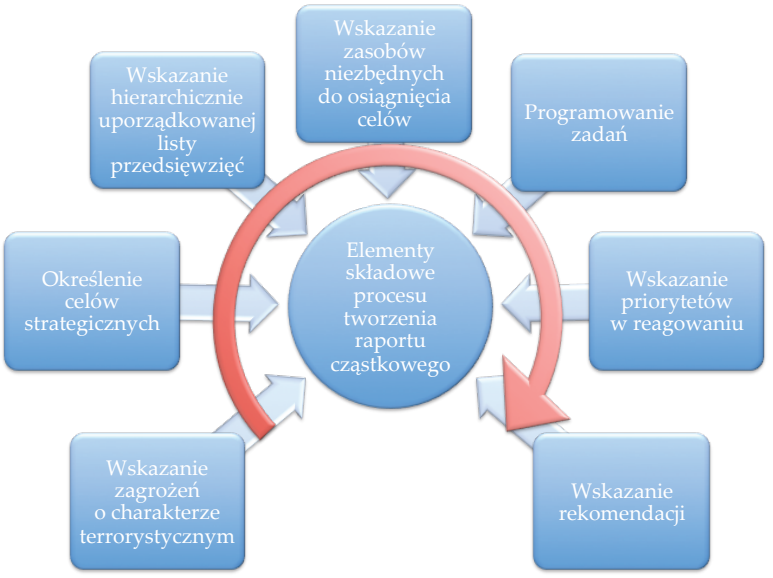
[16] Tamże, s. 18.
[17] Tamże.

Wymagany w nim zakres informacji zawiera m.in. ogólną charakterystykę zagrożenia, opis scenariusza, potencjalne miejsce wystąpienia, jego przyczyny, typ zagrożenia, analizę skutków dla: ludności, gospodarki, mienia, środowiska, wpływ na infrastrukturę krytyczną, jak również rezultaty szacowania prawdopodobieństwa, skutków, wartości ryzyka oraz akceptacji ryzyka wraz z jej uzasadnieniem.

Dane zawarte w arkuszu *Zagrożenia* stanowią bazę informacji na temat specyfiki wszystkich zagrożeń bezpieczeństwa narodowego pozostających w kompetencji danego wykonawcy. Przyjęte narzędzia: matryca ryzyka oraz metody oceny i analizy ryzyka, mają pozwolić na skupienie się na przygotowaniu na najbardziej prawdopodobne i dotkliwe w skutkach zagrożenia.

Jak już wcześniej wspomniano, wśród dokumentów planistycznych zawierających ocenę ryzyka znajduje się Raport o zagrożeniach bezpieczeństwa narodowego. W części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, koordynację przygotowania dokumentu raportu cząstkowego zapewnia Szef ABW. Procedura opracowania raportu cząstkowego do RoZBN, przygotowana przez ABW, zawiera metodykę oceny ryzyka do zastosowania przy stworzeniu wspomnianego dokumentu.

Zgodnie z instrukcją, jaką jest procedura opracowania raportu cząstkowego, to dokument zawierający:

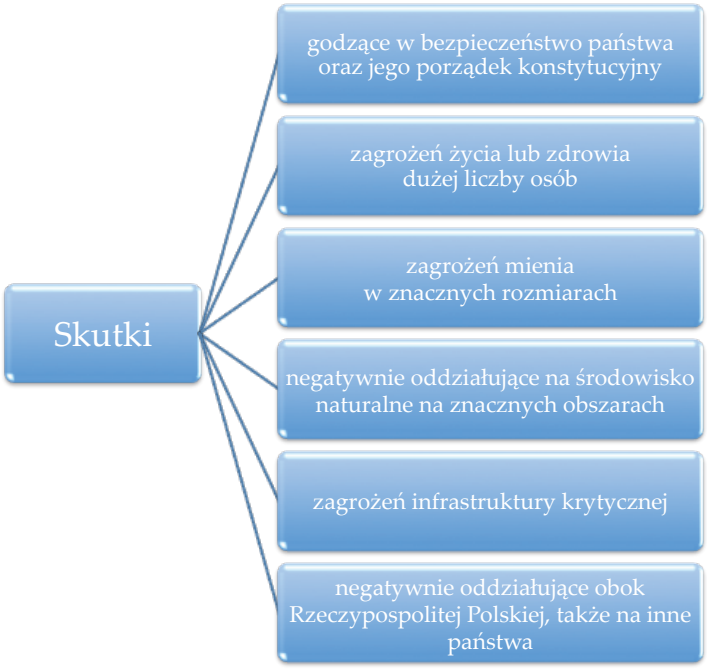


Rysunek 1.2. Elementy składowe procesu tworzenia raportu cząstkowego

Źródło: opracowanie własne na podstawie Procedury opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej

W pierwszym kroku, zgodnie z metodyką ABW, wykonujący ocenę ryzyka w kontekście zagrożeń terrorystycznych są zobligowani do dokonania identyfika-

cji tego typu zagrożeń w swoim obszarze zadaniowym. Kwestia ta dotyczy także zdarzeń, które mogą mieć miejsce poza granicami kraju, a których skutki w bliższej lub dalszej perspektywie mogą również dosięgnąć państwa polskiego lub jego obywateli. Ze względu na różny stopień wiedzy oraz narzędzi, jakimi dysponują podmioty wykonujące ocenę ryzyka dla zagrożenia terrorystycznego, podkreślono w dokumencie, iż nie wymaga się określenia prawdopodobieństwa wystąpienia zdarzenia[18]. Wystarczający opis stanowią zidentyfikowane przyczyny oraz możliwe skutki zdarzenia. Metodyka wskazuje, że charakteryzując kolejne przyczyny zdarzenia, należy również wziąć pod uwagę czynniki mające wpływ na zwiększenie prawdopodobieństwa wystąpienia zdarzenia i je wymienić. Służby i instytucje posiadające uprawnienia z zakresu przeciwdziałania zagrożeniom terrorystycznym zobligowano ponadto do wskazania charakteru zagrożenia pod kątem źródła inspiracji[19]. Określając skutki, zgodnie z dokumentem należy kierować się listą opracowaną przez ABW i wybrać odpowiadający lub odpowiadające danemu zagrożeniu.



Rysunek 1.3. Identyfikacja źródeł zagrożeń dla raportu cząstkowego

Źródło: opracowanie własne na podstawie Procedury opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej

[18] Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, s. 3.

[19] Tamże, s. 4.

W kolejnych krokach podmioty opracowujące raport cząstkowy zostały zobligowane do przedstawienia priorytetów działania w poszczególnych fazach zarządzania kryzysowego: zapobiegania, przygotowania i reagowania (pominięto fazę odbudowy). Dla fazy zapobiegania wskazano na potrzebę zdefiniowania przez podmioty celów strategicznych, które pozwolą na zmniejszenie szansy wystąpienia danego zagrożenia. Powyższe cele należy uzupełnić listą zadań oraz sił i środków umożliwiających ich osiągnięcie[20].

Elementami do scharakteryzowania w fazie przygotowania, które określa w kolejnym punkcie instrukcja, są działania związane z programowaniem zadań. W obszar ten wchodzą informacje dotyczące realizowanych oraz planowanych inicjatyw, projektów, programów mających wpływ na podniesienie poziomu bezpieczeństwa państwa w kontekście zagrożeń terrorystycznych. Na etapie określenia priorytetów w zakresie reagowania podmioty w ramach swojego obszaru kompetencyjnego zostały zobligowane do przedstawienia informacji związanych z obowiązującymi zasadami, procedurami na wypadek zagrożeń związanych z aktami terrorystycznymi.

Finalnym elementem raportu cząstkowego, za który jego wykonawcy są odpowiedzialni, jest wskazanie wniosków, rekomendacji oraz wszelkich spostrzeżeń w kontekście zagrożeń terrorystycznych i w zakresie odpowiedzialności danego podmiotu wypełniającego dokument.

Podobnie jak w przypadku Raportu o zagrożeniach bezpieczeństwa narodowego, na potrzeby planów zarządzania kryzysowego dla poszczególnych szczebli administracji publicznej przygotowano wytyczne i zalecenia, które odwołują się do problematyki oceny i mapowania ryzyka. Zgodnie z zapisami ustawowymi wydającymi je organami są:

- minister właściwy do spraw administracji publicznej, który w uzgodnieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii dyrektora RCB, wydaje wojewodom, w drodze zarządzenia, wytyczne do wojewódzkich planów zarządzania kryzysowego[21],
- wojewoda, który wydaje starostom zalecenia do powiatowych planów zarządzania kryzysowego[22],
- starosta, który wydaje organom gminy zalecenia do gminnego planu zarządzania kryzysowego[23].

Wytyczne wskazują na konieczność identyfikacji zagrożeń wymagających podjęcia działań koordynacyjnych przez wojewodę, w tym takich, które mogą mieć wpływ na sąsiednie województwa, cały kraj oraz zagrożenia o charakterze transgranicznym. Rekomenduje się również konieczność dokonania oceny ryzyka ich wystąpienia w oparciu o doświadczenia historyczne, dotyczące zagrożeń zaistniałych na terenie województwa, jak również odniesienia do trendów oraz zagrożeń

[20] Tamże, s. 5-6.
[21] Art. 14 ust. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, (Dz.U. z 2013, poz. 1166).
[22] Tamże, art. 14 ust. 2 pkt 2a.
[23] Tamże, art. 17 ust. 2 lit. c.

wynikających z rozwoju technologicznego, doświadczeń innych województw oraz sytuacji kryzysowych w innych krajach. Ponadto zaleca się dokonanie identyfikacji obszarów szczególnie podatnych na zagrożenia (np. terenu całego województwa lub jego części). Zezwala się przy tym na wykorzystanie metod opisowych, matematycznych oraz wsparcia eksperckiego.

Wytyczne odnoszą się również do zakresu oraz formy wykonania mapy ryzyka oraz mapy zagrożeń. Powinny one przedstawiać odpowiednio:

- wpływ, jaki wystąpienie danego zagrożenia może mieć na ludzi, środowisko, mienie i infrastrukturę (mapa ryzyka),
- obszar objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń (mapa zagrożeń).

Zalecenia do powiatowych planów zarządzania kryzysowego (oraz gminnych planów zarządzania kryzysowego) podejmują z kolei problematykę oceny oraz mapowania ryzyka w sposób analogiczny do wyżej wymienionych wytycznych. Niemniej jednak zalecenia wydane na przykład przez wojewodę mazowieckiego zawierają dodatkowy załącznik, który ma pomóc we właściwej identyfikacji zagrożeń naturalnych. Obejmuje on klasyfikację stopni zagrożenia dla zjawisk meteorologicznych stosowaną w ostrzeżeniach meteorologicznych Instytutu Meteorologii i Gospodarki Wodnej – Państwowego Instytutu Badawczego (zwracając uwagę na natężenie zjawiska, zasięg jego wystąpienia oraz czas trwania). Zawiera także wykaz stopni zagrożenia w zależności od kryteriów wydawania ostrzeżeń meteorologicznych dla poszczególnych zjawisk.

W niniejszym dokumencie zaleca się także zastosowanie półilościowej metody oceny ryzyka, tj. metody stosowanej na potrzeby opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego. Podkreśla się przy tym, że przygotowanie planu powinno zostać poprzedzone sporządzeniem przez właściwego wojewodę raportu cząstkowego. Zgodnie bowiem z logiką procesu planowania cywilnego w Polsce, wnioski i kierunki z niego wynikające są uwzględniane w planie, zwłaszcza w odniesieniu do części dokumentu obejmującej identyfikację oraz hierarchizację zagrożeń[24].

Zagadnienia oceny ryzyka wiążą się również z ochroną infrastruktury krytycznej, tj. z ustawowym obowiązkiem opracowania planów ochrony infrastruktury krytycznej nałożonego na właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Ich elementy składowe określa Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej. Zgodnie z nim jednym z elementów struktury planu jest charakterystyka zagrożeń dla infrastruktury krytycznej oraz ocena ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami zdarzeń[25]. Przepis ten rozszerza więc przyjętą na potrzeby opracowania planów zarządzania kryzysowe-

[24] Zalecenia do powiatowych planów zarządzania kryzysowego, Wojewódzkie Centrum Zarządzania Kryzysowego, Warszawa, marzec 2014 r.

[25] § 2 ust. 3 pkt 3a Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. 2010 nr 83, poz. 542).

go metodykę oceny ryzyka o wskazane narzędzie dedykowane temu procesowi, jakim jest metoda scenariuszowa.

Z zagadnieniami ochrony infrastruktury krytycznej (przy uwzględnieniu problematyki oceny ryzyka) wiąże się również drugi obok Raportu dokument planistyczny o charakterze strategicznym, jakim jest Narodowy Program Ochrony Infrastruktury Krytycznej. Jego celem jest stworzenie warunków do poprawy bezpieczeństwa IK w zakresie zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej, przygotowania na sytuacje kryzysowe mogące niekorzystnie na nią wpływać, reagowania w sytuacjach zniszczenia lub zakłócenia jej funkcjonowania oraz odtwarzania[26]. Sposób realizacji obowiązków i współpracy w zakresie NPOiK określa Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej. Wskazuje ono, że na potrzeby opracowania dokumentu dyrektor RCB opracowuje kryteria pozwalające wyodrębnić infrastrukturę krytyczną w ramach systemów IK[27]. Przepisy rozporządzenia odnoszą się również do zagadnienia oceny ryzyka. Zgodnie z nim ministrowie i kierownicy urzędów centralnych w terminie sześciu miesięcy od dnia otrzymania kryteriów, przygotowują w zakresie ich właściwości i przedkładają dyrektorowi Centrum informacje zawierające ogólną ocenę ryzyka dla funkcjonowania opisywanego obszaru zadaniowego, uwzględniającą zagrożenia, podatności na zagrożenie oraz konsekwencje zakłócenia funkcjonowania infrastruktury krytycznej[28].

Podejście do oceny ryzyka w ramach ochrony infrastruktury krytycznej rozwinięte jest w przyjętym 26 marca 2013 r. przez Radę Ministrów Narodowym Programie Ochrony Infrastruktury Krytycznej. Podkreśla się w nim, że wszelkie działania podejmowane w celu podniesienia poziomu ochrony IK powinny być proporcjonalne do poziomu ryzyka zakłócenia jej funkcjonowania w zakresie przyjętego modelu ochrony, jej rodzajów, a także użytych sił i środków[29]. Element ten determinuje działania podejmowane w celu obniżenia ryzyka funkcjonowania IK do poziomu akceptowalnego i stanowi podstawę określenia standardów ochrony IK oraz ustalenia priorytetów działań[30].

W kontekście NPOiK ryzyko definiuje się jako funkcję zagrożenia, podatności oraz skutków. Na potrzeby dokonania oceny ryzyka stosuje się metodę scenariuszową, która wykorzystuje wszystkie powyższe czynniki w odniesieniu do obiektu, urządzenia, instalacji lub systemu. Wskazana w NPOiK metoda scenariuszowa, za pomocą której dokonywana jest ocena ryzyka, złożona jest z następujących kroków:

---

[26] Tamże, art. 56 ust. 1 pkt 1-4.

[27] § 3 Rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. 2010 nr 83, poz. 541).

[28] Tamże, § 5 ust. 1 pkt. 3.

[29] Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2013 r., s. 25.

[30] Tamże.

1) Identyfikacja zagrożeń i budowa scenariuszy.
2) Określenie prawdopodobieństwa wystąpienia danego scenariusza.
3) Określenie podatności IK oraz środków ochrony.
4) Określenie skutków wystąpienia danego scenariusza.
5) Ocena ryzyka zakłócenia IK w danym scenariuszu[31].

W ramach identyfikacji zagrożeń oraz budowania scenariuszy (krok nr 1) zaleca się pozyskiwanie informacji o zagrożeniach występujących lokalnie od władz województwa, powiatu i gminy, które identyfikują zagrożenia na potrzeby opracowania planów zarządzania kryzysowego. Wyjątek stanowią zagrożenia o charakterze terrorystycznym, dla których źródłem informacji są służby ochrony państwa. Scenariusze budowane na potrzeby ochrony IK powinny być wiarygodne, poprawne merytorycznie, funkcjonalne, proste oraz reprezentatywne dla danego typu zagrożenia[32].

Przy określeniu prawdopodobieństwa wystąpienia danego scenariusza (krok nr 2) zaleca się oparcie na informacjach zawartych w Raporcie o zagrożeniach bezpieczeństwa narodowego oraz zaczerpniętych od władz województwa, powiatu i gminy oraz służb ochrony państwa. Innymi rekomendowanymi źródłami informacji, niezbędnymi do określenia prawdopodobieństwa, są:
- analiza danych statystycznych,
- analiza danych historycznych,
- szacowanie eksperckie,
- analiza studiów przypadków, które wystąpiły w kraju lub zagranicą,
- modelowanie matematyczne,
- analiza HAZOP[33].

Kolejny etap stanowi określenie podatności IK oraz podatności środków ochrony (krok nr 3). Definiuje się je jako cechy charakterystyczne, które czynią je wrażliwymi na zniszczenie, zakłócenie funkcjonowania, zmniejszenie potencjału lub efektywności działania oraz niewłaściwe wykorzystanie. Podkreśla się, że sama podatność nie powoduje szkody, lecz jest warunkiem lub zbiorem warunków, które mogą pozwolić zagrożeniu oddziaływać na IK. Przy oszacowaniu podatności zaleca się uwzględnienie czynnika ludzkiego, wykorzystanie do funkcjonowania IK systemów i sieci teleinformatycznych, techniczne aspekty budowy oraz eksploatacji IK, jak również zależności i współzależności[34].

W ramach określenia skutków danego scenariusza (krok nr 4) rekomenduje się wzięcie pod uwagę negatywnego oddziaływania zniszczenia lub zakłócenia funkcjonowania IK na ludność, gospodarkę, środowisko i stabilność państwa. Jednocześnie zakłada się, że skutki zakłócenia funkcjonowania IK mogą wystąpić bezpośrednio po niekorzystnym zdarzeniu lub być rozłożone w czasie[35].

---

31 Tamże, s. 25-26.
32 Tamże, s. 27.
33 Tamże, s. 28.
34 Tamże, s. 28-29.
35 Tamże.

Ostatnim z etapów jest ocena ryzyka zakłócenia IK w danym scenariuszu (krok nr 5). Zdaniem autorów Programu jej dokonanie wymaga zrozumienia pomiędzy zagrożeniem, podatnością i skutkami. Najprościej rzecz ujmując, zagrożenie, wykorzystując podatność, oddziałuje na IK, powodując określone skutki. Ryzyko mierzone jest za pomocą metod ilościowych oraz jakościowych. W ramach zdefiniowania każdego z czynników ryzyka dopuszczane jest zastosowanie skalowania i przypisania im skal np. 1–5 z użyciem zakresów liczbowych lub szczegółowego opisu[36].

Podobnie jak w procedurze opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego proces oceny ryzyka powinien także wskazywać na poziomu akceptowalności ryzyka. W tej sytuacji uwzględniany jest najgorszy możliwy scenariusz. Ponadto podkreśla się, że dokonywaniu okresowej oceny ryzyka powinny towarzyszyć: identyfikacja nowych zagrożeń, które wpływają lub mogą wpłynąć na poprawne funkcjonowanie IK, przegląd (aktualizacja planu ochrony infrastruktury krytycznej) oraz zapewnienie zgodności ze wszystkimi dokumentami rządowymi.

W zakończeniu Programu w części dotyczącej oceny ryzyka zezwala się na stosowanie innych metod oceny ryzyka, pod warunkiem spełnienia wymogu porównywalności i wiarygodności (do czasu opracowania właściwych narzędzi pozwalających na dokonywanie oceny ryzyka)[37].

1.2. Pozostałe regulacje w zakresie zarządzania ryzykiem

Rozpatrując problematykę wykorzystania oceny ryzyka na potrzeby planowania kryzysowego, należy wziąć pod uwagę przede wszystkim Decyzję Parlamentu Europejskiego i Rady nr 1313/2013/EU z 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności[38]. Określa ona bowiem sposób, w jaki państwa członkowskie UE powinny realizować zadania związane z zarządzaniem ryzykiem. Wprowadzono w niej termin oceny ryzyka, rozumianej jako proces obejmujący identyfikację ryzyka, analizę ryzyka oraz szacowanie ryzyka w odniesieniu do szczebla krajowego lub odpowiednio niższego szczebla. Ponadto dodano pojęcie zdolności zarządzania ryzykiem definiowanej w kontekście konieczności podejmowania przez państwa członkowskie działań w zakresie zmniejszania ryzyka, dostosowania się do ryzyka, lub ograniczenia ryzyka w odniesieniu do klęsk i katastrof zidentyfikowanych w przeprowadzonej przez państwa członkowskie ocenie ryzyka do poziomu akceptowalnego przyjętego przez każde z nich. Decyzja nakłada również na państwa obowiązek opracowania oceny ryzyka na szczeblu krajowym lub odpowiednio niższym szczeblu, jak również obliguje do sporządzania i doskonalenia swoich planów zarządzania ryzykiem odnoszących się do klęsk i katastrof na szczeblu krajowym lub odpowiednio niższym szczeblu. Wskazuje, że w związ-

[36] Tamże, s. 30-31.

[37] Tamże, s. 31.

[38] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

ku z nowymi wymogami związanymi z mechanizmem ochrony ludności kontynuacji wymagają prace badawcze w obszarze oceny ryzyka na szczeblu krajowym oraz budowy planów zarządzania ryzykiem[39].

Zapisy Decyzji Parlamentu Europejskiego i Rady w sprawie Unijnego Mechanizmu Ochrony Ludności wprowadzają pojęcie zdolności do zarządzania ryzykiem oznaczającej *umiejętność państwa członkowskiego lub jego regionów zmniejszenia ryzyka, dostosowania się do ryzyka, lub ograniczenia ryzyka, w szczególności jego skutków i prawdopodobieństwa klęski lub katastrofy zidentyfikowanego w przeprowadzonej przez to państwo lub regiony ocenie ryzyka do poziomu akceptowanego*. Termin ten ma być rozpatrywany w kontekście potencjału technicznego, finansowego oraz administracyjnego w odniesieniu do przeprowadzenia:

- *odpowiednich ocen ryzyka*,
- *odpowiedniego planowania zarządzania ryzykiem do celów zapobiegania ryzyku i zapewniania gotowości*,
- *podjęcia odpowiednich środków zapobiegania ryzyku i zapewniania gotowości*[40].

Pierwszym z aspektów determinujących zdolności zarządzania ryzykiem jest przeprowadzenie odpowiednich ocen ryzyka. Według zapisów Decyzji samo pojęcie oceny ryzyka oznacza *całościowy, przekrojowy proces identyfikacji ryzyka, analizy ryzyka i szacowanie ryzyka podejmowany na szczeblu krajowym lub odpowiednio niższym szczeblu*[41].

Zgodnie z powyższą definicją proces ten obejmuje trzy etapy, tj. identyfikację, analizę oraz szacowanie. Pierwszy z nich odnosi się do identyfikacji ryzyka wystąpienia klęsk żywiołowych oraz katastrof uznanych za *sytuacje, które mogą mieć poważne skutki dla ludzi, środowiska naturalnego lub mienia, w tym dziedzictwa narodowego*[42]. Definicja ta zbliżona jest do rozumienia pojęcia sytuacji kryzysowej[43], rozumianej w myśl ustawy o zarządzaniu kryzysowym *za sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych obszarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków*[44].

Kolejny z nich, analiza ryzyka, ma na celu analizę zidentyfikowanych wcześniej ryzyk, biorąc pod uwagę kategorie prawdopodobieństwa i skutków dla ludzi, środowiska naturalnego lub mienia, w tym dziedzictwa kulturowego.

Ostatnim krokiem jest szacowanie ryzyka, a zatem wskazanie, do jakiego stopnia dane ryzyko jest dla państwa członkowskiego lub władz regionalnych ak-

---

39 W. Skomra, *Zdolność zarządzania ryzykiem jako nowe wyzwanie dla systemu zarządzania kryzysowego,* Prezentacja z Konferencji Naukowej Zarządzanie Kryzysowe na poziomie województwa i w jednostkach samorządu terytorialnego, AON, 12–13 maja 2014 r.

40 Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

41 Tamże.

42 Tamże.

43 D. Leduchowska, *Zarządzanie ryzykiem w ramach unijnego mechanizmu ochrony ludności*, Biuletyn Wydziału Analiz RCB, październik 2014 r.

44 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89, poz. 590, ze zm).

ceptowalne. Istotą tego etapu jest więc wskazanie, do jakiego poziomu dane ryzyko jest dla nich do przyjęcia, jak również ustalenie, czy posiadają one wystarczające siły i środki w celu ich przeciwdziałania. Oznacza to, że w związku z tym istnieje konieczność zaangażowania w proces oceny ryzyka zarówno ekspertów, jak i decydentów[45].

Drugim z obszarów zdolności zarządzania ryzykiem jest odpowiednie planowanie zarządzania ryzykiem. Zapis art. 4 ust. 8 Decyzji mówiący o planowaniu zarządzania ryzykiem uszczegółowiony jest poprzez wskazanie, że służy ono zapobieganiu ryzyku, czyli wszelkim działaniom mającym na celu ograniczenie ryzyka lub łagodzenie negatywnych następstw klęsk lub katastrof dla ludzi, środowiska naturalnego oraz mienia, w tym dziedzictwa kulturowego. Wiąże się również z zapewnieniem gotowości, tj. przygotowaniem zasobów ludzkich i środków materialnych, struktur, społeczności i organizacji do skutecznego reagowania na klęskę lub katastrofę[46]. Ostatni z aspektów dotyczy podjęcia odpowiednich środków zapobiegania ryzyku lub zapewnienia gotowości.

Można więc uznać, że poszczególne jej elementy układają się w cykliczny, wieloetapowy proces, które rozpoczyna się od zidentyfikowania ryzyk (w ramach oceny ryzyka), poprzez fazę planowania zarządzania nimi (plany zarządzania ryzykiem), kończąc na podjęciu konkretnych działań ukierunkowanych na zapobieganie katastrofom i klęskom żywiołowym, oraz przygotowanie się na ich wystąpienie.

Niniejsza Decyzja obejmuje również wiele obowiązków związanych z nabyciem zdolności do zarządzania ryzykiem, przypisanych zarówno Komisji Europejskiej, jak i poszczególnym państwom członkowskim. Zapisy art. 5 ust. 1f) Decyzji nakładają na Komisję obowiązek sprawowania ogólnej koordynacji przedsięwzięć związanych z przeprowadzanymi przez państwa członkowskie ocenami zdolności zarządzania ryzykiem. Do jej zadań należy m.in. kompilowanie i rozsyłanie informacji udostępnianych przez państwa oraz organizacja wymiany doświadczeń w przedmiotowym zakresie.

Z powyższych zapisów Decyzji wyłania się koordynacyjna rola Komisji Europejskiej jako podmiotu odpowiedzialnego zarówno za zapewnienie sprawnego wykonania zadań związanych z przeprowadzeniem ocen zdolności zarządzania ryzykiem, jak również wskazującego kierunki działań i wyznaczającego standardy postępowania w tym zakresie.

Z kolei w rozdziale szóstym niniejszego dokumentu na państwa członkowskie nakłada się obowiązek:

- opracowania oceny ryzyka na szczeblu krajowym lub odpowiednio niższym szczeblu oraz udostępnienia Komisji streszczeń istotnych elementów tych ocen do 22 grudnia 2015 r.,

[45] D. Leduchowska, *Zarządzanie ryzykiem w ramach unijnego mechanizmu ochrony ludności*, Biuletyn Wydziału Analiz RCB, październik 2014 r.

[46] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

- co trzy lata opracowania i doskonalenia swoich planów zarządzania ryzykiem związanym z klęskami i katastrofami na szczeblu krajowym lub odpowiednio niższym szczeblu,
- co trzy lata udostępnienia Komisji oceny swojej zdolności zarządzania ryzykiem na szczeblu krajowym lub odpowiednio niższym szczeblu,
- uczestnictwa, na zasadzie dobrowolności, w ocenie wzajemnej dotyczącej zdolności zarządzania ryzykiem[47].

Powyższe zapisy wyznaczają trzyletni cykl planowania w przedmiotowym zakresie. Umożliwiają również fakultatywny udział państw członkowskich w kształtowaniu ocen zdolności zarządzania ryzykiem innych członków Unii Europejskiej.

Analizując zgodność polskiego ustawodawstwa z wymogami Mechanizmu, ze szczególnym uwzględnieniem zapisów dotyczących wykorzystania procesu zarządzania ryzykiem na potrzeby opracowania dokumentów z zakresu planowania cywilnego, można wskazać, że:

- o ile Decyzja w sprawie Unijnego Mechanizmu definiuje pojęcie oceny ryzyka, to w polskim prawie termin ten nie został objaśniony, mimo że ocena ryzyka pojawia się jako element planów zarządzania kryzysowego oraz Raportu o zagrożeniach bezpieczeństwa narodowego,
- wymogiem Mechanizmu jest uwzględnienie w przeprowadzonej ocenie ryzyka działań mających na celu zmniejszenie ryzyka, ograniczenie ryzyka, dostosowanie się do ryzyka w celu doprowadzenia go do poziomu akceptowalnego w danym państwie członkowskim; z drugiej strony ustawa o zarządzaniu kryzysowym nie wskazuje podmiotu, który byłby odpowiedzialny za realizację tego typu zadania,
- na potrzeby Mechanizmu przyjmuje się trzyletni cykl planistyczny, w przypadku polskiego systemu zarządzania kryzysowego jest to cykl dwuletni,
- wymogiem Mechanizmu jest opracowanie oceny ryzyka na szczeblu krajowym, w przypadku naszego systemu formą jego spełnienia mogą być elementy Raportu o zagrożeniach bezpieczeństwa narodowego,
- Decyzja w sprawie Mechanizmu nakłada obowiązek opracowania planów zarządzania ryzykiem; w przypadku rozwiązań polskich może on zostać wyczerpany przez wskazanie wybranych elementów Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów zarządzania kryzysowego,
- wymogiem Mechanizmu jest podejmowanie działań mających na celu zapobieganie ryzyku oraz zapewnienie gotowości; w przypadku zarządzania kryzysowego odpowiada to przedsięwzięciom podejmowanym w fazie zapobiegania oraz przygotowania[48],
- Decyzja w sprawie Mechanizmu definiuje pojęcie zdolności zarządzania ryzykiem, z kolei w żadnym z naszych rodzimych aktów prawnych z obszaru zarządzania kryzysowego termin ten nie został zdefiniowany,

[47] Tamże.

[48] Prezentacja: *Zbieżność krajowych dokumentów planistycznych z wymogami Mechanizmu*, Rządowe Centrum Bezpieczeństwa, wrzesień 2014.

- wymogiem Mechanizmu jest przekazywanie co trzy lata oceny zdolności zarządzania ryzykiem na szczeblu krajowym lub odpowiednio niższym szczeblu; z kolei w polskim systemie zarządzania kryzysowego nie ma żadnych mechanizmów, w oparciu o które zdolność zarządzania ryzykiem mogłaby być oceniana, nie wskazuje się również podmiotów, które byłyby odpowiedzialne za jej przeprowadzenie oraz przekazanie wyników do UE[49].

W ślad za Decyzją Parlamentu Europejskiego i Rady w sprawie Unijnego Mechanizmu Ochrony Ludności uruchomiono prace związane z opracowaniem wytycznych dotyczących oceny zdolności zarządzania ryzykiem. Bazą dla przygotowywanego materiału stały się sprawdzone praktyki działania państw członkowskich w aspekcie oceny ryzyka oraz ustalenia poczynione podczas warsztatów w Rzymie w ramach włoskiej prezydencji (15–16 lipca 2014 r.). Jak wskazano bezpośrednio w dokumencie, ich celem jest *dostarczenie państwom członkowskim niewiążącej, ogólnej oraz elastycznej metodyki, która pomoże im w przeprowadzeniu oceny zdolności zarządzania ryzykiem*[50].

Prowadzona ocena ryzyka powinna umożliwiać (dobrowolne) przyjęcie uniwersalnej metodyki, wspierającej poszczególne państwa członkowskie w identyfikacji ryzyka, ocenie ryzyka oraz w procesie ustalenia priorytetów działania względem tych ryzyk. Działania te mają także prowadzić do ujednolicenia zasad planowania zarządzania ryzykiem oraz adekwatnego doboru i wdrażania środków kontroli ryzyka, w tym zapewnienia odpowiedniego stopnia gotowości. Zgodnie z dokumentem wytycznych zasadniczym aspektem planowania zarządzania ryzykiem jest wybór najlepszej dostępnej formy postępowania ze zidentyfikowanym ryzykiem od jego ograniczania bądź tolerowania do łagodzenia jego prawdopodobieństwa lub skutków[51].

Głównymi przedsięwzięciami w ramach planowania zarządzania ryzykiem powinny być wskazanie wymaganych środków bezpieczeństwa i harmonogramu działań z tym związanych. Ponadto nieodłącznym aspektem jest w tym zakresie przyporządkowanie zadań i odpowiedzialności za ich realizację. Aby osiągnąć wzajemne zrozumienie wszystkich interesariuszy, wymagany jest ich wspólny udział w procesie identyfikacji środków bezpieczeństwa oraz ustaleniu priorytetów ich doboru. Istotnym elementem zdolności zarządzania ryzykiem jest także ocena zdolności wdrożenia środków zapobiegania i zapewnienia gotowości, która powinna obejmować problemy alokacji środków bezpieczeństwa, jak również zadań i odpowiedzialności w tym zakresie, obowiązki związane z monitorowaniem, a także ewaluację, w tym wykorzystanie wniosków i doświadczeń z przeszłości[52].

---

[49] Prezentacja Zakładu Ochrony Ludności CNBOP–PIB, *Szacowanie ryzyka na potrzeby systemu ochrony ludności w Polsce. Stan obecny oraz kierunki przyszłych rozwiązań, materiał konferencyjny*, Kraków 2014 r.

[50] *Risk Management Capability Assessment Guidelines – Draft*, Bruksela 2014 r., s. 3.

[51] Tamże, s. 5.

[52] Tamże, s. 6.

Realizację poszczególnych aspektów oceny zdolności oparto o listę pytań dotyczących: koordynacji działań, posiadanych doświadczeń, stosowanych metodyk, pozostałych interesariuszy, procesu przekazywania informacji i komunikowania, sprzętu oraz finansowania. Pod uwagę przy ocenie ryzyka brano przede wszystkim potencjał administracyjny (najważniejszy weryfikowany element: przygotowanie personelu oraz ekspertów), potencjał techniczny (najważniejszy weryfikowany element: wypracowanie i wdrożenie własnej metodyki oceny ryzyka oraz udział w tym procesie sprzętu lub narzędzi wspomagających go teleinformatycznie) oraz potencjał finansowy (najważniejszy weryfikowany element: pozyskiwanie środków finansowych na powyższe cele).

Wytyczne dotyczące oceny zdolności zarządzania ryzykiem stanowi zbiór wskazówek, które mogą być pomocne dla państw członkowskich w ramach realizacji obowiązku przeprowadzenia oceny zdolności zarządzania ryzykiem. Wydaje się, iż mogą być również przydatne na potrzeby opracowania krajowych metodyk oceny ryzyka. Wytyczne, wskazując kryteria oceny zdolności zarządzania ryzykiem, jednocześnie wyznaczają elementy niezbędne do wdrożenia całościowego procesu zarządzania ryzykiem na potrzeby planowania kryzysowego.

Rozważając problematykę oceny ryzyka, zasadne wydaje się poruszenie zagadnienia oceny ryzyka powodziowego. W pierwotnej wersji ustawy o zarządzaniu kryzysowym zakładano bowiem, że część ówczesnego planu reagowania kryzysowego, obejmująca charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, powinna uwzględniać mapy ryzyka i zagrożenia powodziowego. Kolejne nowelizacje ustawy pomijały jednak powyższe ustalenia, a obecne brzmienie przepisów ustawy o zarządzaniu kryzysowym, również nie obejmuje regulacji w tym zakresie. Nie oznacza to jednak, że problematyka nie jest obecna w polskim porządku prawnym, tym bardziej że stanowi ona wyraz zobowiązań nałożonych na Polskę jako państwo członkowskie Unii Europejskiej.

W ujęciu ogólnym UE kształtuje politykę wodną poprzez kilkanaście dyrektyw, regulując przede wszystkim kwestie związane z jakością wód, co ostatecznie zostało ujęte w Ramowej Dyrektywie Wodnej (RDW) 2000/60/WE[53] i w znacznej części opiera się o nie przede wszystkim Ustawa Prawo wodne, jak również Ustawa Prawo ochrony środowiska[54]. RDW pominęła jednak kwestię powodzi, zatem rozpoczęto prace nad Dyrektywą Powodziową, która oficjalnie została zatwierdzona 23 października 2007 r., a jej publikacja nastąpiła 6 listopada 2007 r.[55].

Dyrektywa Powodziowa 2007/60/WE nakazuje każdej jednostce zarządzającej lub w każdym obszarze dorzecza prowadzić ocenę ryzyka powodziowego, a także działania mające na celu usuwanie następstw powodzi i negatywnych konsekwencji dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności

[53] Ramowa Dyrektywa Wodna 2000/60/WE (RDW) z dnia 23 października 2000 r. ustanawiająca ramy wspólnotowego działania w dziedzinie polityki wodnej.

[54] Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz.U. z 2013, poz. 1232).

[55] http://www.kzgw.gov.pl/Dyrektywa-Powodziowa.html, z dnia 12 lutego 2015 r.

gospodarczej poprzez ustanowienie priorytetów działania w wymiarze finansowym, technicznym oraz politycznym[56].

Dyrektywa obliguje państwa członkowskie do sporządzenia:

- Wstępnej oceny ryzyka powodziowego do 22 grudnia 2011 roku, czyli określenia ryzyka z uwzględnieniem wpływu na ludzi i ich zdrowie, działalność gospodarczą i infrastrukturę[57].
- Map zagrożenia i map ryzyka powodziowego do 22 grudnia 2013 roku, przedstawiających potencjalne szkody związane z powodzią, która może wystąpić zgodnie z różnymi scenariuszami powodzi, w tym informacje o potencjalnych źródłach zanieczyszczenia środowiska w wyniku powodzi[58].
- Planów zarządzania ryzykiem powodziowym do 22 grudnia 2015 roku sporządzonych na podstawie map zagrożenia i map ryzyka powodziowego[59].

Zgodnie z Ustawą Prawo wodne ochrona przed powodzią jest zadaniem organów administracji rządowej oraz samorządowej, a nadzorowana przez Prezesa Krajowego Zarządu Gospodarki Wodnej i prowadzi się ją z uwzględnieniem map zagrożenia powodziowego, map ryzyka powodziowego oraz planów zarządzania ryzykiem powodziowym[60].

Celem wstępnej oceny ryzyka powodziowego jest wyznaczenie obszarów narażonych na niebezpieczeństwo powodzi, czyli obszarów, na których istnieje znaczące ryzyko powodziowe, lub na których wystąpienie dużego ryzyka jest prawdopodobne. Ustawa zawiera także ogólne wytyczne dla sporządzenia map zagrożenia powodziowego, map ryzyka powodziowego, a także planów zarządzania ryzykiem powodziowym.

Szczegółowe wymagania dotyczące opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego w oparciu o powyższą ustawę określa Rozporządzenie Ministra Środowiska, Ministra Transportu, Budownictwa i Gospodarki Morskiej, Ministra Administracji i Cyfryzacji oraz Ministra Spraw Wewnętrznych z 21 grudnia 2012 r.[61]. Mapy ryzyka powodziowego przygotowuje się, biorąc pod uwagę zagrożenie dla ludności oraz potencjalne straty powodziowe i oddzielnie ze względu na użytkowanie terenu oraz obszary i obiekty o szczególnym znaczeniu kulturowym, przyrodniczym i gospodarczym. W rozporządzeniu zamieszczony jest także model matematyczny sposobu obliczania wartości potencjalnych strat powodziowych.

---

56 Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim, Wstęp pkt 11.

57 Tamże, art. 4 ust. 4.

58 Tamże, art. 6 ust. 8.

59 Tamże, art. 7 ust. 5.

60 Art. 88a ustawy z dnia 18 lipca 2001 r. Prawo Wodne (Dz.U. z 2015, poz. 469).

61 Rozporządzenie Ministra Środowiska, Ministra Transportu, Budownictwa i Gospodarki Morskiej, Ministra Administracji i Cyfryzacji oraz Ministra Spraw Wewnętrznych z dnia 21 grudnia 2012 r. w sprawie opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego (Dz.U. z 2013, poz. 104).

Wskazane powyżej krajowe akty prawne z zakresu zarządzania ryzykiem powodziowym uwzględniają wszystkie zobowiązania unijne wynikające z Dyrektywy Powodziowej.

Kolejnym rozwiązaniem, które odwołuje się do pojęcia ryzyka i zarządzania nim, jest kontrola zarządcza, dawniej określana terminem kontroli wewnętrznej czy też finansowej. Obejmuje działania w zakresie zapewnienia realizacji celów i zadań organizacji. W art. 68 ustawy o finansach publicznych sprecyzowano odpowiednim zapisem, iż sposób, w jaki powinno to się odbywać, musi być przede wszystkim zgodny z prawem, ale także cechować się efektywnością, oszczędnością i terminowością realizacji[62].

W rozdziale 6 ustawy zdefiniowano pojęcie kontroli zarządczej, ale także cele, jakie ma zapewniać. Do tych celów zaliczyć należy zapewnienie zgodności prowadzonej działalności z przepisami prawa oraz procedurami wewnętrznymi, skuteczność i efektywność działania, wiarygodność sprawozdań, ochrona zasobów, przestrzeganie i promowanie zasad etycznego postępowania, efektywność i skuteczność przepływu informacji, oraz zarządzanie ryzykiem[63].

W załączniku do Komunikatu nr 6 Ministra Finansów z 6 grudnia 2012 r. czytamy, że zarządzanie ryzykiem to *procedury i polityki oraz skoordynowane działania, podejmowane zarówno przez kierownictwo jednostki, jak i jej pracowników, które poprzez identyfikację i analizę ryzyka oraz określanie adekwatnych reakcji na ryzyko zwiększają prawdopodobieństwo osiągnięcia celów i realizacji zadań*[64]. W związku z czym dostrzega się powiązanie występujące pomiędzy kontrolą zarządczą a zarządzaniem ryzykiem. Jak wynika z ustawy o finansach publicznych zarządzanie ryzykiem stanowi istotny element realizacji celów danej jednostki w systemie kontroli zarządczej. Nie dostrzega się natomiast już powiązania kontroli zarządczej z systemem zarządzania kryzysowego. A przecież zauważyć należy, iż podmiotami odpowiedzialnymi za funkcjonowanie kontroli zarządczej są: wójt, burmistrz, prezydent miasta, przewodniczący zarządu jednostki samorządu terytorialnego[65], wojewoda. Wymienione organy funkcjonują także w ramach systemu zarządzania kryzysowego, a w przypadku takich, jak wójt, prezydent miasta czy wojewoda są w tym obszarze wiodącymi na obszarze przez siebie administrowanym. W ramach kontroli zarządczej są oni zobligowani do delegowania uprawnień z nią związanych na swoich pracowników. Zatem mechanizmy związane z zarządzaniem ryzykiem, wynikające z kontroli zarządczej są szerzej obecne także przy organach występujących w strukturze i uczestniczących w zadaniach z zakresu zarządzania

---

62 Art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2013, poz. 885).

63 Tamże.

64 Komunikat nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (Dz.Urz. MF z 2012, poz. 56).

65 Art. 69 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2013, poz. 885).

kryzysowego. Wiedza ta może zostać z powodzeniem wykorzystana przez kadrę pracowniczą w tym obszarze, ponieważ w ramach swoich kompetencji i obowiązków zawodowych nabywane są umiejętności (identyfikacji, analizy i oceny ryzyka), które mogą zostać wykorzystane na potrzeby realizacji zadań związanych z procesem zarządzania ryzykiem tak w organizacji, jak i w zarządzaniu kryzysowym.

W specyficznej i bardzo newralgicznej dla bezpieczeństwa państwa dziedzinie, jaką jest cyberbezpieczeństwo, zidentyfikowana została potrzeba koordynacji spójnych działań związanych z organizacją na szczeblu kraju w celu zapewnienia przeciwdziałania zagrożeniom w tej dziedzinie funkcjonowania wszystkich istotnych instytucji państwowych. Naprzeciw tym wyzwaniom wyszło Ministerstwo Administracji i Cyfryzacji, opracowując *Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*. Dokument wyznaczył kierunki i standardy działania w obszarze cyberprzestrzeni, a jego wynikiem stała się m.in. metodyka oceny ryzyka do sprawozdania dotyczącego cyberbezpieczeństwa, wykonywanego przez podmioty sektora publicznego.

Opracowana metodyka oceny ryzyka do sprawozdania dotyczącego cyberbezpieczeństwa składa się z czterech zasadniczych etapów: identyfikacja systemów teleinformatycznych, identyfikacja ryzyka, analiza ryzyka oraz ewaluacja. Każdy etap z kolei zawiera szereg kroków do realizacji.

W ramach identyfikacji systemów teleinformatycznych (STI) podmioty zostały zobligowane do wskazania realizowanej funkcji państwa i identyfikacji jego zadań, które jednostka wykonuje. Kolejnym istotnym krokiem jest identyfikacja STI administrowanych przez daną jednostkę i wybór/dobór własnego STI. Powinien się on odbywać w kontekście roli, jaką ma spełniać w jednostce z uwzględnieniem i zinterpretowaniem ewentualnej możliwości jego awarii i wpływu na bezpieczeństwo (analiza procesów krytycznych realizowanych przez system – szczególnie przypisanych służbom i centralnym instytucjom w kraju) państwa i obywateli. Ostatnim krokiem w etapie pierwszym jest zidentyfikowanie wszelkich zasobów niezbędnych do funkcjonowania STI[66]. Wykorzystując terminologię zgodną z normą ISO 31000:2009 *Risk Management – Principles and Guidelines*, można zdefiniować ten etap jako ustanowienie kontekstu funkcjonowania STI.

Na dalszym etapie wykonywana jest już identyfikacja zagrożeń związanych z STI. Można ją przeprowadzić z wykorzystaniem wielu rekomendowanych metod, m.in. tymi najpopularniejszymi ujętymi w normie ISO/IEC 31010:2010 *Risk management – Risk assessment techniques*. Po stworzeniu listy zagrożeń, kolejnym działaniem w ramach etapu jest wybór kluczowych zagrożeń. Dla zidentyfikowanych zagrożeń należy przeprowadzić analizę możliwych skutków (dla czterech kategorii: życia i zdrowia ludzi, finansowe i gospodarcze, dysfunkcja realizacji zadań państwa, utrata zaufania obywateli do władzy publicznej oraz uszkodzenia, znisz-

[66] Metodyka oceny ryzyka do przygotowania sprawozdania za rok 2014, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014 r., s. 1.

czenia lub strata w mieniu, infrastrukturze i środowisku) i prawdopodobieństwa ich wystąpienia. Podczas realizacji etapu analizy ryzyka wykorzystuje się pięciostopniową skalę punktową i ocenia dla zidentyfikowanych zagrożeń: prawdopodobieństwo oraz skutki.

Przy analizie i ocenie ryzyka należy pamiętać, aby zakładać możliwie najgorszy scenariusz wystąpienia zagrożenia[67].

Trzeba także pamiętać, że określając wartość skutku, należy zakładać możliwy, ale najbardziej negatywny scenariusz wystąpienia zagrożenia. W ostatnim kroku etapu analizy ryzyka dokonuje się ustalenia poziomu ryzyka, podstawiając uzyskane punkty skutków i prawdopodobieństwa danego zagrożenia do wzoru:

Poziom ryzyka = skutki x prawdopodobieństwo

Ostatnim etapem w metodyce oceny ryzyka jest ewaluacja, którą wykonuje się

Tabela 1.3. Ewaluacja ryzyka

Kryteria		Ewaluacja ryzyka
Wartość punktowa PR	**Poziom ryzyka**	
1 ÷ 5	Małe	Akceptowalne
6 ÷ 9	Średnie	Akceptowalne, wymagające decyzji co do postępowania z ryzykiem osoby odpowiedzialnej za STI
10 ÷ 16 oraz 5 gdzie P = 1 a S = 5	Duże	Nieakceptowalne, wymagające decyzji osoby odpowiedzialnej za STI w zakresie dalszego postępowania z ryzykiem
18 ÷ 25	Bardzo duże	Nieakceptowalne, wymagające decyzji kierownika jednostki w zakresie dalszego postępowania z ryzykiem

Źródło: Metodyka oceny ryzyka do przygotowania sprawozdania za rok 2014, s. 6

zgodnie z tabelą 1.3. zawartą w dokumencie.

Przejście całego procesu oceny ryzyka doprowadza do etapu postępowania z ryzykiem. Przewidziano w MAiC następujące możliwości: zapobieganie, przeniesienie ryzyka na inną jednostkę, unikanie, tolerowanie (akceptowanie) ryzyka[68]. Ostatnim krokiem w metodyce oceny ryzyka do sprawozdania za rok 2014 jest wypełnienie dokumentu sprawozdania wyłącznie o ryzyka o dużym i bardzo dużym poziomie (tabela 1.4.).

Elementy zarządzania ryzykiem pojawiają się w polskim porządku prawnym bardzo często. Ustawa o zarządzaniu kryzysowym, Prawo wodne czy usta-

[67] Tamże, s. 4.
[68] Tamże, s. 6-7.

Tabela 1.4. Sprawozdanie *(projekt)* podsumowujące wyniki oceny ryzyka za rok 2014 i lata kolejne

Sektor: Publiczny

1. Informacje o ocenie ryzyka

Lp.	Funkcja	Zadanie	KZTI	**Identyfikacja ryzyka**				**Analiza ryzyka**			**Ewaluacja ryzyka**	**Sposób postępowania z ryzykiem przyjęty w jednostce**
				Rodzaj ryzyka	Zdarzenie	Skutek (opis) (S)	Prawdopodobieństwo (opis, w tym podatności) (P)	Ocena (S)	Ocena (P)	Poziom ryzyka = S × P		

2. Proponowane przez jednostkę działania zmniejszające ryzyko, o charakterze systemowym i horyzontalnym: ……
3. Informacje o zmaterializowaniu się ryzyka w roku 2014 o poziomie *Bardzo duże* : ……
4. Informacje dodatkowe: ……..

Źródło: sprawozdanie (projekt) podsumowujące wyniki oceny ryzyka za rok 2014 i lata kolejne, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014

wa o finansach publicznych odwołują się do kategorii ryzyka, jego oceny, czy wprost zarządzania nim. Przegląd tych rozwiązań daje pogląd, jak często w ostatnich czasach państwo polskie zwracało się w kierunku zarządzania ryzykiem, szukając rozwiązania swoich problemów. Już sam ten fakt wskazuje, na ile istotne jest rozpatrywanie zagrożeń w kontekście dyskursu o ryzyku. Jednak to, co budzi niepokój, to fakt, że większość z tych rozwiązań postrzegana jest jako odrębne zadanie, realizowane przez inne podmioty i w oparciu o metodyki, których wyników nie można ze sobą porównać. W kontekście rozważań nad bezpieczeństwem narodowym należy uznać to zjawisko za wysoce dysfunkcjonalne.

2. Kompetencje administracji publicznej w zakresie zarządzania ryzykiem

Administracja publiczna posiada w obszarze bezpieczeństwa szereg zadań, które wynikają z różnorodnych uwarunkowań formalnych. W ramach każdego z nich występują procesy krytyczne, na które należy zwrócić szczególną uwagę, gdyż są one obarczone różnym stopniem ryzyka i ich przerwanie prowadzić może do sytuacji kryzysowej. Dlatego też zarówno dla administracji samorządowej (samorządu gminnego, powiatowego i wojewódzkiego) oraz rządowej (administracji rządowej w województwie oraz działów administracji rządowej) istotne jest, aby na potrzeby zarządzania ryzykiem wprowadzić kategorie procesów krytycznych. Rozważając zdolność administracji publicznej do zarządzania ryzykiem, konieczne jest także zwrócenie uwagi na problemy, na jakie napotyka ona podczas dokonywanej oceny ryzyka oraz określenie jej potrzeby w tym zakresie.

2.1. Przegląd zadań administracji publicznej

Podstawowym zadaniem gminy jest zaspokojenie zbiorowych potrzeb wspólnoty gminnej. Dużą część zadań gminy określa ustawa z 8 marca 1990 r. o samorządzie gminnym[1]. Spośród wskazanych w ustawie, najważniejszymi zadaniami związanymi z bezpieczeństwem są:

1. Nadzór nad gminnymi drogami, ulicami, mostami itd.
2. Organizacja lokalnego transportu oraz ruchu drogowego.
3. Zapewnienie potrzeb w zakresie zaopatrzenia w wodę.
4. Zapewnienie potrzeb w zakresie zaopatrzenia w energię cieplną, elektryczną i gaz.
5. Zapewnienie ochrony zdrowia i świadczeń w tym zakresie.
6. Zapewnienie pomocy społecznej i psychologicznej.
7. Zapewnienie porządku publicznego i bezpieczeństwa obywateli.

Odnosząc się do zaspokajania zbiorowych potrzeb wspólnoty w zakresie gminnych dróg, ulic, mostów, placów oraz organizacji ruchu drogowego, zaznaczyć należy, iż zarządcą drogi w gminie jest organ jednostki samorządu terytorialnego. Zarządcą dróg gminnych jest wójt (burmistrz, prezydent). Do jego obowiązków należą czynności z zakresu planowania, remontu, przebudowy, budowy, utrzymania

[1] Art. 7 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2013, poz. 594).

i ochrony dróg zgodnie z art. 19 i 20 ustawy z 21 marca 1985 r. o drogach publicznych[2].

W zakresie zaspokajania zbiorowych potrzeb wspólnoty w lokalnym transporcie zbiorowym zadania zostały doprecyzowane w usawie o publicznym transporcie drogowym[3]:

- Zgodnie z art. 7 organizatorem transportu zbiorowego jest gmina na linii lub sieci komunikacyjnej w gminnych przewozach pasażerskich.
- W myśl art. 8 do zadań organizatora należy planowanie rozwoju transportu i organizacja publicznego transportu zbiorowego. W kolejnym artykule dodaje się, że gmina licząca co najmniej 50 000 mieszkańców opracowuje tzw. plan transportowy w zakresie linii lub sieci komunikacyjnej w gminnych przewozach pasażerskich. Gmina, której powierzono zadanie organizacji publicznego transportu zbiorowego na mocy porozumienia między gminami (których obszar liczy co najmniej 80 000 mieszkańców) opracowuje plan transportowy w zakresie linii lub sieci komunikacyjnej na określonym obszarze.

Zaspokajanie zbiorowych potrzeb wspólnoty w zakresie wodociągów i zaopatrzenia w wodę, kanalizacji, usuwania i oczyszczania ścieków komunalnych, utrzymania czystości i porządku oraz urządzeń sanitarnych, wysypisk i unieszkodliwiania odpadów komunalnych, zaopatrzenia w energię elektryczną i cieplną oraz gaz, w tym działalności w zakresie telekomunikacji to zadania, które zostały doprecyzowane w ustawie z 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków[4].

Art. 8 ust. 3 ustawy mówi, że przedsiębiorstwo wodociągowo-kanalizacyjne powinno zawiadomić odpowiednie organy (tzn. państwowego powiatowego inspektora sanitarnego, wójta/burmistrza prezydenta miasta oraz odbiorcę usług) o zamiarze odcięcia dostawy wody lub zamknięcia przyłącza kanalizacyjnego oraz o miejscach i sposobie udostępniania zastępczych punktów poboru wody. Powinno to nastąpić co najmniej na 20 dni przed planowanym terminem odcięcia dostaw wody lub zamknięcia przyłącza kanalizacyjnego. Z kolei zgodnie z art. 12 ust. 5 ustawy wójt (burmistrz, prezydent miasta) powinien regularnie informować mieszkańców o jakości wody przeznaczonej do spożycia przez ludzi. W art. 16 ust. 1 wskazano na wymóg uzyskania zezwolenia wydawanego przez wójta (burmistrza, prezydenta miasta), na prowadzenie zbiorowego zaopatrzenia w wodę lub zbiorowego odprowadzania ścieków. Natomiast w art. 19 ust. 1 czytamy, że rada gminy dokonuje analizy projektów regulaminów dostarczania wody i odprowadzania ścieków, które są opracowane przez przedsiębiorstwa wodociągowo-kanalizacyjne. Następnie uchwala regulamin dostarczania wody i odprowadzania ścieków, zwany dalej *regulaminem*. Obowiązuje on na obszarze gminy.

---

2 Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz.U. z 2015, poz. 460).

3 Ustawa z dnia 16 grudnia 2010 r. o publicznym transporcie drogowym (Dz.U z 2011 nr 5, poz. 13).

4 Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz.U. z 2015, poz. 139).

Zadania gminy są także doprecyzowane w Prawie energetycznym[5]. W art. 18 ust. 1 ww. ustawy wskazuje się, że obowiązkiem gminy wynikającym z jej zadań własnych jest planowanie i organizacja zaopatrzenia w energię elektryczną, ciepło i paliwa gazowe na obszarze gminy, a także za planowanie oświetlenia miejsc publicznych oraz finansowanie oświetlenia ulic, placów, dróg na terenie gminy, z wyjątkiem autostrad.

Co więcej z zgodnie z art. 19 wójt (burmistrz, prezydent miasta) opracowuje dla obszaru gminy tzw. projekt założeń do planu zaopatrzenia w ciepło, energię elektryczną i paliwa gazowe. Określa on m.in. zakres współpracy z innymi gminami, ocenę stanu aktualnego i przewidywanych zmian zapotrzebowania na ciepło oraz możliwość wykorzystania istniejących nadwyżek i lokalnych zasobów energii.

Jak już wspomniano w ustawie o samorządzie gminnym w art. 7 ust. 1, określono, że zaspokajanie zbiorowych potrzeb wspólnoty należy do zadań własnych gminy, a w tym ochrona zdrowia. Ochrona zdrowia jest pojęciem szerokim i na gruncie obowiązującego ustawodawstwa nie znajdziemy jego definicji jak też brak jest wskazania przez ustawodawcę istotnych elementów składających się na konstrukcję tego pojęcia. W skład ochrony zdrowia wchodzi podstawowa opieka zdrowotna, która jest również zadaniem publicznym o znaczeniu lokalnym leżącym w gestii samorządu gminnego, mimo że żaden przepis prawa bezpośrednio o tym nie mówi. W myśl art. 5 pkt 27 ustawy z dnia 21 marca 2014 r. o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz niektórych innych ustaw[6] podstawowa opieka zdrowotna to świadczenie zdrowotne profilaktyczne, diagnostyczne, lecznicze, rehabilitacyjne oraz pielęgnacyjne z zakresu medycyny ogólnej, rodzinnej i pediatrii, udzielane w ramach ambulatoryjnej opieki zdrowotnej.[7]

Zgodnie z ustawą z 12 marca 2004 r. o pomocy społecznej gmina zobowiązana jest do wykonywania zadań pomocy społecznej. W związku z tym nie może odmówić pomocy osobie potrzebującej, mimo istniejącego obowiązku osób fizycznych lub osób prawnych do zaspokajania jej niezbędnych potrzeb życiowych[8].

Zgodnie z ustawą o ochronie przeciwpożarowej[9] wójt (burmistrz, prezydent miasta) koordynuje funkcjonowanie krajowego systemu ratowniczo-gaśniczego na obszarze gminy w zakresie ustalonym przez wojewodę. Zadanie to może być wykonywane przy pomocy komendanta gminnego ochrony przeciwpożarowej, jeżeli komendant taki został zatrudniony przez wójta (burmistrza, prezydenta

[5] Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. z 2012, poz. 1059).

[6] Ustawa z dnia 21 marca 2014 r. o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz niektórych innych ustaw (Dz.U. 2014, poz. 1138).

[7] Witryna internetowa http://www.samorzad.lex.pl/czytaj/-/artykul/podstawowa-opieka-zdrowotna-nalezy-do-zadan-wlasnych-gminy z dnia 16.01.2015 r.

[8] Art. 16 pkt 2 ustawy z 12 marca 2004 r. o pomocy społecznej (Dz.U. z 2015, poz. 163).

[9] Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U. z 2009 nr 174, poz. 1380).

miasta), albo przy pomocy komendanta gminnego związku ochotniczych straży pożarnych.

Ustawa o samorządzie powiatowym określa wszelkie kwestie dotyczące funkcjonowania powiatów, wśród których wymienione są również zadania publiczne o charakterze ponadgminnym wymienione poniżej[10]. Wśród nich wyszczególniono zadania związane z zapewnieniem bezpieczeństwa na terenie powiatu.

Powiat wśród wielu zadań własnych wykonuje również działania o charakterze ponadgminnym np. w zakresie promocji i ochrony zdrowia. Szczegółowy zakres kompetencji powiatu w obszarze ochrony zdrowia określają jednak inne ustawy, odnoszące się m.in. do takich zagadnień, jak przeciwdziałanie alkoholizmowi, narkomanii, zwalczanie zagrożeń epidemiologicznych, zapewnienie dostępu do opieki ambulatoryjnej.

W wyniku wprowadzenia w 1999 roku reformy ochrony zdrowia oraz nowego podziału administracyjnego kraju, powiat stał się organem założycielskim[11] dla samodzielnych publicznych zakładów opieki zdrowotnej.

Kolejnym zadaniem powiatu jest realizacja polityki państwa w zakresie pomocy społecznej, do których należy m.in. realizacja zadań wymienionych w ustawie z 12 marca 2004 r. o pomocy społecznej[12]:

- opracowanie i realizacja powiatowej strategii rozwiązywania problemów społecznych, ze szczególnym uwzględnieniem programów pomocy społecznej, wspierania osób niepełnosprawnych i innych, których celem jest integracja osób i rodzin z grup szczególnego ryzyka,
- prowadzenie ośrodków interwencji kryzysowej,
- prowadzenie ośrodka interwencji kryzysowej oraz zorganizowania pomocy w sytuacji kryzysowej.

Ustawa w artykule 20 nakłada na powiaty dodatkowe zadania (poza zadaniami własnymi) z zakresu administracji rządowej:

- pomoc cudzoziemcom, którzy uzyskali w Rzeczypospolitej Polskiej status uchodźcy lub ochronę uzupełniającą, w zakresie indywidualnego programu integracji, oraz opłacanie za te osoby składek na ubezpieczenie zdrowotne określonych w przepisach o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
- prowadzenie i rozwój infrastruktury ośrodków wsparcia dla osób z zaburzeniami psychicznymi,
- realizację zadań wynikających z rządowych programów pomocy społecznej, mających na celu ochronę poziomu życia osób, rodzin i grup społecznych oraz rozwój specjalistycznego wsparcia,
- udzielanie cudzoziemcom pomocy w zakresie interwencji kryzysowej.

---

[10] Art. 4 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz.U. z 2013, poz. 595).

[11] Art. 47 ust. 1 ustawy z dnia 13 października 1998 r. Przepisy wprowadzające ustawy reformujące administrację publiczną (Dz.U. 1998 nr 133, poz. 872).

[12] Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz.U. z 2015, poz. 163).

Powiat wykonuje określone zadania publiczne o charakterze ponadgminnym w zakresie transportu i dróg publicznych. Podobnie jak gmina, powiat może zawierać porozumienia w sprawie powierzenia zadań publicznych z jednostkami lokalnego samorządu terytorialnego, a także z województwem, na którego obszarze znajduje się terytorium powiatu. Zarządca drogi może wykonywać swoje obowiązki przy pomocy rady powiatu.

Do dróg powiatowych zalicza się inne drogi niż drogi krajowe i wojewódzkie stanowiące połączenia miast będących siedzibami powiatów z siedzibami gmin i siedzib gmin między sobą[13].

Do zadań zarządcy drogi[14] należy m.in.:

- opracowywanie projektów planów rozwoju sieci drogowej oraz bieżące informowanie o tych planach organów właściwych do sporządzania miejscowych planów zagospodarowania przestrzennego,
- utrzymanie nawierzchni drogi, chodników, drogowych obiektów inżynierskich, urządzeń zabezpieczających ruch i innych urządzeń związanych z drogą, z wyjątkiem części pasa drogowego,
- realizacja zadań w zakresie inżynierii ruchu,
- przygotowanie infrastruktury drogowej na potrzeby obronne oraz wykonywanie innych zadań na rzecz obronności kraju,
- przeprowadzanie okresowych kontroli stanu dróg i drogowych obiektów inżynierskich oraz przepraw promowych, ze szczególnym uwzględnieniem ich wpływu na stan bezpieczeństwa ruchu drogowego,
- wykonywanie robót interwencyjnych, robót utrzymaniowych i zabezpieczających,
- przeciwdziałanie niszczeniu dróg przez ich użytkowników,
- przeciwdziałanie niekorzystnym przeobrażeniom środowiska mogącym powstać lub powstającym w następstwie budowy lub utrzymania dróg,
- wprowadzanie ograniczeń lub zamykanie dróg i drogowych obiektów inżynierskich dla ruchu oraz wyznaczanie objazdów drogami różnej kategorii, gdy występuje bezpośrednie zagrożenie bezpieczeństwa osób lub mienia.

W samorządach powiatowych za gospodarkę wodną odpowiedzialni są starosta i rada powiatu. Do zadań powiatu w zakresie gospodarki wodnej należy m.in.:

- wydawanie pozwoleń wodnoprawnych na szczególne korzystanie z wód (pobór oraz odprowadzanie wód powierzchniowych lub podziemnych, wprowadzanie ścieków do wód lub do ziemi, piętrzenie i retencjonowanie śródlądowych wód powierzchniowych, korzystanie z wód do celów energetycznych, wydobywanie żwiru i piasku z dna zbiorników wodnych i rzek),
- wydawanie pozwoleń wodnoprawnych na wykonywanie urządzeń wodnych,

[13] Art. 6a ustawy o drogach publicznych z dnia 21 marca 1985 r. (Dz.U. z 2015, poz. 460).
[14] Tamże, art. 20.

- przeprowadzanie rozpraw wodnoprawnych w sprawach wynikających z ustawy Prawo wodne,
- decydowanie o wykonywaniu przez państwowe jednostki organizacyjne koniecznych robót i urządzeń w celu polepszenia stosunków wodnych na gruncie,
- nadzór nad gminnymi spółkami wodnymi[15].

Zadania powiatu z zakresu ochrony środowiska i przyrody można podzielić na zadania z zakresu[16]:

Ochrony środowiska:

- wydawanie decyzji zintegrowanych dla instalacji i przedsięwzięć mogących powodować znaczne zanieczyszczenia poszczególnych elementów przyrodniczych lub środowiska jako całości,
- przeciwdziałanie naruszeniom przepisów ochrony środowiska wynikających z przepisów ochrony środowiska, dla których starosta sprawuje nadzór,
- wydawanie decyzji o sporządzeniu i przedstawieniu przeglądu ekologicznego dla instalacji powodującej negatywne oddziaływanie na środowisko,
- ustalanie sposobu i zakresu działań w celu usunięcia przyczyny szkodliwego oddziaływania na środowisko i przywrócenia środowiska do stanu właściwego,
- przygotowywanie do zatwierdzenia Powiatowego Programu Ochrony Środowiska i Planu Gospodarki Odpadami.

Gospodarki odpadami:

- wydawanie zezwoleń na zbieranie, transport, odzysk i unieszkodliwianie odpadów,
- wydawanie zezwoleń na prowadzenie działalności w zakresie prowadzenia punktu zbierania pojazdów wycofanych z eksploatacji,
- prowadzenie rejestrów posiadaczy odpadów zwolnionych z obowiązku uzyskania zezwoleń na zbieranie, transport, odzysk i unieszkodliwianie odpadów,
- nadzór i monitorowanie miejsc po zlikwidowanych i zrekultywowanych mogilnikach,
- wydawanie decyzji o wyłączeniu wysypisk odpadów z eksploatacji i ich rekultywacji.

Emisji powietrza:

- ustalanie rodzajów i ilości substancji zanieczyszczających dopuszczonych i wprowadzanych do powietrza,
- nakazywanie prowadzenia pomiarów stężeń substancji zanieczyszczających dla instalacji wprowadzających substancje niebezpieczne do powietrza,
- koordynacja i nakładanie obowiązków wynikających z potrzeb ochrony powietrza na podmioty i jednostki organizacyjne,
- prowadzenie rejestrów instalacji, dla których nie jest wymagane pozwolenie na emisję, a które wymagają zgłoszenia.

---

[15] Ustawa z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. z 2005 nr 239, poz. 2019, z późn. zm.).

[16] Witryna internetowa http://www.szydlowiecpowiat.pl/wydzial_rolnictwa_ochrony_srodowiska_gospodarki_wodnej_i_lesnictwa.php z dnia 7.10.2014 r.

Na podstawie ustawy samorząd powiatowy realizuje zadania w zakresie zwierzchnictwa nad powiatowymi służbami, inspekcjami i strażami oraz zadania określone w ustawach w zakresie porządku publicznego i bezpieczeństwa obywateli.[17] Do ww. zadań należy m.in.:

- ocena zagrożeń porządku publicznego i bezpieczeństwa obywateli na terenie powiatu,
- przygotowywanie projektu powiatowego programu zapobiegania przestępczości oraz porządku publicznego i bezpieczeństwa obywateli,
- opiniowanie projektów innych programów współdziałania Policji i innych powiatowych służb, inspekcji i straży oraz jednostek organizacyjnych wykonujących na terenie powiatu zadania z zakresu porządku publicznego i bezpieczeństwa obywateli,
- opiniowanie projektów aktów prawa miejscowego i innych dokumentów w sprawach związanych z wykonywaniem zadań z zakresu porządku publicznego i bezpieczeństwa obywateli,
- opiniowanie, zleconych przez starostę, innych zagadnień dotyczących porządku publicznego i bezpieczeństwa obywateli.

Do zadań samorządu powiatowego w zakresie ochrony przeciwpożarowej i przeciwpowodziowej należy:

- opracowywanie planu operacyjnego ochrony przed powodzią oraz ogłaszanie i odwoływanie pogotowia i alarmu przeciwpowodziowego,
- zabezpieczenie ochrony:
  - przeciwpowodziowej, w tym wyposażenie i utrzymanie powiatowego magazynu przeciwpowodziowego,
  - przeciwpożarowej oraz zapobieganie innym nadzwyczajnym zagrożeniom życia i zdrowia ludzi oraz środowiska,
- prowadzenie analiz i opracowywanie prognoz dotyczących pożarów, klęsk żywiołowych oraz innych miejscowych zagrożeń,
- określenie zadań krajowego systemu ratowniczo-gaśniczego na obszarze powiatu, koordynowanie jego funkcjonowania i kontrolowanie wykonywania tych zadań, a także w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia lub środowiska kierowanie tym systemem,
- prowadzenie analizy sił i środków krajowego systemu ratowniczo-gaśniczego na obszarze powiatu,
- udział w przygotowaniu materiałów dot. dokonywania przez radę powiatu oceny stanu bezpieczeństwa przeciwpożarowego i zabezpieczenia przeciwpowodziowego powiatu.

Do podstawowego zakresu działania powiatu w zakresie obronności, obrony cywilnej i zarządzania kryzysowego należą:

[17] Art. 38a ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. z 2013, poz. 595).

W zakresie obronności:
- powoływanie do wykonania obowiązku świadczeń osobistych i rzeczowych,
- opracowywanie planów i programów szkolenia obronnego, a także organizowanie szkolenia,
- opracowywanie, uzgadnianie i przedkładanie do akceptacji planu operacyjnego funkcjonowania powiatu, a także stosownych programów obronnych,
- opracowanie i uaktualnianie planu przygotowań służby zdrowia w powiecie na potrzeby obronne,
- realizowanie przedsięwzięć związanych z przygotowaniem Stanowiska Kierowania Starosty, zapewniającego realizację zadań obronnych w wyższych stanach gotowości obronnej państwa,
- prowadzenie spraw związanych z reklamowaniem żołnierzy rezerwy od obowiązku pełnienia czynnej służby wojskowej w czasie ogłoszenia mobilizacji i wojny.

W zakresie obrony cywilnej:
- dokonywanie oceny stanu przygotowań formacji obrony cywilnej,
- opracowywanie planów obrony cywilnej,
- uzgadnianie planów obrony cywilnej miast, gmin,
- organizowanie szkolenia ludności w zakresie obrony cywilnej,
- przygotowanie i zapewnienie działania systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania o zagrożeniach,
- przygotowywanie i organizowanie ewakuacji ludności na wypadek powstania masowego zagrożenia dla życia i zdrowia na znacznym obszarze,
- planowanie i zapewnienie środków transportowych, pomocy medycznej i społecznej dla ewakuowanej ludności,
- planowanie i zapewnienie ochrony oraz ewakuacji dóbr kultury,
- zapewnienie dostaw wody pitnej dla ludności i wyznaczonych zakładów przemysłu spożywczego oraz wody dla urządzeń specjalnych do likwidacji skażeń i do celów przeciwpożarowych,
- zapewnienie odpowiednich warunków przechowywania, konserwacji, eksploatacji, remontu i wymiany sprzętu obrony cywilnej,

W zakresie zarządzania kryzysowego:
- prowadzenie spraw związanych z tworzeniem i funkcjonowaniem na terenie powiatu systemu zarządzania kryzysowego,
- kierowanie działaniami związanymi z monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie powiatu,
- opracowywanie i przedkładanie wojewodzie do zatwierdzenia powiatowego planu reagowania kryzysowego,
- realizacja zaleceń do powiatowych planów reagowania kryzysowego,
- zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu reagowania na potencjalne zagrożenia,
- ustalanie procedur w zakresie zarządzania kryzysowego,
- przeciwdziałanie skutkom zdarzeń o charakterze terrorystycznym,

- gromadzenie i przetwarzanie informacji dotyczących infrastruktury krytycznej,
- opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej.

Podstawowym zadaniem samorządu województwa jest zaspokojenie zbiorowych potrzeb wspólnoty regionalnej. Do zakresu działania samorządu województwa należy w głównej mierze wykonywanie zadań publicznych o charakterze wojewódzkim, niezastrzeżonych ustawami na rzecz organów administracji rządowej[18].

Zadania własne województwa możemy podzielić zasadniczo na 17 grup. Wśród zadań własnych określonych przez ustawę o samorządzie województw znajdujemy zadania z zakresu:

1) edukacji publicznej, w tym szkolnictwa wyższego,
2) promocji i ochrony zdrowia,
3) kultury oraz ochrony zabytków i opieki nad zabytkami,
4) pomocy społecznej,
5) wspierania rodziny i systemu pieczy zastępczej, w tym polityki prorodzinnej,
6) modernizacji terenów wiejskich,
7) zagospodarowania przestrzennego,
8) ochrony środowiska,
9) gospodarki wodnej, w tym ochrony przeciwpowodziowej, a w szczególności wyposażenia i utrzymania wojewódzkich magazynów przeciwpowodziowych,
10) transportu zbiorowego i dróg publicznych,
11) kultury fizycznej i turystyki,
12) ochrony praw konsumentów,
13) obronności,
14) bezpieczeństwa publicznego,
15) przeciwdziałania bezrobociu i aktywizacji lokalnego rynku pracy,
16) działalności w zakresie telekomunikacji,
17) ochrony roszczeń pracowniczych w razie niewypłacalności pracodawcy.

Sejmik województwa w uzgodnieniu z ministrem do spraw szkolnictwa wyższego może wnioskować o stworzenie publicznej uczelni zawodowej, jej zamknięcie, zmianę jej nazewnictwa lub związanie jej z inną uczelnią. Tworzenie oraz utrzymywanie działania publicznych zakładów kształcenia, jak również placówek podnoszących kwalifikacje nauczycieli, bibliotek, szkół oraz placówek specjalnych oraz sportowych, które mają status regionalnych lub ponadregionalnych, znajduje się w zakresie zadań samorządu województwa.

Zgodnie z art. 14 ust. 1 pkt 2 ustawy o samorządzie województwa, samorząd ten prowadzi zadania, które mają zasięg wojewódzki, określone ustawami, w szczególności w zakresie promocji i ochrony zdrowia.

---

[18] Art. 2 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie województwa (Dz.U. z 2013, poz. 596).

Kompetencje samorządu województwa w zakresie ochrony zdrowia określone zostały jednak w innych ustawach, które odwołują się do zagadnień związanych z przeciwdziałaniem alkoholizmowi, narkomanii, zwalczaniem zagrożeń epidemiologicznych, zapewnieniem dostępu do opieki ambulatoryjnej.

Zadania samorządu województwa w obszarze ochrony zdrowia wynikają z pełnienia funkcji organu założycielskiego dla samodzielnych publicznych zakładów opieki zdrowotnej (dotyczące pełnienia funkcji właścicielskich).

W 1999 r. na skutek przemian w naszym kraju, które były związane z wprowadzeniem nowego podziału administracyjnego oraz reformą zdrowia, samorząd wojewódzki został określony mianem organu założycielskiego dla publicznych zakładów opieki zdrowotnej[19, 20].

Wśród uprawnień właścicielskich można wymienić m.in.:

- *możliwość tworzenia, przekształcenia i likwidacji publicznego zakładu opieki zdrowotnej,*
- *nadawanie statutu zakładowi opieki zdrowotnej,*
- *nawiązywanie z kierownikiem zakładu stosunku pracy,*
- *delegowanie przedstawiciela do rady społecznej zakładu,*
- *nadzór nad zakładami opieki zdrowotnej zgodnie z rozporządzeniem z dnia 18 listopada 1999 r. W sprawie szczegółowych zasad sprawowania nadzoru nad samodzielnymi publicznymi zakładami opieki zdrowotnej i nad jednostkami transportu sanitarnego*[21].

Do zadań województwa w obszarze promocji i ochrony zdrowia należy również:

- tworzenie i utrzymywanie wojewódzkich ośrodków medycyny pracy,
- prowadzenie zakładów psychiatrycznej opieki zdrowotnej oraz udział w realizacji zadań z zakresu ochrony zdrowia psychicznego,
- prowadzenie profilaktyki i rozwiązań związanych z problemami alkoholowymi,
- udział w realizacji zadań z zakresu ochrony przed następstwami używania tytoniu.

W województwie można wyodrębnić dwie niezależne struktury organizacyjne administracji rządowej i samorządowej. Za wykonywanie zadań rządowych na poziomie województwa odpowiedzialny jest wojewoda, a jego zadania w obszarze pomocy społecznej wykonywane są przez wydziały polityki społecznej znajdujące się w urzędach wojewódzkich. Za wykonywanie zadań samorządowych na poziomie województwa odpowiedzialny jest marszałek województwa, a jego zadania w obszarze pomocy społecznej wykonywane są przez odpowiednie jednostki, które zostały powołane do wykonywania zadań związanych z pomocą społeczną w województwach.

---

[19] Art. 47 ust. 1 ustawy z dnia 13 października 1998 r. Przepisy wprowadzające ustawy reformujące administrację publiczną (Dz.U. 1998 nr 133, poz. 872).

[20] Rozporządzenia Prezesa Rady Ministrów z dnia 22 czerwca 2001 r. w sprawie wykazu samodzielnych publicznych zakładów opieki zdrowotnej, które zostały przejęte przez gminy, powiaty i samorządy województw (Dz.U. 2001 nr 65, poz. 659).

[21] Witryna internetowa http://www2.mz.gov.pl z dnia 18.03.2014 r.

W ramach modernizacji terenów wiejskich władze województwa odpowiedzialne są za:
- rozwój infrastruktury,
- wspieranie rozwoju sektora prywatnego,
- walkę z bezrobociem,
- wspieranie i rozwój systemu edukacji,
- odnowę wsi oraz przestrzeni wiejskiej.

Za ochronę środowiska na poziomie województwa odpowiedzialne są Wojewódzkie Inspektoraty Ochrony Środowiska (WIOŚ). Do zadań WIOŚ należy m.in.:
- kontrola przestrzegania przepisów o ochronie środowiska i racjonalnym użytkowaniu zasobów przyrody,
- kontrola eksploatacji instalacji i urządzeń chroniących środowisko przed zanieczyszczeniem,
- kontrola przestrzegania decyzji ustalających warunki użytkowania środowiska,
- udział w postępowaniu dotyczącym lokalizacji inwestycji,
- udział w przekazywaniu do użytku obiektów lub instalacji realizowanych jako przedsięwzięcie mogące znacząco oddziaływać na środowisko,
- współdziałanie w zakresie ochrony środowiska z innymi organami kontrolnymi, organami ścigania i wymiaru sprawiedliwości oraz organami administracji państwowej i rządowej, samorządu terytorialnego i obrony cywilnej, a także organizacjami społecznymi i opiekunami społecznymi,
- realizowanie zadań państwowego monitoringu środowiska określonych przez Głównego Inspektora Ochrony Środowiska, organizowanie i koordynowanie wojewódzkiego monitoringu środowiska, prowadzenie badań jakości środowiska, obserwacji i oceny jego stanu oraz zachodzących w nim zmian,
- opracowywanie i wdrażanie metod analityczno-badawczych i kontrolno-pomiarowych,
- kontrola podmiotów, których działalność może stanowić przyczynę powstania poważnej awarii,
- badanie przyczyn powstawania oraz sposobów likwidacji skutków poważnych awarii dla środowiska,
- inicjowanie działań tworzących warunki zapobiegania poważnym awariom oraz usuwania ich skutków i przywracania środowiska do stanu właściwego,
- kontrola przestrzegania przepisów o opakowaniach i odpadach opakowaniowych,
- kontrola przestrzegania przepisów o obowiązkach przedsiębiorców w zakresie gospodarowania niektórymi odpadami oraz o opłacie produktowej i opłacie depozytowej,
- kontrola przestrzegania przepisów i uzyskanych na ich podstawie zezwoleń, z wyłączeniem kontroli laboratoryjnej, w zakresie postępowania z organizmami genetycznie zmodyfikowanymi,
- kontrola gospodarowania wodami w zakresie określonym w ustawie z dnia 18 lipca 2001 r. Prawo wodne,

- kontrola przestrzegania przepisów o postępowaniu z substancjami zubożającymi warstwę ozonową,
- kontrola przestrzegania przepisów o odpadach,
- kontrola przestrzegania przepisów w zakresie ustawy o substancjach i preparatach chemicznych,
- kontrola środków transportu,
- prowadzenie wykazów publicznie dostępnych dokumentów,
- informowanie społeczeństwa o stanie środowiska,
- udostępnianie organom administracji rządowej oraz organom samorządu terytorialnego wyników badań i obserwacji oraz ocen stanu środowiska na obszarze województwa objętych państwowym monitoringiem środowiska,
- wykonywanie innych zadań wynikających z obowiązujących przepisów prawa[22].

Zgodnie z art. 88a ust. 1 Ustawy Prawo wodne[23], ochrona przed powodzią należy do zadań organów administracji rządowej i samorządowej. Na podstawie tej ustawy oraz ustawy o samorządzie województwa województwo ma za zadanie:

- opracowywanie planu operacyjnego ochrony przed powodzią oraz ogłaszanie i odwoływanie pogotowia i alarmu przeciwpowodziowego,
- zabezpieczenie ochrony:
  - przeciwpowodziowej, w tym wyposażenie i utrzymanie wojewódzkiego magazynu przeciwpowodziowego,
  - przeciwpożarowej oraz zapobieganie innym nadzwyczajnym zagrożeniom życia i zdrowia ludzi oraz środowiska,
- określenie zadań krajowego systemu ratowniczo-gaśniczego na obszarze województwa,
- prowadzenie analizy sił i środków krajowego systemu ratowniczo-gaśniczego na obszarze województwa.

Wojewoda pełni funkcję reprezentanta Rady Ministrów w terenie (odpowiada za wykonywanie polityki rządu). Powierzono mu również zwierzchnictwo nad kierownictwem służb i inspekcji oraz innych jednostek organizacyjnych w województwie, wykonujących zadania z zakresu bezpieczeństwa. Wojewoda odpowiada za wykonywanie polityki rządu w województwie, a w szczególności:

- zapewnia współdziałanie wszystkich organów administracji rządowej i samorządowej działających w województwie i kieruje ich działalnością w zakresie zapobiegania zagrożeniu życia, zdrowia lub mienia oraz zagrożeniom środowiska, bezpieczeństwa państwa i utrzymania porządku publicznego, ochrony praw obywatelskich, a także zapobiegania klęskom żywiołowym i innym nadzwyczajnym zagrożeniom oraz zwalczania i usuwania ich skutków,
- dokonuje oceny stanu zabezpieczenia przeciwpowodziowego województwa, opracowuje plan operacyjny ochrony przed powodzią oraz ogłasza i odwołuje pogotowie i alarm przeciwpowodziowy,

[22] Witryna internetowa http://www.wios.szczecin.pl/bip/chapter_16037.asp z dnia 22.02.2015 r.
[23] Ustawa z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. z 2015, poz. 469).

- wykonuje i koordynuje zadania w zakresie obronności i bezpieczeństwa państwa oraz zarządzania kryzysowego.

Ustawa z 5 czerwca 1998 r. uczyniła wojewodę, obok organów administracji niezespolonej, najważniejszym organem administracji rządowej w województwie. Wspomniana ustawa określa również uprawnienia wojewody do wydawania poleceń w sytuacjach nadzwyczajnych, które obowiązują zarówno organy administracji rządowej, jak i samorząd terytorialny. Ponadto wojewoda jest organem właściwym w sprawach zarządzania kryzysowego na terenie województwa, które wykonuje przy pomocy urzędu wojewódzkiego oraz zespolonych służb, inspekcji i straży.

Do jego zadań w sprawach zarządzania kryzysowego należy:

1) kierowanie działaniami związanymi z monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa,
2) realizacja zadań z zakresu planowania cywilnego, w tym:
   - wydawanie starostom zaleceń do powiatowych planów reagowania kryzysowego,
   - zatwierdzanie powiatowych planów reagowania kryzysowego,
   - przygotowywanie i przedkładanie do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej wojewódzkiego planu zarządzania kryzysowego,
   - realizacja wytycznych do wojewódzkich planów zarządzania kryzysowego,
3) zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego,
4) wnioskowanie o użycie pododdziałów lub oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej,
5) wykonywanie przedsięwzięć wynikających z dokumentów planistycznych wykonywanych w ramach planowania operacyjnego realizowanego w województwie,
6) zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym,
7) współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym,
8) organizacja wykonywania zadań z zakresu ochrony infrastruktury krytycznej.

Powyższe zadania z zakresu zarządzania kryzysowego wojewoda wykonuje przy pomocy urzędu wojewódzkiego oraz zespolonych służb, inspekcji i straży.

W zakresie zarządzania kryzysowego województwo odpowiedzialne jest także za:

1) zapewnienie współdziałania wszystkich jednostek organizacyjnych administracji rządowej i samorządowej z terenu województwa w zakresie zapobiegania zagrożeniu mienia oraz zagrożeniom środowiska, bezpieczeństwa państwa i utrzymania porządku publicznego, ochrony praw obywatelskich, a także zapobiegania klęskom żywiołowym i innym nadzwyczajnym zagro-

żeniom oraz zwalczania i usuwania ich skutków na zasadach określonych w ustawach,
2) gromadzenie i przetwarzanie danych oraz ocena i prognozowanie rozwoju zagrożeń występujących na obszarze województwa,
3) współpracę z powiatowymi zespołami zarządzania kryzysowego,
4) zapewnienie funkcjonowania Wojewódzkiego Zespołu Zarządzania Kryzysowego, w tym dokumentowanie jego prac,
5) realizację zadań stałego dyżuru w ramach gotowości obronnej państwa,
6) planowanie wsparcia innych organów właściwych w sprawach zarządzania kryzysowego,
7) planowanie wsparcia przez organy administracji publicznej realizacji zadań Sił Zbrojnych Rzeczypospolitej Polskiej,
8) współpracę z właściwymi ministrami odpowiedzialnymi za zadania związane z przeciwdziałaniem i usuwaniem skutków klęsk żywiołowych oraz zdarzeń noszących znamiona klęsk żywiołowych,
9) przekazywanie, za pośrednictwem rzecznika prasowego wojewody, do środków masowego przekazu, komunikatów i ostrzeżeń, w celu zapobieżenia zagrożeniom i skutkom klęski żywiołowej,
10) współpracę z podmiotami realizującymi monitoring środowiska,
11) współdziałanie z podmiotami prowadzącymi akcje ratownicze i humanitarne,
12) opracowywanie i aktualizacja wojewódzkiego planu postępowania awaryjnego na wypadek zdarzeń radiacyjnych, a także planu dystrybucji preparatów jodowych na terenie województwa, na wypadek wystąpienia zagrożenia radiacyjnego,
13) realizację zadań z zakresu ochrony infrastruktury krytycznej, w tym związanych z wykazem infrastruktury krytycznej znajdującej się na terenie województwa, objętej planem zarządzania kryzysowego,
14) nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,
15) rozpatrywanie decyzji wydanych przez organy I instancji w sprawach zgromadzeń,
16) prowadzenie stałego całodobowego dyżuru operacyjnego w Wojewódzkim Centrum Zarządzania Kryzysowego[24].

Zgodnie z art. 20 ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej[25] w zakresie obronności, wojewoda kieruje sprawami obronności w województwie oraz w ramach kierowania, wykonuje zadania w zakresie i na zasadach określonych w ustawach, a w szczególności:

- określa szczegółowe kierunki działania dla kierowników zespolonych służb, inspekcji i straży, organów administracji niezespolonej oraz jednostek samorządu terytorialnego w zakresie realizacji zadań obronnych,

[24] Witryna internetowa www.mazowieckie.pl.z dnia 7.02.2015 r.
[25] Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2015, poz. 827).

- kieruje realizacją przedsięwzięć związanych z podwyższaniem gotowości obronnej państwa wykonywanych przez marszałków województw, starostów, wójtów lub burmistrzów (prezydentów miast), przedsiębiorców oraz inne jednostki organizacyjne i organizacje społeczne mające swoją siedzibę na terenie województwa,
- koordynuje przedsięwzięcia niezbędne do zabezpieczenia mobilizacji jednostek wojskowych i wykonywania świadczeń na rzecz obrony,
- kieruje realizacją przedsięwzięć związanych z przygotowaniem stanowisk kierowania dla organów terenowych,
- organizuje wykorzystanie miejscowych sił i środków na potrzeby obronności państwa i obszaru województwa, w tym ochrony ludności oraz dóbr materialnych i kultury przed środkami rażenia, jak również niesienia pomocy poszkodowanym,
- kontroluje i ocenia wykonywanie zadań obronnych przez organy, podmioty, jednostki organizacyjne i organizacje,
- organizuje edukację społeczeństwa dotyczącą przygotowania obronnego oraz prowadzi szkolenia i ćwiczenia obronne.

Jak już wspomniano, na poziomie województwa szefem obrony cywilnej jest wojewoda, który nadzoruje tworzenie odpowiedniego planu, i w przypadku wystąpienia zagrożenia prowadzi działania ratownicze na poziomie województwa. W zakresie obrony cywilnej wojewoda jest zobowiązany do stworzenia planu obrony cywilnej. Jest to dokument, który posiada największe znaczenie dla władz cywilnych w przypadku wystąpienia zagrożeń zewnętrznych państwa.

Zakres zadań realizowanych przez ministrów określa natomiast ustawa o działach administracji rządowej. Zadania te są uszczegółowione w innych aktach prawnych regulujących kolejne obszary aktywności państwa. Poniżej dla wybranych działów administracji rządowej wskazano najważniejsze zadania realizowane na rzecz lub powiązane właśnie z szeroko pojmowanym bezpieczeństwem państwa[26].

Dla działu sprawy wewnętrzne zidentyfikowano sześć zadań z zakresu zarządzania kryzysowego:

- przeciwdziałanie zagrożeniom ludzi, ich mieniu i środowisku spowodowanym: zakłóceniem bezpieczeństwa i porządku publicznego, naruszeniem bezpieczeństwa powszechnego, katastrofą naturalną lub awarią techniczną,
- przeciwdziałanie nielegalnemu przemieszczaniu się osób i towarów przez granice RP,
- zapewnienie bezpieczeństwa osobom, obiektom i urządzeniom podlegającym ochronie oraz wskazanym obiektom infrastruktury krytycznej,
- zabezpieczenie systemów i sieci teleinformatycznych oraz baz danych,
- zabezpieczenie funkcjonowania ośrodków dla cudzoziemców i przeciwdziałanie negatywnym oddziaływaniom znajdujących się tam osób na poziom bezpieczeństwa,

[26] Zadania przygotowane zostały w oparciu o Krajowy Plan Zarządzania Kryzysowego.

- koordynowanie przygotowania wojewodów do wykonywania zadań zarządzania kryzysowego oraz koordynacja wykonania zadań z zakresu obrony cywilnej w kraju.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie bezpieczeństwa powszechnego i porządku publicznego.

Do zadań działów administracja publiczna i łączność należy:

- organizacja świadczeń przez operatorów usług telekomunikacyjnych i pocztowych w warunkach szczególnych zagrożeń,
- zapewnienie bezpieczeństwa infrastruktury telekomunikacyjnej.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie funkcjonowania telekomunikacyjnej i pocztowej infrastruktury krytycznej oraz ciągłości świadczenia usług telekomunikacyjnych i pocztowych.

Zadaniami z zakresu zarządzania kryzysowego dla działu zdrowie są:

- zapewnienie bezpieczeństwa sanitarno-epidemiologicznego w kraju,
- nadzór nad państwowym ratownictwem medycznym,
- organizacja działań systemu opieki zdrowotnej w warunkach epidemii,
- przygotowanie placówek ochrony zdrowia oraz sił i środków do zapewnienia opieki medycznej w warunkach sytuacji kryzysowych,
- zapewnienie bezpieczeństwa zdrowia i życia obywateli przy stosowaniu produktów leczniczych i wyrobów medycznych.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie ciągłości funkcjonowania opieki zdrowotnej.

Zadaniami z zakresu zarządzania kryzysowego działu środowisko są:

- monitorowanie zagrożeń środowiska, w tym zagrożeń transgranicznych,
- przeciwdziałanie zagrożeniom środowiska spowodowanym działalnością człowieka,
- przeciwdziałanie zagrożeniom bezpieczeństwa ludzi i środowiska w zakresie organizmów genetycznie zmodyfikowanych,
- ocena sytuacji radiacyjnej kraju,
- działania wspierające w zakresie identyfikacji oraz oceny skutków zdarzenia radiacyjnego,
- realizacja przedsięwzięć inwestycyjnych, organizacyjnych i planistycznych w celu właściwego gospodarowania wodami oraz ochrony przed powodzią i przeciwdziałania skutkom suszy.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać przeciwdziałanie zagrożeniom dla ludzi, ich mienia i środowiska spowodowanym katastrofami naturalnymi i zdarzeniami radiacyjnymi.

Zadania działu budownictwo, lokalne planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo z zakresu zarządzania kryzysowego to:

- zachowanie bezpieczeństwa przy budowie i eksploatacji obiektów użyteczności publicznej,
- zgłaszanie propozycji rozwiązań prawnych dotyczących zachowania bezpieczeństwa w trakcie budowy i użytkowania obiektów użyteczności publicznej.

Zadania z zakresu zarządzania kryzysowego działu gospodarka morska to:
- przeciwdziałanie zagrożeniom środowiska na morzu i wodach śródlądowych,
- opracowanie i zarządzanie systemem poszukiwania i ratownictwa morskiego,
- ochrona portów morskich i żeglugi morskiej, w tym wykonywanie zadań obronnych oraz zadań o charakterze niemilitarnym, w szczególności zapobieganie aktom terroru.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie funkcjonowania transportu morskiego, w tym na potrzeby Sił Zbrojnych RP i służb.

Zadania działu transport z zakresu zarządzania kryzysowego to:
- zapewnienie bezpieczeństwa w ruchu drogowym, kolejowym i lotniczym,
- zapewnienie bezpieczeństwa infrastruktury drogowej kolejowej i lotniskowej.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać:
- zarządzanie ruchem na drogach krajowych na potrzeby zabezpieczenia funkcjonowania transportu drogowego,
- zapewnienie funkcjonowania publicznego transportu zbiorowego na linii komunikacyjnej albo sieci komunikacyjnej w międzywojewódzkich i międzynarodowych przewozach pasażerskich w transporcie kolejowym na potrzeby Sił Zbrojnych i służb.

Do zadań działów rolnictwo i rozwój wsi z zakresu zarządzania kryzysowego należy:
- monitoring i przeciwdziałanie wystąpieniom chorób roślin,
- przeciwdziałanie zagrożeniom dla zdrowia ludzi, spowodowanym spożyciem żywności pochodzenia zwierzęcego o niewłaściwej jakości zdrowotnej,
- przeciwdziałanie naruszeniu równowagi na rynku rolnym lub w poszczególnych jego segmentach,
- zapewnienie funkcjonowania Systemu Monitoringu Suszy Rolniczej oraz zabezpieczenie baz danych KRUS.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać:
- zapewnienie ciągłości produkcji rolno-hodowlanej,
- zapewnienie właściwej, jakości zdrowotnej żywności pochodzenia zwierzęcego,
- zapewnienie ciągłości zaopatrzenia w produkty rolno-spożywcze.

Do zadań działu obrona narodowa należy:
- przygotowanie potencjału Sił Zbrojnych do działania w przypadku zewnętrznych zagrożeń bezpieczeństwa państwa,
- przygotowanie wydzielonych komponentów Sił Zbrojnych do wsparcia działań innych służb w warunkach sytuacji kryzysowych.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie nienaruszalności terytorialnej Rzeczypospolitej Polskiej i wsparcie działań innych organów w przypadku wystąpienia zagrożeń pozamilitarnych.

Zadania działów praca i zabezpieczenie społeczne w zakresie zarządzania kryzysowego obejmują:

- przeciwdziałanie negatywnym zjawiskom na rynku pracy, w celu zminimalizowania wystąpienia niepokojów społecznych, przede wszystkim poprzez skierowanie w rejony kryzysowe środków Funduszu Pracy będących w rezerwie Ministra Pracy i Polityki Społecznej na szybkie zwiększenie możliwości dodatkowego aktywizowania osób bezrobotnych na tych terenach,
- zabezpieczenie w FGŚP (Fundusz Gwarantowanych Świadczeń Pracowniczych) środków na dodatkowe wypłaty świadczeń wynikające ze zdarzeń losowych,
- przeciwdziałanie pogłębianiu się ubóstwa wśród rodzin z dziećmi na utrzymaniu w razie zaistnienia sytuacji kryzysowej poprzez wypłatę świadczeń obligatoryjnych, a w razie potrzeby przygotowanie szczególnych rozwiązań legislacyjnych,
- zabezpieczenie baz danych ZUS, zabezpieczenie systemów informatycznych FGŚP.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie ciągłości funkcjonowania systemu pomocy społecznej oraz zapewnienie w pierwszej kolejności wypłat świadczeń obligatoryjnych.

Zadania działu gospodarka z zakresu zarządzania kryzysowego to przeciwdziałanie zagrożeniom w funkcjonowaniu systemów energetycznych oraz utrzymywanie rezerw strategicznych.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie dostaw energii elektrycznej, paliw i gazu.

Zadaniami działów finanse publiczne i budżet z zakresu zarządzania kryzysowego są:

- przeciwdziałanie zagrożeniom związanym z praniem pieniędzy i finansowaniem terroryzmu,
- zapewnienie płynnego zaopatrywania w środki finansowe obywateli i instytucji publicznych,
- planowanie środków finansowych na potrzeby ofiar sytuacji kryzysowych i pokrycie dodatkowych kosztów działań służb,
- podjęcie decyzji o zwiększeniu wydatków z rezerwy ogólnej budżetu państwa na działania związane z usuwaniem skutków zaistniałej sytuacji kryzysowej na wniosek właściwego ministra lub innego dysponenta części budżetowej,
- przeciwdziałanie nielegalnemu wwozowi/wywozowi towarów przez granice RP, w tym materiałów niebezpiecznych, broni, amunicji, materiałów wybuchowych oraz towarów i technologii o znaczeniu strategicznym.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie płynnego zaopatrywania w środki finansowe.

Do zadań działu Skarb Państwa z zakresu zarządzania kryzysowego należy:

- zapewnienie racjonalnego wykorzystania zasobów majątku państwowego dla zapewnienia prawidłowego funkcjonowania gospodarki narodowej,
- zapewnienie bezpieczeństwa infrastruktury wskazanych obiektów i systemów będących w zasobach majątku państwowego poprzez nadzór właścicielski nad infrastrukturą służącą do wytwarzania/dystrybucji energii elektrycznej, jak również produkcji, wydobycia, rafinacji, przetwarzania, magazynowania, przesyła-

nia paliw gazowych gazociągami oraz terminalami skroplonego gazu ziemnego (LNG).

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie funkcjonowania, ciągłości działania oraz integralności mienia Skarbu Państwa.

Do zadań działu oświata i wychowanie z zakresu zarządzania kryzysowego należy:

- upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń i sytuacji nadzwyczajnych,
- realizacja programów edukacyjnych z zakresu bezpieczeństwa i zachowania się w sytuacjach kryzysowych,
- opracowywanie i wdrażanie programów pomocy dla dzieci i młodzieży, udzielanie pomocy psychologiczno-pedagogicznej w szkołach i placówkach,
- opracowywanie i wdrażanie rozwiązań prawno-organizacyjnych dotyczących funkcjonowania systemu oświaty w warunkach sytuacji kryzysowych (stanów nadzwyczajnych).

Zadaniem ministra właściwego w sprawach działu jest również rozpatrywanie wniosków o zwiększenie części oświatowej subwencji ogólnej na dofinansowanie likwidacji szkód w obiektach oświatowych spowodowanych zdarzeniami wywołanymi przez żywioły.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie ciągłości funkcjonowania systemu oświaty.

Do zadań działów nauka i szkolnictwo wyższe z zakresu zarządzania kryzysowego należy:

- wdrożenie rozwiązania systemowego w zakresie organizacji i funkcjonowania uczelni i jednostek naukowych, finansowania nauki, w sytuacji kryzysowej,
- po wprowadzeniu stanu nadzwyczajnego oraz zarządzanie realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie ciągłości finansowania badań naukowych i prac rozwojowych.

Zadania działu kultura i dziedzictwo narodowe z zakresu zarządzania kryzysowego obejmują:

- zabezpieczenie dóbr kultury i archiwów państwowych przed skutkami zagrożeń (w tym zagrożeń militarnych),
- finansowanie ochrony dziedzictwa narodowego, działalności kulturalnej oraz wyższego szkolnictwa artystycznego,
- rozpatrywanie wniosków o dofinansowanie likwidacji szkód spowodowanych przez powódź, skażenia chemiczne, silne mrozy, huragany w dziedzictwie narodowym.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zabezpieczenie dóbr kultury i archiwów państwowych przed skutkami zagrożeń.

Do zadań działu rozwój regionalny należy:

- utrzymanie dopływu funduszy europejskich oraz w ramach mechanizmów finansowych na realizację rozpoczętych i planowanych inwestycji,

- utrzymanie finansowania projektów z budżetu państwa lub środków własnych beneficjentów,
- zapewnienie stałego dostępu do usługi wszystkim użytkownikom KSI SIMIK (System Informatyczny Monitoringu i Kontroli Finansowej Funduszy Strukturalnych i Funduszu Spójności) oraz sprawnego i niezakłóconego działania systemu,
- zapewnienie wysokiej wiarygodności danych operacyjnych

Za główne zadania w warunkach sytuacji kryzysowej należy uznać:

- zapewnienie środków na realizację programów współfinansowanych ze środków pomocowych,
- koordynowanie przesunięć środków w ramach obszarów priorytetowych celem koncentracji na terytorium dotkniętym kryzysem.

Zadania działu sprawy zagraniczne z zakresu zarządzania kryzysowego to:

- przeciwdziałanie zagrożeniom dla obywateli polskich poza granicami RP,
- zorganizowanie i realizacja przedsięwzięć ewakuacyjnych obywateli polskich z terenów zagrożonych do kraju.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać zapewnienie bezpieczeństwa obywatelom polskim poza granicami RP.

Dla działów kultura fizyczna i turystyka wyróżniono zadania wspólne. Należy do nich:

- upowszechnianie kultury fizycznej i sportu wśród dzieci i młodzieży w ramach działań na rzecz zapewnienia bezpieczeństwa,
- przygotowanie posiadanych obiektów na potrzeby wykorzystania celem zapewnienia pomocy osobom poszkodowanym w sytuacji kryzysowej.

Za główne zadania w warunkach sytuacji kryzysowej należy uznać:

- udzielenie pomocy osobom poszkodowanym w sytuacji kryzysowej poprzez udostępnienie posiadanych obiektów i infrastruktury,
- koordynowanie powrotu do kraju obywateli polskich oraz wyjazdu z Polski obywateli państw obcych – uczestników imprezy sportowej.

Zadania działu sprawiedliwość z zakresu zarządzania to:

- przeciwdziałanie buntom i ucieczkom z zakładów karnych i aresztów śledczych,
- przygotowanie rozwiązań prawno-organizacyjnych funkcjonowania placówek penitencjarnych w warunkach sytuacji kryzysowych, spowodowanych przez czynniki zewnętrzne, oraz zabezpieczenie baz danych.

Za główne zadanie w warunkach sytuacji kryzysowej należy uznać zapewnienie bezpieczeństwa funkcjonowania placówek penitencjarnych.

2.2. Procesy krytyczne dla zadań administracji publicznej

Zadania przedstawione w pierwszym podrozdziale składają się z szeregu procesów, których przerwanie prowadzi do utraty zdolności organu ich realizacji, a w konsekwencji do sytuacji kryzysowej. Określenie krytycznych procesów dla zadań gminy, powiatu, samorządu wojewódzkiego, administracji rządowej w wo-

jewództwie i działów administracji rządowej, wraz z określeniem sposobów, w jaki mogą zostać przerwane, oraz wskazaniem przyczyn i priorytetów działania powinno być pierwszym krokiem pozwalającym na identyfikację zagrożeń. Poniższe tabele pokazują jedynie ogólną dyspozycję dla tego procesu. Szukając właściwych dla określonego organu procesów, należy wziąć pod uwagę szczególny charakter rozwiązań przyjętych na danym terenie (gminnym, powiatowym, wojewódzkim) lub w obszarze odpowiedzialności (ministrowie i kierownicy urzędów centralnych).

Tabela 2.1. Procesy krytyczne zadań gminy

Proces krytyczny:	**Przerwanie procesu krytycznego:**	**Przykładowe przyczyny:**	**Priorytet działania:**
utrzymanie przejezdności dróg gminnych	nieprzejezdna droga gminna	wypadek komunikacyjny, działanie sił natury (śnieżyce, zniszczenie drogi przez powódź)	działania prowadzące do udrożnienia drogi, wyznaczanie objazdów innymi drogami
prawidłowo działające wodociągi	niedziałające wodociągi lub wstrzymanie ich pracy w wyniku zanieczyszczeń wody	awaria zasilania, awaria sieci wodociągowej, zatrucie wody	dostarczanie wody dla ludności oraz obiektów użyteczności publicznej (szpitali, szkół, urzędów)
sprawowanie nadzoru nad publicznym zakładem opieki zdrowotnej	utrata zdolności nadzoru nad publicznym zakładem opieki zdrowotnej	nieprawidłowe funkcjonowanie publicznego zakładu opieki zdrowotnej, brak środków finansowych, okupacja	koordynacja nad zarządzaniem w publicznym zakładzie opieki zdrowotnej
funkcjonowanie ośrodka pomocy społecznej	zakłócenie pracy ośrodków interwencji kryzysowej (zbyt mała ilość środków w stosunku do potrzeb)	duża liczba zgłaszających się osób potrzebujących pomocy	wskazanie innych sposobów udzielenia pomocy osobom potrzebującym
zapewnienie ochrony przeciwpożarowej	deficyt sił i środków determinujących powodzenie akcji ratowniczo- gaśniczej	brak środków finansowych, brak ratowników	wsparcie działań przez podmioty ratowniczo-gaśnicze z innych gmin, zapewnienie środków finansowych z innych źródeł lub poprawa zarządzania tymi środkami

Źródło: opracowanie własne

Tabela 2.2. Procesy krytyczne zadań powiatu

Proces krytyczny:	**Przerwanie procesu krytycznego:**	**Przykładowe przyczyny:**	**Priorytet działania:**
udzielanie świadczeń zdrowotnych	brak możliwości udzielania świadczeń zdrowotnych i/lub brak dostępności tych świadczeń	zniszczenie/uszkodzenie zakładu opieki zdrowotnej, brak dostępności medykamentów, brak lekarzy, strajk	zorganizowanie doraźnej pomocy medycznej i przywrócenie możliwości udzielania świadczeń
funkcjonowanie ośrodków interwencji kryzysowej	brak możliwości pracy ośrodków interwencji kryzysowej	likwidacja ośrodków interwencji kryzysowej	organizacja pomocy społecznej, pomocy psychologicznej dla poszkodowanych w sytuacjach kryzysowych – organizacja pomocy przy użyciu sił i środków z sąsiednich terenów, budowa zespołów interwentów kryzysowych na zasadzie wolontariatu
utrzymanie drożności dróg o znaczeniu strategicznym	zablokowanie szlaku komunikacyjnego o znaczeniu strategicznym (droga wojewódzka, krajowa, międzynarodowa)	wypadek drogowy, działanie sił natury	organizacja objazdów – udrożnienie szlaku, informowanie o utrudnieniach
wydawanie zezwoleń na unieszkodliwianie odpadów	brak firm prowadzących przedmiotową działalność	strajk, zwiększone ceny unieszkodliwiania odpadów, rozwój *czarnego rynku*	zabezpieczenie możliwości unieszkodliwienia odpadów niebezpiecznych; zapewnienie alternatywnych metod unieszkodliwiania odpadów, opracowanie planu gospodarowania odpadami na wypadek awarii systemu powiatowego – nowe miejsca unieszkodliwiania odpadów
możliwość oceny zagrożeń porządku publicznego i bezpieczeństwa	brak monitoringu zagrożeń	zamieszki z udziałem dużej liczby ludzi i na dużym obszarze mające charakter agresywny, wymagające zaangażowania decydentów	przejęcie monitorowania zagrożeń na terenie powiatu przez szczebel wyższy, np. województwo

Proces krytyczny:	Przerwanie procesu krytycznego:	Przykładowe przyczyny:	Priorytet działania:
zabezpieczenie ochrony przeciwpowodziowej i przeciwpożarowej	brak lub niewystarczające siły i środki niezbędne do ochrony przed powodzią lub pożarem	niesprawny sprzęt, zniszczenie magazynu przeciwpowodziowego z całym wyposażeniem np. w wyniku pożaru	wzmocnienie sił i środków powiatu poprzez zadysponowanie ich z sąsiednich powiatów bądź centrali, uruchomienie odwodów operacyjnych
reagowanie na zagrożenia, które wystąpiły na terenie powiatu	brak zdolności reagowania lub podejmowane działania są niewystarczające	niewystarczające siły i środki, brak właściwych procedur dot. kierowania działaniami, koordynowania i współpracy powodujący chaos wśród służb	zapewnienie sił i środków adekwatnych do aktualnych potrzeb powiatu, ustalenie służby/ organizacji wiodącej odpowiedzialnej za kierowanie działaniami

Źródło: opracowanie własne

Tabela 2.3. Procesy krytyczne zadań samorządu wojewódzkiego

Proces krytyczny:	Przerwanie procesu krytycznego:	Przykładowe przyczyny:	Priorytet działania:
funkcjonowanie domów pomocy społecznej, funkcjonowanie placówek opieki zdrowotnej	brak możliwości udzielenia skutecznej pomocy społecznej lub zdrowotnej	zniszczenia lub dysfunkcjonalność spowodowane zdarzeniem niekorzystnym	wyznaczenie zapasowych ośrodków zdrowia lub pomocy społecznej, do których mogą być przewiezieni chorzy lub potrzebujący, określenie sposobu ewakuacji osób, jak również wyznaczenie miejsc noclegowych
zaopatrzenie w wodę, zaopatrzenie w środki przeciwpowodziowe, zaopatrzenie w siły do reagowania	zatrucie zbiornika wody pitnej	awaria wodociągów, powódź, atak terrorystyczny	wyznaczenie terenów, które wymagają natychmiastowej pomocy, uruchomienie rezerwy do zwalczenia skutków powodzi

Proces krytyczny:	Przerwanie procesu krytycznego:	Przykładowe przyczyny:	Priorytet działania:
utrzymywanie wojskowych komisji uzupełnień, planowanie, organizacja, szkolenia i kontrolne, mające na celu utrzymywanie w sprawności systemu obronnego, pozyskiwanie osób do pracy w służbach mundurowych lub cywilnych celem utrzymania stałego poziomu bezpieczeństwa, podpisywanie zobowiązań i umów z instytucjami, w tym prywatnymi, w celu pozyskania sił i środków niezbędnych przy naruszeniu obronności kraju	przerwanie procesu poboru rekrutów, szkoleń na rzecz bezpieczeństwa i obronności państwa	zamieszki społeczne, atak na suwerenność kraju, sabotaż	podjęcie odpowiednich działań celem stłumienia zamieszek lub obrony kraju. W tym celu województwo powinno dokonać: oceny występujących i potencjalnych zagrożeń mogących mieć wpływ na bezpieczeństwo publiczne i prognozowanie tych zagrożeń, przedstawienia propozycji działań wojewodzie oraz wniosków dotyczących wykonania zadań wynikających z rozporządzenia prezydenta RP i innych aktów prawnych dotyczących tego stanu, przekazania do wiadomości publicznej informacji związanych z zagrożeniami

Źródło: opracowanie własne

Tabela 2.4. Procesy krytyczne zadań administracji rządowej w województwie

Proces krytyczny:	Przerwanie procesu krytycznego:	Przykładowe przyczyny:	Priorytet działania:
właściwe współdziałanie wszystkich organów administracji rządowej i samorządowej działających w województwie, zapewnienie powyższym organom odpowiednich sił i środków służących ochronie zdrowia i życia obywateli utrzymania porządku	brak możliwości koordynacji działań, dysfunkcja procesu wymiany informacji, awaria systemów teleinformatycznych, brak możliwości działania CZK	brak zdolności koordynacji i współpracy organów administracji rządowej i samorządowej w województwie, brak odpowiedniej ilości sił i środków niezbędnych do monitorowania, planowania, reagowania i usuwania skutków zagrożeń na terenie województwa,	zapewnienie odpowiedniej rezerwy finansowej na działania niezbędne do realizacji w sytuacjach wystąpienia zagrożenia dla bezpieczeństwa społeczeństwa, zapewnienie sił i środków służących bezpieczeństwu publicznemu spoza terenu województwa, raportowanie do krajowego centrum zarządzania kryzysowego

Źródło: opracowanie własne

Tabela 2.5. Procesy krytyczne zadań działów administracji rządowej

Proces krytyczny:	Przerwanie procesu krytycznego:	Przykładowe przyczyny:	Priorytet działania:
bezpieczeństwo powszechne i porządek publiczny	zagrożenie bezpieczeństwa powszechnego i porządku publicznego	protesty społeczne, zagrożenie terrorystyczne	analiza sytuacji, raportów i ostrzeżeń, koordynacja działań podległych służb i instytucji, wystąpienie z wnioskiem do Ministra Obrony Narodowej o udzielenie pomocy Policji, przez oddziały i pododdziały Sił Zbrojnych
funkcjonowanie opieki zdrowotnej	przerwanie funkcjonowania opieki zdrowotnej	klęski żywiołowe, ataki terrorystyczne, protesty społeczne, działania wojenne	przywrócenie zdolności państwa do świadczenia pomocy medycznej, uruchomienie zastępczych miejsc szpitalnych

Proces krytyczny:	Przerwanie procesu krytycznego:	Przykładowe przyczyny:	Priorytet działania:
ochrona ludzi, ich mienia oraz środowiska przed katastrofami naturalnymi i zdarzeniami radiacyjnymi	wystąpienie zagrożenia ludzi, ich mienia lub środowiska spowodowanego katastrofami naturalnymi i zdarzeniami radiacyjnymi	katastrofy naturalne, zdarzenia radiacyjne	monitorowanie oraz przeciwdziałanie zagrożeniom środowiska, ocena sytuacji radiacyjnej kraju, działania wspierające w zakresie identyfikacji oraz oceny skutków zdarzenia radiacyjnego
funkcjonowanie transportu morskiego	przerwanie funkcjonowania transportu morskiego	katastrofy naturalne, protesty społeczne, ataki terrorystyczne, działania wojenne	ochrona infrastruktury transportu morskiego
funkcjonowanie transportu zbiorowego	przerwanie funkcjonowania transportu zbiorowego	katastrofy naturalne, protesty społeczne, ataki terrorystyczne, działania wojenne	ochrona infrastruktury transportu zbiorowego
ciągłość produkcji rolno-hodowlanej	przerwanie ciągłości produkcji rolno-hodowlanej	katastrofy naturalne, protesty społeczne, działania wojenne, zakłócenia w systemie elektroenergetycznym lub paliwowym	udzielanie pomocy finansowej na wznowienie produkcji w gospodarstwach rolnych
utrzymanie właściwej jakości zdrowotnej żywności pochodzenia zwierzęcego	niewłaściwa jakość zdrowotna żywności pochodzenia zwierzęcego	skażenia chemiczne, skażenia radiacyjne, epizootie, epifitozy	działania mające na celu odseparowanie obszarów, na których doszło do przerwania procesu krytycznego, niedopuszczenie do rozprzestrzeniania się zagrożenia
nienaruszalność terytorialna Rzeczypospolitej Polskiej	naruszenie terytorium Rzeczypospolitej Polskiej przez obce wojsko	działania wojenne, manewry wojskowe w pobliżu granic RP	identyfikacja zagrożenia, a następnie prowadzenie działań zbrojnych lub pozamilitarnych, mających na celu zażegnanie konfliktu
ciągłość dostaw energii elektrycznej, paliw i gazu	brak dostaw energii elektrycznej, paliw i gazu	katastrofy naturalne, działania wojenne, niekorzystna sytuacja dyplomatyczna, zakłócenia w systemie elektroenergetycznym lub paliwowym	wprowadzanie ograniczeń poboru energii elektrycznej w poszczególnych regionach, decyzja o wykorzystaniu zapasów obowiązkowych paliw lub gazu

Proces krytyczny:	Przerwanie procesu krytycznego:	Przykładowe przyczyny:	Priorytet działania:
ochrona dóbr kultury i archiwów państwowych	zagrożenie istnienia i nienaruszonego stanu dóbr kultury i archiwów państwowych	działania wojenne, katastrofy naturalne, katastrofy budowlane, akty wandalizmu, atak terrorystyczny	ewakuacja dóbr kultury
bezpieczeństwo obywateli polskich poza granicami RP	zagrożenie bezpieczeństwa obywateli polskich poza granicami RP	działania wojenne, katastrofy naturalne, akty terroryzmu	ewakuacja obywateli polskich do kraju
bezpieczeństwo funkcjonowania placówek penitencjarnych	zagrożenie bezpieczeństwa funkcjonowania placówek penitencjarnych	działania wojenne, katastrofy naturalne, katastrofy budowlane, akty terroryzmu, protesty społeczne	zapewnienie placówek zastępczych

Źródło: opracowanie własne

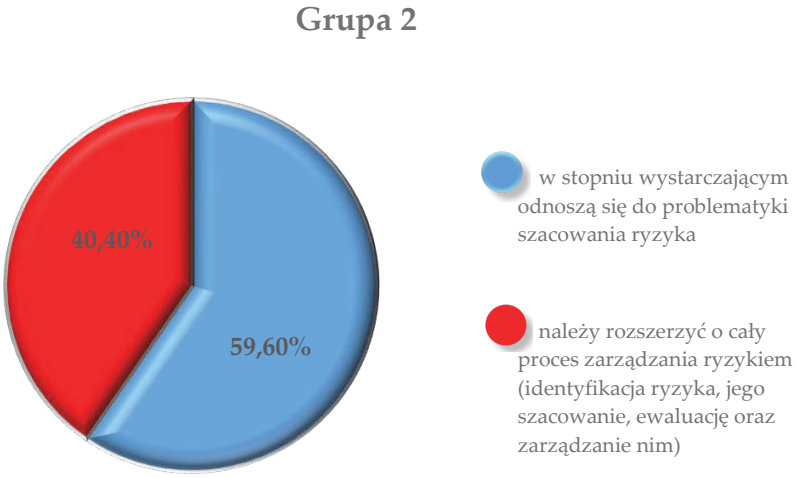
2.3. Analiza potrzeb organów zarządzania kryzysowego wszystkich szczebli systemu w zakresie oceny ryzyka

Oprócz wskazania kompetencji administracji publicznej w zakresie zarządzania ryzykiem istotną kwestią jest zbadanie jej podejścia do możliwości wdrożenia całego tego procesu na potrzeby planowania kryzysowego. Zasadne jest również określenie potrzeb organów zarządzania kryzysowego wszystkich szczebli systemu w zakresie oceny ryzyka w ramach realizacji zadań z zakresu planowania cywilnego.

W tym celu przeprowadzono badanie ankietowe mające na celu poznanie ich opinii na temat obecnego stanu rozwiązań formalnoprawnych w zakresie identyfikacji zagrożeń oraz procesu szacowania ryzyka, jak również wskazanie propozycji ewentualnych zmian w tym obszarze.

Kwestionariusz ankiety skierowano do dwóch grup respondentów: przedstawicieli administracji rządowej oraz jednostek samorządu terytorialnego. Pierwszą z nich stanowili wykonawcy raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego (RoZBN), w tym ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie oraz Rządowe Centrum Bezpieczeństwa jako koordynator prac nad dokumentem (Grupa 1). Drugą zaś tworzyli starostowie, wójtowie, burmistrzowie oraz prezydenci miast (Grupa 2).

Mimo że część pytań była identyczna dla obu grup respondentów, na potrzeby przeprowadzonego badania przygotowano dwa kwestionariusze ankiety (oddzielne dla każdej z nich). Zabieg ten pozwolił na analizę oraz syntezę uzyskanych wyników.



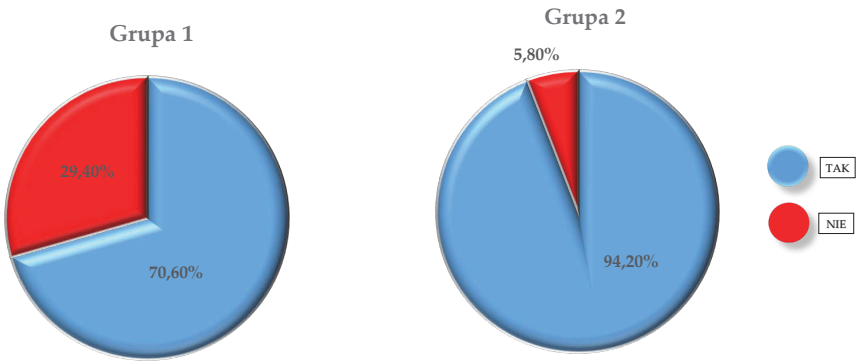
Wykres 2.1. Rozkład odpowiedzi na pytanie o ocenę obowiązujących zapisów ustawy o zarządzaniu kryzysowym, w części dotyczącej problematyki szacowania ryzyka (Grupa 2).

Źródło: opracowanie własne

Wyniki ankiety wskazują, iż w opinii niespełna dwóch trzecich ankietowanych (Grupa 1) zapisy ustawy o zarządzaniu kryzysowym należy rozszerzyć o cały proces zarządzania ryzykiem obejmujący identyfikację ryzyka, jego szacowanie, jak również ewaluację oraz zarządzanie nim. Prowadzi to do refleksji nad koniecznością zmian obowiązujących regulacji prawnych w kierunku prawnego usankcjonowania całościowego procesu zarządzania ryzykiem. Świadczy to również o tym, iż wiedza przedstawicieli administracji rządowej wykonujących pracę z zakresu planowania cywilnego oraz szacowania ryzyka na temat dobrych praktyk i standardów w tym zakresie, jest coraz większa. W tym względzie ich punkt widzenia podąża za założeniami wybranych norm z obszaru zarządzania ryzykiem.

Wśród drugiej grupy respondentów (przedstawiciele administracji samorządowej) poziom aprobaty dla wprowadzenia tego rozwiązania był dużo mniejszy (niespełna połowa badanych). Brak przekonania do konieczności uwzględnienia dodatkowych elementów w treści planów zarządzania kryzysowego (jako skutków wprowadzenia ww. zmian w przepisach prawnych) może wynikać z braku właściwych wytycznych dotyczących tego, w jaki sposób należy zarządzać ryzykiem w obszarze planowania cywilnego. W związku z tym zagadnienia te mogą być nieznane części z respondentów, przekładając się tym samym na stosunkowo wysoki procent wskazań dla odpowiedzi sugerujących, iż obecnie obowiązujące zapisy ustawy o zarządzaniu kryzysowym w sposób wystarczający odnoszą się do problematyki szacowania ryzyka.

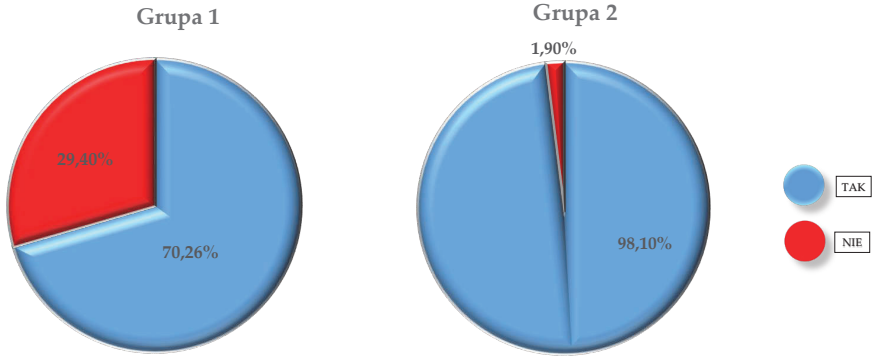
Wyniki przeprowadzonej ankiety dostarczają również informacji na temat oceny jasności i przejrzystości wybranych zapisów ustawy o zarządzaniu kryzysowym w części dotyczącej oceny ryzyka.



Wykres 2.2. Rozkład odpowiedzi na pytanie: Czy definicja mapy ryzyka zawarta w art. 3 pkt 10 ustawy o zarządzaniu kryzysowym jest dla Pani/Pana zrozumiała?
Źródło: opracowanie własne

W opinii zdecydowanej większości ankietowanych wśród obu grup respondentów, definicja mapy ryzyka jest zrozumiała. Uznaje się więc, iż uzasadnione jest dalsze funkcjonowanie tego zapisu w obecnym brzmieniu. Pozwala to również sądzić, iż ankietowani rozumieją intencję, jaka przyświecała ustawodawcy przy ustanowieniu mapy ryzyka jako elementu wchodzącego w skład dokumentów planistycznych z obszaru zarządzania kryzysowego.

Wniosek ten zweryfikowano w kolejnym pytaniu skierowanym do respondentów.

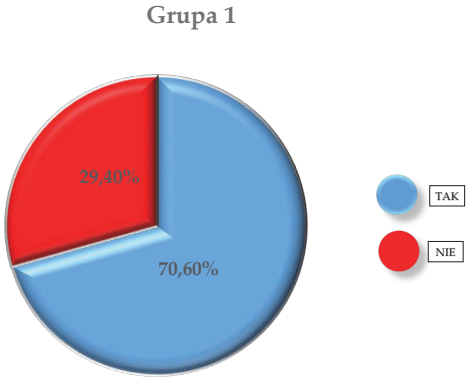


Wykres 2.3. Rozkład odpowiedzi na pytanie o konieczność uwzględnienia mapy ryzyka jako elementu dokumentów planistycznych z obszaru zarządzania kryzysowego.
Źródło: opracowanie własne

Uzyskane odpowiedzi wskazują, iż respondenci są zgodni co do konieczności uwzględnienia oceny ryzyka oraz mapy ryzyka w treści planów zarządzania kryzysowego oraz raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego. Dotyczy to zarówno odpowiedzi udzielonych przez ankietowanych

z Grupy 1 (przedstawiciele administracji rządowej), jak i z Grupy 2 (przedstawiciele administracji samorządowej).

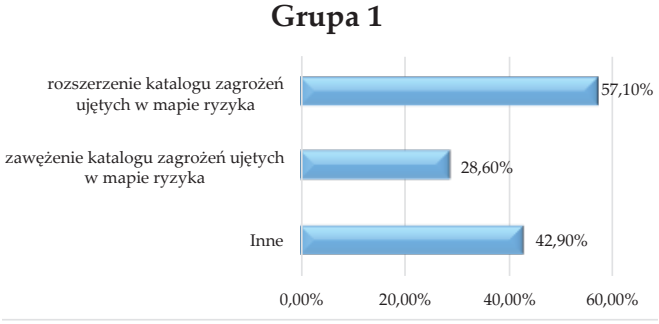
Pierwszą grupę respondentów poproszono również o weryfikację wykazu rodzajów zagrożeń ujętych w mapie ryzyka na potrzeby opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego.



Wykres 2.4. Rozkład odpowiedzi na pytanie: Czy zdaniem Pani/Pana określony w § 4 pkt 1 Rozporządzenia w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego wykaz rodzajów zagrożeń (zamieszczonych poniżej) ujętych w mapie ryzyka został zdefiniowany właściwie?

Źródło: opracowanie własne

Uzyskane odpowiedzi wskazują, iż zdecydowana większość respondentów uznaje obowiązujący wykaz rodzajów zagrożeń ujętych w mapie ryzyka za poprawnie zdefiniowany. Zastanawiające jest, że stosunkowo duża liczba ankietowanych (aż blisko 30%) opowiedziała się za koniecznością wprowadzenia zmian w tym zakresie. Skłania to do refleksji nad koniecznością poddania analizie i weryfikacji obowiązującego wykazu rodzajów zagrożeń ujętych w RoZBN pod kątem możliwości jego aktualizacji.

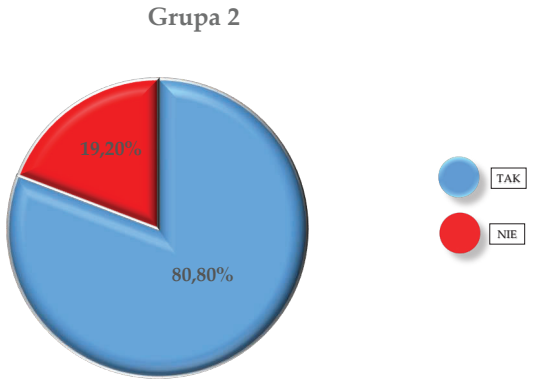


Wykres 2.5. Rozkład odpowiedzi na pytanie: Jeżeli NIE, to co zdaniem Pani/Pana należałoby w nim zmienić? (można zaznaczyć kilka odpowiedzi)

Źródło: opracowanie własne

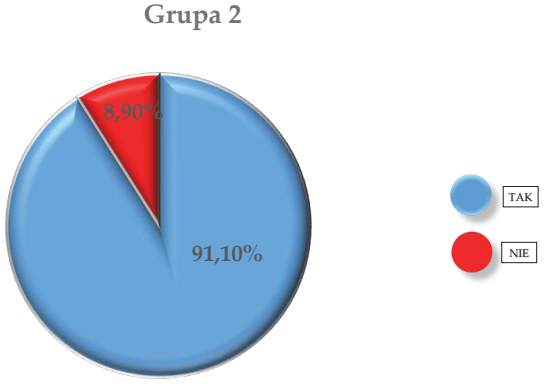
Wśród propozycji zmian najczęściej wskazywano na konieczność rozszerzenia katalogu zagrożeń ujętych w mapie ryzyka. Zdaniem części respondentów brakuje więc w nim zagrożeń, które nie są, a powinny zostać zidentyfikowane na potrzeby opracowania Raportu o zagrożeniach bezpieczeństwa narodowego. Pytaniem otwartym pozostaje, jakiego rodzaju zagrożenia zdaniem badanych powinny zostać wzięte pod uwagę.

Drugą grupę ankietowanych (przedstawiciele administracji samorządowej) zapytano również, czy otrzymywane przez nich wytyczne do planów zarządzania kryzysowego odnoszą się do problematyki identyfikacji i szacowania ryzyka. Rozważono również kwestię tego, czy są one zrozumiałe dla ich odbiorców.



Wykres 2.6. Rozkład odpowiedzi na pytanie: Czy wydane przez właściwy organ wytyczne/zalecenia do planów zarządzania kryzysowego odnoszą się do zagadnień identyfikacji i szacowania ryzyka?

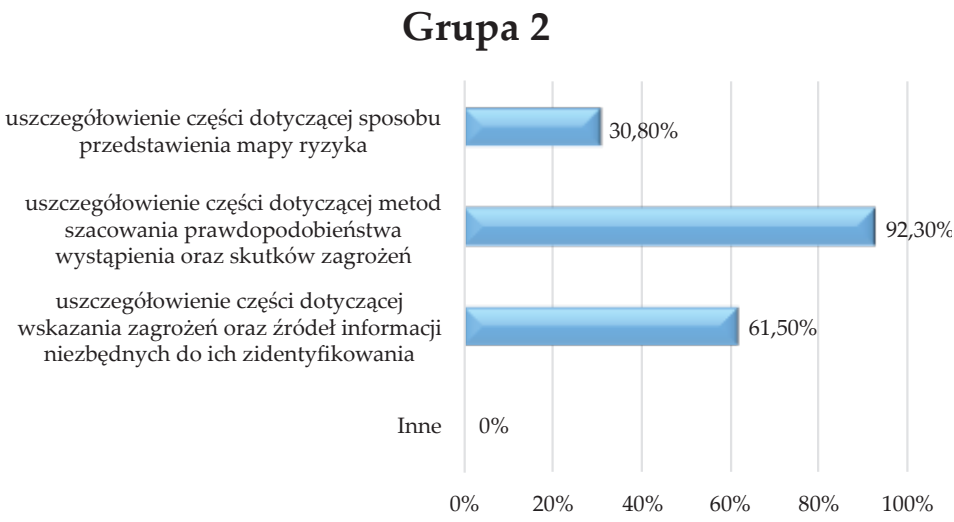
Źródło: opracowanie własne



Wykres 2.7. Rozkład odpowiedzi na pytanie: Jeśli TAK, to czy są one dla Pani/Pana zrozumiałe?

Źródło: opracowanie własne

Z uzyskanych odpowiedzi wynika, iż zdecydowana większość ankietowanych otrzymuje wskazówki w tym zakresie. Co więcej, dla aż ponad 90 procent z nich są one zrozumiałe. Jednak mimo bardzo dużego procentu wskazań dla tej odpowiedzi, uwagę zwraca grupa blisko 10 procent respondentów, którzy byli przeciwnego zdania. W kolejnym pytaniu osoby zostały poproszone o wskazanie treści wymagających ich zdaniem doszczegółowienia.



Wykres 2.8. Rozkład odpowiedzi na pytanie: Jeżeli NIE, to które z wymienionych zmian w wytycznych/zaleceniach do planów zarządzania kryzysowego w zakresie identyfikacji i szacowania ryzyka należałoby wprowadzić? (można zaznaczyć kilka odpowiedzi)

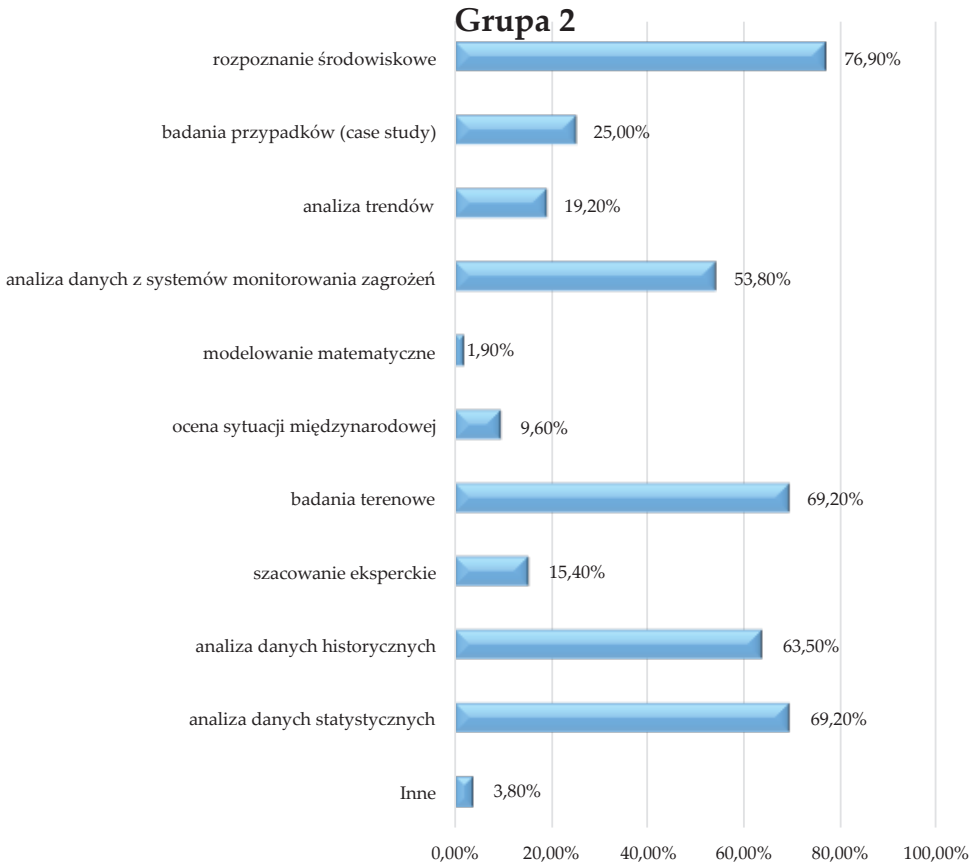
Źródło: opracowanie własne

Respondenci, dla których ww. wytyczne oraz zalecenia w części dotyczącej identyfikacji i szacowania ryzyka nie są zrozumiałe, byli zgodni, iż należałoby uszczegółowić część dotyczącą metod szacowania prawdopodobieństwa wystąpienia oraz skutków zagrożeń. Za inną pożądaną zmianę uznano konieczność doprecyzowania części dotyczącej identyfikacji zagrożeń oraz źródeł informacji niezbędnych do ich zidentyfikowania. Co trzeci z badanych był z kolei zdania, iż należałoby uszczegółowić część dotyczącą sposobu przedstawienia mapy ryzyka.

Przedstawicieli administracji rządowej zapytano również o to, z jakich źródeł informacji korzystają w celu zdobycia danych niezbędnych do zidentyfikowania zagrożeń na potrzeby opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego.

Pierwsza grupa ankietowanych wskazała na analizę danych historycznych, analizę danych statystycznych, analizę danych z systemów monitorowania zagrożeń oraz szacowanie eksperckie, jako najbardziej przydatne działania na potrzeby zbierania danych niezbędnych do zidentyfikowania zagrożeń.

Za metodę najrzadziej wykorzystywaną na potrzeby identyfikacji zagrożeń ankietowani uznali modelowanie matematyczne.

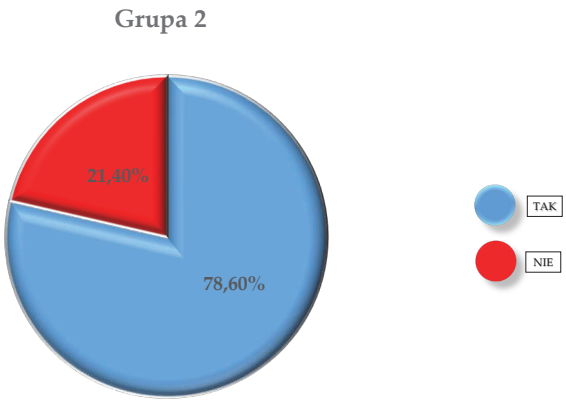


Wykres 2.9. Rozkład odpowiedzi na pytanie: Które z wymienionych działań podejmuje się w Pani/Pana instytucji w celu zdobycia danych do zidentyfikowania zagrożeń na potrzeby opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego? (można zaznaczyć kilka odpowiedzi)

Źródło: opracowanie własne

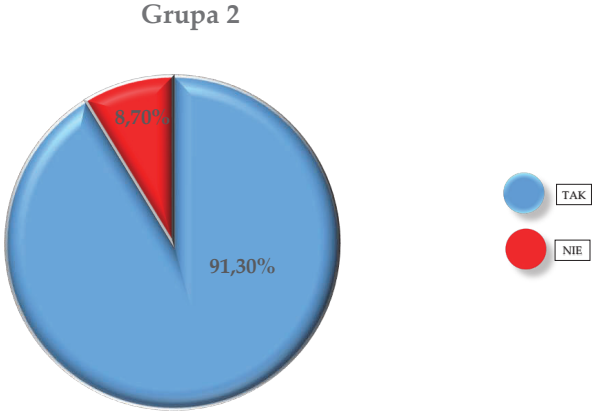
Podobne wyniki uzyskano wśród drugiej grupy respondentów. Mimo że rozkład odpowiedzi wskazuje na różnorodność wykorzystywanych metod, uwagę zwraca to, iż szczególny nacisk kładzie się zwłaszcza na rejestrację danych z przeszłości oraz analizę statystyk z tym związanych.

Z przeprowadzonego badania wynika również, że istotnym źródłem informacji w procesie szacowania ryzyka są dane pochodzące z sąsiednich lub znajdujących się na niższym szczeblu jednostek samorządu terytorialnego. Poniższe wykresy wskazują procent wskazań starostów w odpowiedzi na pytanie o praktykę wykorzystania tych działań na potrzeby zbierania informacji niezbędnych do identyfikacji zagrożeń.



Wykres 2.10. Rozkład odpowiedzi na pytanie: Czy zbierając dane niezbędne do opracowania planu zarządzania kryzysowego w części dotyczącej oceny ryzyka wystąpienia zagrożeń czerpie Pani/Pan informacje z sąsiednich powiatów?

Źródło: opracowanie własne

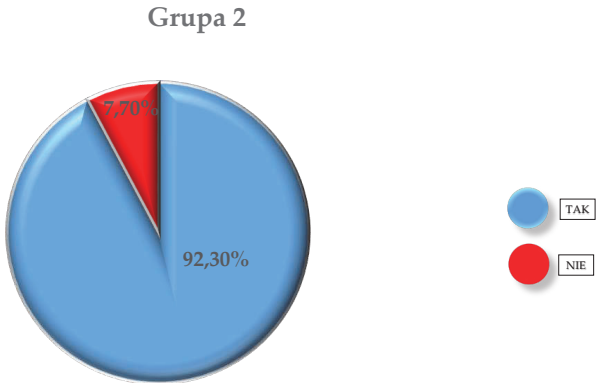


Wykres 2.11. Rozkład odpowiedzi na pytanie: Czy zbierając dane niezbędne do opracowania planu zarządzania kryzysowego w części dotyczącej oceny ryzyka wystąpienia zagrożeń czerpie Pani/Pan informacje z poszczególnych gmin wchodzących w skład powiatu?

Źródło: opracowanie własne

W ramach niniejszej ankiety rozważono również problematykę uzgadniania oraz zatwierdzania planów zarządzania kryzysowego w części planu głównego dotyczącej oceny ryzyka wystąpienia zagrożeń.

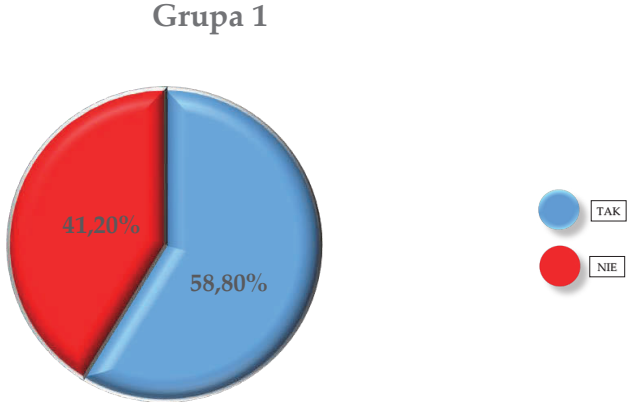
Zarówno starostowie, jak i wójtowie, burmistrzowie i prezydenci miast zgodnie uznali, iż prowadzona współpraca w zakresie uzgadniania oraz zatwierdzania planów zarządzania kryzysowego (w części obejmującej ocenę ryzyka) przebiega w sposób wystarczający.



Wykres 2.12. Rozkład odpowiedzi na pytanie: Czy zdaniem Pani/Pana współpraca z podmiotami biorącymi udział w uzgadnianiu oraz zatwierdzaniu planów zarządzania kryzysowego w części planu głównego dotyczącej oceny ryzyka wystąpienia zagrożeń jest wystarczająca?

Źródło: opracowanie własne

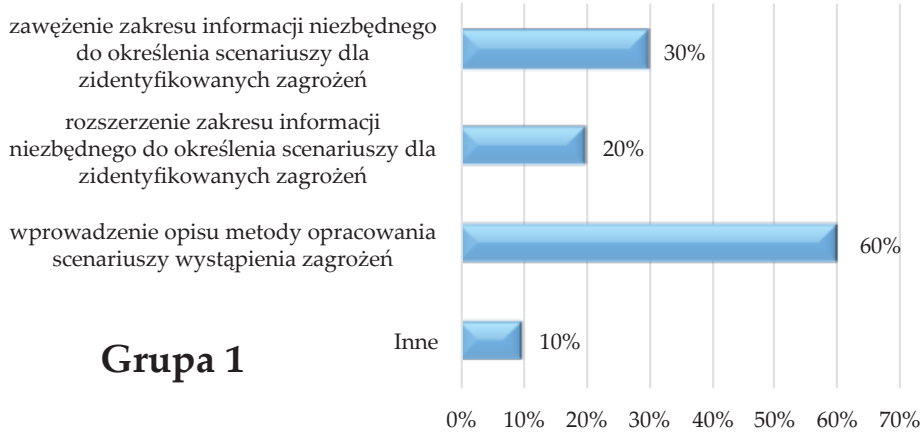
Pytania zawarte w kwestionariuszu ankiety dotyczyły także kwestii weryfikacji poprawności opisu scenariuszy zdarzeń zawartego w Procedurze opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego.



Wykres 2.13. Rozkład odpowiedzi na pytanie: Czy zawarty w procedurze opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego opis opracowania scenariuszy zdarzeń w ramach zagrożeń został zdefiniowany właściwie (czy jest zrozumiały)?

Źródło: opracowanie własne

W opinii większości respondentów z Grupy 1 należy dokonać zmian w opisie scenariuszy zdarzeń w ramach zagrożeń. Konkretne propozycje zmian ankietowani wskazali w odpowiedzi na pytanie kolejne.

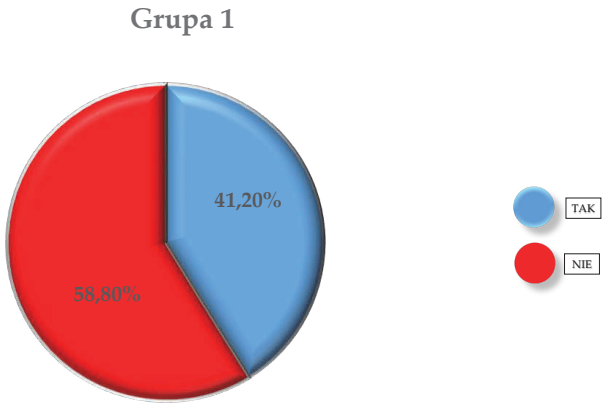


Wykres 2.14. Rozkład odpowiedzi na pytanie: Jeżeli NIE, to jakie zmiany w części procedury dotyczącej określenia scenariuszy dla zidentyfikowanych zagrożeń należałoby wprowadzić? (można zaznaczyć kilka odpowiedzi)

Źródło: opracowanie własne

Z uzyskanych odpowiedzi wynika, iż zdaniem ankietowanych niezbędną zmianą w części procedury dotyczącej określenia scenariuszy dla zidentyfikowanych zagrożeń jest wprowadzenie opisu metody scenariuszy wystąpienia zagrożeń. Ponadto część z nich wskazuje, że należałoby poszerzyć lub zawęzić zakres informacji niezbędny do określania scenariuszy dla zidentyfikowanych zagrożeń.

Ankietowanych z Grupy 1 poproszono również o opinię na temat przyjętej w procedurze opracowania raportów cząstkowych do RoZBN metody oceny ryzyka.

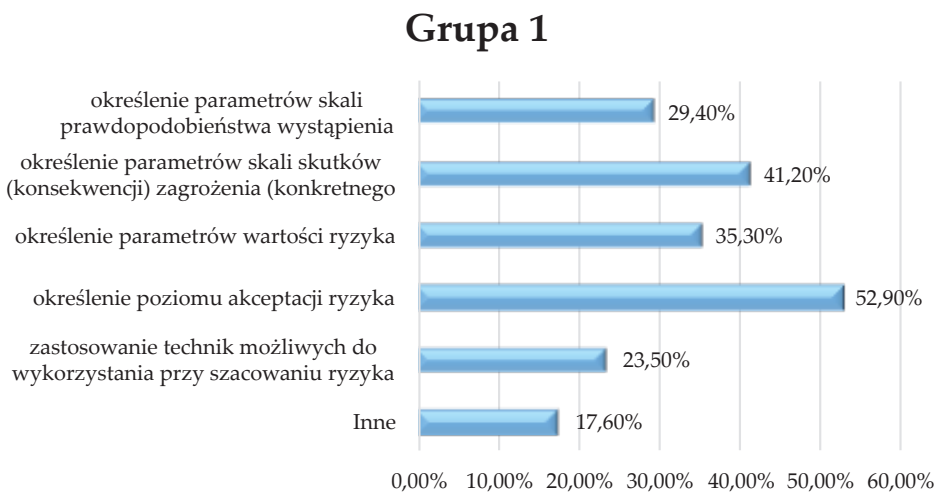


Wykres 2.15. Rozkład odpowiedzi na pytanie: Czy zdaniem Pani/Pana przyjęta w procedurze opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego metoda oceny ryzyka pozwala na właściwie jego oszacowanie?

Źródło: opracowanie własne

W opinii nieco ponad połowy respondentów z Grupy 1 (przedstawiciele administracji rządowej) przyjęta w ramach Procedury opracowania raportów cząstkowych do RoZBN metoda oceny ryzyka nie pozwala na właściwe jego oszacowanie. Uzyskane odpowiedzi wskazują więc, iż należałoby zastanowić się nad wprowadzeniem zmian w obowiązującej metodzie oceny ryzyka.

W kolejnym pytaniu ankietowani, którzy udzielili odpowiedzi przeczącej, zostali poproszeni o wskazanie trudności, z jakimi zmagają się w procesie szacowania ryzyka na potrzeby opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego.

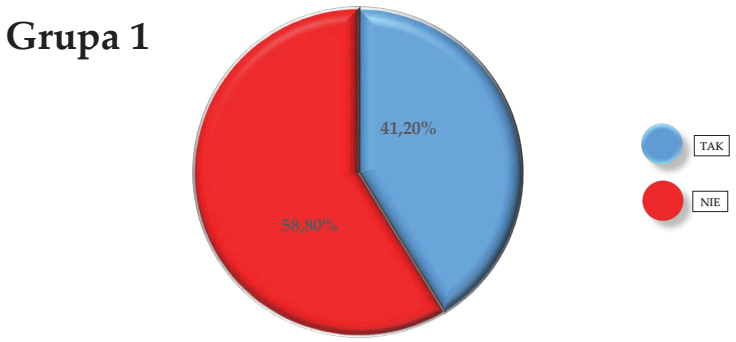


Wykres 2.16. Rozkład odpowiedzi na pytanie: Jeżeli NIE, to co sprawiło Pani/Panu największą trudność w procesie szacowania ryzyka? (można zaznaczyć kilka odpowiedzi)

Źródło: opracowanie własne

Za największą trudność w procesie szacowania ryzyka respondenci uznali określenie poziomu akceptacji oceny ryzyka. Wysoki procent wskazań dla tej odpowiedzi może wskazywać, iż kryteria akceptacji ryzyka przyjęte w Procedurze opracowania raportów cząstkowych nie są jasne dla wykonawców tych dokumentów, a w tym względzie należałoby rozważyć opracowanie metody określenia akceptowalności zidentyfikowanego ryzyka.

Zdaniem ankietowanych problematyczne są również kwestie m.in. zastosowania technik możliwych do wykorzystania przy szacowaniu ryzyka, określenia parametrów wartości ryzyka, parametrów skali skutków zagrożenia (konkretnego scenariusza) czy też parametrów skali prawdopodobieństwa wystąpienia zagrożenia (konkretnego scenariusza).

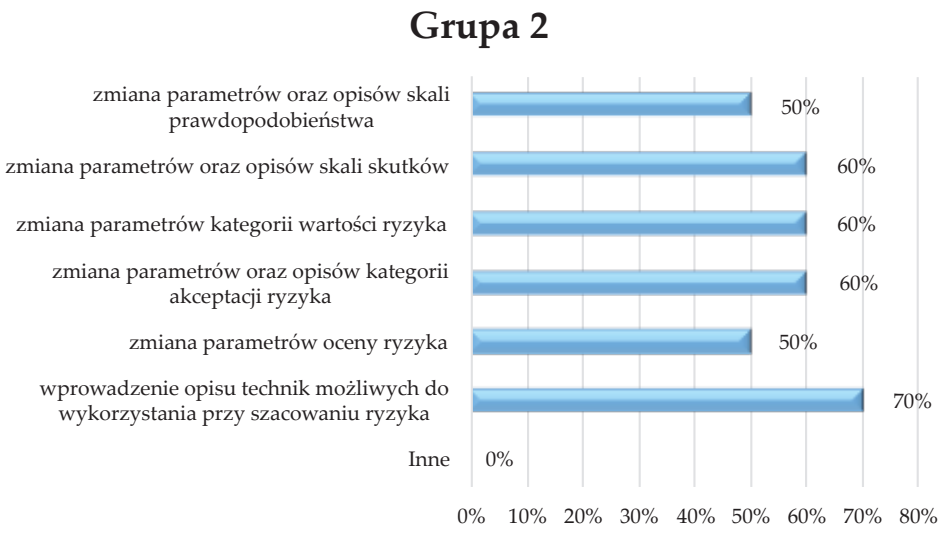


Wykres 2.17. Rozkład odpowiedzi na pytanie: Czy zdaniem Pani/Pana należałoby wprowadzić zmiany w procedurze opracowania raportów cząstkowych w części odnoszącej się do procesu szacowania ryzyka?

Źródło: opracowanie własne

W odniesieniu do kolejnego pytania dotyczącego kwestii tego, czy należałoby wprowadzić zmiany w Procedurze opracowania raportów cząstkowych w części odnoszącej się do procesu szacowania ryzyka, odpowiedzi rozkładały się na podobnym poziomie, jak w pytaniu o opinię na temat poprawności przyjętej metody oceny ryzyka (58,8%).

Kolejne pytanie dotyczyło wskazania przez respondentów propozycji zmian w Procedurze opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego.



Wykres 2.18. Rozkład odpowiedzi na pytanie: Jeżeli TAK, to zdaniem Pani/Pana, które z wymienionych zmian należałoby wprowadzić? (można zaznaczyć kilka odpowiedzi)

Źródło: opracowanie własne

Procent wskazań dla poszczególnych odpowiedzi w tym pytaniu ułożył się na podobnym poziomie. Największa liczba respondentów wskazała, iż należałoby wprowadzić opis technik możliwych do zastosowania przy szacowaniu ryzyka. Informacji takich brakuje bowiem w obecnie obowiązującej Procedurze opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego. Ponad połowa badanych opowiedziała się za zmianą parametrów oceny ryzyka, parametrów opisów kategorii akceptacji ryzyka, parametrów oraz opisów skali skutków, jak również zmianą parametrów oraz opisów skali prawdopodobieństwa i skutków. Tak wysoki procent wskazań dla wszystkich proponowanych odpowiedzi oznacza, iż zmiany w treści Procedury opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego są niezbędne. W tym względzie należy wziąć pod uwagę wszystkie opinie wykonawców raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego, jako osób na co dzień zajmujących się ww. problematyką w praktyce realizacji zadań z zakresu planowania kryzysowego.

Polski system prawny w ustawach o samorządzie gminnym, powiatowym i wojewódzkim, wojewodzie oraz działach administracji definiuje zadania organów władzy w zakresie bezpieczeństwa. Właściwy sposób realizacji tych zadań jest nie tylko gwarantem utrzymania reputacji instytucji władzy ale przede wszystkim bezpieczeństwa ludzi, mienia i środowiska. Struktura administracji wraz z przypisanymi organom odpowiedzialnościami tworzy spójny system bezpieczeństwa państwa. Budując system zarządzania ryzykiem, należy skoncentrować się nie tylko na zadaniach administracji publicznej, ale co ważniejsze na zdolnościach do ich realizacji. Stąd bierze się potrzeba określenia kluczowych procesów, których przerwanie prowadzi do dysfunkcji władzy, a w konsekwencji do powstawania sytuacji kryzysowych. Spośród procesów do najważniejszych należą te, które wiążą się z zaspokojeniem podstawowych potrzeb ludności, włączając w to funkcjonowanie infrastruktury, tj. zaopatrzenie w wodę, prąd, energię cieplną i elektryczną, jak również zapewnienie pomocy społecznej, czy też utrzymanie dróg publicznych.

3. Normy z zakresu zarządzania ryzykiem

Obecnie istnieje wiele norm z zakresu zarządzania ryzykiem, znajdujących swoje zastosowanie w sektorze publicznym oraz prywatnym. Są to zarówno dokumenty zawierające standardy o charakterze uniwersalnym dla zarządzania różnego rodzaju organizacjami, jak i specyficzne dla danego obszaru, np. bezpieczeństwa i higieny pracy, zarządzania środowiskowego, zarządzania jakością, analizy ryzyka w systemach technicznych czy też bezpieczeństwa maszyn. W ramach prowadzonych badań zidentyfikowano kilkanaście norm z zakresu zarządzania ryzykiem. Dokumenty te w sposób szczegółowy odnoszą się do rozpatrywanego obszaru tematycznego, biorąc pod uwagę specyfikę organizacji, w której mogą zostać wykorzystane, jak również realizowane przez nią zadania oraz cele.

W tabeli 3.1. przedstawiono wykaz wybranych norm z zakresu zarządzania ryzykiem wraz ze wskazaniem zakresu tematycznego, jaki obejmują:

Tabela nr 3.1. Wykaz wybranych norm z zakresu zarządzania ryzykiem wraz z określeniem ich zakresu tematycznego

Lp.	Nazwa normy	Zakres tematyczny
1	PN-ISO 31000 *Zarządzanie ryzykiem – Zasady i wytyczne*	• terminologia pojęć z zakresu zarządzania ryzykiem • zasady zarządzania ryzykiem • struktura ramowa zarządzania ryzykiem • proces zarządzania ryzykiem
2	PKN-ISO Guide 73 *Zarządzanie ryzykiem – Terminologia*	terminologia pojęć z zakresu zarządzania ryzykiem
3	IEC/FDIS 31010 *Risk management – Risk assessment techniques*	• proces oceny ryzyka • katalog technik i narzędzi oceny ryzyka • opis i charakterystyka technik i narzędzi oceny ryzyka • kryteria doboru odpowiedniej techniki, narzędzia oceny ryzyka
4	ISO 22301 *Bezpieczeństwo Powszechne – Systemy Zarządzania Ciągłością Działania*	• terminologia pojęć związanych z zarządzaniem ciągłością działania, • wymagania związane z planowaniem, ustanawianiem, wdrażaniem, funkcjonowaniem, monitorowaniem, przeglądaniem, utrzymywaniem i ciągłym doskonaleniem udokumentowanego systemu zarządzania ciągłością działania

5	BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki*	wytyczne dotyczące planowania, opracowywania, wykorzystania, utrzymywania i poprawiania zdolności zarządzania kryzysowego
6	PN-EN ISO 9000 *System zarządzania jakością – Podstawy i terminologia*	• opis podstaw systemów zarządzania jakością • terminologia dotycząca systemów zarządzania jakością
7	PN-EN ISO 9004 *Zarządzanie mające na celu osiągnięcie trwałego sukcesu organizacji – Podejście przez zarządzanie jakością*	• wytyczne uwzględniające skuteczność oraz efektywność systemu zarządzania jakością • wytyczne dotyczące samooceny • ciągłość doskonalenia procesów
8	PN-EN ISO 14001:2005 *Systemy zarządzania środowiskowego – Wymagania i wytyczne stosowania*	wymagania dotyczące systemu zarządzania środowiskowego
9	PN-N 18004 *Systemy zarządzania bezpieczeństwem i higieną pracy – Wytyczne*	wytyczne dotyczące opracowania, wdrożenia, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem i higieną pracy, w tym identyfikacja zagrożeń i ocena ryzyka zawodowego
10	PN-N-18002 *Systemy zarządzania bezpieczeństwem i higieną pracy – Ogólne wytyczne do oceny ryzyka zawodowego*	wytyczne umożliwiające przeprowadzenie postępowania mającego na celu ocenę ryzyka zawodowego na stanowiskach pracy
11	PN-IEC 60300-3-9 *Analiza ryzyka w systemach technicznych*	wytyczne dotyczące analizy ryzyka obejmujące koncepcje analizy ryzyka, procedury analizowania ryzyka, metody analizy ryzyka
12	PN-EN ISO 12100 *Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i zmniejszanie ryzyka*	proces oceny ryzyka i zmniejszenia ryzyka stwarzanego przez maszyny (ocena ryzyka, redukcja ryzyka, dokumentowanie oceny i redukcji ryzyka)

Źródło: opracowanie własne

Powyższe dokumenty poruszają problematykę zasad i wytycznych do zarządzania ryzykiem oraz zarządzania ciągłością działania, zawierają terminologię pojęć w tym zakresie, jak również obejmują opis technik i narzędzi służących do oceny ryzyka. Zdaniem autorów, z punktu widzenia niniejszego opracowania istotne znaczenie ma omówienie głównych założeń następujących norm:

- PN-ISO 31000 *Zarządzanie ryzykiem – Zasady i wytyczne,*
- PKN-ISO Guide 73 *Zarządzanie ryzykiem – Terminologia,*
- IEC/FDIS 31010 *Risk management – Risk assessment techniques,*
- ISO 22301 *Bezpieczeństwo Powszechne – Systemy Zarządzania Ciągłością Działania,*
- BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki.*

Dokumenty te mogą znaleźć swoje zastosowanie w obszarze funkcjonowania administracji publicznej w ramach systemu zarządzania kryzysowego RP, tym samym mogą okazać się przydatne w ramach przeprowadzenia analizy ryzyka na potrzeby planowania kryzysowego na poszczególnych szczeblach podziału terytorialnego.

3.1. Norma PN-ISO 31000 Zarządzanie ryzykiem – Zasady i wytyczne

Norma międzynarodowa PN-ISO 31000 *Zarządzanie ryzykiem – Zasady i wytyczne* została opracowana przez Grupę Roboczą Zarządu Technicznego ISO ds. zarządzania Ryzykiem. Wprowadza ona ISO 31000:2009 *Risk management – Principles and Guidelines*. Norma ta jest zbiorem zasad, jakie należy rozpatrywać przy wdrażaniu procesu analizy ryzyka w każdej organizacji. W tym względzie bez znaczenia jest, czy analiza ryzyka dotyczy bezpieczeństwa informacji, ryzyka finansowego, czy też innego obszaru. Niniejsza norma nie jest bowiem specyficzna dla żadnego przemysłu ani sektora. Może być stosowana przez każde publiczne, prywatne lub spółdzielcze przedsiębiorstwo, stowarzyszenie, grupę lub osobę fizyczną. Można ją więc uznać za normę o charakterze uniwersalnym, tym bardziej że wskazuje się, iż może znaleźć swoje zastosowanie w odniesieniu do każdego typu ryzyka, bez względu na jego charakter oraz niezależnie od pozytywnych bądź negatywnych konsekwencji.

Norma PN-ISO 31000 adresowana jest do szerokiego grona ekspertów, w tym osób odpowiedzialnych za rozwijanie polityki zarządzania ryzykiem oraz zapewnienie skutecznego zarządzania ryzykiem w organizacji jako całości lub w ramach określonych obszarów, projektów lub działań. Ponadto kierowana jest do osób zajmujących się oceną skuteczności organizacji w zakresie zarządzania ryzykiem. Adresowana jest również do osób opracowujących normy, przewodniki, procedury i kodeksy postępowania. Wskazuje się w nich, w jaki sposób należy zarządzać ryzykiem.

Norma PN-ISO 31000 szczegółowo opisuje proces zarządzania ryzykiem. Ustanawia zasady, których przestrzeganie uważa się za niezbędne do osiągnięcia skuteczności zarządzania ryzykiem. Norma zaleca, aby organizacje opracowały, wdrożyły oraz ciągle udoskonalały strukturę ramową. Jej celem jest integracja procesu zarządzania ryzykiem z całościowym ładem organizacyjnym, a także z jej strategią i planowaniem, zarządzaniem, procesami raportowania, politykami, wartościami oraz kulturą.

Ogólne podejście przyjęte w normie PN-ISO 31000 dostarcza zasad oraz wytycznych do zarządzania każdym typem ryzyka w sposób systematyczny, przejrzysty i wiarygodny w ramach dowolnego zakresu oraz kontekstu. Kluczowym aspektem w projektowaniu struktury ramowej zarządzania ryzykiem według normy jest *ustalenie kontekstu*. Element ten pomaga poznać oraz ocenić charakter, jak również złożoność ryzyk właściwych dla danej organizacji.

Wdrożenie niniejszej normy w procesie zarządzania ryzykiem pozwala na zwiększenie prawdopodobieństwa osiągnięcia celów, wsparcie proaktywnego zarządzania, jak również zwiększenie świadomości na temat potrzeby identyfikacji i postępowania z ryzykiem w całej organizacji. Umożliwia również spełnienie wymagań prawnych, regulacyjnych norm międzynarodowych oraz doskonalenie obowiązkowego i dobrowolnego raportowania. Inną korzyścią wynikającą z wdrożenia normy jest doskonalenie ładu organizacyjnego oraz zwiększenie zaufania interesariuszy. Ponadto pozwala ona na ustalenie wiarygodnej podstawy do podejmowania decyzji oraz planowania oraz doskonalenie środków kontroli. Dzięki jej zastosowaniu możliwe jest skuteczne alokowanie i wykorzystywanie zasobów do postępowania z ryzykiem, jak również poprawienie skuteczności i efektywności operacyjnej wyników w obszarze bezpieczeństwa i higieny pracy oraz ochrony środowiska. Efektem wdrożenia normy jest też skuteczniejsze zarządzanie incydentami, minimalizacja strat z tym związanych oraz poprawa odporności organizacji.

Norma PN-ISO 31000 definiuje pojęcie ryzyka jako wpływ niepewności na cele. Z kolei zarządzanie ryzykiem rozumiane jest jako skoordynowane działania dotyczące kierowania organizacją i jej nadzorowania w odniesieniu do ryzyka. Sam proces zarządzania ryzykiem określa się jako systematyczne stosowanie polityk, procedur i praktyk zarządzania do działań w zakresie komunikacji, konsultacji, ustalania kontekstu, oraz identyfikowania, analizowania, ewaluacji, postępowania z ryzykiem, monitorowania i przeglądu ryzyka. Termin oceny ryzyka oznacza zaś całościowy proces identyfikacji ryzyka, analizy ryzyka oraz ewaluacji ryzyka. Pierwszy element tego procesu, tj. identyfikacja ryzyka, to proces wyszukiwania, rozpoznawania i opisywania ryzyka. Z kolei analiza ryzyka rozumiana jest jako proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka. Ewaluacja ryzyka oznacza zaś proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane.

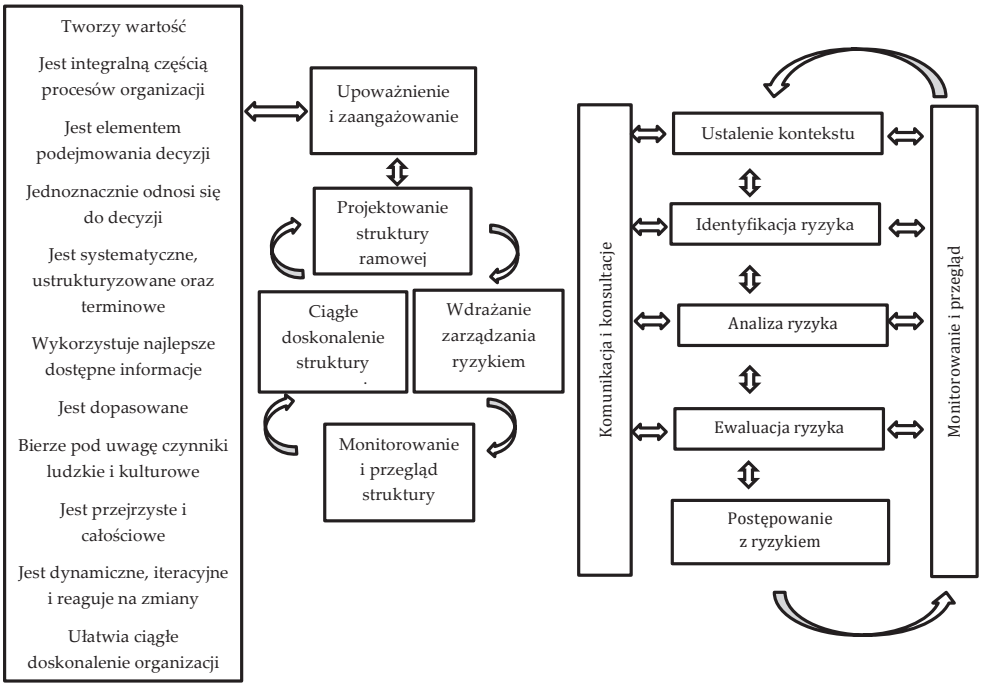
Zakłada się, że norma ISO 31000 będzie stosowana do harmonizowania procesów zarządzania ryzykiem w istniejących normach, oraz tych, które dopiero powstaną. Norma określa ogólne podejście związane ze wspieraniem norm dotyczących specyficznych ryzyk, ale ich nie zastępuje. W dokumencie nie rekomenduje się żadnej specyficznej metodyki ryzyka. Wskazuje się natomiast, na czym proces ten polega, jak również jakie dodatkowe czynniki należy uwzględnić w tym procesie.

Norma wskazuje dwa obszary zarządzania ryzykiem. Pierwszy z nich (z ang. *risk management*) odnosi się do zasad, struktury ramowej i procesu skutecznego zarządzania ryzykiem. Z kolei zgodnie z drugim podejściem (z ang. *managing risk*) zarządzanie ryzykiem rozumiane jest jako konkretne działanie, zarządzanie konkretnym ryzykiem.

Szerszego omówienia wymaga zwłaszcza pierwszy z wymienionych obszarów, pozwala bowiem na zwrócenie szczególnej uwagi na wszystkie elementy

zarządzania ryzykiem, jak również na występujące pomiędzy nimi zależności. Podejście to zostało szczegółowo opisane oraz zobrazowane w normie PN-ISO 31000. Drugie z omawianych podejść jest również istotne, niemniej jednak jego skuteczna realizacja nie jest możliwa bez zbudowania wspomnianych powyżej relacji.

Norma PN-ISO 31000 zaleca stosowanie na każdym poziomie ściśle określonych zasad dotyczących postępowania z ryzykiem. Pozwala to na zapewnienie skuteczności zarządzania ryzykiem. Na rysunku 3.1., w pierwszej kolumnie przedstawiono 11 podstawowych zasad zarządzania ryzykiem.



Rysunek 3.1. Relacje pomiędzy zasadami, strukturą ramową i procesem zarządzania ryzykiem

Źródło: Norma PN-ISO 31000 Zarządzanie ryzykiem – Zasady i wytyczne

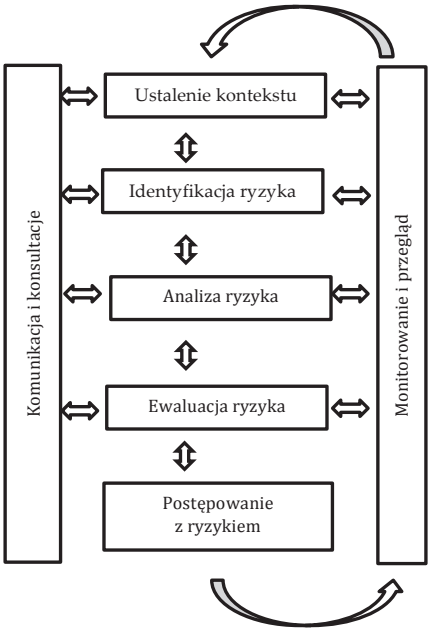
Wdrożeniu na każdym poziomie organizacji określonych zasad powinno towarzyszyć ustalenie struktury ramowej, która pozwala na zaangażowanie całej struktury organizacji i właściwe zaplanowanie sposobu zarządzania przez nią informacją. Kluczowe znaczenie w tym względzie ma zagwarantowanie włączenia się w proces zarządzania ryzykiem kierownictwa organizacji. Jest to jeden z warunków, który pozwala na przystąpienie do programowania struktury ramowej. Zaangażowanie kierownictwa w tym zakresie wyraża się poprzez strategiczne planowanie polityki organizacji. Podjęcie wszystkich powyższych działań jest

warunkiem wdrożenia skutecznego zarządzania ryzykiem na wszystkich etapach tego procesu.

Istotną rolę w tym zakresie pełni wspomniana struktura ramowa (rys. nr 3.2.), gdyż wskazuje ona ramy funkcjonowania organizacji na każdym jej poziomie. Innymi słowy chodzi o wdrożenie procesu zarządzania ryzykiem. Struktura ramowa pozwala na to, aby informacje o ryzyku pochodzącym z procesu zarządzania ryzykiem mogły być właściwie raportowane i wykorzystywane, stanowiąc tym samym podstawę do podejmowania decyzji. Wspomaga również organizację w integracji zarządzania ryzykiem z ogólnym systemem zarządzania. W związku z tym kluczową kwestią jest, aby organizacja, która decyduje się na wdrożenie procesu zarządzania ryzykiem, dopasowała elementy struktury ramowej do swoich potrzeb. Na rysunku 3.2. przedstawiono niezbędne elementy struktury ramowej dla zarządzania ryzykiem. Wskazano również, w jaki sposób komponenty te są ze sobą powiązane. Jednym z elementów wyróżnionych na poniższym rysunku jest ciągłe doskonalenie struktury ramowej. Pozwala to na wdrażanie coraz doskonalszego zarządzania ryzykiem.

Rysunek 3.2. Relacje pomiędzy elementami struktury ramowej zarządzania ryzykiem
Źródło: Norma PN-ISO 31000 Zarządzanie ryzykiem – Zasady i wytyczne

Norma PN-ISO 31000 obejmuje również szczegółowy opis procesu zarządzania ryzykiem (rys. nr 3.3.).



Rysunek 3.3. Proces zarządzania ryzykiem
Źródło: Norma PN-ISO 31000 Zarządzanie ryzykiem – Zasady i wytyczne

Rozpoczyna się on od elementu zwanego *ustaleniem kontekstu*. Poprzez ustalenie kontekstu możliwe jest zdefiniowanie celów, wskazanie zewnętrznych i wewnętrznych parametrów branych pod uwagę podczas zarządzania ryzykiem, jak również ustalenie zakresu i kryteriów ryzyka dla pozostałych procesów.

Kluczowym, o ile nie najistotniejszym, elementem procesu zarządzania ryzykiem jest ocena ryzyka. Norma zaleca zidentyfikowanie źródeł ryzyka, obszarów wpływów, zdarzeń, jak również ich przyczyn oraz potencjalnych następstw. Na tym etapie należy stworzyć wyczerpującą listę ryzyk opartych na zidentyfikowanych zdarzeniach, które mogą mieć pozytywny lub negatywny wpływ na cele postawione przez organizację. Mogą one tworzyć, stymulować, zapobiegać, przeszkadzać, jak również przyspieszać lub opóźniać ich osiągnięcie. Za konieczną uznaje się identyfikację zarówno ryzyk będących pod kontrolą organizacji, jak i tych, których organizacja nie kontroluje.

Analiza ryzyka, którą należy przeprowadzić w kolejnym kroku oceny ryzyka, dostarcza danych wejściowych do ewaluacji ryzyka oraz podjęcia decyzji co do postępowania z ryzykiem i wyboru najodpowiedniejszej metody postępowania z nim. Obejmuje ona wskazanie przyczyn i źródeł ryzyka, jak również pozytywnych i negatywnych następstw, wraz z określeniem prawdopodobieństwa ich wystąpienia. W normie wskazuje się, że analiza ryzyka może być jakościowa, półilościowa, ilościowa, a także stanowić kombinację powyższych metod w zależności od okoliczności. Następstwa i ich prawdopodobieństwo mogą być określone poprzez modelowanie wyników zdarzeń bądź zestawu zdarzeń, albo poprzez pro-

gnozę wynikającą z eksperymentalnych badań lub dostępnych danych. Dopuszcza się możliwość podziału następstw na skutki materialne i niematerialne. W pewnych przypadkach, na potrzeby określenia następstw i ich prawdopodobieństwa w odniesieniu do różnych okresów, miejsc, grup lub sytuacji, niezbędne jest wskazanie więcej niż jednej wartości lub cechy.

Nieodłącznym elementem procesu zarządzania ryzykiem jest również postępowanie z ryzykiem. Związane jest to z wyborem jednej lub kilku opcji modyfikowania ryzyka, jak również ich zastosowania. Zgodnie z normą PN-ISO 31000 można wyróżnić następujące sposoby postępowania z ryzykiem:

- unikanie ryzyka poprzez decyzję o zaprzestaniu działań powodujących ryzyko lub o powstrzymaniu się od ich rozpoczęcia,
- podjęcie lub zwiększenie ryzyka w celu wykorzystania szansy,
- usunięcie źródła ryzyka,
- zmianę prawdopodobieństwa,
- zmianę następstw,
- dzielenie ryzyka z inną stroną lub stronami,
- zatrzymanie ryzyka na podstawie świadomej decyzji.

Wybór najbardziej odpowiedniego rozwiązania uzależniony jest od wyników analizy kosztów oraz nakładów ich wdrażania w stosunku do uzyskiwanych korzyści. W tym względzie bierze się pod uwagę wymagania prawne, funkcjonalne oraz inne, takie jak odpowiedzialność społeczna i ochrona środowiska naturalnego.

Znajomość takich zagadnień, jak zasady zarządzania ryzykiem, struktura ramowa oraz proces zarządzania ryzykiem jest kwestią kluczową dla zarządzania organizacją, w tym zidentyfikowanymi przez nią ryzykami. Pomimo iż norma nie wskazuje metodologii oceny ryzyka, to zawiera zalecenia, istotne z punktu widzenia budowy systemu zarządzania ryzykiem w każdej organizacji.

3.2. Norma PKN-ISO Guide 73 Zarządzanie ryzykiem – Terminologia

Norma PKN-ISO Guide 73 *Zarządzanie ryzykiem – Terminologia* (*Risk management – Vocabulary – Guidelines for use in standards*) stanowi przewodnik, który obejmuje podstawowe słownictwo niezbędne do ujednolicenia postrzegania zagadnień związanych z zarządzaniem ryzykiem wśród organizacji i funkcji, biorąc pod uwagę ich różne zastosowania i rodzaje. Zaleca się więc, aby w rozpatrywanym obszarze, w pierwszej kolejności stosować definicje ujęte w przywołanej normie. Niemniej jednak, w uzasadnionych przypadkach dopuszcza się możliwość uzupełnienia terminologii przyjętej w niniejszym przewodniku.

Celem normy PKN-ISO Guide 73 jest zachęcenie do wzajemnego zrozumienia, przyjęcia zintegrowanego podejścia do opisania działań związanych z zarządzaniem ryzykiem, jak również do użycia jednolitej terminologii odnoszącej się do procesu zarządzania ryzykiem oraz struktury ramowej zarządzania ryzykiem.

Wskazuje się, iż niniejszy przewodnik przeznaczony jest do stosowania przez:
- osoby zaangażowane w zarządzanie ryzykiem,
- osoby zaangażowane w działalność ISO, IEC oraz
- osoby opracowujące krajowe lub sektorowe normy, przewodniki, procedury i kodeksy postępowania związane z zarządzaniem ryzykiem.

Norma PKN-ISO Guide 73 ma charakter ogólny i dotyczy ogólnie pojętej dziedziny zarządzania ryzykiem. Przewodnik obejmuje definicje:
- podstawowych pojęć dotyczących zarządzania ryzykiem, w tym: ryzyko, zarządzanie ryzykiem, proces zarządzania ryzykiem, struktura ramowa zarządzania ryzykiem, polityka zarządzania ryzykiem, plan zarządzania ryzykiem,
- pojęć właściwych dla nazw poszczególnych etapów składających się na proces zarządzania ryzykiem oraz terminów towarzyszących tym etapom, w tym: ustalenie kontekstu, ocena ryzyka, identyfikacja ryzyka, analiza ryzyka, ewaluacja ryzyka, postępowanie z ryzykiem, komunikacja i konsultacje, monitorowanie,
- pojęć specyficznych dla etapu ustalenia kontekstu, w tym: kontekst zewnętrzny, kontekst wewnętrzny, kryteria ryzyka,
- pojęć specyficznych dla etapu identyfikacji ryzyka, w tym: opis ryzyka, źródło ryzyka, zdarzenie, zagrożenie, właściciel ryzyka,
- pojęć specyficznych dla etapu analizy ryzyka, w tym: prawdopodobieństwo, ekspozycja, następstwo, częstość, podatność, macierz ryzyka, poziom ryzyka,
- pojęć specyficznych dla etapu ewaluacji ryzyka, w tym: nastawienie do ryzyka, apetyt na ryzyko, tolerancja ryzyka, awersja do ryzyka, agregacja ryzyka, akceptacja ryzyka,
- pojęć specyficznych dla etapu postępowania z ryzykiem, w tym: środek kontroli, unikanie ryzyka, dzielenie ryzyka, finansowanie ryzyka, retencja ryzyka, ryzyko rezydualne, elastyczność,
- pojęć specyficznych dla komunikacji i konsultacji, w tym: interesariusz, postrzeganie ryzyka,
- pojęć specyficznych dla monitorowania, w tym: przegląd, raportowanie ryzyka, rejestr ryzyka, profil ryzyka, audyt zarządzania ryzykiem.

Poniżej zamieszczono definicje wybranych pojęć zaczerpniętych z normy PKN-ISO Guide 73, zdaniem autorów niezbędnych do właściwego zrozumienia procesu zarządzania ryzykiem i do posługiwania się właściwą terminologią przy przeprowadzaniu analizy ryzyka na potrzeby planowania kryzysowego w obszarze zarządzania kryzysowego[1]:

Ryzyko – *wpływ niepewności na cele.*

Ryzyko rezydualne – *ryzyko pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem, może zawierać ryzyka niezidentyfikowane;* jest również nazywane *ryzykiem podlegającym retencji.*

[1] Norma PKN-ISO Guide 73 *Zarządzanie ryzykiem – Terminologia.*

Retencja ryzyka – *akceptacja potencjalnej korzyści z zysku, lub ciężaru straty, wynikających z konkretnego ryzyka.*

Zarządzanie ryzykiem – *skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka.*

Proces zarządzania ryzykiem – *systematyczne stosowanie polityk, procedur i praktyk zarządzania do działań w zakresie komunikacji, konsultacji, ustalenia kontekstu, oraz identyfikowania, analizowania, ewaluacji, postępowania z ryzykiem, monitorowania i przeglądu ryzyka.*

Ocena ryzyka – *całościowy proces identyfikacji ryzyka, analizy ryzyka oraz ewaluacji ryzyka.*

Identyfikacja ryzyka – *proces wyszukiwania, rozpoznawania i opisywania ryzyka.*

Polityka zarządzania ryzykiem – *deklaracja dotycząca ogółu zamierzeń i ukierunkowania organizacji odnoszących się do zarządzania ryzykiem.*

Plan zarządzania ryzykiem – *plan zawarty w strukturze ramowej zarządzania ryzykiem określający podejście, elementy zarządzania i zasoby, które będą zastosowane w zarządzaniu ryzykiem.*

Zagrożenie – *źródło potencjalnej szkody.*

Właściciel ryzyka – *osoba lub jednostka rozliczana z zarządzania ryzykiem i uprawniona do tego zarządzania.*

Analiza ryzyka – *proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka.*

Prawdopodobieństwo – *możliwość, szansa wystąpienia zdarzenia.*

Podatność – *wewnętrzne właściwości skutkujące narażeniem na źródło ryzyka, które może prowadzić do zdarzenia z jego następstwami.*

Macierz ryzyka – *narzędzie służące uszeregowaniu i przedstawieniu ryzyk poprzez określenie zakresów dla następstwa oraz ich prawdopodobieństwa.*

Poziom ryzyka – *wielkość ryzyka lub kombinacji ryzyk, wyrażona w postaci kombinacji następstw oraz ich prawdopodobieństwa.*

Ewaluacja ryzyka – *proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane.*

Postępowanie z ryzykiem – *proces modyfikacji ryzyka poprzez: unikanie ryzyka w wyniku decyzji o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko; podjęcie lub zwiększenie ryzyka w celu wykorzystania szansy; usunięcie źródła ryzyka; zmianę prawdopodobieństwa; zmianę następstw; dzielenie ryzyka wraz z inną stroną lub stronami oraz retencję ryzyka na podstawie świadomej decyzji.*

Agregacja ryzyka – *kombinacja kilku ryzyk w jedno ryzyko w celu uzyskania szerszego spojrzenia na całość ryzyka.*

Akceptacja ryzyka – *świadoma decyzja o podjęciu danego ryzyka.*

Unikanie ryzyka – *świadoma decyzja o nieangażowaniu się lub odejściu od ryzyka, działanie w celu eliminacji narażenia na konkretne ryzyko.*

Struktura ramowa zarządzania ryzykiem – *zestaw elementów zapewniających podstawy i ustalenia organizacyjne w zakresie projektowania, wdrażania, monitorowania, dokonywania przeglądów i ciągłego doskonalenia zarządzania ryzykiem w całej organizacji.*

Ustalenie kontekstu – *definiowanie zewnętrznych i wewnętrznych parametrów, które powinny być uwzględniane podczas zarządzania ryzykiem, jak również podczas określania zakresu i kryteriów ryzyka dla polityki zarządzania ryzykiem.*

Kontekst zewnętrzny – *środowisko zewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów.*

Kontekst wewnętrzny – *środowisko wewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów.*

Norma ISO Guide 73 ma kluczowe znaczenie dla zarządzania ryzykiem, w tym oceny ryzyka jako istotnego elementu tego procesu. Niniejszy przewodnik pozwala bowiem na ujednolicenie słownictwa z zakresu zarządzania ryzykiem, dając tym samym wszystkim potencjalnym interesariuszom, możliwość mówienia *wspólnym językiem.*

3.3. Norma IEC/FDIS 31010 Risk management – Risk assessment techniques

Międzynarodowa norma IEC/FDIS 31010 *Risk management – Risk assessment techniques* wspiera założenia normy PN-ISO 31000, dostarczając wskazówek dotyczących kryteriów doboru oraz zastosowania metodycznych technik i narzędzi służących do oceny ryzyka. Ocena ryzyka, przeprowadzona zgodnie z niniejszą normą, wspomaga pozostałe działania podejmowane w ramach procesu zarządzania ryzykiem. Porusza zagadnienia związane z zastosowaniem różnego rodzaju technik i narzędzi, odwołując się do innych dokumentów międzynarodowych, w których koncepcja ich wykorzystania została opisana bardziej szczegółowo. Norma nie odnosi się do wszystkich możliwych technik i narzędzi oceny ryzyka, co nie oznacza, że nie mogą one zostać zastosowane w rozpatrywanym zakresie.

W normie IEC/FDIS 31010 *Risk management – Risk assessment techniques* narzędzia i techniki oceny ryzyka podzielono pod kątem możliwości ich wykorzystania na poszczególnych etapach tego procesu. W związku z tym wyróżniono narzędzia i techniki, które mogą zostać użyte na potrzeby:

- identyfikacji ryzyka,
- analizy ryzyka (analizy skutków),
- analizy ryzyka (jakościowe, półilościowe lub ilościowe pozwalające na określenie prawdopodobieństwa),
- analizy ryzyka (ocena efektywności istniejących środków kontrolnych),
- analizy ryzyka (określenie poziomu ryzyka),
- ewaluacji ryzyka.

Wszystkie możliwe do zastosowania metody i narzędzia, wskazane w normie IEC/FDIS 31010 *Risk management — Risk assessment techniques*, przedstawiono

w poniższej tabeli. Plusami zaznaczono stopień przydatności każdej techniki na poszczególnych etapach procesu oceny ryzyka (im więcej plusów, tym większa przydatność danej techniki).

Tabela 3.2. Techniki i narzędzia możliwe do zastosowania przy ocenie ryzyka

Narzędzia i techniki oceny ryzyka	**Procesy oceny ryzyka**				
	Identyfikacja	**Analiza ryzyka**			**Ewaluacja ryzyka**
		Skutki	**Prawdopodobieństwo**	**Poziom ryzyka**	
Burza mózgów	++	-	-	-	-
Wywiady ustrukturalizowane lub częściowo ustrukturalizowane	++	-	-	-	-
Metoda delficka	++	-	-	-	-
Listy kontrolne	++	-	-	-	-
Podstawowa analiza zagrożeń	++	-	-	-	-
Analiza zagrożeń i zdolności operacyjnych	++	++	+	+	+
Analiza Zagrożeń i Krytycznych Punktów Kontroli	++	++	-	-	++
Ocena ryzyka środowiskowego	++	++	++	++	++
Analiza *Co jeśli?*	++	++	++	++	++
Analiza scenariuszy	++	++	+	+	+
Analiza wpływu na działalność	+	++	+	+	+
Analiza przyczyn źródłowych	-	++	++	++	++
Analiza rodzajów i skutków możliwych błędów	++	++	++	++	++
Analiza drzewa błędów	+	-	++	+	+
Analiza drzewa zdarzeń	+	++	+	+	-
Analiza przypadków i konsekwencji	+	++	++	+	+
Analiza przyczynowo-skutkowa	++	++	-	-	-
Analiza warstw zabezpieczeń	+	++	+	+	-

Narzędzia i techniki oceny ryzyka	Procesy oceny ryzyka				
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka
		Skutki	Prawdopodobieństwo	Poziom ryzyka	
Drzewo decyzyjne	-	++	++	-	-
Analiza niezawodności człowieka	++	++	++	++	-
Analiza *Bow-tie*	-	+	++	++	-
Utrzymanie ruchu skierowane na niezawodność	++	++	++	++	++
Analiza Markova	+	++	-	-	-
Symulacja Monte Carlo	-	-	-	-	++
Statystyki i sieci Bayes'a	-	++	-	-	-
Krzywe wyniku fałszywie ujemnego	+	++	++	+	++
Wskaźniki ryzyka	+	++	++	+	++
Matryca skutek/prawdopodobieństwo	++	++	++	++	+
Analiza koszty/korzyści	+	++	+	+	+
Analiza wielokryterialnej decyzji	+	++	+	+	+

Źródło: Norma IEC/FDIS 31010 Risk management – Risk assessment techniques

W normie wskazuje się, że, dokonując wyboru odpowiedniej techniki oceny ryzyka, należy wziąć pod uwagę następujące czynniki:
- cele rozpatrywanego przypadku,
- potrzeby decydentów,
- typ i rozmiar ryzyka poddanego analizie,
- potencjalną wielkość skutków,
- dostępność informacji i danych,
- konieczność modyfikacji/aktualizacji oceny ryzyka,
- wymagania regulacyjne i kontraktowe.

Poniżej omówiono wybrane narzędzia i techniki oceny ryzyka, zdaniem autorów najbardziej przydatne w ramach przeprowadzenia analizy ryzyka na potrzeby planowania kryzysowego. Wśród nich znalazły się: analiza drzewa zdarzeń, analiza drzewa błędów, Bow-tie, metoda *Co jeśli?*, BIA oraz metoda analizy scenariuszy.

Metoda ETA (analiza drzewa zdarzeń) jest graficzną techniką zobrazowania ciągów zdarzeń następujących po zdarzeniu początkowym. Drzewo ma więc formę drzewa logicznego, podążając od przyczyn do skutku, a zatem opisuje progresję od

zdarzenia początkowego do końcowego, przy czym każde kolejne zdarzenie ma dwa rozgałęzienia wskazujące na jego powodzenie lub brak (innymi słowy jego pozytywny bądź negatywny efekt). Bierze się przy tym pod uwagę funkcjonowanie (lub brak) różnych systemów bezpieczeństwa przeznaczonych do ograniczenia konsekwencji tych zdarzeń[2].

Metoda ta może więc zostać użyta do modelowania, wyliczania oraz pozycjonowania różnych scenariuszy zdarzeń następujących po głównym zdarzeniu. Stosuje się ją zarówno pod kątem analizy jakościowej, jak i ilościowej. Jakościowo metoda ta może być pomocna w czasie przeprowadzania burzy mózgów przy opracowaniu potencjalnych scenariuszy i określenia sekwencji zdarzeń, poczynając od zdarzenia początkowego. Przeprowadzenie analizy ilościowej za pomocą ETA pozwala zaś na sprawdzenie skuteczności zabezpieczeń. Bardzo często jest ona stosowana do modelowania awarii systemów, wyposażonych w wielokrotne zabezpieczenia[3].

Wśród zalet niniejszej metody wskazuje się na to, że w jasny oraz schematyczny sposób opisuje ona potencjalne scenariusze zdarzeń następujące po zdarzeniu inicjującym, jak również pozwala na analizę wpływu działania każdego z elementów systemu. Ponadto uwzględnia ona czas, zależności i efekt domina, a zatem elementy, których nie bierze się pod uwagę w ramach analizy drzewa błędów. Inną znaczącą zaletą w porównaniu do metody FTA jest możliwość czytelnego przedstawienia sekwencji zdarzeń w formie graficznej.

Ograniczeniem w zastosowaniu metody ETA jest fakt, że wymaga ona wyczerpującej analizy i identyfikacji wszystkich potencjalnie możliwych zdarzeń (zarówno zdarzenia początkowego, jak i jego skutków). Co więcej, definiuje ona stan każdego zdarzenia w kontekście sukcesu lub porażki, nie biorąc pod uwagę możliwości opóźnień związanych z poprawą danego działania[4].

Na rysunku 3.4. przedstawiono przykładowe drzewo zdarzeń dla awarii cysterny.

FTA (analiza drzewa błędów) jest jedną z metod QRA: *Qualitative Risk Assessment* (ilościowe metody oceny). Podobnie jako pozostałe z nich, przyjmuje konstrukcję drzewa logicznego[5]. FTA jest techniką służącą do identyfikacji i analizy czynników przyczyniających się do określonego niepożądanego zdarzenia (nazwanego zdarzeniem szczytowym). Czynniki te są identyfikowane, uporządkowane w logiczny sposób oraz przedstawione graficznie na diagramie[6].

Konstrukcję drzewa rozpoczyna się od pierwszego zidentyfikowanego zdarzenia, które stanowi górę diagramu. Kolejnym krokiem jest uporządkowanie w sposób logiczny zdarzeń mających wpływ na zaistnienie wydarzenia. Są one powiązane za pomocą dwóch rodzajów tzw. bramek logicznych. tj. *I* oraz *LUB*. Bram-

---

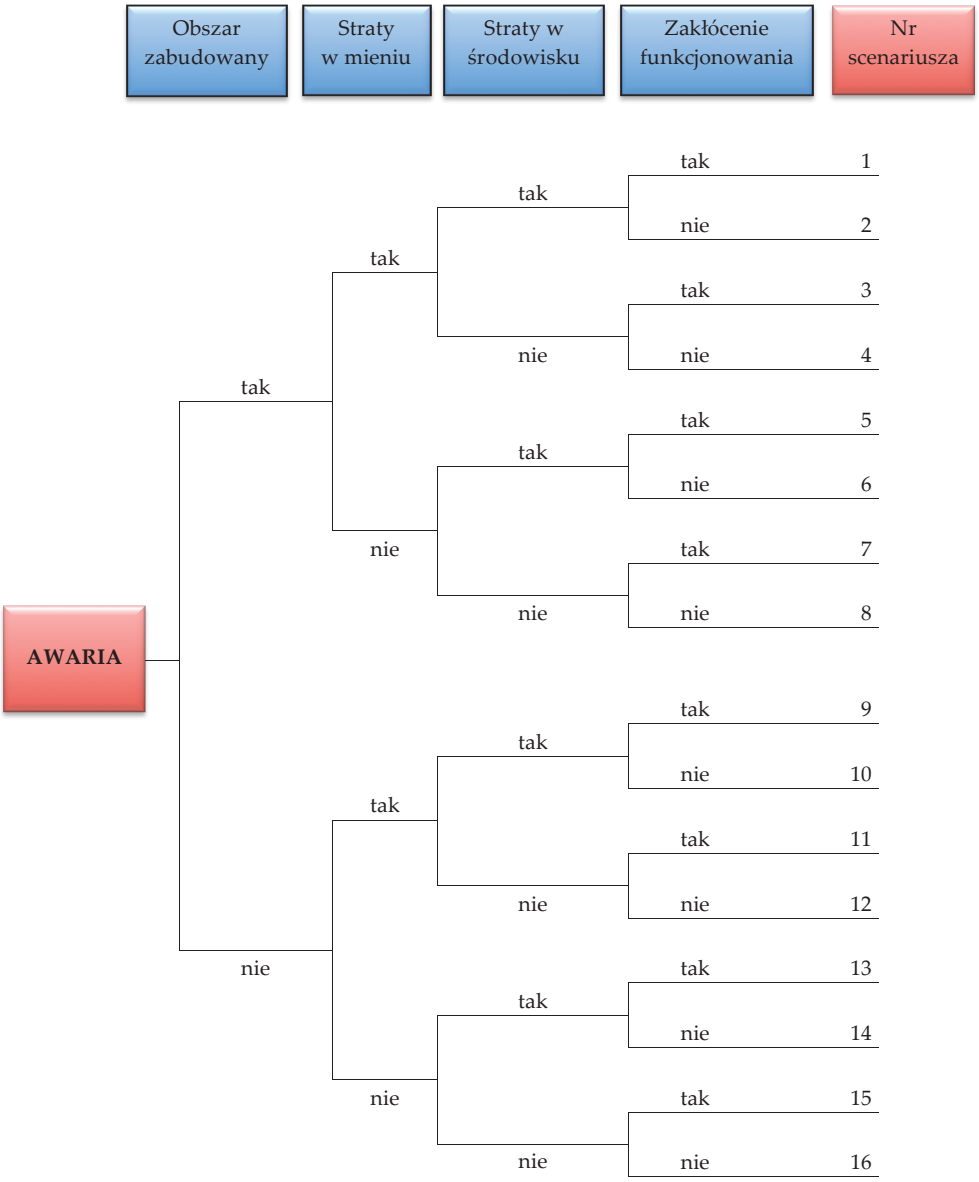
2 P. Mitkowski, *Ocena ilościowa ryzyka: analiza drzewa zdarzeń*, materiały dydaktyczne.

3 IEC/FDIS 31010 *Risk management — Risk assessment techniques*; s. 54.

4 Tamże, s. 55.

5 P. Mitkowski, *Ocena ilościowa ryzyka: analiza drzewa błędów (konsekwencji)*, materiały dydaktyczne.

6 IEC/FDIS 31010 *Risk management — Risk assessment techniques*; s. 51.



Rysunek 3.4. Przykładowe drzewo zdarzeń dla awarii cysterny

Źródło: Materiał zgromadzony w toku realizacji projektu: Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. PE.VII.6 Opracowanie metodyki analizy ryzyka możliwej do zastosowania na różnych poziomach zarządzania kryzysowego, w tym opracowanie procedury tworzenia map ryzyka i map zagrożeń

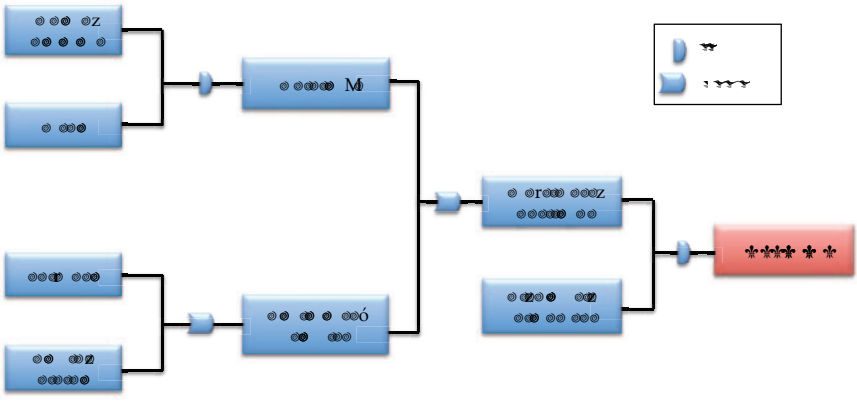
ka *LUB* opisuje sytuację, zgodnie z którą kolejne wydarzenie nastąpi, w przypadku gdy przynajmniej jedno ze zdarzeń *wychodzących* zaistnieje. Z kolei bramka *I* wiąże się z sytuacją, w której następne wydarzenie nastąpi tylko i wyłącznie, gdy zaistnieją wszystkie zdarzenia *wchodzące*[7].

Metodę tę stosuje się pod kątem analizy jakościowej oraz ilościowej. Jakościowo analiza drzewa błędów może zostać wykorzystana na potrzeby identyfikacji potencjalnych przyczyn wystąpienia danego zdarzenia. Z kolei w ujęciu ilościowym może znaleźć zastosowanie w ramach szacowania prawdopodobieństwa wystąpienia rozpatrywanego zdarzenia[8].

Zaletą metody FTA jest metodyczne, usystematyzowane podejście, które jest na tyle elastyczne, że pozwala na analizę różnorodnych czynników, tj. np. działań ludzi czy też zjawisk fizycznych. Przyjęcie podejścia *z góry na dół* umożliwia skupienie uwagi na związkach przyczynowych pomiędzy poszczególnymi zdarzeniami. Ze względu na fakt, że drzewa błędów są często duże i skomplikowane, na potrzeby przeprowadzenia takich analiz wykorzystuje się narzędzia informatyczne[9].

Wśród ograniczeń w zastosowaniu analizy drzewa błędów wskazuje się na niepewność oszacowania prawdopodobieństwa zdarzeń umieszczonych na drzewie, co może wpłynąć na mniej precyzyjne wyliczenie prawdopodobieństwa zdarzenia szczytowego. Wadą tej metody jest również fakt, że rozważa ona tylko dwie opcje, tj. że system zadziała lub nie zadziała. Analizie nie mogą więc zostać poddane zdarzenia o bardziej skomplikowanej strukturze[10].

Przykładowe drzewo błędów przedstawiono na rysunku 3.5.



Rysunek 3.5. Przykładowe drzewo błędów dla awarii cysterny w wyniku wypadku

Źródło: Materiał zgromadzony w toku realizacji projektu: Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. PE.VII.6 Opracowanie metodyki analizy ryzyka możliwej do zastosowania na różnych poziomach zarządzania kryzysowego, w tym opracowanie procedury tworzenia map ryzyka i map zagrożeń

---

7 P. Mitkowski, *Ocena ilościowa ryzyka: analiza drzewa błędów (konsekwencji)*, materiały dydaktyczne.

8 IEC/FDIS 31010 *Risk management — Risk assessment techniques*; s. 51.

9 Tamże, s. 52.

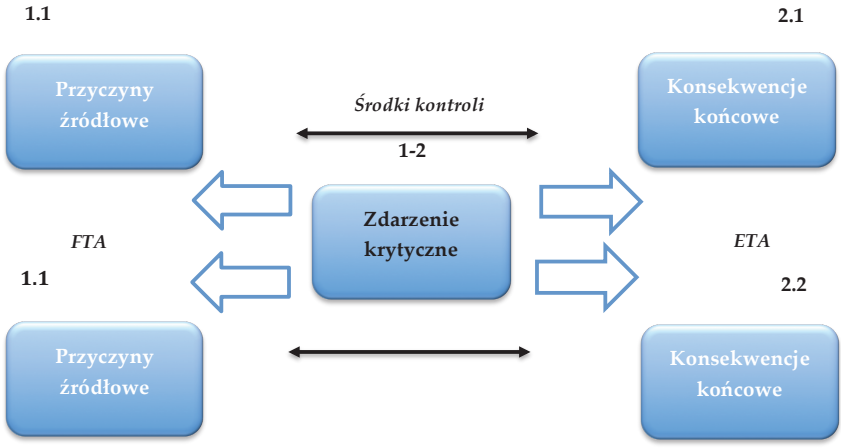
10 Tamże, s. 53.

Umieszczony na rysunku 3.5. niebieski łącznik *LUB* oznacza, że warunkiem zaistnienia kolejnego zdarzenia rozgałęziającego jest wystąpienie przynajmniej jednego z dwóch zdarzeń poprzedzających, np. dla zdarzenia *zanieczyszczenia* są to zdarzenia: *Śnieżyca LUB Lawina błotna*. Z kolei niebieski łącznik nie oznaczony wyrazem *LUB*, dotyczy możliwości wystąpienia zdarzenia warunkowanego koniecznością pojawienia się obu zdarzeń poprzedzających jednocześnie, np. wystąpienie zdarzenia *wypadek* determinowane jest równoczesnym wystąpieniem zdarzeń: *Możliwość poślizgu I Zła reakcja kierowcy*.

Metoda Bow-tie (muszka) służy do oceny ryzyka i zarządzania ryzykiem. Bow-tie w schematyczny sposób opisuje i analizuje ścieżki ryzyka od przyczyn do skutków. Można ją uznać za połączenie drzewa błędów (analiza przyczyn zdarzenia) i drzewa zdarzeń (analiza konsekwencji). Metoda skupia się wokół wskazania barier zapobiegających przyczynom oraz skutkom danego zdarzenia. Jest ona rozpoczynana po *burzy mózgów*.

Proces analizy za pomocą metody Bow-tie uwzględnia następujące założenia:
- zidentyfikowane ryzyko znajduje się w centralnej części – jako zdarzenie krytyczne,
- określenie potencjalnych przyczyn zdarzenia – po lewej stronie,
- określenie potencjalnych skutków zdarzenia – po prawej stronie,
- połączenie schematu z uwzględnieniem czynników, które mogą doprowadzić do eskalacji,
- określenie barier, które powinny zapobiec każdej z przyczyn oraz do niepożądanych skutków[11].

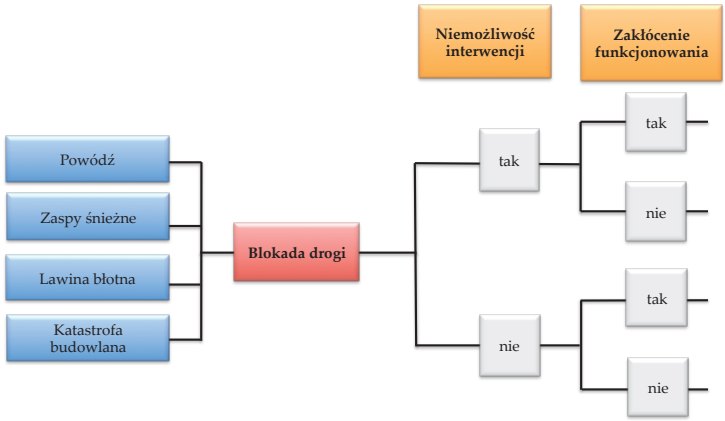
Poniższy przykład (wraz ze schematem, rys. 3.6.) przedstawia wykorzystanie analizy Bow-tie w odniesieniu do hipotetycznego zdarzenia krytycznego.



Rysunek 3.6. Schemat metody Bow-tie

Źródło: Materiał zgromadzony w toku realizacji projektu: Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. Projekt dokumentu opisującego wytyczne dla jednostek samorządu terytorialnego i administracji rządowej dotyczące identyfikacji zagrożeń i analizy ryzyka Zad. VII.7 1.1.PZ.OP.PK.1

[11] IEC/FDIS 31010 *Risk management — Risk assessment techniques.*



Rysunek 3.7. Drzewo błędów i zdarzeń dla przypadku blokady drogi. Metoda Bow-tie

Źródło: Materiał zgromadzony w toku realizacji projektu: Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. PE.VII.6 Opracowanie metodyki analizy ryzyka możliwej do zastosowania na różnych poziomach zarządzania kryzysowego, w tym opracowanie procedury tworzenia map ryzyka i map zagrożeń

Rysunek 3.7. ilustruje z kolei przykład wykorzystania metody Bow-tie dla zdarzenia związanego z blokadą drogi:

Istotą metody *Co jeśli*? jest budowanie zwrotów pod kątem pytań *co jeśli?*, dzięki czemu udziela się odpowiedzi na pytania, co się stanie w przypadku wystąpienia różnych zdarzeń. Metoda może być wykorzystywana w wielu sytuacjach i w różnych dziedzinach. Zaletą niniejszej techniki jest także ukierunkowanie uczestnika na analizę przyczyn i skutków poprzez uzyskanie odpowiedzi na szereg pytań, takich jak *co jeśli…? co mogłoby się stać…? czy ktokolwiek, kiedykolwiek…?*

Pytania za każdym razem są przygotowywane przed przystąpieniem do badania i mają na celu omówienie:

- znanych czynników ryzyka i zagrożeń,
- dotychczasowych doświadczeń,
- znanych i istniejących środków kontroli i zabezpieczeń,
- wymogów prawnych i ograniczeń.

Ponadto technika nie wymaga dużego nakładu pracy przez zespół i dzięki jej zastosowaniu stosunkowo szybko można wytypować główne zagrożenia[12].

Przykładowa procedura zastosowania analizy SWIFT obejmuje:

1. Wyselekcjonowanie podstawowych pojęć (słowa klucze), które będą stosowane w SWIFT.
2. Wybór uczestników warsztatu opartego na podstawie wiedzy i znajomości procesu.
3. Opisanie: zmian regulacyjnych, zdarzeń niepożądanych.

[12] Based on the PHA Waterfall Model Beyond FMEA: The structured what-if technique (SWIFT) © 2012 American Society for Healthcare VOLUME 31, NUMBER 4 23 By Alan J. Card, MPH, CPH, CPHQ James R.Ward, BEng, CEng,PhD, MIET, and P. John Clarkson, PhD, BA(Eng).

4. Wyjaśnienie celu stosowania SWIFT (np. w celu poprawy bezpieczeństwa ludności lokalnej).
5. Określenie kryteriów sukcesu (np. zmniejszenie liczby wypadków z udziałem pieszych).
6. Zapewnienie wysokiego poziomu opisów tekstowych i graficznych systemu lub procesu, w celu dokonania oceny ryzyka.
7. Rozpoznanie ryzyka/zagrożeń za pomocą zwrotów *co jeśli...*, *jak mógłbyś...*, aby wywołać potencjalne ryzyka/zagrożenia zgodnie z ustalonymi pojęciami. Na przykład: jak możemy zapobiegać wypadkom na drogach?
8. Ocena ryzyka związana ze zidentyfikowanymi zagrożeniami.
9. Redukcja zidentyfikowanego ryzyka do dopuszczalnego poziomu.
10. Ustalenie, czy SWIFT osiągnął swoje cele, czy też wymagana jest bardziej szczegółowa ocena ryzyka dla poszczególnych zagrożeń.

Technika *Co jeśli* (SWIFT) jest elastyczna i może być wykorzystywana samodzielnie lub jako element składowy innych metod szacowania ryzyka.

Poniżej przedstawiono przykład zastosowania metody *Co jeśli?* dla zdarzenia: Awaria w zakładzie produkującym i magazynującym niebezpieczne substancje chemiczne.

Cel analizy: wskazanie potencjalnych przyczyn i skutków wystąpienia awarii w zakładzie produkującym i magazynującym niebezpieczne substancje chemiczne pod kątem określenia prawdopodobieństwa wystąpienia zdarzenia oraz dotkliwości jego skutków.

Uczestnicy *warsztatów/burzy mózgów*: przedstawiciele administracji publicznej, służb ratowniczych, właściciele obiektów przemysłowych, specjaliści z dziedziny chemii.

Pytania badawcze:

1) Co mogłoby być przyczyną wystąpienia awarii w zakładzie (błąd ludzki, błąd techniczny, brak nadzoru, wypadek, rozszczelnienie zbiornika lub instalacji z toksyczną substancją, nieprzestrzeganie przepisów przeciwpożarowych, katastrofa naturalna, atak terrorystyczny)?
2) Co jeśli w wyniku awarii wystąpiłoby bezpośrednie zagrożenie dla życia i zdrowia osób? Ile osób mogłoby zginąć/ucierpieć w wyniku awarii/wymagałoby udzielenia pomocy medycznej/ile osób musiałoby zostać ewakuowanych?
3) Co jeśli w wyniku awarii pojawiłyby się okresowe utrudnienia w przemieszczaniu się? Jak długo mogłyby one potrwać? Jak szybko udałoby się przywrócić możliwość przemieszczania się?
4) Co jeśli w wyniku awarii zniszczone zostaną zbiory w gospodarstwach rolnych? Które z gospodarstw byłyby najbardziej narażone na zniszczenia? Jak bardzo mógłby zostać osłabiony przemysł spożywczy, biorąc pod uwagę aspekt ekonomiczny? Czy w konsekwencji mogłyby wzrosnąć ceny produktów żywnościowych? Jak wysoki mógłby być koszt odszkodowań dla przedsiębiorców

zajmujących się przetwarzaniem i sprzedażą żywności? Którzy z nich mogliby zostać najbardziej poszkodowani w wyniku awarii?

5) Co jeśli wystąpią zniszczenia w infrastrukturze komunalnej i transportowej? Który rodzaj infrastruktury byłby najbardziej narażony? Z jak dużymi kosztami wiązałaby się ich modernizacja/naprawa? Co się stanie, jeśli skażone zostaną źródła wody lub sieci wodociągowe? Które źródła wody lub sieci wodociągowe byłyby najbardziej narażone na wystąpienie awarii? Czy udałoby się zapewnić wszystkim poszkodowanym awaryjne dostawy wody?
6) Co jeśli dojdzie do długoterminowego zablokowania szlaków komunikacyjnych? Jak duże mogłyby być utrudnienia w transporcie? Po jakim czasie udałoby się przywrócić drożność ciągów komunikacyjnych?
7) Co jeśli zakłócone zostaną procesy technologiczne w zakładach pracy? Jak bardzo mogłaby zmniejszyć się produkcja określonych artykułów lub świadczenie usług?
8) Co jeśli wystąpią straty w dziedzictwie narodowym? Które zabytki ruchome lub nieruchome mogłyby zostać zniszczone?

Analiza wpływu na organizację (*Business Impact Analysis*) jest elementem planu działalności biznesowej pozwalającym określić potencjalne zagrożenia i ich wpływ na daną działalność, a także strategię minimalizacji ryzyka.

Jednym z podstawowych założeń metody BIA jest uszeregowanie i ocena kluczowych procesów i składników organizacji wraz z określeniem strat finansowych i niefinansowych w przypadku przerwania lub zakłócenia ocenianych elementów. Ponadto BIA ma na celu wskazanie relacji krytyczności procesów w ramach ocenianej jednostki, w stosunku do krytyczności tych procesów w skali całej organizacji (np. satysfakcja klienta, wizerunek organizacji, zależność innych procesów od ocenianego procesu)[13]. Posiadając wiedzę na temat procesów krytycznych zachodzących w organizacji oraz wyniki analizy wpływu na organizację procesów krytycznych, można przystąpić do szacowania ryzyka dla procesów organizacji.

Analiza BIA wykorzystywana jest przy tworzeniu planów ciągłości działania. Składa się ona z następujących czterech głównych etapów:

1. Działania przygotowawcze (w tym: określenie zakresu analizy, wyznaczenie celów, wybór metod, określenie ról i przyporządkowanie do nich osób, szkolenie i udzielanie wyjaśnień oraz uzyskanie wsparcia kierownictwa).
2. Gromadzenie danych (w tym: wypełnianie formularzy, wyliczenie potencjalnych strat, m.in. finansowych, reputacyjnych, zdefiniowanie wymagań odtworzeniowych dla czasu, po upływie którego określone straty są dla organizacji nieakceptowalne (RTO) oraz akceptowalnego przez organizację poziomu utraty danych (RPO).

[13] D. Romańczuk, *Analiza wpływu zdarzenia na biznes*, NetApp Data Center Fitness, 20 czerwca 2013 r.

3. Opracowanie wyników (w tym: weryfikacja wymagań odtworzeniowych dla RTO oraz RPO, określenie procesów krytycznych oraz wyznaczenie priorytetów dla odtworzenia procesów).
4. Wdrożenie (w tym: prezentacja wyników kierownictwu, zatwierdzenie wyników przez kierownictwo oraz wprowadzenie ich w życie)[14].

Analiza BIA może być przeprowadzona za pomocą kwestionariuszy ankiet, wywiadów, warsztatów (lub kombinacji tych trzech metod) na potrzeby zrozumienia procesów krytycznych, konsekwencji strat dla tych procesów, jak również wymagań czasowych ich odtworzenia[15].

Zaletą tej metody jest to, że umożliwia ona zrozumienie procesów, które zapewniają ciągłość działania organizacji oraz osiągnięcie wyznaczonego celu. Ponadto pozwala na określenie niezbędnych zasobów, jak również na zdefiniowanie procesu operacyjnego, dzięki któremu możliwe jest podniesienie odporności danej organizacji.

Z kolei ograniczeniem w wykorzystaniu tej metody może być: trudność w odpowiednim zrozumieniu działalności podmiotu oraz zbyt uproszczone bądź zbyt optymistyczne oczekiwania w stosunku do wymagań odtworzeniowych[16].

Poniższy przykład ilustruje wykorzystanie analizy BIA dla zdarzenia krytycznego, jakim jest brak prądu[17]. W odniesieniu do tego zdarzenia oraz jego konsekwencji wyznaczono:

- czas krytyczny, tj. czas przerwy funkcjonowania danego procesu (CzK),
- czas odtworzenia, tj. czas od wystąpienia zdarzenia (katastrofy) do odtworzenia funkcjonowania procesu na akceptowalnym poziomie (CzO),
- plan działań na wypadek *katastrofy*, np. poważnej awarii (DRP).

1. Brak prądu (CzK: 4 h; CzO:9 h; DRP: x).
1.1. Wyłączenie instalacji domowych (CzK:8 h; CzO: 24 h; DRP: x).
1.1.1. Utrata możliwości ogrzewania domu/mieszkania (CzK: 24 h, CzO: 24 h, DRP: wydanie ciepłej odzieży/ewakuacja z miejsc pozbawionych prądu).
1.1.2. Brak ciepłej wody (CzK:48 h; CzO: 48h; DRP: x).
1.1.3. Oświetlenie domu (CzK: 8 h; CzO: 48 h; DRP: wydanie lamp naftowych, świeczek, solarek).
1.1.4. Utrata możliwości przygotowania/przechowywania posiłków (CzK:8 h. CzO: 8 h. DRP: dostawa żywności niepsującej się).
1.1.5. Wyłączenie Internet/telefon (CzK: 48 h; CzO: 96 h; DRP: agregaty prądotwórcze).
1.2. Wyłączenie instalacji komunalnych (CzK: 4 h; CzO: 24 h; DRP: x).

---

[14] R.W. Kaszubski, D. Romańczuk (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania (Business Continuity Management), Forum Technologii Bankowych przy Związku Banków Polskich*, Warszawa 2011, s. 78-79.

[15] IEC/FDIS 31010 *Risk management — Risk assessment techniques*; s. 43.

[16] Tamże, s. 43-44.

[17] Przykład pochodzi z materiałów ze szkolenia PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym.

1.2.1. Brak dostaw wody bieżącej (CzK: 4h; CzO: 24 h, DRP: dostawy wody w beczkowozach).
1.2.2. Wyłączenie pompy ścieków (CzK: 4 h; CzO: 24 h; DRP: wywóz ścieków szambiarkami).
1.3. Wyłączenie komunikacji publicznej, tj. tramwajów, trolejbusów, metra i kolei (CzK: 24 h, CzO: 24 h; DRP: wprowadzenie komunikacji zastępczej).
1.4. Ograniczenie pracy służb porządkowych i ratowniczych (CzK: 2 h; CzO: 24 h; DRP: agregaty prądotwórcze).

Metoda analizy scenariuszy może być stosowana do identyfikacji ryzyka poprzez rozważenie ewentualnych przyszłych zmian i badanie ich skutków. Technika używana jest do pomocy w podejmowaniu decyzji i planowaniu, jak również do rozważenia dotychczasowych działań. Analiza scenariuszowa może mieć zastosowanie we wszystkich komponentach oceny ryzyka.

Identyfikacja i analiza zestawów scenariuszy odzwierciedlających *najlepszy przypadek*, *najgorszy przypadek* i *spodziewany przypadek* może być stosowana do identyfikacji zdarzeń niepożądanych i analizować potencjalne konsekwencje ich wystąpienia. Symulacje mogą być użyteczne, gdy istnieją istotne różnice w przestrzeni, czasie i w danej grupie społecznej czy organizacji. Analiza scenariuszowa bada różne konteksty, przewiduje zmiany, a także wpływ na wynik końcowy[18].

Metoda scenariuszowa obejmuje następujące etapy:
- ustalenie zakresu analizy,
- identyfikacja czynników determinujących wyniki decyzji strategicznych,
- określenie sił zewnętrznych,
- ustalenie logiki scenariuszy,
- analiza skutków scenariuszy,
- analiza skutków decyzji[19].

W procesie analizy scenariuszowej warto uwzględnić:
- zmiany zewnętrzne (takie jak zmiany technologiczne),
- decyzje, które muszą być wykonane w najbliższej przyszłości, a które mogą mieć różne wyniki,
- potrzeby zainteresowanych stron z uwzględnieniem ich zmian,
- zmiany w otoczeniu makro (regulacyjne, demografii itp.). Niektóre z nich będą nieuniknione, a niektóre będą niepewne.

Analiza scenariuszy może być przydatnym narzędziem oceny ryzyka, jednak warto uzupełnić ją elementami metodyk ilościowych, narzędzie staje się wtedy bardziej wiarygodne. Wadą tej metody jest dość wysoka niepewność wiarygodności scenariusza – może okazać się, że opracowany scenariusz nie będzie miał zastosowania w rzeczywistości.

Tabela 3.3. przedstawia przykładowe scenariusze wystąpienia powodzi na danym terenie.

---

[18] IEC/FDIS 31010 *Risk management — Risk assessment techniques.*

[19] M. Lisiński, *Metody planowania strategicznego,* Polskie Wydawnictwo Ekonomiczne, Warszawa 2004, ISBN: 83-208-1525-8 cytat, s. 106.

Tabela 3.3. Przykładowe scenariusze wystąpienia powodzi

POWÓDŹ			
NAZWA CZYNNIKA	**SKALA OCEN (1-5)**	**PRAWDOPODOBIEŃSTWO WYSTĄPIENIA**	**ŚREDNI WPŁYW**
SCENARIUSZ OPTYMISTYCZNY			
Nasilenie się opadów atmosferycznych	3	0,2	1,6
Fala przepływu	2	0,2	1,1
Przerwanie wału	1	0,1	0,55
Nieodpowiednie podjęcie działań służb	2	0,2	1,1
Zasięgi zalewów historycznych	3	0,3	1,5
SCENARIUSZ PESYMISTYCZNY			
Nasilenie się opadów atmosferycznych	4	0,5	2,25
Fala przepływu	4	0,4	2,2
Przerwanie wału	3	0,3	1,65
Nieodpowiednie podjęcie działań służb	4	0,5	2,25
Zasięgi zalewów historycznych	3	0,4	1,7
SCENARIUSZ UMIARKOWANY			
Nasilenie się opadów atmosferycznych	3	0,3	1,5
Fala przepływu	2	0,1	1,05
Przerwanie wału	2	0,4	1,5
Nieodpowiednie podjęcie działań służb	3	0,2	1,6
Zasięgi zalewów historycznych	3	0,2	1,6

Źródło: opracowanie własne

Norma IEC/FDIS 31010 może okazać się przydatna w ramach przeprowadzenia analizy ryzyka na potrzeby planowania kryzysowego w aspekcie użycia wybranych technik i narzędzi oceny ryzyka. Wydaje się ona o tyle użyteczna, iż obejmuje szczegółowe opisy i charakterystykę poszczególnych metod, jak również wskazuje, na którym etapie procesu oceny ryzyka mogą zostać zastosowane. Kluczową kwestią wydaje się dobór odpowiedniej techniki lub narzędzia oceny ryzyka przez

osobę przeprowadzającą analizę. Zdaniem autorów za najbardziej użyteczne z nich można uznać metody analizy drzewa zdarzeń (ETA), analizy drzewa błędów (FTA), Bow-tie, BIA, *Co jeśli?* oraz analizy scenariuszy. Mogą one znaleźć swoje zastosowanie zwłaszcza na etapie budowy scenariuszy możliwych zdarzeń.

3.4. Norma BS ISO 22301:2012 Bezpieczeństwo powszechne – Systemy Zarządzania Ciągłością Działania

- Norma BS ISO 22301:2012 *Bezpieczeństwo Powszechne – Systemy Zarządzania ciągłością działania – Wymagania* (*Societal security – Business continuity management systems – Requirements*) obejmuje wymagania związane z ustanawianiem skutecznego Systemu Zarządzania Ciągłością Działania (SZCD) oraz zarządzania nim. Zastąpiła ona brytyjskie standardy BS 25999. Pomimo iż założenia normy BS ISO 22301:2012 są w dużej mierze zbieżne z nimi, omawiany dokument wprowadza istotne zmiany, w tym m.in.:
  - *odnosi się do najwyższego kierownictwa każdej organizacji,*
  - *wprowadza bardziej widoczne i bardziej aktywne przywództwo najwyższego kierownictwa,*
  - *wprowadza wymóg bardziej starannego planowania i przygotowania zasobów niezbędnych do zapewnienia ciągłości biznesu,*
  - *znacznie mocniej akcentuje kwestie związane z ustalaniem celów, monitorowaniem skuteczności i pomiarami,*
  - *kładzie większy nacisk na elementy dotyczące komunikacji oraz większą odpowiedzialność przed szerzej zdefiniowaną społecznością, silniej powiązana jest z podejściem organizacji do ryzyka*[20].

Wymagania opisane w normie BS ISO 22301 dotyczą szerokiego spektrum zagadnień, w tym planowania, ustanawiania, wdrażania, funkcjonowania, monitorowania, przeglądania, utrzymywania, jak również ciągłego doskonalenia udokumentowanego systemu zarządzania. Celem funkcjonowania takiego systemu jest zapewnienie ochrony przed incydentami, zmniejszenie prawdopodobieństwa ich wystąpienia, przygotowanie się na nie, jak również umiejętność podjęcia adekwatnej reakcji oraz powrotu do normalnego funkcjonowania w przypadku ich wystąpienia.

Wymagania te mają charakter ogólny. Wskazuje się, iż mogą one zostać wykorzystane w organizacji o dowolnym charakterze, każdego typu oraz rozmiaru. Zakres zastosowania tych wymagań uwarunkowany jest środowiskiem, w którym dana organizacja działa, jak również stopniem jej złożoności. Tym samym norma BS ISO 22301 nie narzuca jednolitej struktury Systemu Zarządzania Ciągłością Działania, lecz stanowi wsparcie na rzecz zaprojektowania SZCD w danej organizacji w zależności od jej potrzeb. Wiążą się one bowiem m.in. z wymogami prawnymi, nadzorczymi, organizacyjnymi oraz branżowymi. Dotyczą również wyrobów

[20] Witryna internetowa http://www.iso.org.pl/iso-22301 z dnia 08.06.2015 r.

i usług, stosowanych procesów, rozmiaru, struktury organizacji, jak również wymagań zainteresowanych stron.

Norma dedykowana jest głównie organizacjom, które chciałyby ustanowić, wdrożyć, zachować i doskonalić SZCD, jak również zapewnić zgodność z ustaloną polityką ciągłości działania oraz wykazywać zgodność w stosunku do innych. Ponadto kierowana jest do tych z nich, które dążą do certyfikacji bądź rejestracji swojego SZCD przez akredytowaną niezależną jednostkę certyfikującą. Norma może znaleźć również zastosowanie w organizacjach, które chcą zadeklarować zgodność z niniejszą normą oraz samodzielnie do tego dążą.

W normie BS ISO 22301:2012 stosuje się szereg terminów i definicji związanych z procesami zarządzania ciągłością działania oraz zarządzania ryzykiem. Część definicji wybranych pojęć zaczerpnięto z takich dokumentów, jak: ISO Guide 73 oraz ISO 22300. Pozostałe z nich przyjęto na potrzeby opracowania niniejszej normy.

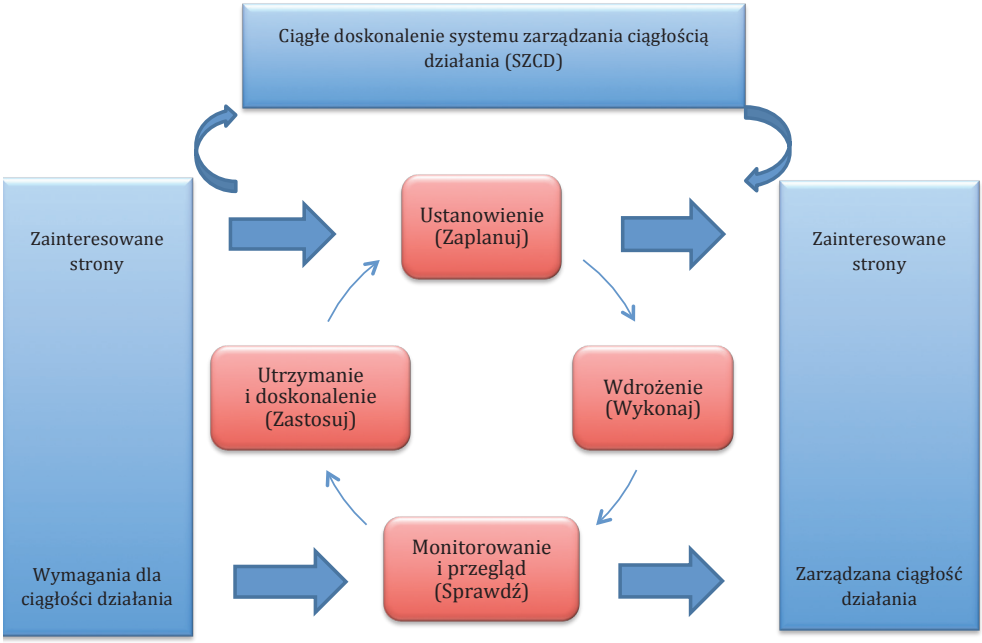
Kluczowe znaczenie dla zrozumienia założeń normy BS ISO 22301:2012 ma zdefiniowanie terminu zarządzania ciągłością działania. Jest ono rozumiane jako *holistyczny proces zarządzania, identyfikujący potencjalne zagrożenia organizacji i skutki, jakie te zagrożenia mogą wywierać na działalność biznesową w przypadku ich wystąpienia*[21]. Umożliwia on zbudowanie odporności organizacji, jak również pozwala na skuteczną reakcję w celu ochrony interesów jej kluczowych interesariuszy, jej reputacji oraz marki. Z kolei za system zarządzania ciągłością działania uznaje się *część ogólnego systemu zarządzania dotyczącą ustanowienia, wdrożenia, funkcjonowania, monitorowania, przeglądu, utrzymania oraz doskonalenia ciągłości działania*[22]. Zgodnie z normą składają się na niego takie elementy, jak: struktura organizacyjna, polityka, działania planistyczne, zakresy odpowiedzialności, procedury, procesy oraz zasoby.

Norma BS ISO 22301:2012 przewiduje użycie modelu PDCA (z ang. *Plan-Do--Check-Act*) na potrzeby ustanowienia SZCD oraz zarządzania nim. Jest on zgodny z ustaleniami wynikającymi z innych norm dotyczących systemów zarządzania. Zasadę działania SZCD przedstawiono rysunku 3.8.

W pierwszym kroku cyklu (tzw. Planuj) ustanawia się politykę ciągłości działania, mechanizmy nadzoru, procesy i procedury właściwe dla doskonalenia ciągłości działania. Dokonuje się tego na potrzeby osiągnięcia wyników zgodnych z ogólną polityką oraz celami organizacji. Istotą kolejnego etapu (tzw. wykonuj) jest wdrożenie i realizacja polityki ciągłości działania, jak również mechanizmów nadzoru, procesów oraz procedur. Trzeci etap (tzw. Sprawdzaj) polega na monitorowaniu oraz przeglądzie efektywności systemu w odniesieniu do polityki i celów ciągłości działania. Obejmuje on również przedsięwzięcia związane z raportowaniem wyników do kierownictwa na potrzeby ich przeglądu. Na tym etapie wskazuje się także działania naprawcze, doskonalące oraz zezwala się na ich wykonanie. Ostatni krok (tzw. Działaj) dotyczy utrzymania i doskonalenia SZCD

[21] Norma BS ISO 22301:2012 *Bezpieczeństwo powszechne – Systemy zarządzania ciągłością działania – Wymagania*, s. 2.

[22] Tamże.



Rysunek 3.8. Cykl PDCA stosowany w procesach systemu zarządzania ciągłością działania

Źródło: Norma BS ISO 22301:2012 Bezpieczeństwo powszechne – Systemy Zarządzania Ciągłością Działania

poprzez podejmowanie działań korygujących, bazując na wynikach przeglądu zarządzania oraz ponownym określeniu zakresu SZCD, jak również polityki i celów ciągłości działania.

Istotnym aspektem działań planistycznych podejmowanych w kroku nr 1 Ustanowienie (Zaplanuj) jest zrozumienie organizacji oraz kontekstu jej działania. W tym względzie zaleca się, aby każda organizacja określiła zewnętrzne i wewnętrzne kwestie, które mają dla niej znaczenie, jak również te, które oddziałują na jej zdolność do osiągnięcia zakładanych wyników SZCD. Wskazuje się, iż definiując kontekst organizacji należy brać pod uwagę elementy takie, jak: swoje działalności, funkcje, usługi, wyroby, partnerstwa, łańcuchy dostaw, jak również relacje ze stronami zainteresowanymi oraz potencjalny wpływ związany z incydentami zakłócającymi jej działania. Istotną kwestią jest również określenie powiązań pomiędzy polityką ciągłości działania a celami i innymi politykami organizacji oraz wyznaczenie apetytu na ryzyko.

Ponadto w normie podkreśla się, iż znaczącą kwestią jest zrozumienie wymagań i oczekiwań zainteresowanych stron. Zaleca się, aby dana organizacja przy ustanawianiu, wdrażaniu i utrzymywaniu SZCD wzięła pod uwagę wymagania prawne oraz nadzorcze.

W oparciu o działania podjęte na etapie ustalenia kontekstu określa się zakres SZCD. Bierze się przy tym pod uwagę misję organizacji, jej cele oraz wewnętrzne

i zewnętrzne zobowiązania. Ponadto identyfikuje się wyroby, usługi, inne powiązane działalności obejmujące zakres SZCD, jak również wymagania i oczekiwania zainteresowanych stron. Wskazuje się, iż ustanawiając zakres SZCD należy uwzględnić również rozmiar, rodzaj oraz złożoność organizacji.

W normie BS ISO 22301:2012 istotną rolę przypisuje się kwestii przywództwa i zaangażowania najwyższego kierownictwa w ramach SZCD. Może ono objawiać się w formie motywowania i upoważniania osób, tak aby istotnie przyczynić się do uzyskania skuteczności SZCD. Zadaniem najwyższego kierownictwa jest również wyznaczenie członkom organizacji odpowiednich ról, związanych z nimi uprawnień oraz odpowiedzialności w zakresie SZCD. Co więcej, powinno ono ustanowić politykę ciągłości działania dostosowaną do celu istnienia organizacji, zgodną z celami ciągłości działania. Te ostatnie muszą być zakomunikowane osobom pełniącym właściwe funkcje na poszczególnych szczeblach organizacji.

Działania przygotowawcze związane z wdrożeniem SZCD powinny obejmować wskazanie ryzyk oraz możliwości. Wspomoże to osiągnięcie przez system zarządzania zamierzonych rezultatów, zapobieżenie niechcianym skutkom lub ich redukcję oraz pozwoli na ciągłe doskonalenie. Organizacja powinna zaplanować ponadto działania uwzględniające zidentyfikowane wcześniej ryzyka i możliwości.

Istotnym aspektem jest konieczność określenia przez organizację zasobów, które są niezbędne do ustanowienia, wdrożenia, utrzymania oraz ciągłego doskonalenia SZCD. Zgodnie z niniejszą normą składają się na nie: kompetencje, świadomość, komunikacja oraz udokumentowane informacje.

W odniesieniu do pierwszego ze wskazanych obszarów, norma wskazuje, iż organizacja powinna określić niezbędne kompetencje osób wykonujących na jej rzecz pracę, tym samym warunkując efekty podejmowanych działań. Za szczególnie ważne uznaje się odpowiednie kształcenie, szkolenie oraz doświadczenie personelu. Dopuszcza się przy tym możliwość podjęcia działań mających na celu podniesienie kompetencji obecnych pracowników oraz doradzanie im.

Oprócz zadbania o wysoki poziom kompetencji pracowników, kluczowe jest zapewnienie świadomości personelu na temat polityki ciągłości działania, jego wkładu w skuteczność SZCD, skutków nieprzestrzegania wymagań SZCD oraz roli pracowników w przypadku wystąpienia incydentów zakłócających działanie.

Ponadto organizacja powinna wypracować mechanizmy wewnętrznej oraz zewnętrznej komunikacji istotnej dla SZCD, określając tematykę komunikacji, czas komunikacji oraz osoby, z którymi będzie ona prowadzona.

Za istotne uważa się również posiadanie przez organizację udokumentowanych informacji zarówno tych wymaganych przez niniejszą normę, jak również tych uznanych przez organizację za niezbędne do osiągnięcia skuteczności SZCD. W tym względzie należy zadbać o odpowiednią identyfikację i opis dokumentu oraz jego odpowiedni format. Ponadto podkreśla się konieczność zapewnienia odpowiedniego nadzoru nad udokumentowanymi informacjami, tak aby były one dostępne w odpowiednim miejscu i czasie oraz aby były we właściwy sposób chronione.

W kroku nr 2 *Wdrożenie (Wykonaj)* istotne jest zaplanowanie, wdrożenie i nadzorowanie przez organizację procesów, które są niezbędne do spełnienia wymagań oraz realizacji działań uwzględniających ryzyka i możliwości. Będzie to możliwe dzięki ustanowieniu kryteriów takich procesów oraz wdrożeniu nadzoru nad nimi zgodnie z tymi kryteriami. Dokonuje się tego również poprzez przechowywanie wszelkich informacji, które pozwalają na stwierdzenie, że procesy zostały przeprowadzone zgodnie z planem.

Nieodłącznym elementem tego etapu jest ustanowienie, wdrożenie oraz utrzymywanie formalnego procesu analizy wpływu biznesowego oraz oceny ryzyka. W procesie tym należy uwzględnić kontekst oceny ryzyka, jak również zdefiniować kryteria oraz ocenić potencjalny wpływ incydentu zakłócającego działanie. Zaleca się również wzięcie pod uwagę wymagań prawnych oraz innych wymagań, które przyjęła organizacja. Niniejszy proces obejmuje także systematyczną analizę oraz wskazanie priorytetów co do postępowania z ryzykiem wraz z związanymi z tym kosztami. Za kluczową dla analizy wpływu biznesowego uznaje się ocenę skutków zakłócenia działalności, wspierających dostarczenie wyrobów i usług przez organizację. Z kolei w odniesieniu do konieczności ustanowienia, wdrożenia oraz utrzymywania procesu oceny ryzyka rekomenduje się jego przeprowadzenie zgodnie z normą ISO 31000. Dzięki temu będzie możliwa systematyczna identyfikacja, analiza i ocena ryzyka incydentu zakłócającego działanie organizacji.

W oparciu o wyniki analizy wpływu biznesowego i oceny ryzyka należy ustalić i dokonać wyboru strategii ciągłości działania. Jej celem jest ochrona priorytetowej działalności, jak również jej ustabilizowanie, kontynuacja, wznawianie, odtwarzanie, ograniczanie skutków oraz reagowanie na ich wystąpienie. Znaczącą kwestią jest również ustalenie ram czasowych, w których zakłócona działalność zostanie wznowiona. Wdrożenie wybranej strategii będzie możliwe dzięki określeniu wymagań dotyczących zasobów przydatnych w tym celu. Wśród nich można wymienić m.in. ludzi, informacje i dane, budynki, środowisko pracy oraz związane z nimi narzędzia, jak również systemy teleinformatyczne. Kolejną podjętą czynnością powinno być zidentyfikowanie ryzyk wymagających postępowania z nimi, jak również dokonanie wyboru i wdrożenie sposobów postępowania z ryzykiem.

Bardzo ważnym aspektem kroku nr 2 jest ustanowienie i wdrożenie procedur ciągłości działania. Dzięki temu organizacja będzie mogła odpowiednio zarządzać incydentem, jak również kontynuować swoją działalność, opierając się na celach wznowienia działania zdefiniowanych w analizie wpływu biznesowego. Co więcej powinna ona ustanowić oraz wdrożyć procedury oraz strukturę zarządczą w celu reagowania na zakłócający działanie incydent. W odpowiedzi na wystąpienie incydentu należy wykorzystać personel posiadający niezbędne kompetencje oraz uprawnienia do zarządzania nim. W takiej strukturze należy uwzględnić wskazanie progów incydentu, decydujących o zainicjowaniu reakcji, jak również ocenę rodzaju i zakresu incydentu zakłócającego działanie oraz jego potencjalne skutki, wywołanie odpowiedniej reakcji związanej z ciągłością działania czy też posiadanie procesów i procedur z tym związanych.

Kolejną grupę procedur znaczących z punktu widzenia funkcjonowania SZCD stanowią procedury komunikacji oraz ostrzegania. Mają one na celu wykrywanie incydentu, jego regularne monitorowanie, jak również otrzymywanie, przechowywanie oraz reagowanie na informacje z regionalnych systemów powiadamiania o zagrożeniach.

Istotną rolę pełni również ustanowienie przez organizację procedur reagowania na incydent zakłócający działanie, jak również procedur obejmujących sposoby kontynuowania lub odtwarzania jej działalności w określonych ramach czasowych. Dokumenty obejmujące wskazany powyżej zakres informacji określa się mianem planów ciągłości działania. Zawierają one m.in. zdefiniowanie ról i odpowiedzialności osób oraz zespołów mających uprawnienia w trakcie trwania incydentu oraz po jego wystąpieniu, proces wywołujący reakcję, szczegółowe informacje na temat zarządzania skutkami incydentu czy też sposób kontynuacji lub odtworzenia działalności priorytetowych przez organizację w określonym czasie. Za nieodłączny element planów ciągłości działania uznaje się również ustalenie strategii komunikacji organizacji z mediami po wystąpieniu incydentu.

Zgodnie z normą BS ISO 22301:2012 każda organizacja powinna również posiadać procedury odtworzenia i powrotu do działalności biznesowych (po wdrożeniu rozwiązań tymczasowych) na potrzeby wsparcia wymagań normalnego biznesu po zakończeniu incydentu.

W normie podkreśla się, iż organizacja powinna nie tylko ustanowić właściwe procedury ciągłości działania, ale również ćwiczyć je oraz testować.

W kroku nr 3 *Monitorowanie i Przegląd (Sprawdź)* zaleca się przeprowadzenie oceny efektywności funkcjonowania systemu zarządzania ciągłością działania. W tym kontekście zadaniem organizacji jest określenie zakresu monitorowania i mierzenia, metod monitorowania, pomiarów, analizy oraz oceny, jak również terminu realizacji tych przedsięwzięć.

Istotną kwestią jest przeprowadzanie oceny procedur i możliwości utrzymania ciągłości działania na potrzeby zapewnienia ich ciągłej przydatności, adekwatności oraz skuteczności. W normie wskazuje się, iż powinny one być przeprowadzane w formie okresowych przeglądów, ćwiczeń, testów, jak również raportów po wystąpieniu incydentów. Ponadto podkreśla się, że w tym względzie należy brać pod uwagę wymagania prawne i nadzorcze oraz najlepsze praktyki branżowe.

Kolejną formą oceny efektywności SZCD jest przeprowadzanie w określonych odstępach czasu audytów wewnętrznych. Mają one na celu ocenę jego zgodności z własnymi wymaganiami organizacji dotyczącymi SZCD oraz wymaganiami niniejszej normy, jak również ocenę skuteczności jego wdrożenia i utrzymywania. Podkreśla się, że program audytu, w tym także jego harmonogram, powinien bazować na wynikach oceny ryzyka dla działalności organizacji oraz rezultatach poprzednich audytów.

W normie zaleca się dokonywanie okresowo przeglądów SZCD w organizacji na potrzeby utrzymania jego przydatności, adekwatności oraz skuteczności. Przeprowadzając je, należy wziąć pod uwagę status działań po poprzednich przeglądach

zarządzania, jak również zmiany w zewnętrznych oraz wewnętrznych kwestiach istotnych z punktu widzenia systemu zarządzania ciągłością działania. Powinno się również uwzględnić informacje o efektywności ciągłości działania. Wiąże się ona z ryzykami lub kwestiami, które nie zostały ostatecznie rozstrzygnięte w czasie wcześniej przeprowadzonej oceny ryzyka. Zakłada się, iż przegląd będzie się kończył podjęciem odpowiednich decyzji związanych z możliwościami ciągłego doskonalenia lub koniecznością zmian w SZCD. Powinien również zawierać m.in. aktualizację oceny ryzyka, analizy wpływu biznesowego, planów ciągłości oraz związanych z nim procedur, jak również zmiany wymagań dotyczących bezpieczeństwa i redukcji ryzyka czy też zmiany poziomu ryzyka i/lub kryteriów akceptowalności ryzyka.

Istotą kroku nr 4 *Utrzymanie i Doskonalenie (Zastosuj)* jest ciągłe doskonalenie przez organizację przydatności, adekwatności oraz skuteczności SCZD. W przypadku wystąpienia niezgodności zaleca się ich zidentyfikowanie, podjęcie odpowiedniej reakcji na nie, jak również przeprowadzenie oceny potrzeby zainicjowania działań, których podjęcie pozwoli na wyeliminowanie ich ponownego wystąpienia w przyszłości.

Obecnie zarządzanie ciągłością działania staje się fundamentalnym wymogiem w funkcjonowaniu każdej organizacji. Zapewnia bowiem nieprzerwane działanie w przypadku pojawienia się zakłóceń wynikających z wystąpienia dużej katastrofy czy też małego incydentu. Wytyczne w tym zakresie rekomenduje omówiona powyżej norma BS ISO 22301:2012. Jest ona właściwa dla organizacji z różnych sektorów, w tym związanych z finansami, telekomunikacją, transportem oraz sektorem publicznym. Łączy się więc z szeroko rozumianymi systemami infrastruktury krytycznej, które zgodnie z zapisami ustawy o zarządzaniu kryzysowym obejmują m.in. systemy zaopatrzenia w energię, surowce energetyczne i paliwa czy też systemy ratownicze oraz zapewniające ciągłość działania administracji publicznej. O certyfikaty BS ISO 22301:2012 za działalność w oparciu o System Zarządzania Ciągłością Działania ubiegają się coraz częściej urzędy administracji publicznej. Tym bardziej że zadania własne w dziedzinie bezpieczeństwa, realizowane przez gminę, powiat, województwo oraz administrację rządową rozpatruje się w kontekście procesów krytycznych, których przerwanie może stanowić zagrożenie dla realizacji tych zadań. W związku z tym norma BS ISO 22301:2012 może okazać się przydatna w ramach przeprowadzenia analizy ryzyka na potrzeby planowania kryzysowego.

3.5. Norma BS 11200:2014 Zarządzanie kryzysowe – Wytyczne i dobre praktyki

Norma BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki* obejmuje wytyczne dotyczące zarządzania kryzysowego do wsparcia najwyższego kierownictwa danej organizacji w celu wdrażania i rozwijania zdolności zarządzania kryzysowego. Kierowana jest do każdej organizacji, niezależnie od jej lokalizacji, wielkości, rodzaju działalności czy też sektora.

W szczególności dedykowana jest:

- najwyższemu kierownictwu wypełniającemu obowiązki strategiczne z punktu widzenia zdolności zarządzania kryzysowego,
- osobom odpowiedzialnym za wdrażanie planów oraz struktur kryzysowych,
- osobom odpowiedzialnym za utrzymywanie i testowanie procedur dotyczących zdolności zarządzania kryzysowego, które realizują działania pod nadzorem najwyższego kierownictwa oraz w ramach jego wytycznych.

Pomimo że norma nie odwołuje się bezpośrednio do problematyki zarządzania ryzykiem, powinna być wdrażana jako odpowiedź danej organizacji na konieczność zarządzania zidentyfikowanymi ryzykami. Innymi słowy, jest ona przydatna na potrzeby określenia sposobów postępowania z ryzykiem.

Niniejsza norma obejmuje terminologię wybranych pojęć z zakresu zarządzania kryzysowego, zarządzania ciągłością działania oraz zarządzania ryzykiem. Pochodzą one z dokumentów, takich jak: BS ISO 22301:2012, BS EN ISO 9000:2005, jak również ISO Guide 73:2009. Pozostałe z nich przyjęto na potrzeby opracowania niniejszej normy.

Kluczowe znaczenie dla zrozumienia założeń BS 11200:2014 ma zdefiniowanie terminu zarządzanie kryzysowe. Określa się je jako *rozwijanie i wykorzystanie zdolności organizacji do radzenia sobie z kryzysem*[23]. Zdolność zarządzania kryzysem jest cechą organizacji uznawanej za odporną, tj. takiej, która posiada umiejętność przetrwania i ciągłego działania podczas różnego rodzaju incydentów zakłócających jej pracę. Owa odporność łączy się z konieczności zapewnienia skuteczności zarządzania kryzysowego, które należy rozpatrywać w kontekście innych powiązanych dziedzin, tj. zarządzania ryzykiem, zarządzania ciągłością działania oraz zarządzania bezpieczeństwem.

W normie wprowadza się również rozróżnienie pomiędzy pojęciami incydentu oraz kryzysu. Incydent oznacza *niekorzystne zdarzenie, które może spowodować zakłócenie, szkody lub sytuację awaryjną, ale nie spełnia przyjętych przez organizację kryteriów kryzysu lub nie wyczerpuje definicji kryzysu*[24]. Z kolei kryzys definiuje się jako *odbiegającą od normy i niestabilną sytuację zagrażającą celom strategicznym, reputacji organizacji lub jej żywotności*[25]. W porównaniu do incydentów, kryzysom nie można zaradzić za pomocą wcześniej zaplanowanych środków, jak również wymagają natychmiastowego reagowania, które czasami trzeba rozciągnąć na dłuższy okres czasu, tak aby zminimalizować konsekwencje. Ponadto trudno je rozwiązać w oparciu o wcześniej ustalone procedury i plany. Sednem kryzysu jest więc jego nadzwyczajny charakter oraz strategiczny wpływ na działanie organizacji.

Zgodnie z normą zarządzanie kryzysowe rozpatruje się w odniesieniu do jego kilku faz. Jest ono bowiem rozwiniętą zdolnością organizacji do przygotowania się do kryzysu, jego przewidywania, reagowania, jak również odbudowy. Pomimo że

[23] Norma BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki*, s. 2.
[24] Tamże.
[25] Norma BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki*, s. 2.

nie stanowi rutynowej części zarządzania organizacją, powinna zostać wypracowana w sposób świadomy i celowy.

Ponadto norma zaleca, aby zarządzając kryzysem nie pomijać fazy odbudowy. Brak poświęcenia jej należytej uwagi może bowiem spowodować, że wysiłek włożony w działania podjęte w fazie reagowania może zostać zmarnowany. W związku z tym wskazuje się, że odbudowa powinna rozpocząć się jak najszybciej.

Istotną kwestią jest umiejętność rozpoznawania ostrzeżeń oraz świadomość potencjalnych źródeł kryzysu przez osoby na każdym szczeblu organizacji. Norma wskazuje, że kryzys może być wywołany na różne sposoby, tj. poprzez:

- ekstremalne incydenty, które zakłócają pracę organizacji (ich strategiczny wpływ widoczny jest natychmiast),
- zdarzenia, które mają swój początek w źle zarządzanych incydentach oraz wahaniach gospodarczych, które nasilając się, doprowadzają do kryzysu,
- utajone problemy, których pojawienie się powoduje poważne następstwa dla zaufania do marki oraz reputacji organizacji.

W normie podkreśla się jednakże, iż wyszczególnienie trzech grup potencjalnych źródeł kryzysu nie oznacza, że może on przejawiać tylko cechy jednej z nich. Co więcej, systemowe wady w sposobie zarządzania organizacją mogą nasilić początkowy kryzys oraz zaszkodzić reputacji organizacji.

W odniesieniu do wpływu wynikającego z kryzysów wskazuje się, że nie zawsze łączą się one z bezpośrednim zagrożeniem dla życia lub środków trwałych. W normie akcentuje się kwestię możliwego niekorzystnego wpływu na wartości materialne organizacji, np. jej reputację, wizerunek oraz markę. Wśród istotnych aspektów decydujących o skutecznym przeciwdziałaniu kryzysowi wyróżnia się czas reakcji. Zwłoka w podejmowaniu działań czy też odmowa ich podjęcia może bowiem zwiększyć podatność organizacji oraz utrudnić jej reagowanie. Skuteczność zarządzania kryzysowego zależy również od pewnego rodzaju elastyczności oraz kreatywności, tj. wyjścia w uzasadnionych przypadkach poza typowe reguły rządzące organizacją lub też poza jej środowisko biznesowe.

Wyrazem koncepcji zarządzania kryzysem przyjętej w niniejszej normie jest oparcie tej działalności na następujących zasadach:

1. Przejmowanie kontroli nad kryzysem we wczesnym stadium.
2. Efektywna komunikacja wewnętrzna i zewnętrzna.
3. Przygotowanie w sposób jasny i zrozumiały struktur, roli i odpowiedzialności.
4. Budowanie świadomości sytuacyjnej przez skuteczne zarządzania informacją, motywowanie oraz wspólne działanie.
5. Jasny proces podejmowania decyzji i prowadzenia działań.
6. Skuteczne przywództwo na wszystkich szczeblach organizacji.
7. Odpowiednie szkolenie i ćwiczenia oraz ocena wiedzy, umiejętności i doświadczenia pracowników.
8. Prowadzenie wyczerpującej dokumentacji i rejestrowanie wszystkich podjętych decyzji.

9. Uczenie się na błędach i wprowadzanie zmian, w celu zapobieżenia ich ponownemu wystąpieniu.

Norma porusza także problematykę budowy zdolności zarządzania kryzysowego. W dokumencie wskazuje się, iż pierwszym krokiem prowadzącym do jej rozwinięcia jest ustalenie struktury ramowej zarządzania kryzysowego. Dzięki temu możliwe jest zapobieganie kryzysom, jak również reagowanie na pojawiające się kryzysy, umożliwiając tym samym ochronę aktywów organizacji. Zaleca się, aby proces rozwoju zdolności zarządzania kryzysowego rozpocząć od zdefiniowania polityki zarządzania kryzysowego. Powinna ona zwięźle określać cele zarządzania kryzysowego, sposób ich realizacji oraz wskazywać zaangażowanie kierownictwa na rzecz utrzymania wysokich standardów zarządzania kryzysowego. Ma ona stanowić podstawę do dalszych przedsięwzięć związanych z planowaniem oraz wdrażaniem procedur zarządzania kryzysowego. Ponadto powinna określać priorytety, standardy oraz terminy dostarczenia kluczowych elementów zdolności zarządzania kryzysowego, jak również odpowiednie środki. Co więcej, istotne jest określenie ról i obowiązków niezbędnych do wdrażania wszystkich zdolności zarządzania kryzysowego, ze szczególnym uwzględnieniem wiedzy, umiejętności, doświadczenia oraz środków niezbędnych dla każdego elementu zdolności.

Skuteczność zdolności zarządzania kryzysowego uwarunkowana jest istnieniem takich elementów, jak:

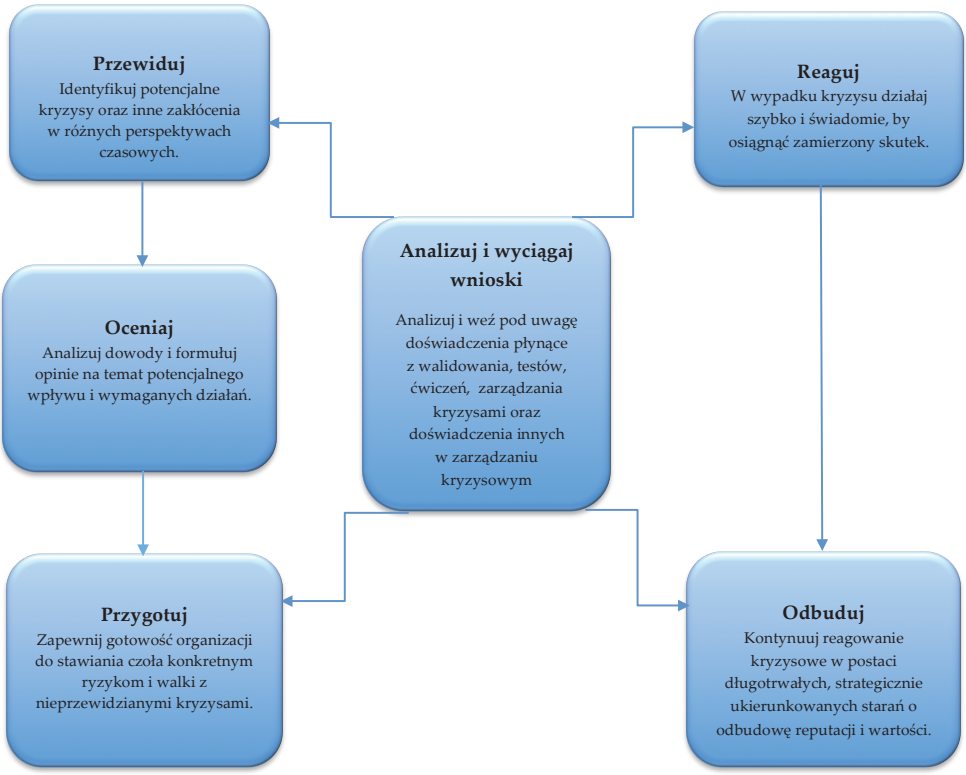
- osoby zdolne do szybkiej analizy sytuacji, ustanowienia strategii, określania opcji, podejmowania decyzji, jak również oceniania ich konsekwencji,
- powszechne zrozumienie pojęć stanowiących o istocie zarządzania kryzysowego,
- struktury i procesy biznesowe, które umożliwiają wcielanie decyzji w życie,
- pracownicy, którzy wdrażają wizję najwyższego kierownictwa,
- możliwość wspierania podejmowanych działań poprzez wykorzystanie adekwatnych środków we właściwym miejscu i czasie.

Ogólną strukturę ramową zarządzania kryzysowego wraz z określeniem kroków niezbędnych do zbudowania zdolności zarządzania kryzysowego przedstawia rysunek 3.9.

Struktura ramowa koncentruje się wokół takich aspektów, jak: przewidywanie i ocena, przygotowanie, reagowanie i odbudowa, jak również analiza i wyciąganie wniosków.

Istotą pierwszych dwóch kroków, tj. *Przewiduj i oceniaj*, jest posiadanie systemów wczesnego ostrzegania przed wystąpieniem potencjalnego kryzysu. Ponadto powinny zostać wykryte nie tylko procesy, które powodują potencjalne ryzyko, ale także zachowania negatywnie wpływające na pracę zespołu.

W kolejnym kroku *Przygotuj* zaleca się, aby rozwijać ogólne zdolności umożliwiające organizację właściwej reakcji w każdej sytuacji. W tym względzie kluczowe są cztery elementy: plan zarządzania kryzysowego, zarządzanie informacją i świadomość sytuacyjna, jak również skład, struktura, upoważnienia i oczekiwania zespołu zarządzania kryzysowego (ZZK) oraz wzmacnianie odporności w strukturze ZZK.



Rysunek 3.9. Struktura ramowa zarządzania kryzysowego

Źródło: Norma BS 11200:2014 Zarządzanie kryzysowe – Wytyczne i dobre praktyki

Kluczowymi przedsięwzięciami podejmowanymi w kroku *Reaguj* powinny być m.in.:

- budowanie świadomości sytuacyjnej (zrozumienie sytuacji oraz jej dynamiki),
- ustanowienie strategii reagowania,
- identyfikacja problemów, podejmowanie decyzji, jak również wskazywanie działań i potwierdzenie ich implementacji oraz skutków z tym związanych,
- potwierdzanie oraz monitorowanie wewnętrznej oraz zewnętrznej komunikacji oraz strategii,
- monitorowanie pracy całej organizacji zarządzania kryzysowego.

Następny krok, *Odbuduj*, koncentruje się wokół radzenia sobie z długofalowymi skutkami lub konsekwencjami kryzysu, jak również powracania do stanu normalnego lub adaptacji do nowych okoliczności, zwłaszcza jeżeli w wyniku pojawienia się kryzysu wystąpiły duże zmiany. W normie podkreśla się konieczność płynnego przejścia od fazy reagowania do odbudowy w ramach zarządzania kryzysem. Decyzje podejmowane jako część reagowania mogą bowiem bezpośrednio oddziaływać na planowanie odbudowy.

W ostatnim kroku *Analizuj i wyciągaj wnioski* zaleca się przeprowadzenie analizy kryzysu, jak również oceny reagowania, planów, procedur, narzędzi oraz obiektów, w celu wskazania obszarów wymagających doskonalenia. Ponadto wskazuje się na konieczność przedstawienia rekomendacji co do zmian wraz z wyznaczeniem terminów ich wprowadzenia oraz obowiązków z tym związanych.

Norma wskazuje, że istotną rolę w zarządzaniu kryzysem pełni przywództwo kryzysowe. Jednocześnie podkreśla się, iż normalne przywództwo w organizacji nie różni się zbytnio od przywództwa kryzysowego. Niemniej jednak, pewne różnice ujawniają się, biorąc pod uwagę ich kontekst. Przywództwo kryzysowe wiąże się bowiem z tempem kryzysu, koniecznością podejmowania decyzji w odpowiednim czasie, złożonością występujących problemów, jak również atmosferą niepewności i niepokoju. Znaczącym aspektem jest budowanie świadomości na temat wyzwań, jakie niesie ze sobą przywództwo kryzysowe, np. podczas szkoleń i ćwiczeń. Przywódcy kryzysowi powinni być starannie przygotowani i przeszkoleni z uwagi na fakt, że posiadanie predyspozycji do zajmowania wyższego stanowiska w trakcie normalnej działalności organizacji nie oznacza, iż osoba taka automatycznie jest gotowa do przywództwa podczas kryzysu.

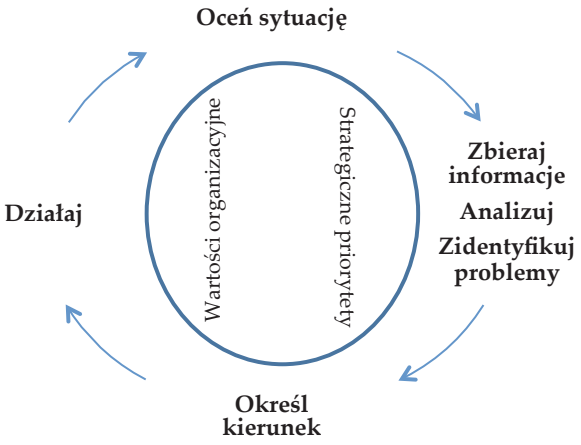
Norma BS 11200:2014 porusza również kwestię podejmowania strategicznych decyzji w kryzysie. Jest to o tyle istotne, gdyż z jednej strony może to pozwolić na wyprowadzenie organizacji z kryzysu i doprowadzenie jej do sukcesu, z drugiej zaś może spowodować pogorszenie sytuacji, mając negatywny wpływ na reputację oraz wartość organizacji. W normie podkreśla się, iż podejmując decyzję w kryzysie, należy wziąć pod uwagę:

- obecną sytuację (wskazanie co się dzieje, jakie są tego skutki, jakie są problemy, ryzyka, jak również co może się zdarzyć i jakie działania są podejmowane, aby temu zaradzić),
- kierunek (wskazanie jaki stan końcowy jest pożądany, jak również jakie są cele reagowania kryzysowego),
- działanie (wskazanie o czym należy zdecydować, jak również co należy zrobić, aby poradzić sobie z zaistniałą sytuacją oraz osiągnąć pożądany stan końcowy).

Rysunek 3.10. przedstawia model podejmowania strategicznych decyzji w kryzysie.

Proces ten na pierwszy rzut oka wydawać się może logiczny i zrozumiały. Niemniej jednak należy pamiętać, iż nie zawsze decydent posiada kompletne informacje, co sprawia, że podjęcie odpowiedniej decyzji staje się wtedy mocno utrudnione. Norma wskazuje, iż skuteczność podejmowania decyzji strategicznych w czasie kryzysu warunkowana jest takimi czynnikami, jak:

- *wdrażanie – na poziomie organizacyjnym – polityk, struktur (zespołów i ról), planów, procesów i narzędzi wspierających zdolność do zarządzania kryzysowego przez całą organizację, a w szczególności przez ZZK,*
- *zdobywanie doświadczenia przez osoby i zespoły w środowiskach podejmowania decyzji kryzysowych,*



Rysunek 3.10. Podejmowanie strategicznych decyzji w czasie kryzysu
Źródło: Norma BS 11200:2014 Zarządzanie kryzysowe – Wytyczne i dobre praktyki

- *szkolenie członków ZZK w wykorzystywaniu technik decyzyjnych, co zmniejsza wpływ niepewności na ich umiejętności poznawcze,*
- *rozpoznawanie oznak niepoprawnego podejmowania decyzji, w tym niekwestionowania dowodów, założeń, metod, logiki i wniosków, a także niepodejmowania odpowiednich kroków w celu ukazania alternatywnych perspektyw*[26].

Norma odwołuje się do kwestii komunikacji kryzysowej rozumianej jako *działania podejmowane przez organizację w celu przekazywania informacji wewnątrz i na zewnątrz w czasie kryzysu*[27]. Skuteczna komunikacja kryzysowa traktuje organizację jako główne źródło informacji, uspokaja strony zainteresowane oraz udowadnia, iż organizacja panuje nad sytuacją. Za niezbędną uznaje się umiejętność przygotowywania i przekazywania informacji definiujących reakcję organizacji na kryzys, biorąc pod uwagę wiedzę, jaką ona w danym momencie posiada. Komunikacja ta związana jest z reagowaniem na poziomach organizacyjnym oraz personalnym. W ramach komunikacji kryzysowej za istotne uważa się przygotowanie przed wystąpieniem kryzysu, zarządzanie reputacją, jak również ustalenie ról poszczególnych członków zespołu do spraw komunikacji.

Ponadto norma wskazuje kluczowe zasady komunikacji kryzysowej. Ich wykaz oraz opis przedstawia tabela 3.4.

[26] Norma BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki*, s. 23.
[27] Tamże, s. 24.

Tabela 3.4. Kluczowe zasady komunikacji kryzysowej

Lp.	Nazwa zasady	Opis zasady
1	Bądź przygotowany	Przygotuj jasny i zrozumiały proces komunikacji
2	Działaj szybko	Przekazuj informacje szybko i w odpowiedni sposób, podkreślając przy tym, że więcej informacji zostanie podanych, kiedy tylko będzie to możliwe
3	Stale monitoruj	Koniecznie śledź wszelkie wydarzenia
4	Utrzymaj przepływ informacji	Informuj o tym, co wiadomo; lepiej publikować *mało i często*, niż czekać na możliwość opublikowania wszystkich informacji
5	Mów jednogłośnie	Lecz niekoniecznie ustami tylko jednego rzecznika
6	Bądź otwarty i szczery	Wszystko i tak wyjdzie w końcu na jaw
7	Rzetelność ma znaczenie	Operuj twardymi faktami, a unikaj pogłosek, domysłów i przypuszczeń
8	Przeproś	Kiedy to odpowiednie i istotne, nie bój się przeprosić
9	Opracuj strategię	Określ podstawowy przekaz oraz tematy pomocnicze i rozwijaj je
10	Zarządzaj terminami	Informuj w pierwszej kolejności najbliższych interesariuszy
11	Bądź człowiekiem	Kiedy to właściwe, okazuj empatię
12	Podpisz	Wiedz, kto ma kompetencje do zatwierdzenia komunikatów do emisji

Źródło: Norma BS 11200:2014 Zarządzanie kryzysowe – Wytyczne i dobre praktyki

W normie BS 11200:2014 wskazuje się, iż niezbędne jest wyciąganie wniosków z kryzysów, stały rozwój oraz testowanie przygotowanych rozwiązań z zakresu zarządzania kryzysowego. Wymaga to posiadania spójnej strategii, co pozwala na zwiększenie zdolności zarządzania kryzysowego organizacji. W tym względzie rekomenduje się przeprowadzenie szkoleń oraz ćwiczeń. Jednocześnie podkreśla się, że inwestując w metody realizacji tych przedsięwzięć, należy odróżnić od siebie szkolenia oraz ćwiczenia. Te pierwsze skupiają się bowiem wokół pogłębiania wiedzy oraz doskonalenia umiejętności. Te drugie z kolei polegają na testowaniu przygotowanych rozwiązań zarządzania kryzysowego. Dają również możliwość praktycznego sprawdzenia umiejętności nabytych podczas szkoleń. W związku z tym to szkolenia powinny poprzedzać ćwiczenia.

Norma BS 11200:2014 stanowi doskonałe podsumowanie głównych obszarów zarządzania kryzysowego. Pozwala kierownictwu organizacji na zwięzły przegląd tego, co jest istotne, jak również na przygotowanie organizacji na wystąpienie sytuacji kryzysowej.

Niniejsza norma została stworzona jako ogólne wytyczne, a nie szczegółowa specyfikacja, tak jak w przypadku ISO 22301. Dokument określa kluczowe obszary, które należy wziąć pod uwagę przy rozwijaniu zdolności zarządzania kryzy-

sowego w organizacji, nie określając dokładnie, co *musi* i *powinno* być wykonane. Niemniej jednak założenia normy BS 11200:2014 stoją w zgodzie z rozumieniem pojęcia zarządzania kryzysowego w myśl ustawy o zarządzaniu kryzysowym z 26 kwietnia 2007 r., wskazującej, iż działalność ta obejmuje cztery poszczególne fazy, tj. zapobieganie, przygotowanie, reagowanie i odbudowa. Biorąc pod uwagę, że norma ta jest uniwersalna do zarządzania różnego rodzaju organizacjami, może ona zostać z powodzeniem wykorzystana w specyficznym obszarze zarządzania bezpieczeństwem, jakim jest zarządzanie kryzysowe. Będzie to możliwe po dostosowaniu głównych założeń niniejszej normy do specyfiki działalności podejmowanej przez organy administracji publicznej w przedmiotowym zakresie.

Przeprowadzenie analizy ryzyka na potrzeby planowania kryzysowego stanowi bardzo złożony proces. Pojawiające się w ostatnich latach normy z obszaru zarządzania ryzykiem mogą w istotny sposób wspomóc jego realizację.

Analiza norm z serii PN-ISO 31000 prowadzi do konstatacji, iż należałoby się zastanowić nad możliwością usankcjonowania prawnego całościowego procesu zarządzania ryzykiem w ramach polskiego systemu zarządzania kryzysowego. W tym względzie norma PN-ISO 3100 wskazuje wytyczne istotne z punktu widzenia realizacji tego postulatu, w tym propozycję przyjęcia zasad zarządzania ryzykiem oraz struktury procesu zarządzania ryzykiem, wraz z dokładną charakterystyką jego poszczególnych etapów. Z kolei wykorzystanie założeń normy PKN-ISO Guide 73 *Zarządzanie ryzykiem – Terminologia* może przyczynić się do ujednolicenia aparatu pojęciowego związanego z obszarem zarządzania ryzykiem. Istotne wsparcie w procesie przeprowadzenia analizy ryzyka na potrzeby planowania kryzysowego mogą też stanowić zapisy normy IEC/FDIS 31010 *Risk management – Risk assessment techniques*. Jej założenia mogą znaleźć swoje zastosowanie w kontekście wyboru odpowiedniej techniki lub narzędzia oceny ryzyka na etapach identyfikacji ryzyka, analizy ryzyka oraz jego ewaluacji.

Całkiem nowe podejście w odniesieniu do konieczności zapewnienia skuteczności zarządzania kryzysowego wnoszą normy: ISO 22301 *Bezpieczeństwo Powszechne – Systemy Zarządzania Ciągłością Działania* oraz BS 11200:2014 *Zarządzanie kryzysowe – Wytyczne i dobre praktyki.*

Ta pierwsza łączy obszar zarządzania kryzysowego ze zdobywającą coraz większą popularność, zwłaszcza w sferze biznesowej, problematyką zarządzania ciągłością działania. Traktuje tym samym podmioty biorące udział w zarządzaniu kryzysowym na poszczególnych szczeblach podziału terytorialnego jako organizacje, które muszą zapewnić ciągłość swojego funkcjonowania, w tym realizowanych przez nie zadań, zarówno w czasie prowadzenia rutynowych działań, jak również w obliczu wystąpienia sytuacji kryzysowej.

Z kolei ta druga, pomimo dużego stopnia ogólności zawartych tam wytycznych, może przyczynić się do ciągłego rozwijania zdolności zarządzania kryzysowego w poszczególnych jego fazach, począwszy do zapobiegania, poprzez przygotowanie i reagowanie, kończąc na odbudowie.

4. Metodyki analizy ryzyka stosowane w innych krajach

Analizę ryzyka na potrzeby planowania kryzysowego prowadzi się w wielu krajach. Państwa te posiadają własną metodykę oceny ryzyka, uwarunkowaną obowiązującymi regulacjami prawnymi, kulturą czy też przyjętą koncepcją funkcjonowania systemu zarządzania kryzysowego (ochrony ludności). W ramach niniejszego rozdziału omówione zostaną rozwiązania stosowane w Szwecji, Niemczech, Irlandii, Kanadzie, Holandii oraz Wielkiej Brytanii. Ich wybór zdeterminowany był faktem, iż państwa te posiadają kilkuletnie doświadczenie związane z wykorzystaniem procesu oceny ryzyka na potrzeby planowania kryzysowego. Rozważania zostały oparte o treść przewodników (wytycznych) opisujących podejścia poszczególnych krajów do tejże problematyki. Pod uwagę wzięto także wyniki krajowej oceny ryzyka przeprowadzonej w Szwecji oraz Irlandii. Problematyka podjęta w tej części podręcznika pozwoli na określenie, w jaki sposób poszczególne państwa identyfikują oraz szacują ryzyko, jak również na przedstawienie narzędzi oraz technik, których używają w tym celu. Umożliwi także wskazanie rozwiązań przydatnych w kontekście przeprowadzania analizy ryzyka na potrzeby planowania kryzysowego w ramach systemu zarządzania kryzysowego RP.

4.1. Szwecja

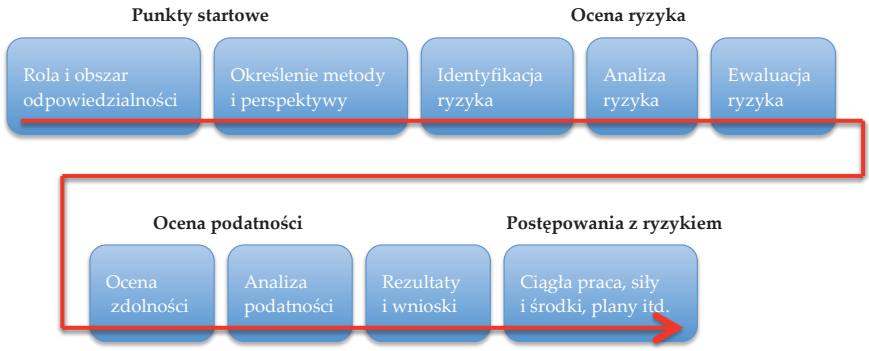
Metodykę oceny ryzyka przyjętą w Szwecji określa dokument *Guide to Risk and vulnerability analyses (Przewodnik po analizie ryzyka i podatności)*[1]. Jest on źródłem wiedzy oraz wsparcia dla organów administracji rządowej i samorządowej, których zadaniem jest przeprowadzenie analizy ryzyka i podatności. Prace z nimi związane prowadzone są na potrzeby podniesienia świadomości oraz poziomu wiedzy decydentów jak również innych podmiotów odpowiedzialnych za przeciwdziałanie zagrożeniom, ryzykom i podatnościom w ramach obszaru ich działalności. Analiza dostarcza informacji, w jaki sposób należy zapobiegać, przygotować się i zarządzać kryzysem. Ma również na celu dostarczenie społeczeństwu podstawowych informacji odnoszących się do istniejących zagrożeń.

W procesie analizy ryzyka uczestniczą agencje rządowe, zarządy okręgów oraz gminy. Pod uwagę brane są dwa rodzaje odpowiedzialności spoczywającej na wyżej wymienionych podmiotach, w tym odpowiedzialność resortową (układ pionowy)

[1] Charakterystyka metodyki bazuje na dokumencie z 2012 r. przygotowanym przez Swedish Civil Contingencies Agency (Szwedzką Agencję Ochrony Ludności).

oraz odpowiedzialność terytorialną (układ poziomy). Przykładowo analizie poddaje się zdarzenia niepożądane, możliwe do wystąpienia na terenie gminy, kładąc szczególny nacisk na to, w jaki sposób mogą one wpłynąć na realizację obowiązków nałożonych na tę jednostkę. Istotną rolę pełni zapewnienie przepływu informacji na poziomach krajowym, regionalnym oraz lokalnym. Badania przeprowadzane przez poszczególne gminy mają stanowić podstawę do analizy całego regionu, przy czym szczebel wyższy ma zapewnić wsparcie w realizacji tych przedsięwzięć.

Omawiane podejście wpisuje się w cały cykl procesu zarządzania ryzykiem.



Rysunek 4.1. Proces zarządzania ryzykiem w metodyce *szwedzkiej*

Źródło: opracowanie własne na podstawie: Guide to Risk and vulnerability analyses; Swedish Civil Contingencies Agency; 2012 r., s. 14

Punktem wyjścia jest wyznaczenie ról i odpowiedzialności wszystkich podmiotów zaangażowanych na rzecz przeprowadzenia analizy ryzyka. Podkreśla się konieczność odpowiedniego doboru metod i narzędzi pracy, ustalenia jasnego zakresu analizy a także celu działania. Wskazuje się ponadto na potrzebę udziału koordynatora, w gestii którego będzie kontrola całego procesu.

Istotą etapu identyfikacji ryzyka jest określenie tego, co może się wydarzyć w formie scenariusza oraz wskazanie jego źródeł przy zastosowanych dostępnych metod analizy ryzyka. Krok ten rozpoczyna się od opisu systemu w postaci modelu strukturalnego (uwzględniającego podział na poszczególne elementy składowe organizacji), funkcjonalnego (biorąc pod uwagę obszary działalności) lub mieszanego. W kontekście scharakteryzowanego systemu identyfikuje się wewnętrzne lub zewnętrzne czynniki, prowadzące do jego dysfunkcjonalności np. wypadki, katastrofy.

Za szczególnie istotne w fazie analizy ryzyka uznaje się udoskonalenie opisu scenariusza, jak również ocenę prawdopodobieństwa oraz ocenę skutków wystąpienia zdarzenia. W tym względzie zaleca się zastosowanie różnego rodzaju metod, w tym ilościowych oraz jakościowych, które zostały ujęte w czterech zasadniczych grupach obejmujących opis jakościowy prawdopodobieństwa wystąpienia zdarzenia, opis jakościowy z pomocą skali, jak również opis ilościowy z pomocą skali i podziałów oraz opis ilościowy z wykorzystaniem statystyki.

Ocenę ryzyka rozpatruje się jako analizę pozwalającą na określenie, czy poziom danego ryzyka jest akceptowalny, czy nie. W metodyce *szwedzkiej* zaleca się użycie matrycy ryzyka jako narzędzia przydatnego na potrzeby ewaluacji. Obejmuje ona dwie połączone, pięciostopniowe skale: prawdopodobieństwa i skutków. Jako przykłady wskazuje się matrycę 5 x 5 obejmującą tylko i wyłącznie parametry jakościowe oraz matrycę 5 x 5 opartą na wskaźnikach liczbowych (np. czynnik prawdopodobieństwa szacowany jest w odniesieniu do skali częstości wystąpienia zdarzenia, wpływ zaś ocenia się przez pryzmat policzalnych skutków, np. liczby ofiar).

Następnym krokiem jest analiza podatności. Przeprowadza się ją wskazując, na ile incydent poważnie wpływa na społeczeństwo bądź też samą organizację. Aspektem różnicującym analizę podatności od analizy ryzyka jest fakt, że pierwsza odnosi się do specyficznych scenariuszy zidentyfikowanych na etapie analizy ryzyka. Zakłada się zbadanie większej liczby scenariuszy na potrzeby szczegółowej identyfikacji podatności. Punktem wyjścia w tym podejściu jest wyznaczenie zdarzenia bazowego, poprzez jego dokładny opis, określenie przyczyn, jak również sformułowanie bezpośrednich konsekwencji rozpatrywanego zdarzenia. Przy jego *rozwijaniu* bazuje się na zagrożeniu lub źródle ryzyka, zaś scenariusz rozpisuje się na wiele zdarzeń, które pośrednio lub bezpośrednio łączą się ze sobą. Ponadto istotne znaczenie ma określenie kontekstu, czyli sytuacji, w odniesieniu do której scenariusz ma miejsce, np. określone terytorium czy warunki pogodowe.

W ramach przeprowadzenia analizy ryzyka i podatności zaleca się użycie wielu różnych metod oraz narzędzi wspierających proces oceny ryzyka. Na szczególną uwagę zasługują zwłaszcza metody scenariuszowe wykorzystywane podczas cyklu seminariów.

Pierwsza z nich, wielowymiarowa analiza aktywności (MVA), bazuje na tzw. społecznej perspektywie. Tym samym podstawą oceny skutków zdarzenia jest ich wpływ na społeczeństwo (zakładając, że ryzyko określone jest dla poszczególnych obiektów). Innymi słowy, wskazuje się, jakie konsekwencje dla ludności mogą wynikać z ich zniszczenia lub zakłócenia ich funkcjonowania.

Analizę przeprowadza się w trakcie trzech seminariów dotyczących kolejno: identyfikacji, analizy oraz tzw. *zwrotki* (feedback). Na pierwszym z nich grupa robocza definiuje wartości, funkcje a także obiekty, które wymagają ochrony. Kolejne seminarium odnosi się do inwentaryzacji zdarzeń, które mogą doprowadzić do sytuacji kryzysowej. Na tym etapie szacuje się prawdopodobieństwo wystąpienia tych zdarzeń, jak również ocenia skutki zidentyfikowanych uprzednio zagrożeń.

Sam proces tworzenia scenariusza składa się z trzech części. Rozpoczyna się od sporządzenia dokładnego jego opisu, poprzez wskazanie koniecznych zasobów (dostępnych sił i środków) oraz obowiązków i zdolności podmiotów zaangażowanych w zdarzenie. Kończy się zaś określeniem niepożądanych zmian, jakie mogą wystąpić w trakcie zdarzenia (instytucjonalnych, organizacyjnych oraz społecznych).

W trakcie ostatniego seminarium tzw. *feedbacku* przeprowadza się analizę wyników a następnie omawia je w celu poprawy skuteczności zarządzania kryzysowego w przypadku przygotowanego scenariusza.

Kolejną z metod scenariuszowych wykorzystywanych w trakcie seminariów jest analiza zagrożeń i wrażliwości (ROSA). Kładzie się w niej duży nacisk na proces zarządzania ryzykiem. Wykorzystuje się ją na potrzeby oceny zdolności podmiotu do zarządzania niekorzystnym zdarzeniem. W pierwszym etapie należy uzyskać niezbędne wsparcie od kierownictwa organizacji. Następnym krokiem jest analiza, obejmująca identyfikację ryzyka i przypisanych im zagrożeń jak również ocenę dokonaną przez ekspertów pracujących nad danym scenariuszem, przy użyciu matrycy ryzyka pozwalającej na zobrazowanie prawdopodobieństwa oraz skutków zdarzeń. Opisy te stanowią podstawę do kolejnej fazy. W oparciu o katalog scenariuszy grupa ekspercka wybiera te, które zostaną poddane dalszej analizie. Wyniki szczegółowych analiz są opracowywane a następnie przedstawiane przez grupę ds. zarządzania ryzykiem. W dalszej kolejności zbiera się wszystkie analizowane scenariusze co pozwala na stworzenie profilu ryzyka podmiotu (systemu lub obiektu). Co więcej wskazuje się na istniejące słabe punkty (podatności). W końcowej fazie wyniki prac przekazywane są do kierownictwa, które decyduje o tym, jakie dalsze kroki należy podjąć.

Trzecią z metod scenariuszowych jest metoda IBERO. Przy pomocy tego narzędzia wykorzystuje się dedykowany danej jednostce administracyjnej system teleinformatyczny oraz bazodanowy. Oparty jest on na modułach: oceny gotowości dla indywidualnego podmiotu (jednostki administracyjnej), oceny gotowości dla kilku podmiotów, katalogu zinwentaryzowanych zagrożeń i dostępnych zasobów (sił i środków) oraz raportowaniu.

Oprócz wskazanych powyżej metod zaleca się także użycie metod tradycyjnych, w tym: analizy drzewa błędów (ETA), drzewa zarządzania i nadzoru nad ryzykiem (HAZOP), *Co jeśli?*, technik przeglądu zarządzania bezpieczeństwem i organizacją (SMORT), analizy zależności. Dane niezbędne do zarządzania ryzykiem zbierane są przy wykorzystaniu źródeł informacji, takich jak: RIB (narzędzie zintegrowanego wsparcia decyzyjnego na potrzeby przeciwdziałania katastrofom) oraz IDA (baza danych statystycznych na temat katastrof).

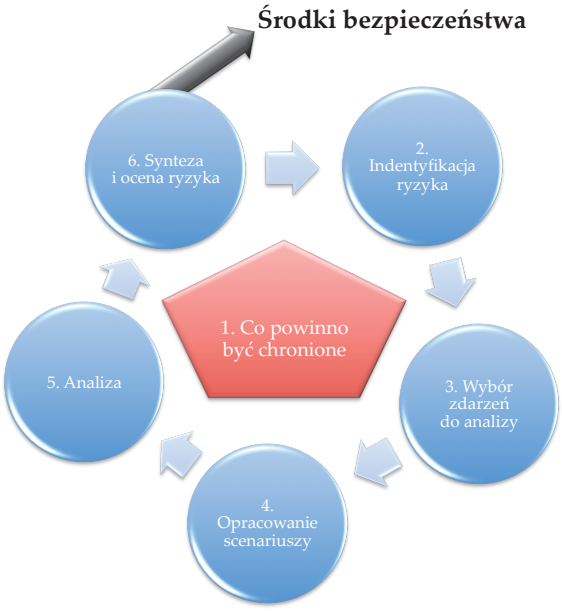
Bazując na wynikach analiz przeprowadzanych przez poszczególne agencje rządowe, zarządy okręgów i gminy, przygotowywana jest Szwedzka Narodowa Ocena Ryzyka[2].

Prace nad Narodową Oceną Ryzyka prowadzone są w sześciu krokach, do których zalicza się:

1. Określenie tego, co powinno być chronione.
2. Identyfikacja ryzyka zdarzeń niekorzystnych.
3. Wybór zdarzeń do analizy.
4. Opracowanie scenariuszy dla wybranych zdarzeń.
5. Analiza scenariuszy.
6. Synteza i ocena ryzyka.

Schemat obrazujący poszczególne kroki narodowej oceny ryzyka przedstawia rysunek 4.2.

[2] Swedish National Risk Assessment; Swedish Civil Contingencies Agency; 2012 r.



Rysunek 4.2. Sześć kroków oceny ryzyka w Szwedzkiej Narodowej Ocenie Ryzyka
Źródło: Swedish National Risk Assessment 2012; Swedish Civil Contingencies Agency, s. 27

W pierwszym etapie definiuje się wartości narodowe podlegające ochronie. Są nimi: życie i zdrowie człowieka, funkcjonowanie społeczne (funkcjonowanie i ciągłość tego, co znacząco wpływa na codzienne życie obywateli, przedsiębiorstw i innych organizacji), demokracja, rządy prawa, prawa i wolności człowieka, mienie prywatne i publiczne, wartość produkcji dóbr i usług oraz niepodległość państwowa.

Drugi krok obejmuje identyfikację zdarzeń, które mogą zagrażać, albo spowodować negatywne skutki dla chronionych wartości. Na tym etapie zdarzenia nie są określane jako ryzyko, lecz jako zdarzenia o charakterze ogólnym. Stanowią one połączenie chronionej wartości, zagrożenia i sposobu jego oddziaływania na tę wartość.

Istotą trzeciego etapu jest selekcja zdarzeń przeznaczonych do dalszej analizy. Dokonywana jest ona podczas warsztatów z udziałem przedstawicieli poszczególnych instytucji[3]. Zdarzenia ocenia się pod kątem wartości narodowych, jak również ich prawdopodobieństwa, wpływu oraz niepewności.

W czwartym etapie opracowuje się scenariusze dla wybranych zdarzeń. W celu zapewnienia jak największej ich przydatności oraz użyteczności do konstrukcji scenariuszy stosuje się jednolite zmienne. Wskazuje się, że zawarty w nich ciąg zdarzeń powinien być wiarygodny (nie tylko dla osób zaangażowanych

[3] Podczas prac nad Szwedzką Narodową Oceną Ryzyka 2012, liczbę zdarzeń zredukowano z 200 do 27. Na tej podstawie wyszczególniono 11 scenariuszy możliwych zdarzeń.

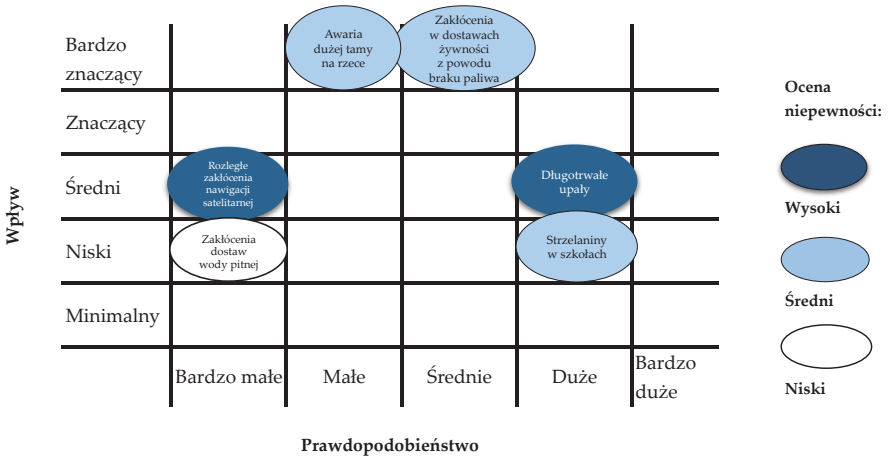
w samą analizę). Scenariusze powinny być również opracowane jako *najgorsze z możliwych*. Oznacza to, iż aby mogły one zostać wzięte pod uwagę, prawdopodobieństwo ich wystąpienia musi być znaczne, a przewidywane skutki poważne. Każdy ze scenariuszy ma wskazywać na zagrożenie co najmniej jednej wartości narodowej.

W kroku *analiza* opracowane scenariusze zostają przebadane pod kątem ich prawdopodobieństwa, wpływu (bezpośredniego i pośredniego), a także niepewności. Ważnym elementem jest udział odpowiednio przygotowanych ekspertów, którzy mają zapewnić wysoki poziom tych analiz. Ocena wpływu dokonywana jest przy pomocy przewodnika po analizie ryzyka i podatności. Wpływ określa się w odniesieniu do narodowych wartości chronionych, podlegających ochronie. Każda wartość oceniana jest na podstawie jednego lub więcej wskaźników. Do poszczególnych wartości podlegających ochronie przyporządkowano następujące wskaźniki:

- funkcjonowanie społeczne (zakłócenia życia codziennego),
- życie i zdrowie ludzkie (liczba ofiar, liczba poważnie poszkodowanych/chorych, brak realizacji podstawowych potrzeb, liczba ludzi, którzy muszą zostać ewakuowani),
- wartość produkcji dóbr i usług oraz środowisko (całkowite wpływy z gospodarki, wpływ na naturę i środowisko),
- demokracja, rządy prawa, prawa i wolności człowieka (niepokoje społeczne skutkujące negatywnymi zmianami w zachowaniu, brak zaufania do instytucji publicznych, poważny wpływ na narodowe decyzje polityczne, brak kontroli nad instytucjami publicznymi, wpływ na reputację Szwecji na arenie międzynarodowej),
- niepodległość państwowa (brak kontroli nad terytorium).

Następnie szacowane są wartości czynników prawdopodobieństwa oraz skutków scenariuszy zdarzeń. W odniesieniu do obu kategorii przyjmuje się pięciostopniową skalę jakościową ze wskaźnikami ilościowymi. Prawdopodobieństwo obejmuje kategorie *bardzo wysokie*, *wysokie*, *średnie*, *niskie* oraz *bardzo niskie*. O przyznaniu odpowiedniej wartości czynnika prawdopodobieństwa decyduje wskaźnik częstości wyrażający się wskazaniem *raz na ile lat* dane zdarzenie może wystąpić. Z kolei skutki obejmują kategorie: *minimalne*, *niewielkie*, *średnie*, *znaczące* i *bardzo znaczące*. Podobnie jak w przypadku czynnika prawdopodobieństwa, tak i dla skutków przyjmuje się wskaźniki ilościowe wyrażające się w liczbie ofiar, poszkodowanych (skutki dla ludzi), wartości finansowej (skutki dla gospodarki i środowiska). Wyjątek stanowią skutki polityczne i społeczne szacowane wyłącznie w skali jakościowej od 1 do 5.

Dalej wyniki analizy ryzyka prezentowane są na matrycy ryzyka. Daje ona obraz połączonej oceny: prawdopodobieństwa, wpływu, niepewności (prawdopodobieństwa i wpływu) dla każdego zdarzenia. Taka matryca nazywana jest matrycą 5 x 5, ponieważ składa się z 5 kolumn i 5 rzędów z 25 możliwymi kombinacjami oceny prawdopodobieństwa i wpływu. Matrycę ryzyka dla Narodowej Oceny Ryzyka przedstawia rysunek 4.3.



Rysunek 4.3. Matryca ryzyka dla Narodowej Oceny Ryzyka 2012

Źródło: opracowanie własne na podstawie: Swedish National Risk Assessment; Swedish Civil Contingencies Agency; 2012, s. 23

Uwagę zwraca konieczność uwzględnienia wartości parametru niepewności. Czynnik niepewności odzwierciedla wiarygodność danych, na których oparto poprzednie oceny. Jest szacunkiem poziomu pewności w dokładności ocen prawdopodobieństwa i wpływu. Dla każdego zdarzenia niepewność została oceniona zgodnie ze skalą, która posiada trzy poziomy w matrycy – czarny (wysoki poziom), szary (średni poziom) oraz biały (niski poziom).

W ostatnim etapie identyfikuje się, ocenia, ustala priorytety oraz proponuje się właściwe środki bezpieczeństwa, bazując na wynikach analizy i ewaluacji ryzyka.

Zaletą metodyki jest rozwinięte podejście scenariuszowe. Uwagę zwraca również fakt, że uwzględnia ona konieczność przeprowadzania analizy podatności, pozwalającej na wskazanie, w jakim stopniu dany incydent wpływa na społeczeństwo i organizację. W metodyce rekomenduje się możliwość wykorzystania wielu narzędzi i technik służących do analizy ryzyka. Wśród nich są zarówno te *tradycyjne*, które są zalecane przez normy międzynarodowe z zakresu zarządzania ryzykiem (np. FTA, *Co jeśli?*), jak również te, które stanowią wyraz autorskich koncepcji przyjętych w Szwecji, np. metody scenariuszowe oparte na seminariach.

4.2. Niemcy

Niemiecką metodykę oceny ryzyka przyjęto w dokumencie *Method of Risk Analysis for Civil Protection (Metodyka analizy ryzyka dla ochrony ludności)*[4]. Jest ona wynikiem

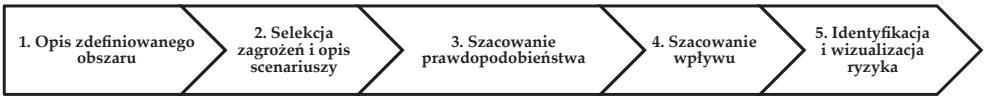
[4] Charakterystyka metodyki bazuje na dokumencie z 2011 r. przygotowanym przez Federal Office of Civil Protection and Disaster Assistance (Federalne Biuro Ochrony Ludności i Wsparcia Katastrof).

badań Federalnego Biura Ochrony Ludności i Wsparcia Katastrof, oraz efektem wymiany doświadczeń pomiędzy władzami federalnymi i ośrodkami naukowymi. Założenia metodyki są zgodne ze standardami międzynarodowymi z obszaru zarządzania ryzykiem, w tym normą ISO 31000 oraz ISO 31010.

W początkowej części dokumentu wskazuje się warunki wstępne, które są niezbędne do zastosowania przyjętej metody:

- integralnymi elementami ryzyka są prawdopodobieństwo i wpływ (pierwsza z kategorii odnosi się do zdarzeń o pewnym stopniu intensywności, druga zaś do kategorii zniszczeń obiektów),
- rozpatrywać należy zagrożenia mające wpływ na własny obszar odpowiedzialności, w tym te, które mogą mieć swoje źródło na zewnątrz zidentyfikowanego obszaru,
- konieczne jest zapewnienie jak największej wiarygodności prowadzonych badań, czemu służyć ma wykorzystanie badań naukowych, danych statystycznych oraz szacowania eksperckiego,
- analiza ryzyka jest ciągle trwającym zadaniem, jest bowiem częścią kompleksowego procesu zarządzania ryzykiem, który składa się z analizy, ewaluacji, postępowania z ryzykiem oraz monitorowania ryzyka.

Analizę ryzyka przeprowadza się w celu prezentacji ryzyk, spowodowanych przez poszczególne rodzaje zagrożeń, na matrycy ryzyka. W ujęciu porównawczym stanowi ona podstawę procesu planowania na rzecz ochrony ludności. Zgodnie z poniższym rysunkiem metodyka obejmuje pięć następujących etapów:



Rysunek 4.4. Etapy *niemieckiej* metodyki oceny ryzyka

Źródło: Method of Risk Analysis for Civil Protection, 2011

Analiza ryzyka koncentruje się wokół zidentyfikowanego obszaru, jakim jest Republika Federalna Niemiec, państwa federalne, okręgi administracyjne, okręgi wiejskie a także gminne. W pierwszym etapie dokonuje się jego dokładnego opisu. Zawiera on dane dotyczące geografii obszaru, populacji, środowiska, gospodarki czy też zaopatrzenia. Informacje te pozyskiwane są w oparciu o źródła biur statystycznych czy biur ochrony środowiska. Pochodzą również od administracji właściwej w sprawach rolnictwa czy gospodarki.

Na etapie selekcji zagrożeń i opisu scenariuszy definiuje się typ zagrożenia, dla którego określa się ryzyko. Opierając się na wybranych zagrożeniach rozwija się scenariusze będące punktami początkowymi dla analizy ryzyka. Zakłada się, że scenariusz powinien opisywać zdarzenie w sposób jasny i szczegółowy, dzięki czemu umożliwi to precyzyjne oszacowanie prawdopodobieństwa i wpływu. Wskazuje się na konieczność określenia typu incydentu, jego wymiaru przestrzennego, intensywności jak również czasu trwania. Scenariusz rozwijany jest w oparciu

o udzielenie odpowiedzi na pytania odnoszące się do parametrów rozpatrywanego zdarzenia.

Tabela 4.1. przedstawia parametry oraz główne pytania niezbędne do sporządzenia opisu scenariusza.

Tabela 4.1. Parametry oraz pytania główne niezbędne do opisu scenariusza

Parametr	Pytania
Niebezpieczeństwo	Jaki typ zdarzenia jest rozpatrywany?
Miejsce wystąpienia	Gdzie zdarzenie ma miejsce?
Wymiar przestrzenny	Jaki teren jest objęty zdarzeniem?
Intensywność	Jak silne jest zdarzenie?
Czas	Kiedy zdarzenie ma miejsce? (pora roku/pora dnia)
Czas trwania	Jak długo trwało zdarzenie i jego bezpośredni efekt?
Rozwój	Jak sytuacja się rozwija?
Czas potrzebny do ostrzeżenia	Czy zdarzenie jest spodziewane? Czy ludność jest w stanie się przygotować na jego przyjście? Czy władze publiczne są w stanie się przygotować na jego przyjście?
Kogo dotyczy zdarzenie	Które podmioty (ludzie, środowisko, obiekty itp.) są dotknięte zdarzeniem?
Podobne zdarzenia	Czy w przeszłości wystąpiły podobne zdarzenia?
Dalsze informacje	Jak przygotowane są odpowiednie podmioty? Co jeszcze jest istotne dla scenariusza, ale nie zostało wcześniej wspomniane?

Źródło: opracowanie własne na podstawie: Method of Risk Analysis for Civil Protection 2011; Federal Office of Civil Protection and Disaster Assistance 2011, s. 26

W trzecim kroku analizy ryzyka określa się prawdopodobieństwo dla wcześniej zdefiniowanych scenariuszy. W tym celu stosuje się pięciostopniową skalę prawdopodobieństwa zawierającą wskaźnik częstości wyrażający się wskazaniem na ile jest prawdopodobne wystąpienie zdarzenia wskazanego w scenariuszu w ciągu roku. Ponadto pozwala na określenie *raz na ile lat* może ono wystąpić. Tabela 4.2. przedstawia przykładowy model klasyfikacji prawdopodobieństwa.

W czwartym kroku analizy ryzyka szacowany jest przewidywany wpływ zdarzenia ujętego w scenariuszu. Proces określenia skutków/konsekwencji zdarzenia jest znacznie bardziej złożony, aniżeli w przypadku szacowania czynnika prawdopodobieństwa. Wpływ rozpatrywany jest bowiem dla pięciu kategorii (*Ludność*, *Środowisko*, *Gospodarka*, *Zaopatrzenie* oraz *Niematerialne*). W odniesieniu do nich wyznacza się kilkanaście parametrów opisujących zdarzenie (tzw. rodzaj szkody), oraz odpowiadające im opisy i jednostki miary (tabela 4.3).

Tabela 4.2. Model pięciostopniowej skali prawdopodobieństwa

Wartość	Nazwa klasyfikacji	Rocznie	Raz na …. lat
5	bardzo prawdopodobne	= lub < 0.1	10
4	Prawdopodobne	= lub < 0.01	100
3	prawdopodobne warunkowo	= lub < 0.001	1 000
2	mało prawdopodobne	= lub < 0.0001	10 000
1	bardzo mało prawdopodobne	= lub < 0.00001	100 000

Źródło: opracowanie własne na podstawie: Method of Risk Analysis for Civil Protection – Federal Office of Civil Protection and Disaster Assistance 2011 r. s. 27

Tabela 4.3. Przykładowe parametry charakteryzujące zdarzenie

Kategoria	Rodzaj szkody	Opis	Jednostka miary
Ludność	Ofiary	Osoby, które poniosły śmierć w wyniku zdarzenia	liczba
	Ranni	Osoby ranne w wyniku zdarzenia oraz osoby chore w wyniku zdarzenia	liczba
	Osoby w potrzebie pow. 14 dni	Osoby potrzebujące pomocy publicznej dłużej niż 14 dni	liczba
	Osoby w potrzebie do 14 dni	Osoby potrzebujące pomocy publicznej dłużej niż 14 dni	liczba
Środowisko	Ubytki w obszarach chronionych	Obszary chronione zniszczone w wyniku zdarzenia (rezerwaty przyrody, rezerwaty biosfery, parki narodowe i krajobrazowe)	ha
	Ubytki w zbiornikach wodnych	Obszar wód powierzchniowych i mórz *zniszczone* w wyniku zdarzenia	km/ha
	Ubytki w wodach gruntowych	Wody gruntowe zanieczyszczone w wyniku zdarzenia	ha
	Ubytki w gruntach rolnych	Grunty rolne zniszczone w wyniku zdarzenia	ha

Kategoria	Rodzaj szkody	Opis	Jednostka miary
Gospodarka	Straty fizyczne	Suma wartości strat zadanych bezpośrednio przez zdarzenie	waluta
	Wtórne uszkodzenia	Suma wartości strat pojawiających się po zdarzeniu (utrata w dostawach itp.)	waluta
Zaopatrzenie	Zakłócenie dostaw wody	Czas trwania i obszar zakłócenia, liczba osób dotkniętych	liczba godzin/ dni
	Zakłócenie dostaw energii elektrycznej	Czas trwania i obszar zakłócenia, liczba osób dotkniętych	liczba godzin/ dni
	Zakłócenie dostaw gazu	Czas trwania i obszar zakłócenia, liczba osób dotkniętych	liczba godzin/ dni
	Zakłócenie dostaw usług telekomunikacyjnych	Czas trwania i obszar zakłócenia, liczba osób dotkniętych	liczba godzin/ dni
Wartości niematerialne	Wpływ na bezpieczeństwo i porządek publiczny	Zakres skutków incydentu na bezpieczeństwo publiczne (np. protesty publiczne, przemoc wobec osób, ataki na obiekty	zasięg
	Konsekwencje polityczne	Zakres skutków incydentu na sektor polityczno-administracyjny (np. wezwanie przez społeczeństwo struktur państwa do podjęcia działań lub do rezygnacji z nich)	zasięg
	Konsekwencje psychologiczne	Stopień utraty zaufania publicznego do organów władzy (np. rządu lub administracji)	zasięg
	Uszkodzenie dóbr kultury	Uszkodzenie w wyniku incydentu dóbr kultury (np. będących pod ochroną konwencji haskiej)	liczba uszkodzonych obiektów i stopień tych uszkodzeń

Źródło: opracowanie własne na podstawie: Method of Risk Analysis for Civil Protection – Federal Office of Civil Protection and Disaster Assistance 2011 , s. 30–31

Czynnik wpływu, analogicznie jak w przypadku skali prawdopodobieństwa obejmuje wartości od 1 (*nieznaczące*) do 5 (*katastrofalne*). Jednakże, celem sklasyfikowania uzyskanego wyniku, oddzielnie dla każdej z pięciu kategorii, przypisuje się im dedykowane wartości progowe. Wskazane są one na podstawie dostępnych regulacji, wyników badań naukowych, jak również rozwiązań stosowanych w innych krajach. Poniższa tabela przedstawia przykład klasyfikacji wpływu dla kategorii *Ludność*.

Tabela 4.4. Model klasyfikacji wpływu dla kategorii *Ludność*

Kategoria		**Ludność**			
wartość	**określenie słowne**	**liczba ofiar śmiertelnych**	**liczba rannych**	**liczba osób potrzebujących pomocy dłużej niż 14 dni**	**liczba osób potrzebujących pomocy dłużej niż 14 dni**
5	katastrofalne	> _	> _	> _	> _ osób przez > _ godzin/dni
4	znaczące	_ - _	_ - _	_ - _	_ - _ osób przez _ - _ godzin/dni
3	umiarkowane	_ - _	_ - _	_ - _	_ - _ osób przez _ - _ godzin/dni
2	niskie	_ - _	_ - _	_ - _	_ - _ osób przez _ - _ godzin/dni
1	nieistotne	=lub< _	=lub< _	=lub< _	=lub< _ osób przez =lub< _ godzin/dni

Źródło: opracowanie własne na podstawie: Method of Risk Analysis for Civil Protection – Federal Office of Civil Protection and Disaster Assistance 2011 r., s. 33

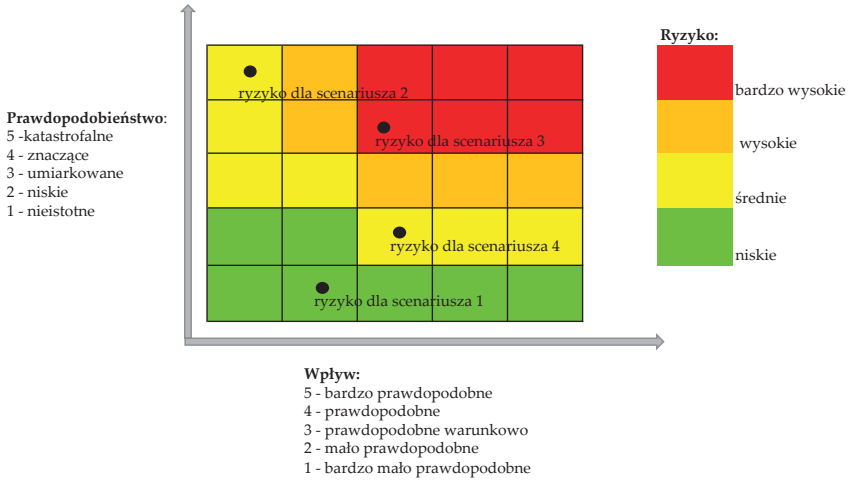
Zgodnie z powyższą tabelą dla każdej z pięciu kategorii wpływu ustala się przedziały liczbowe: *od–do* oraz *równe lub mniejsze/równe niż*. W rozpatrywanym przykładzie wskazuje się konkretne wartości liczbowe (w miejsce znaku podkreślenia dolnego) dla ludności dotkniętej skutkami zdarzenia oraz okresu czasu (godziny/dni), w którym potrzebuje ona pomocy. Pozwala to na wyznaczenie jednej z pięciu wartości dla kategorii wpływu.

Przy wyznaczeniu wartości wpływu dla kategorii: *Ludność*, *Środowisko*, *Gospodarka* oraz *Zaopatrzenie* zezwala się na użycie skali jakościowej. W przypadku kategorii *Niematerialne* uważa się ją za jedyną dopuszczalną formę przedstawienia rezultatu szacowania tego czynnika. Wreszcie, uzyskane wyniki zostają przekonwertowane na wartości liczbowe od 1 do 5.

Następnie szacowana jest całościowa wartość wpływu dla scenariusza zdarzeń. W dalszej kolejności wartości, które zostały przyporządkowane do poszczególnych parametrów wpływu są dodawane oraz ich suma dzielona przez liczbę parametrów[5]. Dzięki temu uzyskuje się całościowy wynik wpływu dla rozpatrywanego scenariusza.

[5] Dopuszcza się przypisanie różnych wag dla parametrów wpływu w celu odzwierciedlenia różnych priorytetów.

Ostatnim etapem metodyki jest identyfikacja i wizualizacja ryzyka. Wyniki analizy ryzyka przedstawia się na matrycy ryzyka (5 x 5). Wartość ryzyka określoną przez czynniki prawdopodobieństwa i wpływu wskazuje się na niej w formie zaznaczonego punktu (od 1 do 5)[6]. Kolejny krok obejmuje przeprowadzenie porównawczej oceny ryzyk związanych z poszczególnymi typami zagrożeń (scenariuszy), przy pomocy zbiorczej matrycy ryzyka. Porównawczą ocenę ryzyka zobrazowano na rysunku 4.5.



Rysunek 4.5. Porównawcza ocena różnych ryzyk na matrycy

Źródło: opracowanie własne na podstawie: Method of Risk Analysis for Civil Protection, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 41

Powyższa metoda może znaleźć swoje zastosowanie na wszystkich szczeblach administracyjnych. Z uwagi na fakt, że wyniki analizy ryzyka na poszczególnych szczeblach administracyjnych są porównywane, a następnie sumowane na szczeblu centralnym, konieczne jest wykorzystanie standardowych scenariuszy, parametrów wpływu, wskaźników ich operacjonalizacji, jak również wartości progowych dla klasyfikacji prawdopodobieństwa i wpływu. Przeprowadzona analiza ma dostarczyć wiarygodnych informacji na temat zagrożeń, ryzyk i dostępnych zdolności w ramach zarządzania kryzysowego. W konsekwencji ma pomóc decydentom w podjęciu decyzji odnoszących się do zarządzania ryzykiem (np. ustalenia priorytetowych środków do minimalizacji ryzyka), planowania kryzysowego (przygotowania na nieuchronne zdarzenia) oraz zarządzania kryzysowego (dostarczenia niezbędnych sił i środków). Ponadto rozważa się możliwość wsparcia analizy ryzyka przez technologie informatyczne poprzez użycie GIS-ów. Mają one pozwolić na stworzenie przestrzennych analiz i wizualizację danych na mapach.

[6] Przy określaniu wartości czynnika wpływu dopuszcza się możliwość posługiwania się numeracją z ułamkami dziesiętnymi, np. może przyjąć wartość 1,9.

4.3. Irlandia

Irlandzką metodykę oceny ryzyka przyjęto w dokumencie *a Framework for Major Emergency Management, a Guide to Risk Assessment in Major Emergency Management (Struktura zarządzania kryzysowego, Przewodnik do oceny ryzyka w zarządzaniu kryzysowym)*[7]. Obejmuje ona cztery etapy zgodnie z poniższym schematem (rys. 4.6).

Rysunek 4.6. Schemat procesu oceny ryzyka w metodyce *irlandzkiej*

Źródło: opracowanie własne na podstawie: a Framework for Major Emergency Management, A Guide to Risk Assessment in Major Emergency Management, January 2010, s. 5

W pierwszym etapie *Ustalenie kontekstu* sporządza się opis terenu/obszaru, w odniesieniu do którego przeprowadza się ocenę ryzyka. Oddziałuje to bowiem na prawdopodobieństwo wystąpienia zdarzenia niebezpiecznego lub sytuacji kryzysowej. Ustalenie lokalnego/regionalnego kontekstu uznaje się za istotne, gdyż pozwala na lepsze zrozumienie wrażliwości oraz podatności danego obszaru. W realizacji tego zadania bierze udział zespół ekspertów.

Zaleca się, aby zespół przeprowadzający analizę ryzyka rozważył krajowe, regionalne i lokalne warunki, które mają wpływ na zarządzanie kryzysowe na ich terenie (tj. na obszarze administrowanym przez organ, na rzecz którego zespół ten pracuje). Wyniki zapisywane są w formie krótkich sprawozdań. Zespół powinien uwzględnić właściwe aspekty obszaru, biorąc pod uwagę oprócz bieżącej sytuacji, również pojawiające się trendy.

Istotne jest także nawiązanie przez zespół współpracy z podmiotami, które mogą zapewnić mu wsparcie oraz dostarczyć niezbędnych informacji do oceny ryzyka. Wśród nich można wymienić m.in. instytucje zajmujące się ochroną środowiska, bezpieczeństwem zdrowotnym czy też bezpieczeństwem żywnościowym.

Podkreśla się, że na tym etapie analizy szczególną uwagę należy zwrócić na czynniki: społeczne, środowiskowe, przemysłowe (infrastruktura) jak również lokalizację potencjalnych zagrożeń.

W drugim etapie metodyki identyfikuje się zagrożenia. Część z nich definiuje się *z góry* i bierze jako *pewnik*. Uznaje się je bowiem za zagrożenia, które mogą wystąpić we wszystkich obszarach, np. pożary, wypadki drogowe, wypadki związane z transportem osób lub transportem materiałów niebezpiecznych. Etap ten ma na celu dokonanie przeglądu oraz wskazanie ogólnych/typowych zagrożeń,

[7] Charakterystyka metodyki bazuje na dokumencie z 2010 r. przygotowanym przez Fire Services and Emergency Planning Section (właściwy w Irlandii Dział Planowania Kryzysowego).

a następnie uzupełnienie ich katalogu o zagrożenia specyficzne dla danego terytorium. Wyróżnia się następujące cztery rodzaje zagrożeń: naturalne, transportowe, technologiczne oraz cywilne.

W celu sporządzenia listy zagrożeń zaleca się wypełnienie tabeli zgodnie z załączonym w metodyce wzorem. W odniesieniu do każdego z rodzajów zagrożeń wskazuje się typ oraz podtyp zagrożenia, w ramach jego poszczególnych kategorii (np. dla zagrożeń naturalnych są nimi zagrożenia meteorologiczne, hydrologiczne, geologiczne). Ponadto do każdego zidentyfikowanego zagrożenia przyporządkowuje się podmioty, narażone na nie.

W trzecim etapie metodyki rozpatrywane są ogólne ryzyka związane z wcześniej zidentyfikowanymi zagrożeniami. Punktem wyjścia do oceny ryzyka jest wskazanie ich wpływu, a zatem dotkliwości skutków dla życia i zdrowia, mienia, infrastruktury oraz środowiska. Rozważa się również prawdopodobieństwo wystąpienia zagrożenia. Ponadto za konieczne uznaje się określenie źródeł informacji, na których oparto ocenę, np. dane wywiadowcze ze szczebla krajowego i lokalnego, ekspertyzy czy też informacje pochodzące od *właścicieli* ryzyka.

Określając potencjalny wpływ zagrożenia, pod uwagę bierze się dwa czynniki: rodzaj i charakter zjawiska oraz jego skalę. Rodzaj i charakter zjawiska rozpatrywać można w trzech obszarach:

- wpływ na życie, zdrowie i dobrobyt społeczności,
- wpływ społeczny i środowiskowy (pierwszy z nich może być postrzegany w odniesieniu do wzburzenia i niepokoju odczuwanego przez poszkodowaną ludność, drugi zaś w kontekście wpływu na obszar poddany ochronie),
- wpływ na gospodarkę w odniesieniu do kosztów/zniszczeń infrastruktury, jak również kosztów odbudowy lub utraty produkcji gospodarczej.

W metodyce podkreśla się również konieczność wzięcia pod uwagę możliwości eskalacji danego zdarzenia lub kombinacji z innymi zagrożeniami w ramach wystąpienia tzw. efektu domino.

Ponadto proponuje się podejście, zgodnie z którym prawdopodobieństwo jest szacowane w oparciu o subiektywne oceny członków zespołu analitycznego. Tym samym rezygnuje się z możliwości wykorzystania do tego celu obliczeń związanych z rachunkiem prawdopodobieństwa (analizą ilościową).

Operacje związane z przeprowadzeniem oceny ryzyka wykonuje się przy użyciu specjalnego arkusza. Zbiera się w nim informacje na temat potencjalnego zagrożenia, w tym m.in. dane historyczne a także ocenę prawdopodobieństwa oraz skutków ich wystąpienia. Dla pierwszego z wymienionych parametrów przyjmuje się pięciostopniową skalę obejmującą wartości od *bardzo prawdopodobne* do *całkiem nieprawdopodobne*. Drugi z nich obejmuje również pięć wartości, poczynając od skutków *niewielkich*, na *katastroficznych* kończąc. Ustala się również dedykowaną danemu zagrożeniu pozycję na matrycy ryzyka (5 x 5).

Kolejnym krokiem po wypełnieniu wspomnianego arkusza jest wskazanie obszarów niepewności, dla których wymagane byłoby pozyskanie technicznego wsparcia eksperckiego. Niemniej jednak nie wymaga się tutaj szczegółowych, tech-

nicznych analiz, lecz szacunkowych informacji opartych na doświadczeniu oraz ocenie istniejących środków bezpieczeństwa.

Ostatni etap analizy związany jest z prezentacją zidentyfikowanych zagrożeń na matrycy ryzyka (5 x 5). Uwzględnia ona parametry czynników prawdopodobieństwa oraz skutków ich wystąpienia. Tabela 4.5. przedstawia model pięciostopniowej skali prawdopodobieństwa.

Tabela 4.5. Model pięciostopniowej skali prawdopodobieństwa w metodyce *irlandzkiej*

Lp.	Klasyfikacja	Prawdopodobieństwo
1.	Ekstremalnie nieprawdopodobne	Może nastąpić tylko w wyjątkowych okolicznościach. Raz na 500 lub więcej lat.
2.	Bardzo nieprawdopodobne	Nie przewiduje się wystąpienia i/lub brak zarejestrowanych incydentów lub niepotwierdzonych dowodów; i/lub bardzo niewiele incydentów związanych z organizacją i/lub mała szansa na wystąpienie, może wystąpić raz na 100–500 lat.
3.	Nieprawdopodobne	Może wystąpić w pewnym momencie, rzadko, nieregularnie, zarejestrowano kilka incydentów lub niepotwierdzonych dowodów; niektóre incydenty w jednostkach powiązanych lub podobnych organizacjach na całym świecie, istnieje szansa na wystąpienie, może wystąpić raz na 10–100 lat.
4.	Prawdopodobne	Prawdopodobne wystąpienie; regularne zarejestrowane przypadki i mocne niepotwierdzone dowody prawdopodobieństwo wystąpienia raz na 1–10 lat.
5.	Bardzo prawdopodobne	Bardzo prawdopodobne, wysoki poziom odnotowanych incydentów i/lub silne niepotwierdzone dowody. Prawdopodobnie wystąpi częściej niż raz w roku.

Źródło: opracowanie własne na podstawie: a Framework for Major Emergency Management, A Guide to Risk Assessment in Major Emergency Management, January 2010, s. 12

Z kolei tabela 4.6. przedstawia pięciostopniowy model skali skutków. Do każdej z pięciu kategorii wpływu przyporządkowuje się cztery parametry charakteryzujące zdarzenie, czyli tzw. rodzaj szkody (życie i zdrowie oraz dobrobyt, środowisko, infrastruktura, społeczeństwo) oraz jej opis w postaci liczbowej (np. liczba poszkodowanych), wartości pieniężnej (np. straty dla gospodarki), czy też w jednostce czasu (liczba godzin, która wyznacza czas przerwania świadczenia usług dla ludności).

Tabela 4.6. Model pięciostopniowej skali skutków w metodyce *irlandzkiej*

Lp.	Klasyfikacja	Wpływ	Opis
1.	Bardzo mały	Życie, zdrowie, opieka	Ograniczona liczba osób poszkodowanych; brak ofiar, ograniczona liczba drobnych urazów wymagających leczenia w ramach pierwszej pomocy.
		Środowisko	Nie dochodzi do zanieczyszczeń.
		Infrastruktura	<0,5 mln euro
		Społeczny	Lokalne zakłócenie usług społecznych lub infrastruktury (<6 godzin).
2.	Ograniczony	Życie, zdrowie, opieka	Pojedyncze ofiary śmiertelne, ograniczona liczba osób poszkodowanych; kilka poważnych urazów z koniecznością hospitalizacji. Miejscowe przemieszczenia nieznacznej liczby osób przez okres 6–24 godzin. Wsparcie realizowane na podstawie lokalnych ustaleń.
		Środowisko	Zanieczyszczenia lokalne, skutki krótkotrwałe.
		Infrastruktura	0,5–3 mln euro
		Społeczny	Wspólnota funkcjonująca normalnie z małymi niedogodnościami.
3.	Umiarkowany	Życie, zdrowie, opieka	Znaczna liczba osób w obszarze zagrożonym z pojedynczymi osobami śmiertelnymi (<5), kilkanaście poważnych i rozległych urazów (20), konieczność zapewnienia znacznej hospitalizacji. Duża liczba osób przemieszczonych przez 6–24 godzin; do 500 ewakuowanych. Potrzeba szczególnych zasobów zewnętrznych do pomocy ludziom.
		Środowisko	Małe zanieczyszczenia, zwiększony obszar skażenia lub przedłużony okres trwania
		Infrastruktura	3–10 mln euro
		Społeczny	Społeczność częściowo nie funkcjonuje, niektóre usługi są dostępne.
4.	Poważny	Życie, zdrowie, opieka	Od 5 do 50 wypadków śmiertelnych, do 100 poważnie rannych, do 2000 ewakuowanych.
		Środowisko	Bardzo duże zanieczyszczenia, określone skutki lub przedłużony czas trwania.
		Infrastruktura	10–25 mln euro
		Społeczny	Wspólnota funkcjonuje słabo, minimalna liczba dostępnych usług

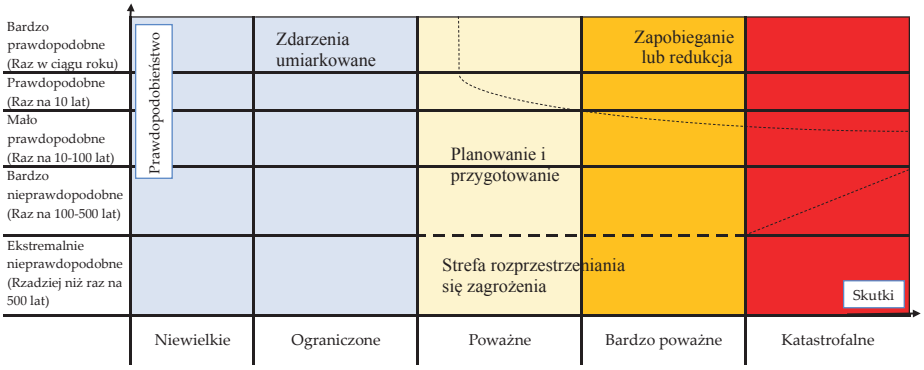
Lp.	Klasyfikacja	Wpływ	Opis
5.	Katastrofalny	Życie, zdrowie, opieka	Duża liczba osób dotkniętych skutkami ze znaczną liczbą zgonów (> 50), setki osób rannych, ponad 2000 ewakuowanych.
		Środowisko	Bardzo duże zanieczyszczenia, rozległe skutki poprzez przedłużony czas trwania.
		Infrastruktura	> 25 mln euro
		Społeczny	Poważne uszkodzenie infrastruktury powoduje znaczne zakłócenia lub utratę kluczowych usług przez dłuższy okres czasu. Wspólnota nie może funkcjonować bez istotnej zewnętrznej pomocy.

Źródło: opracowanie własne na podstawie: a Framework for Major Emergency Management, A Guide to Risk Assessment in Major Emergency Management, January 2010, s. 12

Jak wskazano, wyniki oceny ryzyka są zobrazowane na matrycy ryzyka. Warto podkreślić, że matryca podzielona jest na dwie strefy. Pierwsza z nich obejmuje zdarzenia umiarkowane. Druga strefa odnosi się zaś do zdarzeń, wymagających najwyższego stopnia gotowości. Zawiera ona obszary: zapobiegania i mitygacji ryzyka (gdzie przeprowadzenie działań mających na celu zapobieganie lub redukcję ryzyka są niezbędne), planowania i przygotowania oraz obszar rozprzestrzeniania się katastrofy (dotyczy zagrożeń, w których wystąpienie jest skrajnie nieprawdopodobne i nie planuje się w stosunku do nich szczególnych przygotowań, niemniej jednak można im przeciwdziałać poprzez zwiększenie zasobów reagowania kryzysowego).

Rysunek 4.7. przedstawia przyjętą w Irlandii matrycę ryzyka, uwzględniającą podział na strefy zdarzeń umiarkowanych, jak również zdarzeń wymagających najwyższego stopnia gotowości.

Ocena ryzyka stanowi więc podstawę do określenia czynników determinujących kroki podejmowane w późniejszych etapach zarządzania kryzysowego.



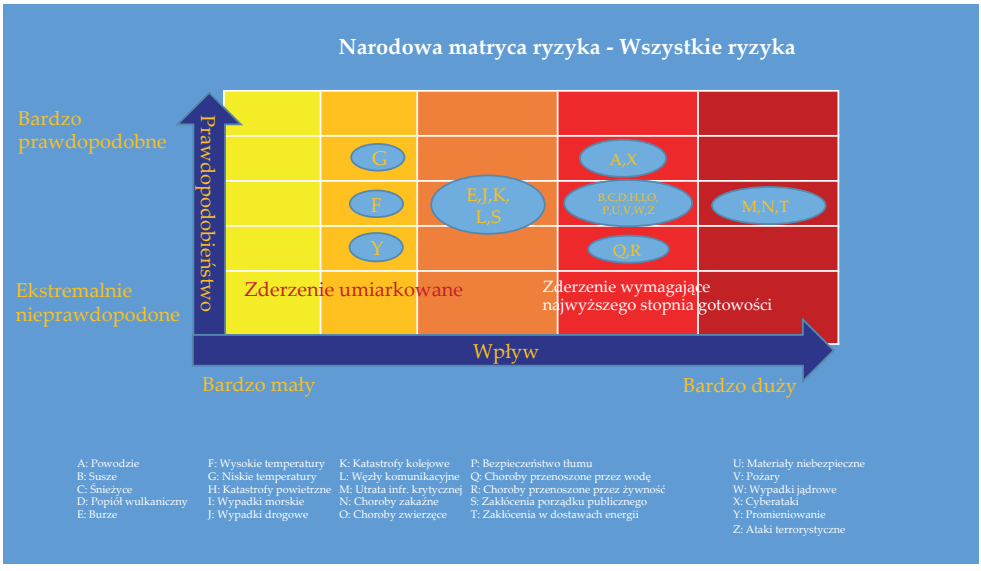
Rysunek 4.7. Matryca ryzyka w metodyce *irlandzkiej*

Źródło: opracowanie własne na podstawie: a Framework for Major Emergency Management, A Guide to Risk Assessment in Major Emergency Management, January 2010, s. 15

W szczególności dotyczy to obszaru planowania cywilnego oraz ograniczenia skutków zdarzeń. Umożliwia również wybór działań prewencyjnych w obszarach, dla których ryzyko wystąpienia jest bardzo prawdopodobne, a jego skutki katastrofalne.

Krajowa Ocena Ryzyka dla Irlandii (*Ireland's National Risk Assessment*) oparta jest na omówionej powyżej metodyce[8]. W stosownych przypadkach metodyka ta jest wspierana przez analizę ilościową, jeżeli dostępne dane mogą ją wspomóc. Koordynację jej przeprowadzenia zapewnia Biuro ds. Planowania Kryzysowego (*Office of Emergency Planning*). Czyni to, we współpracy z rządowymi departamentami i agencjami oraz Szkołą Biznesową DCU. Zagrożenia identyfikowane są na poziomie agent rządowych i definiowane w podobny sposób jak na szczeblach: lokalnym i regionalnym. Kolejnym krokiem jest ich zaklasyfikowanie do jednej z czterech kategorii (naturalne, transportowe, technologiczne, cywilne). Następnie są one rozpatrywane oraz poddawane procesowi oceny ryzyka przez grupy fokusowe skupiające ekspertów z poszczególnych departamentów i agencji państwowych. Kluczowe dla tego procesu są ocena prawdopodobieństwa wystąpienia zagrożenia oraz zbadanie jego potencjalnego wpływu w odniesieniu do skutków dla życia i zdrowia, mienia i infrastruktury i środowiska. Wpływ jest szacowany według *najgorszego możliwego scenariusza.*

Zarówno prawdopodobieństwo, jak i wpływ oceniane są w oparciu o dwie pięciostopniowe skale przyjęte w omówionej metodyce. Na tej podstawie przygotowywane są cztery matryce ryzyka dla poszczególnych kategorii zagrożeń. Efektem finalnym jest zbiorcza matryca ryzyka dla Krajowej Oceny Ryzyka, którą przedstawia rysunek 4.8.



Rysunek 4.8. Zbiorcza matryca ryzyka w Krajowej Ocenie Ryzyka dla Irlandii

Źródło: opracowanie własne na podstawie: a National Risk Assessment for Ireland, December 2012, s. 32

[8] *A National Risk Assessment for Ireland*, December 2012

4.4. Kanada

Na potrzeby efektywnego podejścia do zarządzania zagrożeniami opracowano dokument *All Hazards Risk Assessment Methodology Guidelines.* Zawiera on metodykę oraz wytyczne w procesie oceny ryzyka w Kanadzie[9].

W Kanadzie zarządzanie kryzysowe opiera się na czterech elementach: zapobieganiu, łagodzeniu skutków, gotowości oraz reagowaniu i odbudowie.

Wyniki oceny ryzyka przeprowadzanej w Kanadzie każdego roku zbierane są przez poszczególne federalne instytucje rządowe (każda z nich dokonuje tego w ramach swoich obowiązków z zakresu zarządzania ryzykiem, zgodnie z właściwymi przepisami prawnymi), a następnie zostają one scalone na szczeblu krajowym. Metoda koncentruje się wokół oceny wpływu i prawdopodobieństwa wystąpienia zagrożeń w czasie następnych pięciu lat. Ma na celu uwzględnienie ryzyk, które mają istotne znaczenie dla bezpieczeństwa państwa. Ukierunkowana jest na identyfikację priorytetowych zagrożeń występujących w określonym czasie. Roczna ocena określona jako *All Hazard Risk Assessment* (AHRA) skupia się na najbardziej prawdopodobnych i dotkliwych w skutkach zagrożeniach. Cykl ten obejmuje etapy określone w normie ISO 31000, *Zarządzanie ryzykiem – zasady i wytyczne* i zawiera:

1. Ustalenie kontekstu – charakterystyka instytucji i jej celów, wraz z określeniem zewnętrznych i wewnętrznych parametrów wpływu, które mają być brane pod uwagę przy zarządzaniu ryzykiem.
2. Identyfikację ryzyka – proces poszukiwania i rozpoznawania zagrożeń.
3. Analizę ryzyka – proces zrozumienia charakteru i poziomu ryzyka, pod względem prawdopodobieństwa i skutków.
4. Ocenę ryzyka – proces porównywania wyników analizy ryzyka w celu określenia, czy ryzyko i/lub jego wielkość jest dopuszczalna lub tolerowana.
5. Postępowanie z ryzykiem – proces kontroli ryzyka oraz działania naprawcze.

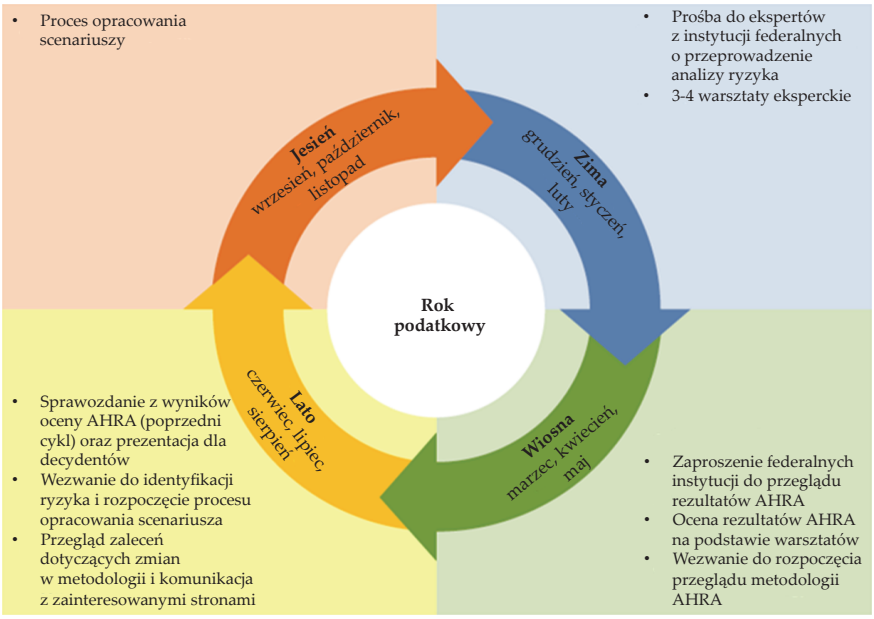
Rysunek 4.9. przedstawia proces analizy ryzyka i poszczególne jego etapy w skali roku.

Proces AHRA wykorzystuje podejście oparte na scenariuszach oceny ryzyka i koncentruje się na pięciu wskazanych powyżej etapach. Ma on na celu stworzenie wielowymiarowego spojrzenia na poziom ryzyka poprzez ukazanie zagrożeń pochodzących z różnych źródeł z uwzględnieniem prawdopodobieństwa ich wystąpienia i wpływ.

W pierwszym etapie metodyki stosowanej przez Kanadyjską Agencję Bezpieczeństwa Publicznego, określa się kontekst operacyjny organizacji. Definiuje się również jej zewnętrzne i wewnętrzne parametry, które powinny być brane pod uwagę przy zarządzaniu ryzykiem.

---

[9] Charakterystyka metodyki bazuje na dokumencie z 2012 r., opracowanym przez Public Safety Canada (Kanadyjską Agencję Bezpieczeństwa Publicznego) przy współpracy z Defence Research and Development Canada – Centre for Security Science (Kanadyjskim Centrum Naukowo-Badawczym – Centrum Nauk nad Bezpieczeństwem).



Rysunek 4.9. Cykl biznesowy procesu oceny ryzyka (AHRA)

Źródło: opracowanie własne na podstawie: All Hazards Risk Assessment Methodology Guidelines 2012/2013, s. 8

Każda jednostka administracji terytorialnej jest odpowiedzialna za badania, przegląd i zebranie odpowiednich danych oraz sporządzenie sprawozdania. W analizie brane są pod uwagę czynniki polityczne, kierunki i trendy społeczne, demograficzne, gospodarcze, technologiczne na poziomie lokalnym, krajowym i międzynarodowym.

Na potrzeby określenia zakresu ryzyka przeprowadza się analizę SWOT (mocne, słabe strony, szanse i zagrożenia), dane historyczne (obejmujące rejestry ryzyk i bazy danych), dane statystyczne (takie, jak informacje o spisie ludności), dane gospodarcze, raporty wywiadowcze a także przepisy prawa krajowego. Wymienione źródła informacji są pomocne w określeniu poziomu tolerancji wobec zagrożeń. Wspierają również kolejne działania - identyfikację ryzyka, (poszukiwanie, rozpoznawanie oraz rejestrowanie ryzyk) celem wskazania zdarzeń, które mają znaczący wpływ na państwo i obywateli.

Przeprowadzona w drugim etapie identyfikacja bazuje na krótkoterminowej analizie zagrożeń i ryzyk, możliwych do wystąpienia w ciągu najbliższych pięciu lat, jak również na analizie długoterminowej (prawdopodobieństwo wystąpienia zagrożenia w przedziale od 5 do 25 lat).

Wskazuje się, że informacje dotyczące ryzyka powinny być udokumentowane danymi historycznymi, raportami wywiadowczymi oraz programem działań ustalanym przez rząd. Każda jednostka administracji terytorialnej zajmuje się identyfikacją ryzyka na swoim obszarze, korzystając z metod takich, jak: burza mózgów, zgrupowania koligacyjne, analiza źródła ryzyka czy analiza scenariuszy. Przeprowadza się również analizę SWOT lub analizę PESTLE. Pierwsza z nich jest narzędziem służącym do oceny mocnych i słabych stron oraz szans i zagrożeń dla

organizacji. Analiza obejmuje wskazanie celów organizacji oraz wewnętrznych i zewnętrznych czynników sprzyjających ich osiągnięciu. W przypadku obszaru planowania kryzysowego chodzi o posiadanie efektywnego programu zarządzania kryzysowego. Druga z kolei, analiza PESTLE, koncentruje się wokół wskazania zewnętrznych czynników, które mogą wpływać na organizację, w tym czynników politycznych, ekonomicznych, społecznych, technologicznych/technicznych, prawnych oraz środowiskowych. Identyfikuje się je drogą burzy mózgów oraz wsparcia eksperckiego.

Ponadto stosowane są inne metody, do których należy zaliczyć badania przy pomocy kwestionariuszy ankiet, wywiady i grupy fokusowe.

Przy użyciu wskazanych powyżej metod określane są zagrożenia priorytetowe. Na tej podstawie tworzona jest lista zidentyfikowanych zagrożeń mających bezpośredni wpływ na funkcjonowanie państwa. Do każdego z nich tworzony jest jeden lub więcej scenariuszy zdarzeń. Są one wykorzystywane w kolejnym etapie procesu AHRA.

Opracowanie scenariuszy wiąże się z koniecznością wyznaczenia odpowiednich instytucji rządowych, grup roboczych oraz nadzoru, jak również zapewnienia konsultacji. Ponadto istotne jest opracowanie planu pracy i określenie ram czasowych do opracowania scenariuszy zdarzeń.

Wskazuje się, że scenariusze zdarzeń powinny być oparte na obecnie występujących zagrożeniach, a nie na danych historycznych. Zaleca się, aby rozwijając scenariusze oceniać sytuacje obiektywnie, co powinno zapewnić weryfikację, na ile zdarzenie faktycznie może mieć miejsce. Scenariusz powinien opisywać istotne informacje, odnosić się do okoliczności zdarzenia jak również wskazywać działania naprawcze. Tak przygotowane scenariusze zdarzeń pozwalają na oszacowanie prawdopodobieństwa i skutków.

Punktem wyjścia do budowy scenariusza jest identyfikacja potencjalnego zdarzenia. W dalszej kolejności jest ono opisywane, przy uwzględnieniu środowisko naturalnego, warunków meteorologicznych oraz rodzaju zagrożonego terenu. Następnie określa się prawdopodobieństwo (wraz ze wskazaniem czasu, w którym zdarzenie może wystąpić oraz skutki (uwzględniając PESTLE). Ostatnim krokiem jest opracowanie planu wskazującego działania naprawcze.

Istotą trzeciego etapu analizy ryzyka jest zrozumienie natury, a także poziomu każdego ryzyka, biorąc pod uwagę prawdopodobieństwo i wpływ. W celu oszacowania prawdopodobieństwa scenariusza wykorzystywane są dane historyczne, z uwzględnieniem częstotliwości występowania danego typu zdarzeń, modele symulacyjne sekwencji zdarzeń oraz związanych z nimi konsekwencji. Pod uwagę brane są także dane ilościowe lub jakościowe opierające się na opiniach ekspertów. Analiza odnosi się do oddziaływania ryzyka na ludzi, gospodarkę, środowisko, terytorium, stosunki międzynarodowe oraz stosunki społeczne.

Prawdopodobieństwo może być szacowane i opisane za pomocą matematycznych zmiennych bądź ogólnych informacji, uwzględniając częstotliwość wystąpienia ryzyka w określonym czasie, jak również to czy zdarzenie powstało z przyczyn

naturalnych. Prawdopodobieństwo można ocenić ilościowo przy użyciu metod deterministycznych (modele i symulacje) albo probabilistycznych (obliczenia prawdopodobieństwa z danych historycznych). Probabilistyczne metody szacowania prawdopodobieństwa dostarczają więcej informacji na temat różnych zagrożeń i mogą skutecznie *wychwycić* niepewność, ale wymagają więcej danych. Jakościową analizę przeprowadza się w przypadkach gdy trudno określić prawdopodobieństwo, np. w kontekście zdarzenia związanego z zamachami terrorystycznymi lub sabotażem, a także gdy brakuje odpowiedniej informacji oraz danych liczbowych. Dane jakościowe pozyskuje się w oparciu o przeprowadzane wywiady eksperckie.

Ryzyko może mieć wiele potencjalnych oddziaływań/konsekwencji. Oddziaływania te mogą również być wyrażone ilościowo poprzez modelowanie fizyczne zdarzeń, dane z wyników ostatnich eksperymentów lub jakościowo, jako opisowe przedstawienie prawdopodobnego wyniku dla każdego ryzyka. Określając konsekwencje wystąpienia danego zdarzenia, należy udzielić odpowiedzi na pytania m.in. o potencjalny wpływ ryzyka na duży obszar geograficzny, środowisko, stan zdrowia obywateli jak również na granicę Kanady ze Stanami Zjednoczonymi.

Analiza wpływu na ogół składa się z następujących kroków:

1. Identyfikacji wszystkich poszczególnych wpływów zagrożeń związanych z ryzykiem wystąpienia danego zdarzenia.
2. Ujęcia ilościowego wpływu wszystkich zagrożeń na sześć kategorii (ludzie, gospodarka, środowisko, terytorium, reputacja i wpływ na państwo, społeczeństwo).
3. Konsolidacji wszystkich wpływów do najwyższego poziomu ich wartości.
4. Agregacji wpływów o wysokim poziomie do całościowego wpływu ryzyka wystąpienia zdarzenia.

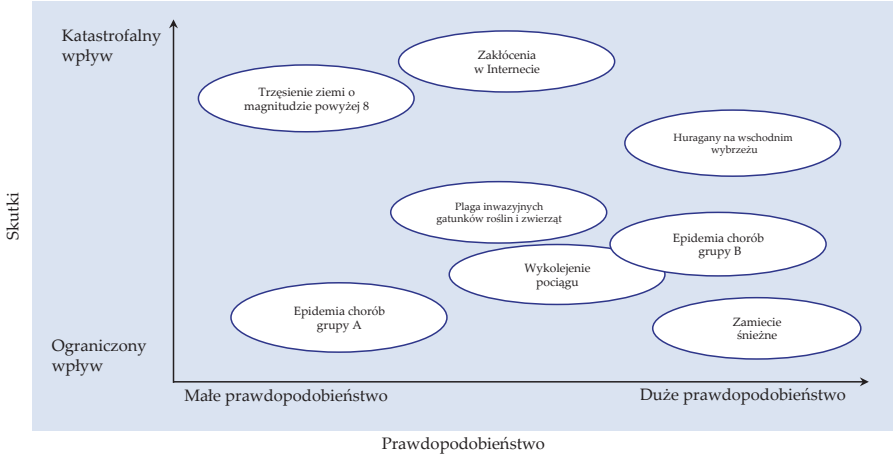
Kategorie skutków powinny być niezależne, aby uniknąć podwójnego liczenia wpływu. Ryzyko należy liczyć w stosunku do każdej jego kategorii. Przykładowo *wpływ na ludzi* jest oceniany względem trzech czynników takich, jak: *zabity*, *ranny* – w tym z urazami fizycznymi i/lub psychicznymi a także *przesiedleni lub z brakiem możliwości zaspokojenia podstawowych potrzeb życiowych*. Pozwala to na przeprowadzenie bardziej szczegółowej oceny, która może okazać się użyteczna na potrzeby udoskonalenia scenariuszy lub zapobiegania czy łagodzenia skutków. Dla każdej kategorii wpływu oceniający zobowiązany jest do wskazania w skali od A do E poziomu wiarygodności oceny zgodnie z tabelą 4.7.

Tabela 4.7. Poziomy wiarygodności oceny w metodyce *kanadyjskiej*

Poziom	Nazwa	Opis
A	bardzo wysoki poziom wiarygodności oceny	opiera się na gruntownej znajomości problemu oraz dużej ilości i jakości odpowiednich danych, a także zgodnej ocenie
B	wysoki poziom wiarygodności oceny	opiera się na dużej wiedzy na temat zagrożenia i spójnych danych jakościowych oraz ilościowych
C	umiarkowany poziom wiarygodności oceny	opiera się na wystarczającej wiedzy oraz danych na temat zagrożenia
D	niski poziom wiarygodności oceny	opiera się na stosunkowo małej wiedzy
E	bardzo niski poziom wiarygodności oceny	w oparciu o mało istotne dane bądź same założenia

Źródło: opracowanie własne na podstawie All Hazards Risk Assessment Methodology Guidelines 2012/2013, s. 25

Podsumowując niniejszy etap, w procesie analizy ryzyka wraz ze wskazaniem poziomu akceptacji ryzyka stosowana jest ocena prawdopodobieństwa wystąpienia zagrożeń i skutków ich wystąpienia, jak również ocena wystąpienia niekorzystnych zdarzeń na każdą z podstawowych kategorii wpływu. Ponadto oceniany jest ogólny wpływ ryzyka oraz inne informacje generowane podczas procesu analizy ryzyka.



Rysunek 4.10. Wykres prawdopodobieństwa i wpływu na podstawie różnych scenariuszy zdarzeń

Źródło: opracowanie własne na podstawie: All Hazards Risk Assessment Methodology Guidelines 2012/2013, s. 6

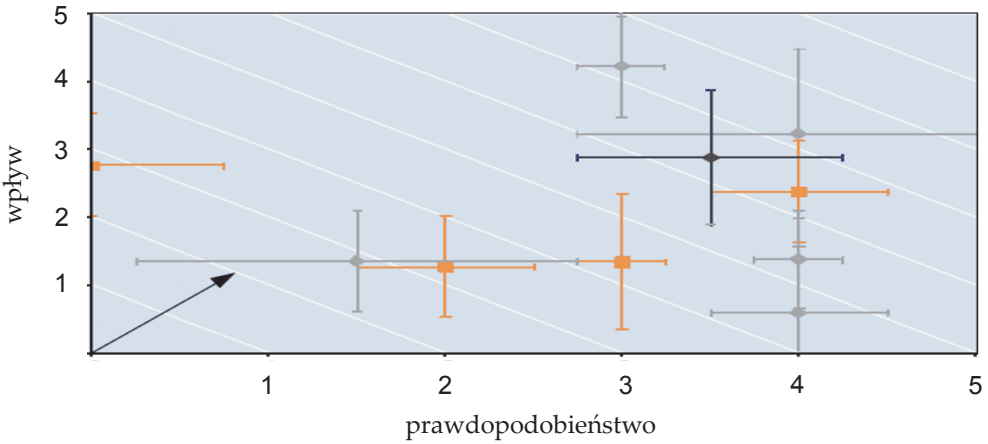
Jak wcześniej wspomniano, ocena prawdopodobieństwa ma na celu określenie możliwości wystąpienia zagrożeń w perspektywie najbliższych pięciu lat. Szacowanie prawdopodobieństwa scenariuszy zdarzeń *złośliwych* bazuje na eksper-

tyzach i wywiadach w połączeniu ze wskaźnikami, takimi jak ocena dostępu do celu ataku, ważnych informacji, dostępnych materiałów, urządzeń, a także wiedzy technicznej[10].

W procesie AHRA próbowano także dokonać oceny wiarygodności dla szkodliwych zdarzeń opartych na częstotliwości, takich jak: *raz na 10 lat*, lub *1–10 razy w roku*. Cel ten został osiągnięty m.in. za pomocą porównania hipotetycznych scenariuszy z już przeprowadzonymi. Ponadto scenariusze zostały dostosowane do trzech kategorii: o wysokim, średnim i niskim prawdopodobieństwie.

W czwartym etapie porównywane są wyniki analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy jest ono dopuszczalne lub tolerowane. Celem oceny ryzyka jest wskazanie zagrożeń, w odniesieniu do których należałoby przeprowadzić działania zapobiegawcze. Proces ten zwykle obejmuje określenie wielkości ryzyka (prawdopodobieństwa i wpływu) oraz scalenie wyników oceny dla wszystkich zagrożeń w państwie z innymi informacjami zgromadzonymi w procesie AHRA.

Zasady postępowania z ryzykiem oparte są na czynnikach wewnętrznych oraz zewnętrznych i mogą odzwierciedlać możliwości danej instytucji – ich siły i środki (czy instytucja jest przygotowana do podjęcia ryzyka lub czy je akceptuje). Ocena ryzyka może być przedstawiana w postaci graficznej na logarytmicznym wykresie ryzyka, matrycy bądź tabeli. Najczęściej używa się matrycy ryzyka, na której wskazane jest prawdopodobieństwo oraz wpływ ryzyka. Inną formą wizualizacji ryzyka jest wykres punktowy analizy ryzyka. Zaznacza się na nim dopuszczalne i niedopuszczalne poziomy ryzyka jak również kierunki jego odziaływania.



Rysunek 4.11. Przykładowy wykres punktowy oceny ryzyka względem prawdopodobieństwa oraz wpływu

Źródło: opracowanie własne na podstawie: All Hazards Risk Assessment Methodology Guidelines 2012/2013, s. 54

[10] Przez scenariusze zdarzeń *złośliwych*, należy rozumieć zdarzenia wynikające z celowych i intencjonalnych działań, np. atak terrorystyczny.

Ponadto wyniki oceny ryzyka lub lista ocenianych scenariuszy zdarzeń jest prowadzona w formie sprawozdania lub prezentacji, a poszczególne jej produkty (prawdopodobieństwo i skutki dla każdego scenariusza w karcie ryzyka) przedstawione są w formie graficznej z uwzględnieniem progów ryzyka (poziomu akceptacji).

W piątym etapie wypracowuje się zalecenia dotyczące postępowania z ryzykiem. Stanowi on proces rozwoju, wyboru oraz podjęcia środków kontroli. Działania podejmowane w tym zakresie obejmują zapobieganie zagrożeniom, ograniczanie negatywnych skutków, a w konsekwencji zmniejszenie lub eliminację ryzyka. Możliwości postępowania z ryzykiem mogą być rozpatrywane w kategoriach szeregu czynników, takich jak: obowiązki instytucjonalne, impulsy polityczne, finansowe czy humanitarne. Pod uwagę należy wziąć również tolerancję ryzyka, skuteczność środków postępowania z ryzykiem, koszty oraz korzyści bazując na wynikach analizy ryzyka.

4.5. Holandia

Przyjęta w Holandii metodyka oceny ryzyka łączy się z Narodową Strategią Bezpieczeństwa Holandii. Integralną częścią niniejszej strategii jest metodyka wzmocnienia bezpieczeństwa narodowego. Jej pierwszą fazą jest *National Risk Assessment – NRA (Narodowa analiza zagrożeń i ocena ich ryzyka).*

Holenderską metodykę oceny ryzyka przyjęto w dokumencie *National Risk Assessment Method Guide (Przewodnik po Narodowej Metodzie Oceny Ryzyka)*[11]. Wskazuje się w nim cel oraz kontekst prowadzonej w Holandii analizy ryzyka. Zawiera on również charakterystykę przyjętej metody oraz szczegółowy opis jej poszczególnych kroków. Dokument, który wydano rok później *Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of Netherlands (Praca ze scenariuszami w Narodowej Strategii Bezpieczeństwa Holandii*) jest uaktualnioną wersją przewodnika[12].

Punkt wyjścia przyjętego w Holandii podejścia do oceny ryzyka stanowi zidentyfikowanie ról i odpowiedzialności podmiotów zaangażowanych w realizację przedsięwzięć wynikających z jej poszczególnych etapów. W pracach tych biorą udział m.in. ministrowie, Grupa Robocza ds. Bezpieczeństwa Narodowego (IWNV), Komitet Sterujący Bezpieczeństwa Narodowego (SNV), oraz grupy ekspertów. Na każdy z tych podmiotów nakłada się zadania do wykonania na poszczególnych etapach realizacji badań.

Przyjęta metoda obejmuje całościowe podejście do zagrożeń. Została ona rozwinięta na potrzeby dokonania oceny ryzyka w skali całego państwa, bazując na założeniu, że zagrożenia bezpieczeństwa narodowego opisane są w formie scenariuszy. Scenariusze dla takich zagrożeń, jak powodzie, pandemie, długotrwałe

[11] *National Security Programme National Risk Assessment Method Guide*, 2008 r.

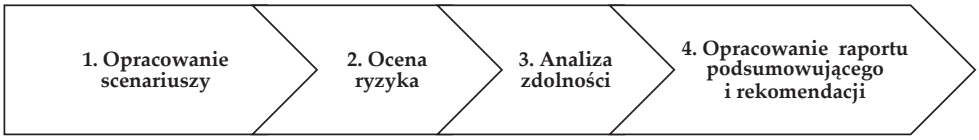
[12] Charakterystyka metodyki bazuje na dokumencie z 2009 r. opracowanym przez grupę roboczą złożoną z ekspertów z Holandii pochodzących z administracji rządowej oraz instytucji naukowo-badawczych.

awarie dostaw usług są opisywane w jednolity sposób, wsparte statystykami oraz agregowane. Pozwala to na porównywanie ryzyk oraz ustalenie priorytetów dla podejmowanych działań.

Ocena ryzyka rozważa prawdopodobieństwo wystąpienia scenariusza i jego wpływu na żywotne interesy Holandii, którymi są: bezpieczeństwo terytorialne, bezpieczeństwo fizyczne, bezpieczeństwo ekonomiczne, bezpieczeństwo ekologiczne oraz stabilność społeczno-polityczna. Czynnik wpływu został podzielony na komponent obiektywny (np. zniszczenie mienia, liczba ofiar) i subiektywny (społeczne wzburzenie związane z konsekwencją wystąpienia danego zdarzenia).

Rezultaty oceny ryzyka publikowane są corocznie w raporcie *bevindingenrapportage*. Bazując na tych ustaleniach, rząd podejmuje decyzje, które ryzyka powinny zostać dokładnej przeanalizowane, wskazuje, czy dostępne siły i środki są wystarczające, jak również czy powinno się dokonać ich wzmocnienia. W konsekwencji ocena ryzyka wskazuje, na które zagrożenia należy przeznaczyć środki w ramach planowania strategicznego.

Na rysunku 4.12. przedstawiono poszczególne etapy metody NRA.



Rysunek 4.12. Etapy *holenderskiej* metodyki oceny ryzyka

Źródło: Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of Netherlands, s. 13

W pierwszym etapie metody NRA przygotowywane są scenariusze, opisujące zagrożenia bezpieczeństwa narodowego w średnioterminowej perspektywie czasowej (w ciągu pięciu najbliższych lat). W kontekście metody scenariusz jest opisem:

- incydentu (w tym, jego charakteru oraz skali), czyli jednego lub wielu powiązanych ze sobą zdarzeń mających swoje konsekwencje dla bezpieczeństwa narodowego,
- tzw. *lead up*, czyli czynnika prowadzącego do wystąpienia incydentu określającego przyczyny, jak również podstawowe fazy, które składają się na ten incydent,
- kontekstu zdarzeń obejmującego ogólne okoliczności i stopień podatności, jak również odporności ludzi, obiektów oraz społeczeństwa w stosunku do opisywanego incydentu,
- konsekwencji incydentu zawierającego opis reakcji i środków kontrolnych,
- oddziaływania incydentu na ciągłość funkcjonowania infrastruktury.

W celu rozwinięcia scenariuszy wymaga się uzyskania informacji pochodzących z wielu specjalistycznych dziedzin. Stąd też często powołuje się multidyscyplinarne grupy robocze z udziałem ekspertów.

Punktem wyjścia do rozwijania scenariuszy możliwych zdarzeń jest założenie, iż istnieje przynajmniej niewielkie prawdopodobieństwo jego wystąpienia.

Ponadto muszą one oddziaływać w skali narodowej, a zatem w odniesieniu do żywotnych interesów Holandii (bezpieczeństwo terytorialne, bezpieczeństwo fizyczne, bezpieczeństwo ekonomiczne, bezpieczeństwo ekologiczne, stabilność społeczno-polityczna).

Każdy scenariusz musi być unikalny, tzn. różnić się skalą, intensywnością zdarzeń, położeniem geograficznym czy prawdopodobieństwem. Tam, gdzie pojawiają się różne warianty tego samego scenariusza rozpatruje się odpowiednie siły i środki w celu wskazania, dla którego poziomu zagrożenia są wystarczające.

Scenariusze dzieli się na dwie zasadnicze grupy: realne do wystąpienia z pewnym prawdopodobieństwem *tu i teraz* (np. związane z powodzią czy pandemią) oraz scenariusze *rozwojowe*, czyli takie, które skutkują opisanym wpływem w dłuższej perspektywie czasowej, np. scenariusze oparte na wpływie starzenia się ludności lub zmianach klimatu.

W ramach etapu oceny ryzyka podejmuje się następujące działania:

- sprawdzenie kompletności opisu scenariusza,
- oszacowanie wpływu scenariusza,
- oszacowanie prawdopodobieństwa scenariusza,
- prezentacja wyników analizy.

Scenariusz musi obejmować informacje, które umożliwią oszacowanie prawdopodobieństwa i wpływu.

Zdarzenia oraz ich wpływ w ramach danego scenariusza analizowane są dla dziesięciu kategorii wpływu.

Tabela 4.8. przedstawia wykaz kryteriów wpływu przyporządkowanych do poszczególnych żywotnych interesów Holandii.

Tabela 4.8. Żywotne interesy Holandii i odnoszące się do nich kryteria wpływu

Żywotne interesy państwa	**Kryterium wpływu**
1. Bezpieczeństwo terytorialne	1.1. Wkroczenie na terytorium Holandii 1.2. Naruszenie międzynarodowej pozycji Holandii
2. Bezpieczeństwo fizyczne	2.1. Ofiary śmiertelne 2.2. Poważne urazy i choroby przewlekłe 2.3. Cierpienie psychiczne (brak podstawowych środków do życia)
3. Bezpieczeństwo ekonomiczne	3.1. Koszty
4. Bezpieczeństwo ekologiczne	4.1. Długoterminowy wpływ na środowisko i naturę (flora i fauna)
5. Stabilność społeczna i polityczna	5.1. Zakłócenie życia codziennego 5.2. Naruszenie systemu demokratycznego 5.3. Społeczne skutki psychologiczne

Źródło: opracowanie własne na podstawie: Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, s. 29

Analiza skutkuje określeniem wartości wpływu dla każdego z dziesięciu wspomnianych kryteriów. Następnie zostają one scalone przy wykorzystaniu procedury agregacji celem wyznaczenia całościowej wartości wpływu.

Wpływy poszczególnych kryteriów mierzy się w podobny sposób dla wszystkich scenariuszy, które mogą potencjalnie wystąpić. W stosunku do każdego z kryteriów wykorzystuje się pięciostopniową skalę A-B-C-D-E wskazującą konsekwencje: *ograniczone*, *istotne*, *poważne*, *bardzo poważne* oraz *katastrofalne*. Każda z tych wartości opisywana jest przez wyznaczony jej zakres (np. od 0 do 10 ofiar).

Tabela 4.9. przedstawia przykład określenia wpływu dla kryterium *ofiary* w ramach żywotnego interesu narodowego, jakim jest bezpieczeństwo fizyczne.

Tabela 4.9. Przykład określenia wpływu dla kryterium ofiar w ramach zapewnienia bezpieczeństwa fizycznego

liczba / **czas**	**<10**	**10-100**	**100-1000**	**1000-10,000**	**>10000**
Natychmiastowa śmierć (w ciągu roku)	A	B	C	D	E
Przedwczesna śmierć (w ciągu 2-20 lat)	A	A	B	C	D

Źródło: opracowanie własne na podstawie: Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, s. 35

Na potrzeby uzyskania jak największej pewności, że szacowana wartość wpływu dla danego kryterium została określona w sposób właściwy, każdemu z nich przyporządkowuje się jedną z trzech wartości wpływu, która stanowi wartość prognozowaną (V), najniższą możliwą wartość (O) oraz najwyższą możliwą wartość (B) pamiętając o konieczności uzasadnienia tego stanu rzeczy.

Następnie przy użyciu analizy multikryterialnej dokonuje się agregacji wartości wpływu dla każdego ze scenariuszy. Wspomniane wartości wpływu zostają przekonwertowane do wyniku X, A, B, C, D, E dla każdego z dziesięciu kryteriów wpływu oraz scalone celem wskazania ostatecznej wartości wpływu dla każdego ze scenariuszy[13]. Uzyskane w ten sposób wyniki sprowadzone zostają do wartości liczbowych za pomocą funkcji liczbowych oraz metody sumy ważonej.

Wskazanie prawdopodobieństwa wystąpienia incydentu jest czynnością wtórną do określenia konsekwencji (wpływu) danego scenariusza. Szacowane jest ono za pomocą pięciostopniowej skali od A do E. Celem stworzenia większej przestrzeni dla uzyskanych wyników dopuszczalne jest wyznaczenie subkategorii (niskie, średnie, wysokie) w obrębie kategorii od A do D. Analogicznie jak w przypadku szacowania wpływu wskazuje się również prognozowaną wartość prawdopodobieństwa wystąpienia scenariusza (V), wyższą granicę wartości prawdopodobieństwa (O) oraz niższą granicę prawdopodobieństwa (B). Ponadto uwzględnia się

[13] Wartość X wskazuje się w przypadku, gdy skutki określonego incydentu nie wiążą z danym kryterium wpływu, np. gdy atak terrorystyczny nie ma wpływu na bezpieczeństwo środowiskowe.

niepewność w określeniu kategorii prawdopodobieństwa dla poszczególnych scenariuszy incydentu wraz ze wskazaniem źródła tej niepewności oraz braku wiarygodności oceny.

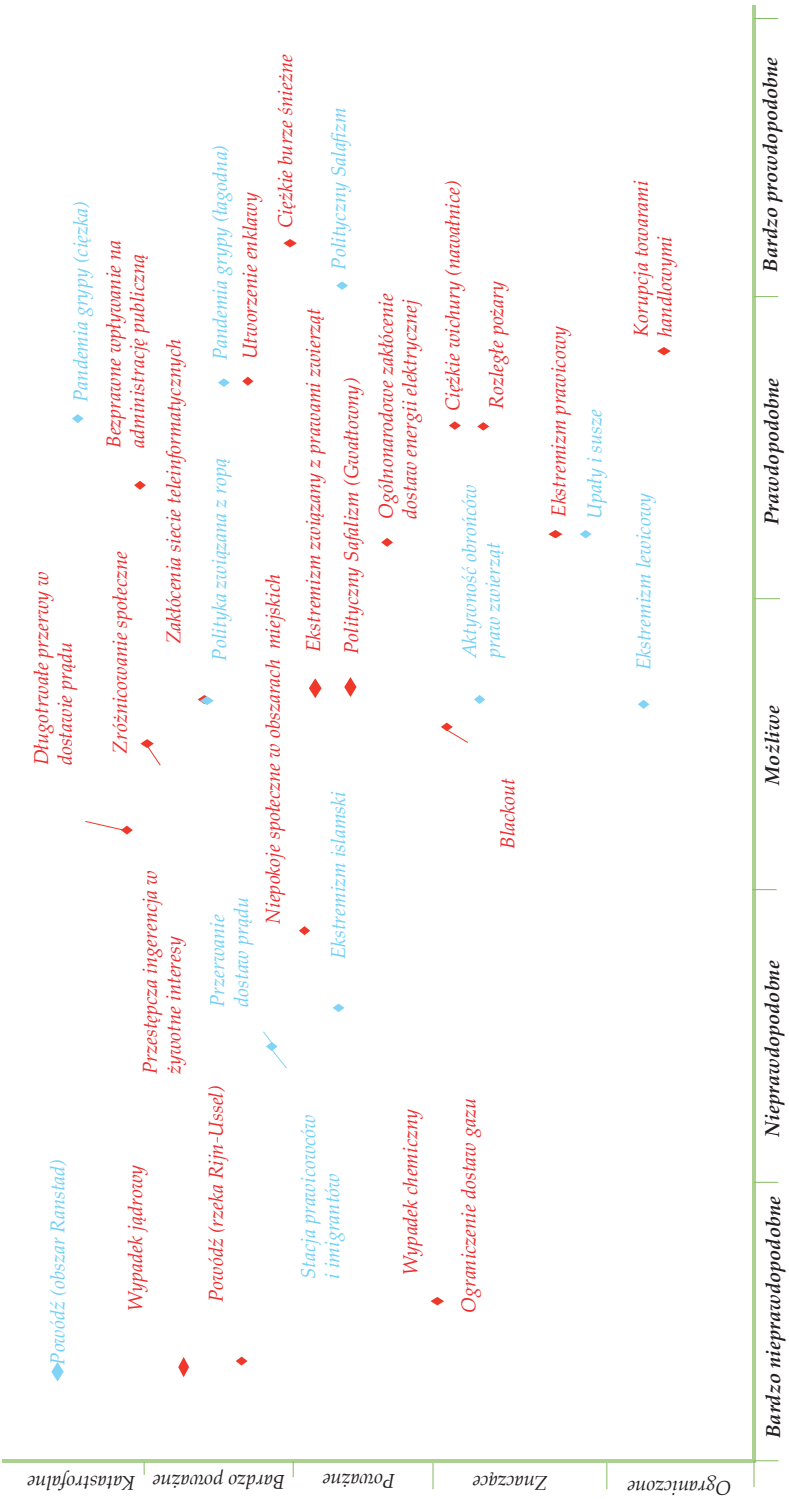
W metodyce *holenderskiej* wprowadza się rozróżnienie pomiędzy czynnościami podejmowanymi na rzecz szacowania prawdopodobieństwa wystąpienia scenariuszy zdarzeń intencjonalnych oraz zdarzeń niecelowych. W odniesieniu do tych pierwszych wynik przedstawia się bazując na skali jakościowej. Z kolei dla drugiej grupy używa się skali jakościowej ze wskaźnikami częstości. W tym względzie wynik szacowania prawdopodobieństwa wystąpienia zdarzenia intencjonalnego warunkowany jest parametrem podatności (niski, średni, wysoki), wpływającym na obniżenie bądź zwiększenie wartości czynnika prawdopodobieństwa.

Określając prawdopodobieństwo, dąży się do jego szacowania w sposób ilościowy. Niemniej jednak w uzasadnionych przypadkach dopuszcza się również przeprowadzenie w tym celu analizy jakościowej. Czynnik prawdopodobieństwa rozpatruje się w kontekście możliwości wystąpienia scenariusza danego zdarzenia w ciągu pięciu lat.

Prawdopodobieństwo wystąpienia scenariuszy szacuje się w oparciu o analizę zdarzeń historycznych a także studia przypadków. Pod uwagę bierze się również potoczne opinie na temat incydentów, niemniej jednak błędne dane wynikające z takich relacji są filtrowane, pod kątem wiarygodności zawartych w nich informacji. Działania te powiązane są z analizą sieciową i drzewem decyzyjnym. Wykorzystuje się również szacowanie eksperckie i analizę trendów.

Wyniki oceny ryzyka przedstawione są na dwuwymiarowym diagramie ryzyka. Przyjmuje się w nim równą wagę dla wszystkich dziesięciu kryteriów wpływu, jak również ilościowo wskazuje się wartości: X, A, B, C, D, E. Diagram ten posiada konstrukcję logarytmiczną. Wpływ zaznacza się na osi pionowej, z kolei prawdopodobieństwo na osi poziomej. Dla każdego scenariusza, NRA *zwraca* wynik dla zagregowanego wpływu oraz prawdopodobieństwa. Przykład diagramu oceny ryzyka przedstawiono na rysunku 4.13.

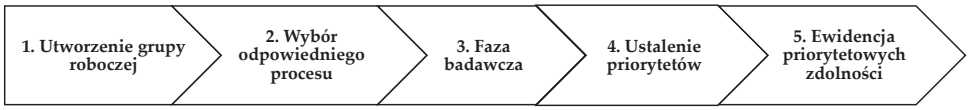
Trzeci etap obejmuje analizę zdolności. Odpowiada się w nim na pytanie, czy posiadane zasoby, niezbędne do redukcji ryzyk są wystarczające. Ponadto rozważa się, czy wykorzystanie dodatkowych sił i środków mogłoby w konkretnym przypadku pozwolić na ograniczenie ryzyka w sposób bardziej efektywny. Zasoby te mogą mieć postać umiejętności lub wiedzy, jak również aparatury pomiarowej, zasobów ludzkich lub ustawodawstwa związanego z zapobieganiem zdarzeniom niebezpiecznym. W ramach analizy zdolności bada się scenariusz danego zagrożenia, a następnie odpowiada na pytanie, które zdolności muszą zostać wzmocnione na potrzeby redukcji wpływu lub prawdopodobieństwa ich wystąpienia. Dzięki analizie, wskazuje się konkretne opcje ograniczenia ryzyka oraz poziom, do jakiego zasoby muszą zostać rozwinięte, aby przyniosły pożądany efekt.



Rysunek 4.13. Diagram ryzyka

Źródło: opracowanie własne na podstawie: Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, s. 63

Poszczególne etapy procesu analizy zdolności przedstawia rysunek 4.14.



Rysunek 4.14. Etapy analizy zdolności w metodyce NRA

Źródło: Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, s. 69–71

W pierwszym etapie analizy zdolności powołuje się grupę roboczą złożoną z ekspertów, którzy posiadają wiedzę z zakresu zdolności odnoszących się do poszczególnych scenariuszy. Następnie dana organizacja wskazuje, harmonogram prac, który doprowadzi do wskazania zdolności. W trzecim etapie procesu należy zbadać, które obszary muszą zostać wzmocnione oraz przygotować ich potencjalną listę. Istotą czwartego etapu jest stworzenie priorytetowej listy około pięciu zdolności, które należy wzmocnić dla każdego z czterech typów zdolności odnoszących się do fazy zapobiegania, przygotowania, reagowania i odbudowy. Ostatnim krokiem jest wskazanie i zewidencjonowanie priorytetowych zdolności wraz z uzasadnieniem w jednolitym dokumencie.

Wyniki poszczególnych analiz mają pomóc rządowi w określeniu, które zdolności powinny zostać wzmocnione, biorąc pod uwagę interes bezpieczeństwa narodowego.

Ostatnim etapem metody NRA jest opracowanie raportu podsumowującego oraz rekomendacji. Poszczególne grupy tematyczne mają za zadanie przedłożyć przygotowane analizy zdolności. Szczególna uwaga powinna zostać położona na specyficzne zdolności tzn. takie, które są niezbędne do przeciwdziałania danemu typowi ryzyka. Raport powinien wskazywać również te, które wymagają wzmocnienia, a jednocześnie są użyteczne w kontekście reakcji na różne rodzaje ryzyka. Na podstawie tych ustaleń rząd powinien podjąć decyzję, które rekomenduje do wdrożenia.

4.6. Wielka Brytania

W Wielkiej Brytanii dokumentem odwołującym się do zarządzania ryzykiem jest *National Risk Register (Krajowy Rejestr Ryzyka*[14]). Prezentuje on wiedzę podmiotów odpowiedzialnych za realizację zadań z zakresu zarządzania kryzysowego. Dokument ten publikowany jest od 2008 roku w oparciu o zapisy zawarte w Strategii Bezpieczeństwa Narodowego. Wskazuje opis głównych typów zagrożeń, sposobów zapobiegania im, jak również ocenę ryzyka. Analiza ryzyka przeprowadzana jest przy pomocy oceny wpływu i prawdopodobieństwa wystąpienia głównych zagrożeń w perspektywie najbliższych pięciu lat i kładzie szczególny nacisk na zagro-

[14] *National Risk Register 2008*.

żenia, które mogą bezpośrednio wpływać na działalność państwa. Każdego roku rząd przeprowadza ocenę ryzyka, która prezentowana jest w dokumencie *National Risk Assessment* – NRA (*Narodowa Ocena Ryzyka*). Bazując na NRA publikowany jest ponadto *National Risk Register of Civil Emergencies* – NRR (*Krajowy Rejestr Ryzyka*)[15].

W edycji NRR z 2010 roku wskazano, że w procesie oceny ryzyka wykorzystuje się historyczne i naukowe dane, modele numeryczne jak również opinie ekspertów[16]. Każdy region w państwie posiada przy tym swój własny profil ryzyka.

Analiza obejmuje trzy etapy. Pierwszym z nich jest identyfikacja ryzyka dokonywana w toku konsultacji eksperckich, dzięki czemu tworzy się obraz potencjalnych zdarzeń, wypadków, zagrożeń naturalnych, oraz ataków, wywołujących znaczne szkody i zakłócenia.

Następnie wybiera się *najgorszy przypadek* o wysokim ryzyku wystąpienia (duże prawdopodobieństwo a także skutki). Wysoce nieprawdopodobne scenariusze są wykluczane z dalszej analizy. W ramach konsultacji z ekspertami z agencji rządowych opracowano listę około osiemdziesięciu rodzajów zagrożeń, które spełniają definicję zdarzeń nagłych zgodnie z ustawą regulującą planowanie i zarządzanie kryzysowe (Civil Contingencies Act 2004). Dalsze czterdzieści zostało umieszczone na liście rezerwowej, pomimo że uznano, iż nie wyczerpują one definicji zdarzeń nagłych. W opinii ekspertów mogą one zostać wzięte pod uwagę w przyszłości oraz powinny być stale monitorowane.

Kolejny etap stanowi ocena prawdopodobieństwa oraz wpływu każdego ryzyka. Na potrzeby oceny prawdopodobieństwa wykorzystuje się dane statystyczne, naukowe i historyczne. Tam, gdzie to tylko możliwe, w ocenie bierze się pod uwagę rozwój zidentyfikowanych lub potencjalnych zagrożeń.

Prawdopodobieństwo wystąpienia ataków terrorystycznych i innych zdarzeń intencjonalnych określa się wykorzystując subiektywne oceny ekspertów. Gotowość jednostek lub grup do przeprowadzenia ataków terrorystycznych przeciwstawiana jest obiektywnej ocenie ich zdolności *tu i teraz* oraz, możliwości ich wystąpienia, a także podatności ich zamierzonych celów.

Za każdym razem zadaje się pytanie, na ile prawdopodobne jest, że dany typ zdarzenia urzeczywistni się gdziekolwiek/kiedykolwiek w kraju ciągu najbliższych pięciu lat. W Narodowej Ocenie Ryzyka nie rozważa się szansy wystąpienia zdarzenia poprzez przyporządkowanie mu jednego konkretnego miejsca, czy też jednej konkretnej społeczności.

Oceniając skutki, bierze się pod uwagę liczbę ofiar śmiertelnych, zranienia i urazy, zakłócenia społeczne (brak dostępu do opieki zdrowotnej lub edukacji, przerwy w świadczeniu podstawowych usług, np. dostępu do wody i prądu, konieczność ewakuacji osób z danego obszaru) jak również straty ekonomiczne. Rozpatrywany jest również wpływ psychologiczny wystąpienia katastrof na społeczeństwo.

---

[15] Charakterystyka metodyki bazuje na dokumentach z lat 2008 i 2010 opracowanych przez Cabinet Office (Urząd Brytyjskiej Rady Ministrów).

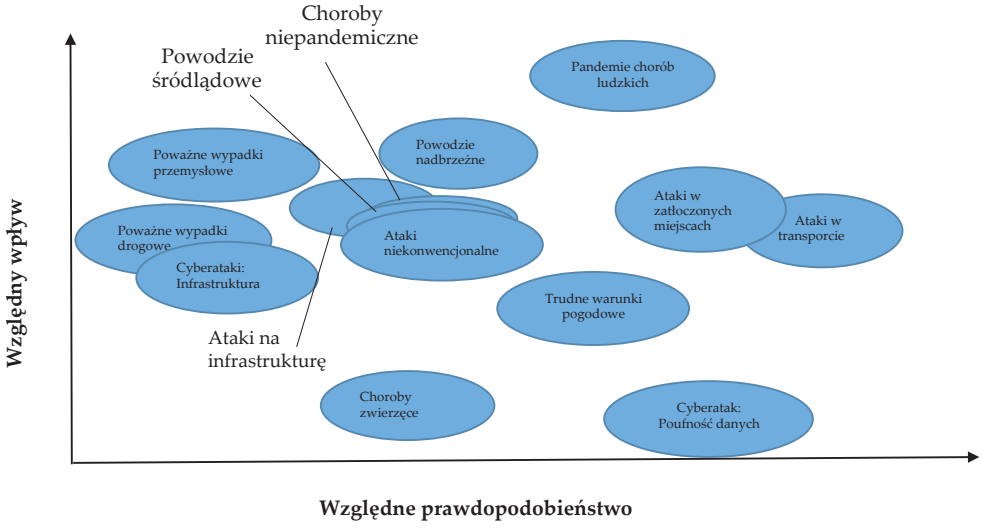
[16] *National Risk Register for Civil Emergencies 2013* (NRR), Cabinet Office; 2010.

Określając ryzyko, rozważa się następujące kwestie:

- Jakie są cele w zarządzaniu ryzykiem?
- Jakie rodzaje ryzyka wymagają natychmiastowego działania? Które mogą zostać przyjęte?
- Jakie problemy pojawiły się w przeszłości i jakie były tego konsekwencje?
- W jaki sposób ograniczone zasoby należy rozmieścić, aby zminimalizować ryzyko?

Wartość zidentyfikowanego ryzyka określa się, biorąc pod uwagę ustalone progi prawdopodobieństwa wystąpienia zdarzenia. Uwzględnia się przy tym różne rodzaje ryzyka, stosując pięciostopniową skalę (od 1 do 5). Połączenie prawdopodobieństw i skutków umożliwia wskazanie liczby priorytetowych ryzyk. Oblicza się to poprzez pomnożenie dwóch indywidualnych danych, uwzględniając ramy czasowe, w których wymagane może być podjęcie działań w reakcji na zidentyfikowane ryzyko. W tym względzie wyższa wartość oszacowanego ryzyka wskazuje na konieczność podjęcia pilnych działań mających na celu przeciwdziałanie mu.

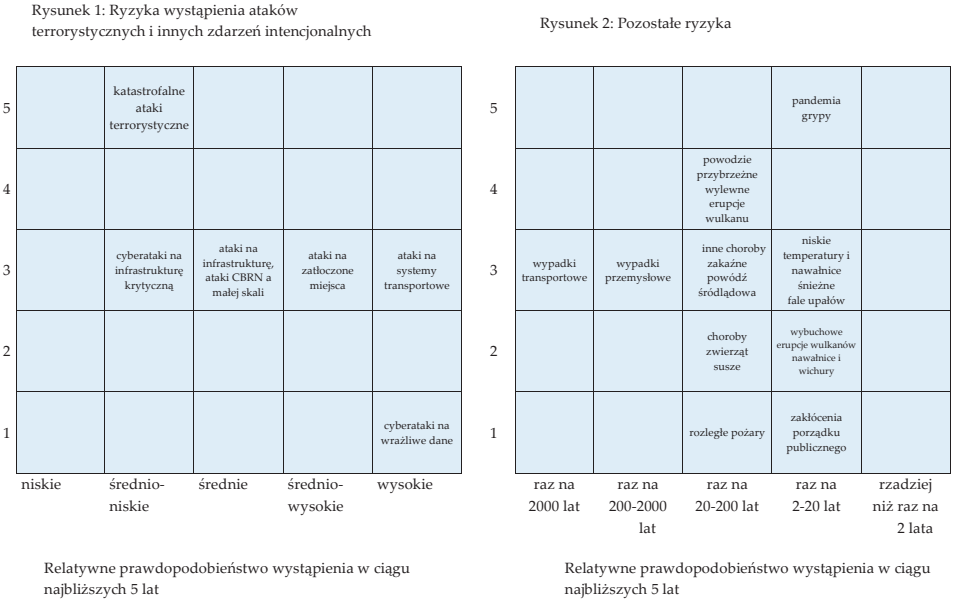
Rysunek 4.15. przedstawia względne prawdopodobieństwo i wpływ każdej z głównych grup ryzyka w odniesieniu do całego kraju. Za największe zagrożenie uznaje się epidemię grypy. Niemniej jednak wskazuje się, iż poziom zidentyfikowanego ryzyka może różnić się w zależności od lokalizacji, w której może ono wystąpić.



Rysunek 4.15. Zagrożenia umieszczone na wykresie względem prawdopodobieństwa oraz wpływu

Źródło: opracowanie własne na podstawie: The National Risk Register of Civil Emergencies (NRR) 2010, s. 5

W celu dywersyfikacji wyników oceny ryzyka praktykuje się również połączenie analizy danych naukowych, historycznych oraz opinii ekspertów. Dzięki temu możliwe jest oszacowanie przybliżonego prawdopodobieństwa. Tam gdzie jest to możliwe, ryzyka prezentowane są pojedynczo na matrycach. Z uwagi na klasyfikację niektórych informacji ujętych w *National Risk Assessment* (NRA), część zagrożeń pogrupowano w różne kategorie (np. *ataki na zatłoczone miejsca*). Kategorie i ryzyka przedstawiono na matrycach (rysunek 4.16.). Analizując je należy zauważyć, że obie skale nie są bezpośrednio porównywalne ze sobą.



Rysunek 4.16. Podstawowe zagrożenia, na jakie narażona jest Wielka Brytania

Źródło: opracowanie własne na podstawie: The National Risk Register of Civil Emergencies (NRR) 2013, s. 10

Zamieszczona po lewej stronie matryca wskazuje na prawdopodobieństwo wystąpienia ataku terrorystycznego, z kolei ta po prawej stronie innych możliwych zagrożeń. W przypadku obu matryc prawdopodobieństwo ocenia się w perspektywie najbliższych pięciu lat.

Krajowy rejestr ryzyka nie obejmuje:

- długoterminowych globalnych zagrożeń – takich jak zmiana klimatu, czy też konkurencja na rynkach dostaw energii,
- ryzyka związanego z poważnymi sytuacjami nadzwyczajnymi występującymi poza granicami kraju, chyba że mają one wpływ bezpośrednio na ludność lub środowisko w Wielkiej Brytanii,
- codziennych zdarzeń, takich jak pospolite przestępstwa czy zakłócenia porządku publicznego.

Wszystkie zagrożenia mające wpływ na bezpieczeństwo narodowe łącznie z zagrożeniem katastrofami naturalnymi oraz atakami terrorystycznymi obejmuje dokument niejawny (*National Security Risk Assessment* – NSRA).

Wielka Brytania uważana jest na świecie za jednego z pionierów w zarządzaniu ryzykiem w ramach sytuacji nadzwyczajnych.

4.7. Komparatystyka metodyk analizy ryzyka stosowanych w wybranych krajach

Rozpatrywane w ramach niniejszego rozdziału metodyki analizy ryzyka, stosowane w wybranych państwach, bazują na obowiązujących, krajowych uregulowaniach prawnych. Niemniej jednak założenia kilku z nich uwzględniają także dyrektywy norm międzynarodowych z obszaru zarządzania ryzykiem. Metodyki przyjęte w Niemczech, Szwecji oraz Kanadzie oparte są na normie ISO 31000:2009 *Risk management – Principles and Guidelines.* W przypadku Szwecji zaleca się również wykorzystanie wytycznych zawartych w dokumencie ISO/IEC 31010:2009 *Risk management – Risk assessment techniques*. Z kolei w przewodnikach obejmujących metodyki analizy ryzyka stosowane w Irlandii, Wielkiej Brytanii oraz Holandii nie rekomenduje się możliwości wdrożenia tych standardów.

Aspektem różnicującym metodyki jest liczba ich poszczególnych etapów oraz nazewnictwo, jednak w każdej z nich uwzględnia się etapy: identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka.

W metodykach *szwedzkiej* oraz *holenderskiej* cały proces rozpoczyna się od określenia ról oraz odpowiedzialności podmiotów przeprowadzających analizę ryzyka na potrzeby planowania kryzysowego. W tym względzie szczególnie istotne jest przypisanie im zadań, określenie ram czasowych ich realizacji, jak również ustalenie mechanizmów wzajemnej współpracy na każdym z etapów metody.

Pierwszym etapem metodyk stosowanych w Irlandii, Niemczech oraz Kanadzie jest tzw. ustalenie kontekstu. W Szwecji zawiera się ono w drugiej fazie procesu, którą jest identyfikacja ryzyka. W podejściu tym uwzględnia się konieczność dokonania opisu obszaru, dla którego przygotowuje się ocenę ryzyka. Obejmuje on informacje dotyczące geografii zidentyfikowanego terenu, klimatu, populacji, środowiska, zaopatrzenia, jak również gospodarki (Irlandia, Niemcy). Etap ten rozumiany jest również jako opis kontekstu danej organizacji, tj. podmiotu biorącego udział w analizie. Zgodnie z takim podejściem definiuje się kontekst operacyjny organizacji. W tym względzie istotnym aspektem jest scharakteryzowanie jej modelu strukturalnego (w tym struktury organizacyjnej) oraz funkcjonalnego, stanowiącego obszar podejmowanych działań (Szwecja).

Wskazuje się również czynniki zewnętrzne i wewnętrzne, które mogą być brane pod uwagę w zarządzaniu ryzykiem, przy uwzględnieniu polityki, trendów, gospodarki, demografii czy też technologii (Kanada). Szeroką gamę metod służących do ustalenia kontekstu proponuje się w metodyce *kanadyjskiej*. Rekomenduje się m.in. wykorzystanie analizy SWOT, analizy danych historycznych, jak również przepisów prawa krajowego.

Kolejnym etapem jest identyfikacja ryzyka. Istotą tego kroku jest podejście scenariuszowe. Rozpoczyna się on od identyfikacji i selekcji zagrożeń. Następnie

w odniesieniu do nich rozwija scenariusze możliwych zdarzeń. Jedynie w metodyce przyjętej w Irlandii rezygnuje się z ich opracowywania.

W przypadku metodyki *irlandzkiej*, identyfikuje się dwie kategorie zagrożeń: ogólne, typowe zagrożenia, takie jak wypadki drogowe, pożary, oraz zagrożenia specyficzne dla danego regionu. Następnie na podstawie listy potencjalnych zagrożeń dokonuje się ich wyboru. Zwraca się przy tym uwagę na dane historyczne odnoszące się do ich wystąpienia w przeszłości. Zakłada się, iż lista ta powinna podlegać ciągłej aktualizacji. W przypadku Kanady pierwotnie wskazuje się zagrożenia priorytetowe oraz mające bezpośredni wpływ na funkcjonowanie państwa. Następnie w stosunku do nich tworzy się jeden lub więcej scenariuszy zdarzeń. Metodyka ta, podobnie jak w przypadku etapu ustalenia kontekstu rekomenduje użycie szerokiej gamy metod służących do identyfikacji zagrożeń. Wśród nich można wymienić burzę mózgów, zgrupowanie koligacyjne, analizę źródła ryzyka, bazy danych, analizę scenariuszy, analizę SWOT/PESTLE, jak również indywidualne lub grupowe formy identyfikacji ryzyka, w tym ankiety i kwestionariusze, wywiady oraz grupy fokusowe.

Scenariusze odnoszące się do zidentyfikowanych zagrożeń stanowią punkt wyjścia do analizy ryzyka. Uwzględnia się w nich zdarzenie bazowe, jego opis, przyczyny, bezpośrednie konsekwencje, czas trwania, jak również kontekst danego scenariusza. Zagadnienie to zostało szczegółowo opisane w metodyce *niemieckiej*, w której opis scenariusza stanowi odpowiedź na szereg pytań dotyczących typu incydentu, wymiaru przestrzennego, intensywności, czasu jego trwania oraz jego rozwoju. Z kolei w metodyce *holenderskiej* podkreśla się konieczność umieszczenia w opisie scenariusza takich zagadnień, jak: czynniki prowadzące do wystąpienia incydentu (przyczyny oraz procesy współtworzące incydent), jak również stopień podatności oraz odporności ludzi, obiektów oraz społeczeństwa w kontekście rozmiaru scenariusza, w tym jego oddziaływania na infrastrukturę. Zgodnie z metodyką *kanadyjską* w opisie scenariusza należy również zawrzeć plan postępowania z ryzykiem wraz z określeniem działań naprawczych. Z kolei w metodyce *holenderskiej* stosuje się gradację scenariuszy pod kątem skali zdarzenia, jego intensywności, położenia geograficznego oraz wyniku szacowania prawdopodobieństwa. Każdy z nich ma być bowiem unikalny. Opracowanie kilku wariantów scenariuszy ma pozwolić na weryfikację, do jakiego stopnia posiadane siły i środki są wystarczające.

We wszystkich metodykach bazujących na podejściu scenariuszowym podkreśla się konieczność rozpatrywania jedynie scenariuszy mających wpływ na bezpieczeństwo narodowe. W tym względzie rozważa się tzw. *the worst case scenario* rozumiany jako *najgorszy możliwy scenariusz*. W przypadku metodyki *szwedzkiej* scenariusz, aby mógł zostać wzięty pod uwagę musi zagrażać co najmniej jednej wartości narodowej, a w Holandii jednemu żywotnemu interesowi narodowemu. Początkowa faza analizy obejmuje selekcję scenariuszy w kierunku wyboru najbardziej prawdopodobnych oraz najbardziej katastrofalnych w skutkach. Pozostałe z nich odrzuca się lub umieszcza na liście rezerwowej celem ich rozpatrzenia w ramach przeglądu w późniejszym czasie (Wielka Brytania, Szwecja).

W odniesieniu do przyjętej metodologii rozwijania scenariuszy możliwych zdarzeń najbardziej różnorodna jest ta stosowana w Szwecji. Wykorzystuje się tam szereg metod specjalnie dedykowanych temu celowi, w tym MVA, ROSA i IBERO. Metody te są oparte na seminariach i zakładają udział w nich grup eksperckich oraz roboczych w danej dziedzinie. Stosuje się również metody bardziej tradycyjne, w tym te zalecane przez normy międzynarodowe, np. analizę drzewa zdarzeń, analizę drzewa błędów, analizę *Co jeśli?* czy też *Broad Analysis*. Konieczność prowadzenia konsultacji eksperckich na tym etapie analizy podnosi się również w metodyce *brytyjskiej*.

W części z metodyk określa się również horyzont czasowy dla opracowywanych scenariuszy możliwych zdarzeń. Dla przykładu w Kanadzie ocenia się możliwość jego wystąpienia w ciągu pięciu najbliższych lat lub w perspektywie długoterminowej (do 25 lat). Podobne podejście przyjmuje się w Holandii, gdzie scenariusze rozpatruje się w ciągu najbliższych pięciu lat, a ponadto bierze się pod uwagę również tzw. scenariusze rozwojowe. Mogą wystąpić one w dłuższym okresie czasu. Przykładem są scenariusze uwzględniające wpływ starzenia się ludności lub zmian klimatu.

W kolejnym kroku przeprowadza się analizę ryzyka. We wszystkich poddanych analizie metodykach, scenariusze możliwych zdarzeń lub zidentyfikowane zagrożenia rozpatrywane są pod kątem dwóch podstawowych czynników, tj. prawdopodobieństwa ich wystąpienia oraz skutków (wpływu). W przypadku metodyki *holenderskiej* oraz *irlandzkiej* analizę rozpoczyna się od określenia czynnika wpływu. W pozostałych krajach ocena skutków stanowi czynność wtórną po szacowaniu prawdopodobieństwa.

W większości poddanych analizie metodyk na potrzeby określenia prawdopodobieństwa stosuje się pięciostopniową skalę jakościową ze wskaźnikami częstości. Wyraża się ona wskazaniem *raz na ile lat* może wystąpić dane zdarzenie. Stosunkowo najwięcej możliwości w tym zakresie proponuje się w metodyce *szwedzkiej*. Dopuszcza się możliwość użycia jakościowego opisu prawdopodobieństwa wystąpienia zdarzenia, opisu jakościowego za pomocą skali, opisu ilościowego za pomocą skali i podziałów oraz opisu ilościowego z wykorzystaniem statystyki.

Informacje niezbędne do szacowania prawdopodobieństwa wystąpienia zdarzenia ujętego w scenariuszu zbierane są w oparciu o analizę danych historycznych oraz statystycznych, jak również bazując na wynikach badań naukowych lub szacowaniu eksperckim. Jedyną metodyką, w której nie rekomenduje się wykorzystania danych historycznych, a pod uwagę bierze się tylko aktualnie występujące zagrożenia, jest metodyka *kanadyjska*.

Zgodnie z przyjętą w tym kraju metodyką prawdopodobieństwo jest szacowane ilościowo za pomocą deterministycznych metod, takich jak modele i symulacje. Generalnie dąży się do szacowania wartości prawdopodobieństwa w sposób ilościowy. Niemniej jednak w przypadku braku danych statystycznych dopuszcza się określenie tego czynnika za pomocą pięciostopniowej skali jakościowej (Niemcy). Metodyka *kanadyjska* za scenariusze zdarzeń, które powinny być rozpatrywane pod

kątem oceny jakościowej, uznaje te związane z zamachami terrorystycznymi lub sabotażem. Z kolei w Holandii ocenę jakościową przeprowadza się dla scenariuszy zdarzeń intencjonalnych. Scenariusze zdarzeń niecelowych podlegają ocenie ilościowej ze wskaźnikami częstości oraz ustanowionymi w miarę równy sposób przedziałami liczbowymi. Co więcej, jedynie w tej metodyce przyjmuje się wewnętrzny podział parametrów dla czterech z pięciu kategorii prawdopodobieństwa na tzw. subkategorie (wysokie, średnie, niskie). Dokonuje się tego na potrzeby stworzenia większej przestrzeni dla uzyskanych wyników szacowania tego czynnika.

W części metodyk w ramach szacowania prawdopodobieństwa i skutków zdarzenia zaleca się, aby dodatkowo uwzględnić parametr podatności. W Holandii stosuje się go w odniesieniu do scenariuszy zdarzeń intencjonalnych. W tym względzie rozważa się podatność obiektów narażonych na atak terrorystyczny, w tym miejscowości, budynków, środków transportu, systemów teleinformatycznych, jak również ludzi. Wyznaczenie jednego z trzech kryteriów podatności determinuje wzrost lub spadek szacowanej wartości czynnika prawdopodobieństwa. Analizę podatności przeprowadza się również w Szwecji, gdzie stanowi ona kolejny etap po dokonaniu wstępnej analizy ryzyka. Ma ona na celu zbadanie jak poważnie zdarzenie oddziałuje na społeczeństwo lub organizację.

Poddane analizie rozwiązania stosowane w wybranych krajach różnią się w odniesieniu do szacowania wpływu danego scenariusza. W tym względzie przyjmuje się dwa główne podejścia. Pierwsze z nich odnosi się do oceny skutków scenariusza zdarzeń w stosunku do kilku przyjętych kategorii, np. *człowiek*, *środowisko*, *gospodarka*, *zaopatrzenie*, *materialne* (Niemcy). W innym ujęciu przyjmuje się podział na skutki w kategoriach takich, jak: *życie i zdrowie ludzkie*, *dobrobyt*, *środowisko*, *infrastruktura* oraz skutki *społeczne* (Irlandia). W metodyce *kanadyjskiej* oprócz kategorii takich, jak: *ludzie*, *środowisko*, *gospodarka* czy też skutki *społeczno-psychologiczne* pod uwagę bierze się również wpływ na bezpieczeństwo terytorialne oraz reputację Kanady. Ostatnie dwie kategorie stanowią sedno drugiego podejścia do szacowania skutków. Podobnie ma się rzecz w Szwecji, gdzie wpływ ocenia się w odniesieniu do wartości narodowych (życie i zdrowie człowieka, funkcjonowanie społeczne, demokracja, rządy prawa, prawa i wolności człowieka, mienie prywatne i publiczne, wartość produkcji dóbr i usług, niepodległość państwowa). W Holandii wpływ rozpatrywany jest w stosunku do żywotnych interesów państwa (bezpieczeństwo terytorialne, bezpieczeństwo fizyczne, bezpieczeństwo ekonomiczne, bezpieczeństwo ekologiczne, społeczno-polityczna stabilność).

Oba omawiane podejścia zakładają, iż w stosunku do przyjętych w danym kraju kategorii skutków należy wyznaczyć poszczególne parametry (kryteria) wpływu (skutków). W metodyce *niemieckiej* określa się je mianem tzw. rodzaju szkody, która może przyjąć postać liczby ofiar, liczby rannych oraz liczby osób potrzebujących pomocy w odniesieniu do kategorii *Ludność*. Podobnie jest w innych metodykach, w tym *irlandzkiej, kanadyjskiej, holenderskiej oraz szwedzkiej.* W państwach tych parametry ustala się odpowiednio dla wartości narodowych oraz żywotnych interesów kraju. Kolejnym krokiem jest wskazanie mierników dla poszczególnych parame-

trów. W zależności od kraju są nimi: wartości liczbowe związane z liczbą osób, długością i wielkością zagrożonego obszaru (np. km, ha), wartością finansową (np. w euro), czy też jednostką czasu (np. w godzinach). W tym względzie ustala się przedziały liczbowe wraz ze wskazaniem wartości progowych. Na ogół analiza ta prowadzi do szacowania wartości wpływu przy użyciu pięciostopniowej skali jakościowej np. od 1 do 5 (skutki: *nieistotne*, *małe*, *średnie*, *duże* i *katastrofalne* w metodyce *niemieckiej*) lub od A do E (konsekwencje: *ograniczone*, *istotne*, *poważne*, *bardzo poważne* oraz *katastrofalne* w metodyce *holenderskiej*). Dodatkowo, ostatnia z wymienionych metodyk wprowadza konieczność szacowania wpływu danego scenariusza, biorąc pod uwagę wartości: *najniższą możliwą*, *prognozowaną* oraz *najwyższą możliwą*.

Istotnym aspektem w ramach szacowania wartości czynnika wpływu jest agregacja wyników. W tym zakresie obliczenia matematyczne przeprowadza się w metodyce *niemieckiej*, gdzie wszelkie wskaźniki liczbowe poszczególnych parametrów, przekonwertowuje się do skali od 1 do 5. Następnie dodaje się je i dzieli na liczbę parametrów, uzyskując tym samym ostateczny, całościowy wynik wpływu. Metodę agregacji przyjmuje się również w metodyce *kanadyjskiej*. Niemniej jednak największy stopień jej skomplikowania charakteryzuje metodykę *holenderską*. W Holandii wykorzystuje się bowiem metodę sumy ważonej oraz szereg funkcji liczbowych. Z kolei w Irlandii całkowicie rezygnuje się z przeprowadzenia wszelkich obliczeń matematycznych związanych z analizą ilościową.

Ciekawym rozwiązaniem jest zbadanie wiarygodności wyniku szacowania czynniku wpływu, które w Kanadzie określane jest mianem poziomu wiarygodności oceny. Wyznaczony jest on w oparciu o pięciostopniową skalę od A do E. O ile w metodyce *kanadyjskiej* dokonuje się tego na etapie analizy wpływu, to w Szwecji poziom niepewności oceny określa się w odniesieniu do połączonego wyniku prawdopodobieństwa i skutków.

Kolejnym krokiem jest przeprowadzenie oceny ryzyka w oparciu o wyniki szacowania prawdopodobieństwa i wpływu. Za powszechnie używane narzędzie przedstawienia wyników oceny ryzyka uważa się matrycę ryzyka. Przyjmuje ona formę matrycy 5 x 5. Pierwotnie zaznacza się na niej poziom zidentyfikowanego ryzyka dla każdego scenariusza zdarzeń. Następnie tworzy się zbiorczą matrycę ryzyka celem przeprowadzenia analizy porównawczej wszystkich ryzyk. Zgodnie z metodyką *irlandzką* tworzy się dodatkowo matrycę ryzyka dla każdej z czterech kategorii zagrożeń, w tym naturalnych, transportowych, technologicznych oraz cywilnych.

Dopuszcza się również możliwość wizualizacji ryzyka za pomocą logarytmicznego wykresu ryzyka, matrycy lub innej formy prezentacji tabelarycznej lub wizualnej. Przykładem może być wykres punktowy oceny ryzyka, który uwzględnia dopuszczalne oraz niedopuszczalne poziomy ryzyka (Kanada). Z kolei w metodyce *holenderskiej* formą przedstawienia wyników oceny ryzyka jest diagram ryzyka, który oparty jest na konstrukcji logarytmicznej. W Irlandii matrycę ryzyka dzieli się na dwie strefy, które obejmują zdarzenia umiarkowane, jak również zdarzenia wymagające najwyższego stopnia gotowości. Tym samym wskazuje się obszary zapobiegania i redukcji ryzyka. Z kolei zgodnie z metodyką *brytyjską* stosuje się od-

dzielne matryce dla ryzyk związanych ze scenariuszami zdarzeń intencjonalnych oraz dla pozostałych ryzyk.

W poddanych analizie metodykach wskazuje się, że ocena ryzyka nie kończy całej analizy. Stanowi bowiem część całościowego procesu zarządzania ryzykiem. W części z omawianych rozwiązań problematyka postępowania z ryzykiem wykracza poza ramy przewodnika po analizie ryzyka, jednakże w kilku z nich została ona uwzględniona. W metodyce *kanadyjskiej* rozpatruje się m.in. kwestie wyboru oraz realizacji środków kontroli ryzyka, jak również działań mających na celu ograniczenie negatywnych skutków. Ponadto rozważa się problematykę zapobiegania zagrożeniom, zmniejszenia lub eliminacji ryzyka, czy też usuwania jego źródła. Z kolei w metodyce *holenderskiej* etap ten określa się mianem oceny zdolności, której celem jest wskazanie sił i środków, które muszą zostać wzmocnione w ramach przeciwdziałania danemu ryzyku. Pozwala to na przekazanie właściwym decydentom rekomendacji co do dalszych działań w tym zakresie.

Metodyka oceny ryzyka jest narzędziem wspierającym proces planowania w ramach zarządzania kryzysowego (ochrony ludności). Określa, w jaki sposób identyfikować zagrożenia, szacować ryzyko ich wystąpienia, jak dokonać ewaluacji ryzyka. Dzięki temu możliwe jest przeprowadzenie dalszych działań w ramach etapu postępowania z ryzykiem. Obejmuje on wszelkie przedsięwzięcia podejmowane w odniesieniu do zidentyfikowanych ryzyk, biorąc pod uwagę poziom ich akceptowalności.

Poddane analizie rozwiązania przyjęte w wybranych krajach różnią się stopniem szczegółowości prezentowanych w nich treści. Część metodyk obejmuje wytyczne odnoszące się do poszczególnych kroków oceny ryzyka, np. Holandia. W Wielkiej Brytanii część materiałów opisujących podejście tego państwa do omawianej problematyki ma charakter niejawny. Analiza dostępnego materiału pozwoliła jednak na określenie zarówno podobieństw poszczególnych podejść, jak i występujących pomiędzy nimi różnic.

Wspólnymi etapami omawianych metodyk są identyfikacja ryzyka, analiza ryzyka oraz ocena ryzyka. Poddane analizie rozwiązania umiejscawiają proces oceny ryzyka w ramach całościowego procesu zarządzania ryzykiem.

W większości z rozpatrywanych metodyk, punktem wyjścia do analizy ryzyka jest budowa scenariuszy możliwych zdarzeń. Wśród nich kluczowe znaczenie mają te skutkujące wpływem w skali narodowej oraz *najgorsze możliwe przypadki* (scenariusze o wysokim prawdopodobieństwie ich wystąpienia oraz poważnych skutkach). Istotą analizy ryzyka jest oszacowanie wartości tych dwóch czynników. Na ogół stosuje się dwie pięciostopniowe skale prawdopodobieństwa i skutków. Dąży się do przeprowadzenia analizy w sposób ilościowy (w przypadku czynnika prawdopodobieństwa przy użyciu wskaźnika częstości, a w stosunku do wpływu przy wykorzystaniu wartości liczbowych oraz przyporządkowanych im wartości progowych). Te ostatnie wyznacza się w odniesieniu do ustalonych parametrów wpływu. W uzasadnionych przypadkach pozostawia się możliwość przeprowadzenia oceny jakościowej.

Za główne źródła informacji, w oparciu o które szacuje się ryzyko, uznaje się dane historyczne, dane statystyczne, szacowanie eksperckie, jak również pojawiające się trendy.

W każdej z metodyk zaleca się stosowanie jakościowych i ilościowych metod na poszczególnych etapach procesu oceny ryzyka. Wśród nich można wyróżnić zarówno te wynikające z międzynarodowych norm i standardów np. analiza drzewa zdarzeń (ETA) czy analiza drzewa błędów (FTA), jak również te, które stanowią rezultat autorskich koncepcji, np. metody scenariuszowe oparte na seminariach stosowane w Szwecji. We wszystkich z omawianych rozwiązań rekomenduje się wykorzystanie narzędzi służących do przedstawienia wyników oceny ryzyka, którymi głównie są matryce ryzyka.

Niniejsza analiza wykazała również wiele różnic pomiędzy założeniami metodyk przyjętych w poszczególnych państwach. Odnoszą się one m.in. do sposobów budowania scenariuszy możliwych zdarzeń. Dotyczą też kwestii szacowania prawdopodobieństwa oraz skutków ich wystąpienia. Poszczególne państwa przyjmują bowiem różne kategorie wpływu oraz odpowiadające im parametry. Wskazują również innego rodzaju wartości progowe służące do wskazania odpowiedniej wartości szacowanych czynników prawdopodobieństwa oraz wpływu. W różnym stopniu wykorzystują parametry *wiarygodności* uzyskanej oceny lub niepewności otrzymanego wyniku, jak również podatności. Ponadto stosują inne metody agregacji wyników wpływu dla scenariuszy możliwych zdarzeń. Część z nich przyjmuje odmienne ścieżki postępowania w ramach analizy ryzyka scenariuszy dla różnych typów zdarzeń. W tym względzie w inny sposób analizowane są scenariusze o charakterze intencjonalnym (np. ataki terrorystyczne), a w inny te o charakterze niecelowym.

5. Metody i techniki wykorzystywane w zarządzaniu ryzykiem

Zarządzanie ryzykiem stanowi złożony proces, w którym wykorzystuje się różnego rodzaju metody i techniki badawcze. Ich wybór zależy od obszaru, który poddawany jest analizie, a także od realizowanego etapu. Pierwszym etapem postępowania z ryzykiem jest identyfikacja wszystkich możliwych zagrożeń. Zagrożenie definiowane jest jako źródło potencjalnej szkody[1]. Może odnosić się do sfery świadomościowej danego podmiotu (człowieka, grupy społecznej, narodu) i jest to pewien stan świadomości wywołany postrzeganiem zjawisk ocenianych jako niekorzystne lub niebezpieczne. Percepcja zagrożeń przez ten podmiot, tym samym i jego poczucie bezpieczeństwa, stanowi odzwierciedlenie w jego świadomości realnego lub potencjalnego zagrożenia[2]. Ryzyko zaś w literaturze przedmiotu najczęściej definiowane jest jako wpływ niepewności na cele[3]. Można powiedzieć, że źródłem ryzyka jest niepełność informacji lub podjęta decyzja, która jest nieoptymalna ze względu na założony cel. W niemal każdej dziedzinie z tych obszarów ma ono swoją specyfikę pojęciową, a zwłaszcza ujęcie w sensie wartościującym – różne są jego miary i sposób wyznaczania.

Identyfikacja zagrożeń odpowiada na pytanie: co złego i gdzie może się stać?[4] – jest to proces poszukiwania, rozpoznawania i rejestrowania ryzyka[5]. Ważne jest, by w procesie szacowania ryzyka zidentyfikować wszystkie zagrożenia – jest to pierwszy i jeden z najważniejszych etapów w całym procesie. Identyfikując zagrożenia, należy korzystać z wszelkiej dostępnej wiedzy na temat zagrożeń oraz zaleca się sprawdzić, czy dostępne na ich temat informacje i dokumenty są wystarczające.

Metoda badania naukowego stanowi wypróbowany, skuteczny sposób zmiany początkowego stanu wiedzy badacza o przedmiocie badania w stan docelowy, do którego badacz ma lub chce dojść w określonych lub odpowiednio dobranych warunkach przy użyciu odpowiednio dobranych środków (technik) stosowanych do przyjętego planu[6]. W praktyce i teorii metod szacowania i oceny ryzyka jest kilkadziesiąt.

---

1 PKL-ISO GUIDE-73:2012. Zarządzanie ryzykiem – Terminologia, s. 17.

2 Witryna internetowa http://www.uwm.edu.pl/mkzk/download/wprowadzenie.pdf, z dnia 25.08.2014 r.

3 PN-ISO 31000:2012, *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN Warszawa 2012; s. 15.

4 Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2010, s. 8.

5 PN-ISO 31000:2012, *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN Warszawa 2012; s. 21.

6 W. Okoń, *Nowy słownik pedagogiczny*, wyd. Żak, Warszawa 1996, s. 333-334.

Metody można podzielić na trzy grupy:
- ilościowe,
- jakościowe,
- mieszane.

Inna klasyfikacja dzieli je na metody subiektywne oraz obiektywne.

Problematyka związana z zarządzaniem ryzykiem jest zagadnieniem stosunkowo nowym, dlatego wśród metod jego pomiaru dominują metody jakościowe. Bazują one na szacowaniu parametrów zagrożeń przez ekspertów, co wiąże się z określeniem skal jakościowych, częstotliwości wystąpienia ryzyka oraz podatności na dane zagrożenie. Jak wskazuje praktyka, nie są one jednak wystarczającym efektywnym narzędziem do analizy ryzyka. Zastosowanie metod jakościowych powinno być uzupełnieniem pomiarów ryzyka wykonanych za pomocą metod ilościowych[7].

Do metod ilościowych zalicza się te, które umożliwiają oszacowanie poziomu ryzyka dzięki przetwarzaniu danych o rzeczywistych skutkach zaistniałych strat oraz potencjalnych skutkach i stratach, wywołanych zdarzeniami, które możemy przewidzieć.

Wśród metod ilościowych stosowanych w zarządzaniu ryzykiem operacyjnym wyróżnia się trzy grupy metod:
1. Metody pomiaru ryzyka zalecane przez Komitet Bazylejski:
   - metoda wskaźnika podstawowego,
   - metoda standardowa,
   - metoda zaawansowanego pomiaru.
2. Metody statystyczne:
   - metody oparte na wskaźniku Value at Risk,
   - metody Monte Carlo,
   - metody porównawcze wykorzystujące metodologie analizy scenariuszy awaryjnych,
   - metody wykorzystujące testy skrajnych warunków, tzw. stress testing,
   - metody oparte na Teorii Wartości Ekstremalnych,
   - metody umożliwiające modelowanie ryzyka operacyjnego przy użyciu sieci beyesowskich.
3. Pozostałe metody ilościowe:
   - metody analizy porównawczej,
   - metody badań operacyjnych,
   - metody six sigma[8].

Metody obiektywne to obserwacja, eksperyment i test psychologiczny, natomiast subiektywne to introspekcja, wypytywanie (ankieta, kwestionariusz), skale postaw, techniki[9]. Analizując natomiast cechy charakterystyczne metod podejścia ilościowego oraz jakościowego, można wyróżnić ich następujące cechy:

---

7 M. Thlon, *Przegląd ilościowych metod szacowania ryzyka operacyjnego*, styczeń 2007

8 J. Orzeł, *Ilościowe metody pomiaru ryzyka operacyjnego* w: BiK, nr 7/2005, NBP, Warszawa 2005.

9 W. Szewczuk, *Encyklopedia psychologii*, wyd. Fundacja Innowacja, Wyższa Szkoła Społeczno-Ekonomiczna, Warszawa 1998, s. 233-234.

Tabela 5.1. Kryteria Yvonny Lincoln i Egona Guby do oceny metodologicznej jakości technik i procedur badawczych

Podejście ilościowe	**Podejście jakościowe**
wewnętrzna trafność	wiarygodność
zewnętrzna trafność	spolegliwość
rzetelność	możliwość przeniesienia
obiektywność	potwierdzalność

Źródło: K. Stemplewska-Żakowicz, Metody jakościowe, metody ilościowe: hamletowski dylemat czy różnorodność do wyboru?; Roczniki Psychologiczne, tom XIII, nr 1-2010

W analizie jakościowej wszelkie ryzyko i potencjalne skutki jego wystąpienia prezentowane są w sposób opisowy. Polega to na użyciu scenariuszy zdarzeń i określeniu skutków potencjalnych realizacji ryzyka. W podejściu ilościowym zaś przy szacowaniu ryzyka najważniejsze jest określenie dwóch podstawowych parametrów, tj. Wartości skutku i prawdopodobieństwa wystąpienia danego ryzyka[10]. Za pomocą metod powinny zostać określone zagrożenia priorytetowe, mające bezpośredni wpływ na funkcjonowanie państwa. Identyfikując zagrożenia, należy korzystać z wszelkiej dostępnej wiedzy na temat zagrożeń oraz zaleca się sprawdzić, czy dostępne na ich temat informacje i dokumenty są wystarczające.

5.1. Identyfikacja zagrożeń

Źródła ryzyka determinowane są przez różne podsystemy. Istotnym czynnikiem generującym ryzyko jest otoczenie ekonomiczne. Kolejnym segmentem otoczenia dalszego jest otoczenie technologiczne. Następnym podsystemem otoczenia dalszego, jest otoczenie społeczne i demograficzne. Źródeł ryzyka należy poszukiwać również w otoczeniu politycznym i prawnym. Ostatnim segmentem otoczenia dalszego generującym ryzyko jest otoczenie międzynarodowe[11]. Ponadto źródła ryzyka podzielić można m.in. ze względu na ryzyko:

- strategiczne (najważniejsze), mające bezpośredni wpływ na strategię organizacji, jest to ryzyko występujące w perspektywie długiego okresu i w znaczny sposób determinujące plan strategiczny firmy,
- operacyjne – dotyczy bieżącej działalności organizacji i tzw. problemów dnia codziennego,
- ryzyko rynkowe wynikające ze zdarzeń na rynku i zmieniających się wartości aktywów na rynku,
- prawne – realizowanie zadań w oparciu o niejasne, zmieniające się przepisy,
- stochastyczne – losowe,
- deterministyczne – wynikające z woli człowieka, jego zaniedbań, złych decyzji, czy złej woli,

[10] *Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001*, zeszyty naukowe Akademia Morska w Szczecinie 2009,19(91) s. 63-70.

[11] A. Wawiernia, *Ryzyko jako szansa i zagrożenie dla działalności przedsiębiorstwa.* Gdańsk 2013

- czyste – przynoszące straty,
- spekulacyjne – gdy przynosi straty lub zysk[12].

Zagrożenia zaś możemy podzielić na pierwotne (awarie, katastrofy, kataklizmy) i wtórne (klęski żywiołowe).

Do pierwotnych zaliczamy zagrożenia:

1) Naturalne (woda, powietrze, ogień, ziemia, kosmos).
2) Techniczne (komunikacyjne, technologiczne, budowlane, komunalne, nielegalne przechowywanie materiałów niebezpiecznych).
3) Militarne (bezpośrednie użycie sił zbrojnych, akty terroru).
4) Nadzwyczajne zagrożenie środowiska — także niektóre zdarzenia z zagrożeń technicznych i militarnych o charakterze antropomorficznym.

Do wtórnych zaś zagrożenia:

1) Egzystencji człowieka (masowe zgony, głód, epidemie i pandemie).
2) Społeczne (patologie społeczne — przestępczość, narkomania, prostytucja, masowe bezrobocie, zaburzenia zdrowia psychicznego).
3) Naruszenie równowagi biologicznej (nadmierny przyrost fauny i flory epizootie, epifitozy).
4) Masowe straty (zniszczenie lub długotrwałe skażenie środowiska naturalnego – klęska ekologiczna, pomór zwierząt, zniszczenie dóbr niezbędnych do przeżycia)[13].

Celem identyfikacji zagrożeń jest określenie, co może się zdarzyć mającego wpływ na osiągnięcie celów systemu lub organizacji. Po identyfikacji ryzyka, organizacja powinna zidentyfikować mechanizmy kontrolne, takie jak ludzie, funkcje i systemy. Proces identyfikacji obejmuje identyfikację przyczyn i źródeł ryzyka, czyli wydarzeń, sytuacji lub okoliczności, które mogłyby mieć wpływ na cele oraz charakter tego wpływu.

Metody identyfikacji ryzyka powinny obejmować:

- materiały oparte na dowodach, np. listy kontrolne i dane historyczne,
- systematyczne podejście (za pomocą uporządkowanego zbioru podpowiedzi lub pytań), np. wywiady eksperckie,
- wnioskowanie indukcyjne, np. metoda HAZOP.

W celu usprawnienia i bardziej precyzyjnej identyfikacji ryzyka powinno się wykorzystywać różne techniki wspierające ten proces. Niezależnie od technik przy identyfikacji ryzyka należy zawsze brać pod uwagę czynniki, takie jak:

- osoby zagrożone,
- rodzaj, częstość i czas narażenia,
- znaczenie szkody,
- współdziałanie człowieka,
- środki bezpieczeństwa,

---

[12] Witryna internetowa http://www.almamer.pl/aa%20materialy.%20dydaktyczne/E_Zarzadzanie_projektami_biznesowymi_Duczkowska-Piasecka.pdf z dnia 20.01.2015 r.

[13] R. Jakubczak, *Obrona narodowa w tworzeniu bezpieczeństwa III RP*, Dom Wydawniczy BELLONA, Warszawa 2003, załącznik 32 wg K. Przeworskiego.

- środowisko,
- czynniki zewnętrzne[14].

Wykorzystywane obecnie przez system zarządzania kryzysowego metody zostały wskazane w Procedurze opracowania raportu cząstkowego. Dokument wymienia następujące działania:

- analiza danych historycznych,
- analiza danych statystycznych,
- szacowanie eksperckie,
- badania terenowe,
- ocena sytuacji międzynarodowej,
- modelowanie matematyczne,
- analiza danych z systemów monitorowania zagrożeń,
- analiza trendów,
- badanie przypadków,
- rozpoznanie środowiskowe.

Niemniej w literaturze przedmiotu identyfikowane są także inne wybrane techniki i metody, z których część wykorzystywana jest w innych etapach, np. w trakcie oceny ryzyka:

- listy kontrolne,
- kwestionariusz ryzyka,
- dokumenty planistyczne,
- diagram sekwencji działań (przyczynowo-skutkowy),
- analiza przyczyn i skutków (PHA),
- mapy zagrożeń,
- burza mózgów,
- metoda FMEA (*Failure Mode and Effect Analysis*),
- metoda HAZOP (*Hazard and Operability Study*),
- metoda HRA (*Human Reliability Analysis*),
- schemat blokowy (Flowchart),
- kwestionariusz ryzyka,
- metody scenariuszowe,
- analiza przyczyn źródłowych,
- metoda delficka.

Najczęściej stosowaną metodą rozpoznawania zagrożeń jest analiza danych historycznych, w której przeglądowi i badaniu poddawane są źródła informacji, m.in. takie jak: rejestry wypadków, ankiety, prognozy i raporty. Podstawą rejestracji danych historycznych jest tabela, w której zawarte są informacje dotyczące przedziału czasowego, miejsca/obszaru wystąpienia, opisu zdarzenia, skutki, konsekwencje oraz funkcje instytucji.

[14] ISO 31010 – *Zarządzanie ryzykiem – Techniki oceny ryzyka (Risk management – Risk assessment techniques)*

Przykład znajduje się w tabeli 5.2.

Tabela 5.2. Rejestracja danych historycznych.

data lub przedział czasowy	**miejsce/ obszar wystąpienia**	**krótki opis**	**skutki/straty/ konsekwencje**	**funkcja instytucji/ organ**	**wnioski, spostrzeżenia i opinie**
Kiedy wystąpiło dane zagrożenie	Gdzie wystąpiło wskazane zagrożenie	Jak doszło do powstania zdarzenia	Jakie skutki wystąpiły w stosunku do mienia, infrastruktury, środowiska i gospodarki	Jaką funkcję pełniła dana instytucja w zwalczaniu danego zagrożenia	

Źródło: opracownie własne na podstawie Procedury opracowania raportu cząstkowego

Analizę danych historycznych można przeprowadzić za pomocą:
- Konsolidacji – połączenia danych, które pochodzą z różnych źródeł.
- Drążenia – wydobycia danych szczegółowych.
- Obracania – przedstawiania tych samych danych z różnych punktów widzenia.

Wadą tej metody jest brak możliwości zidentyfikowania pojawiających się nowych zagrożeń lub też tych, które występują bardzo rzadko.

Celem analizy statystycznej jest wykrycie określonych w procesie badawczym prawidłowości, które występują w poddawanych analizie zjawiskach, określenie ich charakteru, objaśnienie oraz wyciągnięcie właściwych wniosków z pozyskanych danych bez wnikania w ich zawartość. Działania statystyczne stosuje się do opisu zjawisk masowych. Dzięki tym danym można ustalić zmienność zjawisk masowych, tendencji ich przekształceń w czasie. Sporządza się w tym celu wykresy, ilustrujące krzywą rozwoju danego zjawiska czy też to, jaką część większej całości stanowi. Część danych dostarcza badanie metodą grup reprezentatywnych: zbiera się dane nie od wszystkich, ale od odpowiednio wybranej grupy, określanej jako grupa reprezentatywna[15].

Przed rozpoczęciem analizy statystycznej należy:
- uzgodnić, jaką wiedzę o badanym zjawisku mają dostarczyć dane,
- zaplanować badanie,
- podsumować zbiór danych z obserwacji, podkreślając tendencje, ale rezygnując ze szczegółów.

Ankiety eksperckie to zorientowane na ryzyko wywiady z różnymi zainteresowanymi stronami, które pomagają w identyfikacji niezidentyfikowanych w normalnych działaniach planistycznych ryzyk.

Metoda ta składa się z następujących kroków:
1) opracowanie pytań skierowanych do ekspertów,
2) wybór ekspertów z danej dziedziny,

[15] J. Pieter, *Ogólna metodologia pracy naukowej*, Ossolineum, Wrocław 1967.

3) przekazanie pytań ekspertom,
4) analiza odpowiedzi przesłanych przez ekspertów.

Opracowując pytania do ekspertów trzeba wziąć pod uwagę, że:

- eksperci są wrażliwi na poprawność stawianych pytań i zazwyczaj precyzyjnie udzielają odpowiedzi,
- odpowiedź może być poprawna na sformułowane pytanie, lecz nie zawierać treści oczekiwanej przez pytającego,
- pytania kierowane do ekspertów powinny być kontekstowe – związane z określonym rodzajem zagrożenia, specyfiką (właściwościami) podmiotu, któremu mamy zapewnić bezpieczeństwo funkcjonowania i uwarunkowaniami środowiskowymi podmiotu,
- pytania muszą być poprzedzone informacją o ich kontekście.

Osoba przeprowadzająca ankietyzację, dokonując doboru ekspertów do rozwiązania konkretnego problemu, musi:

- być zorientowana w zakresie wiedzy dziedzinowej, posiadanej przez rozpatrywanego eksperta, której dotyczą pytania oraz jego pozycji środowiskowej,
- znać metody opracowywania informacji, dotyczącej tego samego zagadnienia, uzyskanej od kilku ekspertów.

Z takimi przypadkami mamy do czynienia, gdy ze względu na wagę zagadnienia informację zawartą w odpowiedziach chcemy zobiektywizować i uwiarygodnić. Wówczas to samo pytanie kierujemy do kilku ekspertów. Ponadto metoda zakłada, że nie ma konieczności organizowania spotkań ekspertów w ustalonym miejscu, w celu udzielenia odpowiedzi na przygotowane pytania. Wywiad można przeprowadzić za pośrednictwem Internetu[16].

Jedną z odmian metody ankiet eksperckich są wywiady strukturyzowane lub częściowo ustrukturyzowane. W celu zorganizowania wywiadu niezbędne jest przygotowanie kwestionariusza zawierającego pytania dziedzinowe. Badanie tą metodą pozwala uczestnikowi ocenić sytuację z innej perspektywy, a tym samym zidentyfikować ryzyko pod innym kątem (tzw. wywiad strukturalizowany). Ten rodzaj badań zakłada, że pytania stawiane respondentom znane są, zanim zostaną zadane i pojawią się w z góry ustalonej kolejności. Natomiast wywiad częściowo ustrukturyzowany pozwala na większą swobodę w formułowaniu pytań w celu analizy problemów, które powstają w trakcie badania. Osoba przeprowadzająca wywiad ma możliwość w trakcie jego przeprowadzania zadawania kolejnych pojawiających się w trakcie rozmowy pytań. Strukturyzowane i pół-strukturyzowane wywiady są przydatne, gdy trudno jest zorganizować badanie metodą burzy mózgów lub gdy dyskusja w grupie nie jest odpowiednim rozwiązaniem, biorąc pod uwagę sytuacje lub zaangażowane osoby respondentów. Wywiady najczęściej są wykorzystywane do zidentyfikowania zagrożeń lub do oceny skuteczności istniejących środków kontrolnych

[16] E. Kołodziński, *Analiza ryzyka – Eksperckie metody analizy ryzyka w zarządzaniu bezpieczeństwem*.

w ramach analizy ryzyka. Mogą one być stosowane na każdym etapie procesu zarządzania ryzykiem[17].

W celu przeprowadzenia wywiadu niezbędne jest:

- jasne określenie celów wywiadu,
- wybór i przygotowanie listy rozmówców z zainteresowanymi stronami,
- przygotowanie zestawu pytań.

Metoda badań terenowych polega na badaniu wybranych problemów w normalnych warunkach funkcjonowania zbiorowości. Zwykle metoda badań terenowych obejmuje badania typu:

- etnologicznego polegającego na obserwacji życia codziennego i zjawisk oraz zachodzących w nich zmian i powiazań, biorąc pod uwagę zbiorowość. Dzięki tym badaniom możliwe jest opisanie cech danej zbiorowości oraz ocenienie pewnego zachowania,
- socjologicznego, który od typu etnologicznego różni się tym, iż badacz dodatkowo gromadzi materiały i dokumenty, zawierające dane ilościowe, które pozwalają lepiej poznać obserwowane zjawiska. Wykorzystywane materiały to np. sprawozdania, zestawienia statystyczne oraz wyniki badań ankietowych. W badaniach typu socjologicznego obserwacje poparte są faktami i liczbami,
- socjopsychologicznego – nastawionego głównie na poznawanie stanu świadomości obserwowanej zbiorowości.

Podstawowe techniki badań terenowych to wywiad i obserwacja[18].

Monitorowanie zagrożeń, jako kolejna z wykorzystywanych metod, ma za zadanie zestawienia informacji dotyczących struktur odpowiedzialnych za monitorowanie poszczególnych kategorii zagrożeń i zakresu informacji jakich można od nich oczekiwać oraz trybu ich pracy, a także informacji dotycz acych trybu raportowania i systemu wymiany informacji o zagrożeniach, m.in. poprzez CAR (Centralną Aplikację Raportującą) lub inne systemy raportowania. Przy identyfikacji zagrożeń warto uwzględnić dane i doświadczenia w zakresie monitorowania zagrożeń, w tym wnioski z ćwiczeń i realnych sytuacji kryzysowych[19]. Należy wziąć także pod uwagę automatyczne systemy wymiany informacji. Dzięki analizie danych z systemów monitorowania zagrożeń można określić, jak często na danym terenie występuje określone zagrożenie oraz zestawić dane z różnych lat, jednak podobnie jak w przypadku analizy danych historycznych nie wskaże nam ona zagrożeń, które nie występowały wcześniej, a pojawiają się obecnie.

---

[17] ISO 31010 – *Zarządzanie ryzykiem – Techniki oceny ryzyka (Risk management – Risk assessment techniques).*

[18] Witryna internetowa http://www.eduteka.pl/doc/metoda-badan-terenowych-i-odpowiadajace-jej-techniki-badan, z dnia 22.09.2014 r.

[19] Zalecenia do powiatowych planów zarządzania kryzysowego. Wydział bezpieczeństwa i zarządzania kryzysowego Mazowieckiego Urzędu Wojewódzkiego w Warszawie.

Model matematyczny to skończony zbiór symboli i relacji matematycznych oraz ścisłych zasad operowania nimi, przy czym zawarte w modelu symbole i relacje mają interpretację odnoszącą się do konkretnych elementów modelowanego wycinka rzeczywistości[20]. Dobrze zbudowany model stanowi przedmiot badań analitycznych i komputerowych, dzięki którym można poznać własności rozwiązań[21]. Podczas wyznaczania modelu matematycznego rzeczywiste zjawisko jest upraszczane i przedstawiane w postaci schematycznej. W modelu powinny być uwzględnione jedynie najważniejsze elementy wpływające na proces. Opis matematyczny modelu przedstawia się w postaci układu równań algebraicznych lub różniczkowych[22].

Listy kontrolne to łatwe w użyciu narzędzie, które może zostać wykorzystane przy identyfikacji zagrożeń lub też w procesie oceny ryzyka. Zastosowanie tego narzędzia składa się z przygotowania odpowiedniego do potencjalnego zagrożenia kwestionariusza pytań i przeglądu pytań, odpowiedzi na pytania identyfikujące znane rodzaje zagrożeń i potencjalnie niebezpieczne sytuacje związane ze stosowanymi procesami i operacjami oraz analizy wyników.

Wadą tej metody jest czasochłonne przygotowanie listy z pytaniami. Ponadto gdy oceniający zamierza uzyskać dokładniejsze informacje, analiza dokonana w oparciu o listę kontrolną może okazać się niewystarczająca.

Poniżej przykładowa lista kontrolna dotycząca pożaru:

1) Czy na terenie są obszary, na których występuje zagrożenie pożarem?/Czy teren jest pokryty lasami/nieużytkami?
2) Czy na terenie występują jakiekolwiek źródła wysokiej temperatury, szczególnie w obszarze zagrożonym pożarem?
3) Czy w okolicy występują zakłady przemysłowe, produkcyjne, w których znajdują się palne, łatwopalne, lub utleniające substancje/preparaty chemiczne, np. farby, lakiery, preparaty czyszczące, kleje, rozpuszczalniki?
4) Czy miejsca zagrożone pożarem są prawidłowo oznakowane?
5) Czy w miejscach zagrożenia pożarem jest odpowiedni sprzęt przeciwpożarowy?
6) Czy sprzęt przeciwpożarowy jest sprawny i systematycznie sprawdzany?
7) Czy drogi ewakuacji są odpowiednio oznakowane?
8) Czy jest zainstalowana sygnalizacja informująca o zagrożeniu pożarowym?
9) Czy łączność ze służbami działa bez zarzutów?

Odpowiedziami na pytania powinny być: tak/nie.

Źródłem informacji o zagrożeniach mogą być również dokumenty planistyczne systemu zarządzania kryzysowego lub plany sporządzane przez służby, inspekcje i straże w zakresie realizacji swoich kompetencji ustawowych. Dokumentacja ta opracowywana jest na podstawie doświadczeń i wniosków wynikających z działań

---

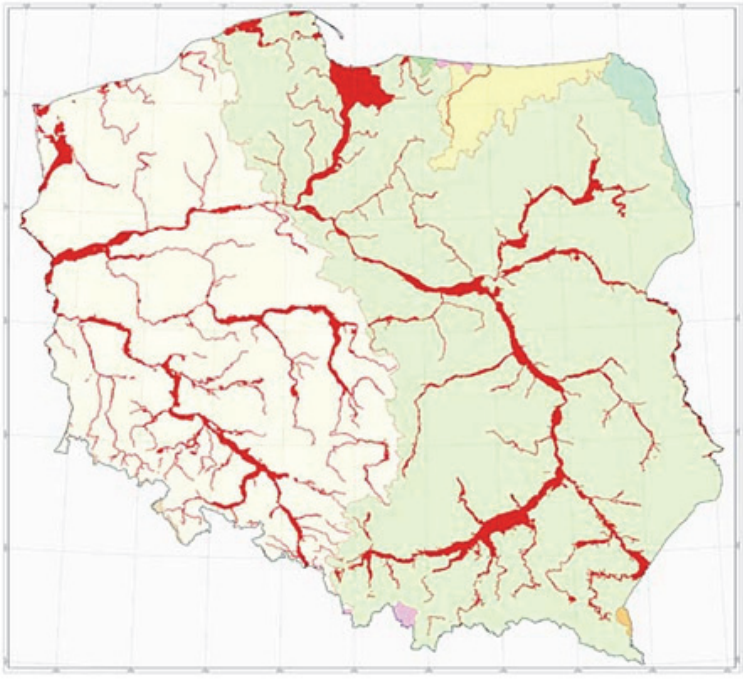
[20] A. Kubala, *Efekty termiczne przy odwadnianiu etanolu w cyklicznym procesie adsorpcyjno-desorpcyjnym zmiennociśnieniowym*, Rozprawa doktorska, Politechnika Krakowska, s. 47.

[21] Witryna internetowa http://www.fuw.edu.pl/~jarekz/MODELOWANIE/M1_wstep_dyskretne.pdf z dnia 11.09.2014 r.

[22] Witryna internetowa http://www.retsat1.com.pl/michauer/chemia/inne/modelowanie.pdf z dnia 11.09.2014 r.

podczas zdarzeń niekorzystnych oraz sytuacji kryzysowych. Ponadto w celu identyfikacji zagrożeń można dokonać przeglądu strategii czy polityk odnoszących się do określonego w nich obszaru geograficznego lub zadaniowego.

Mapa zagrożeń to dokument będący wykazem zagrożeń dla życia i zdrowia ludzkiego oraz mienia, uwzględniający zagrożenia o różnym charakterze zarówno zewnętrzne, jak i wewnętrzne oraz oddziałujące na procesy i informacje mające wpływ na bezpieczeństwo. Mapę sporządza się z uwzględnieniem rozkładu przestrzennego i czasowego danego zagrożenia. Mapa powinna także identyfikować krytyczne procesy i przewidywać możliwe straty w wyniku ich wystąpienia[23].



Rysunek 5.1. Obszary narażone na niebezpieczeństwo powodzi wyznaczone we wstępnej ocenie ryzyka powodziowego[24].

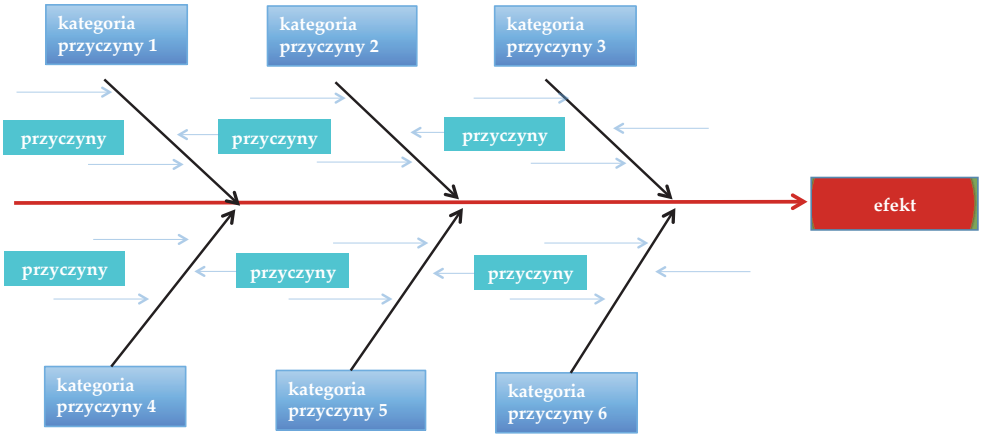
Źródło: http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego

Techniki diagramów powszechnie stosowane w zarządzaniu jakością to: diagramy przyczynowo-skutkowe, zwane również diagramami Ishikawy lub schematami rybiego szkieletu, które pokazują, jak różne przyczyny lub *podprzyczyny* wpływają na powstanie prawdopodobieństwa wystąpienia niekorzystnego zdarze-

[23] Witryna internetowa http://www.powiatwroclawski.pl/index.php?option=com_content&id=1142:mapa-zagroe-powiatu-wrocawskiego&Itemid=8,0 z dnia 04.09.2014 r.

[24] Witryna internetowa http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego, z dnia 04.09.2014 r.

nia lub na efekty. Schemat blokowy, jak każdy schemat, pokazuje zależności pomiędzy elementami systemu. Najczęściej stosowaną metodą przy przygotowywaniu diagramu i jego konstrukcji jest burza mózgów. W ten sposób można uzyskać jak najszerszy obraz problemu, gdyż zazwyczaj problemy tkwią w różnych dziedzinach działania. Wypracowane zespołowo sugestie mają większą szansę na wprowadzenie w życie niż propozycje pojedynczych pracowników. Poniżej znajduje się schemat przedstawiający zależności przyczyn i skutków.



Rysunek 5.2. Przykład schematu przyczynowo-skutkowego

Źródło: opracowanie własne

W dyskusji nad sposobem rozwiązania problemu wykorzystywana jest umiejętność logicznego myślenia, wiedza dziedzinowa, doświadczenia ekspertów ze zdarzeń analogicznych oraz ich zdolność do przewidywania zdarzeń przyszłych. Metodą pozwalającą na to jest burza mózgów.

Skuteczność metody burzy mózgów w dużej mierze zależy od:

- sposobu jasnego przedstawienia problemu,
- utrzymania dyskusji w ryzach tematycznych oraz w wyznaczonych ramach godzinowych,
- poprowadzenia spotkania tak, aby nie została zdominowana przez jedną osobę.

Zaletami tej metody są:

- kreatywne poszukiwanie rozwiązań,
- szybki sposób gromadzenia informacji,
- możliwość wzajemnej inspiracji pomiędzy uczestnikami.

Burza mózgów daje także możliwość formułowania własnych sądów i opinii w sprawie przez uczestników spotkania oraz oceny zgłaszanych rozwiązań i ewentualnych ich modyfikacji.

PHA jest prostą metodą indukcyjną i półilościową, której celem jest wstępne rozpoznanie niebezpiecznych sytuacji i zdarzeń powodujących zagrożenie dla danej działalności, obiektu lub systemu.

Analizę PHA wykonuje się w pięciu podstawowych etapach, które obejmują:
- określenie celu oraz zakresu analizy,
- zgromadzenie informacji o projektowanej lub istniejącej instalacji,
- wybór ekspertów do zespołu wykonującego analizę,
- przeprowadzenie analizy,
- opracowanie wyników analizy.

Dla każdego z wytypowanych zagrożeń określa się możliwe prawdopodobieństwo (P) i skutki – wielkość szkody (S) oraz konstruuje tabelę ryzyka, w której podaje się oszacowane prawdopodobieństwo wystąpienia skutków, ich skalę i ryzyko.

Poziomy prawdopodobieństwa skalowane są następująco:
1 – bardzo prawdopodobne/bardzo częste,
2 – prawdopodobne/częste,
3 – średnio prawdopodobne/umiarkowanie,
4 – mało prawdopodobne/rzadkie,
5 – bardzo mało prawdopodobne/bardzo rzadkie.

Wielkość szkody natomiast na:
1 – bardzo duże/bardzo ciężkie szkody,
2 – duże/ciężkie szkody,
3 – średnie/umiarkowane szkody,
4 –małe/niewielkie szkody,
5 – bardzo małe/nieznaczne szkody.

Na podstawie wyników analizy są formułowane wytyczne do następnych faz projektowania, dotyczące redukcji poziomu zagrożenia lub eliminacji wykrytych źródeł tego zagrożenia. Dzięki zastosowaniu PHA zagrożenia mogą zostać zidentyfikowane we wczesnym procesie oceny ryzyka.

Technika HRA może być stosowana do analizy procesów, w których istotnym elementem jest działalność człowieka i gdzie niewłaściwe jego zachowanie może doprowadzić do sytuacji krytycznej. Określa wpływ człowieka na działalność systemu i mierzy poziom wpływu ludzkiego błędu na system. Technika może być stosowana jakościowo lub ilościowo. Jakościowo – do określenia potencjału ludzkiego błędu i oceny potencjalnych jego skutków. Ilościowo – w celu przygotowania danych do innych analiz, na przykład analizy drzewa błędów (*Fault Tree Analysis* – FTA).

Analiza przyczyn źródłowych jest techniką opartą na analizie przyczyn niekorzystnych zdarzeń lub pojawiających się problemów. Umożliwia zrozumienie ich źródeł oraz konsekwencji, jakie niosą one ze sobą dla procesów zachodzących w organizacji (lub całych systemów). Analiza odwołuje się do sekwencji następujących po sobie zdarzeń lub chronologii wydarzenia, tak by można było zrozumieć relacje zachodzące pomiędzy istotnymi czynnikami (elementami struktury czy procesami lub podprocesami). Metoda ta pozwala na zapobieganie niepożądanym incydentom przez przygotowanie działań naprawczych.

Metoda *analiza scenariuszowa* koncentruje się na tworzeniu możliwych scenariuszy przyszłych zdarzeń budowanych bądź na podstawie twardych danych ilościowych będących w posiadaniu organizacji, bądź bazując na wyobraźni analityków

lub zespołu analitycznego. Podobnie jak w przypadku analizy przyczyn źródłowych technika ta opiera się na wskazaniu sekwencji zdarzeń oraz zbadaniu, w jaki sposób zdarzenia te oddziałują na organizację.

Kwestionariusz identyfikacji ryzyka jest wstępnie uzgodnioną listą pytań, które umożliwiają identyfikację obszarów ryzyka. Powinien on być przesłany do jak największej liczby osób, które mogą pomóc nam w zidentyfikowaniu ryzyka dla określonego zadania. Wyliczenie poszczególnych ryzyk pozwala mieć pewność, że najbardziej interesujące nas ryzyka znajdują się na liście i będą wzięte pod uwagę. Wadą tego narzędzia jest to, iż kwestionariusz nie rozwija kreatywnego myślenia na temat ryzyk (dysponuje on tylko zamkniętym katalogiem, a rzeczywistość się zmienia). Ponadto istnieje obawa, że ryzyka zostaną źle zinterpretowane lub otrzymamy niską liczbę ankiet zwrotnych.

Tabela 5.3. Przykładowy kwestionariusz ryzyka

Czynniki	Obszary potencjalnego ryzyka	Występowanie ryzyka TAK/NIE	Opis ryzyka
polityczne	ważne decyzje polityczne		
organizacyjne	przygotowanie i planowanie		
ludzkie	posiadanie niezbędnej wiedzy/ umiejętności/doświadczenia dla realizacji zadania		
finansowe	płynność finansowa		

Źródło: opracowanie własne

Metoda schematu blokowego (*flowchart*) służy do prostej, graficznej prezentacji działania danego procesu oraz sposobu, w jaki elementy tego procesu są ze sobą powiązane. Każdy etap procesu jest przedstawiony za pomocą innego symbolu i zawiera krótki opis. Symbole są połączone razem ze strzałkami wskazującymi kierunek przepływu procesu. Korzyścią zastosowania schematu blokowego przy identyfikacji ryzyka jest to, że zespół zarządzania ryzykiem może zidentyfikować punkty potencjalnych problemów w diagramie przepływu. Narzędzie flowchartingu może pomóc przewidzieć, co, gdzie i jaki rodzaj problemu może wystąpić i może przyczynić się do ich rozwiązania.

Na rysunku 5.3. przedstawiono przykład prostego schematu blokowego dla zobrazowania przypadku zagrożenia trzęsieniem ziemi:

FEMA (*Failure Mode and Effect Analysis*) jest metodą analizy skutków i rodzajów możliwych błędów, która pozwala na zidentyfikowanie:

- możliwych trybów powstawania niepowodzeń w różnych częściach systemu,
- skutków błędów mogących powstać w systemie,
- mechanizmów powstawania niepowodzeń,
- metod unikania niepowodzeń i/lub sposoby łagodzenia ich skutków w systemie.

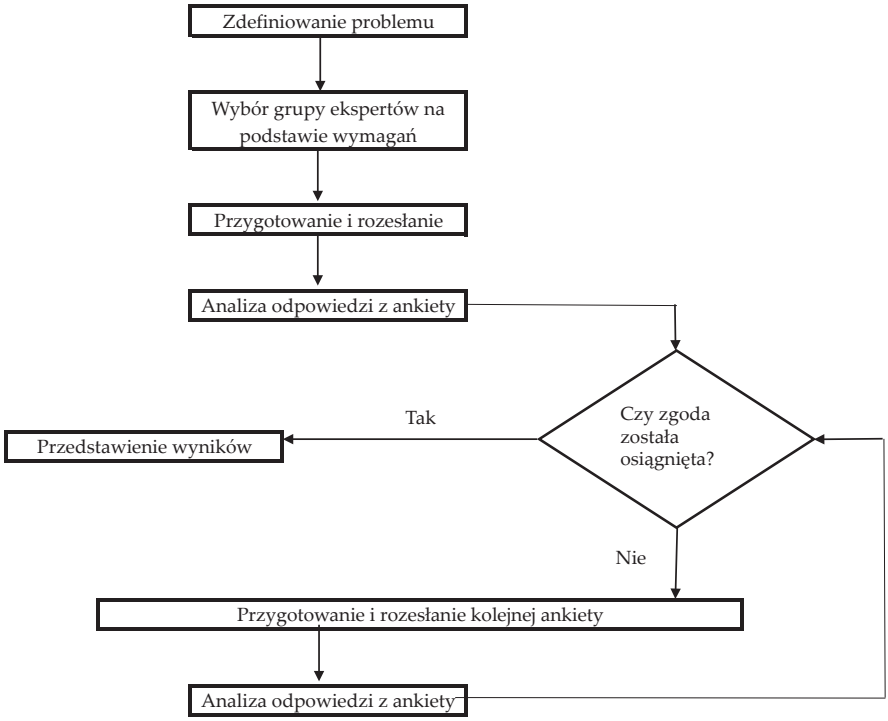
Rysunek 5.3. Schemat blokowy

Źródło: opracowanie własne

W normie ISO 31010:2009 (w czterostopniowej skali: dobrze, przeciętnie, słabo, wcale) opisane zostały zasoby i zdolności systemu, rodzaje i stopnie niepewności oraz stopnie skomplikowania procesu. Ponadto technika FMEA bardzo dobrze sprawdza się podczas identyfikacji ryzyka, analizy skutków i określania prawdopodobieństwa oraz oceny poziomu ryzyka.

HAZOP (*Hazard and Operability Study*) służy do analizy zagrożeń i zdolności operacyjnych. Metoda ta polega na podzieleniu rozpatrywanego procesu na oddzielne elementy i analizowania każdego z nich osobno. Ponadto prowadzony jest systematyczny przegląd założeń projektowych i procesu technologicznego pod kątem mogących się pojawić odchyleń parametrów. Wykorzystywana najczęściej do oceny ryzyka procesowego analiza zagrożeń i zdolności operacyjnych (HAZOP) jest strukturalną metodą identyfikacji potencjalnych zagrożeń występujących w procesach przemysłowych. W technice HAZOP wykorzystywany jest zestaw słów kluczowych i możliwych odchyleń w aspekcie możliwych zmian (oddziaływania) na przebieg procesu technologicznego.

Podstawę metody delfickiej stanowią opracowane w kwestionariuszu pytania. Metoda delficka jest szeroko stosowana do określenia prawdopodobieństwa zaistnienia zjawiska lub przyszłych zdarzeń. W przypadku zarządzania kryzysowego, na postawioną diagnozę można uzyskać odpowiedź przez przeprowadzenie serii opinii (ankiet) wśród ekspertów, wykorzystując do tego ich wiedzę oraz przez doświadczenie, lub też posługując się ich opiniami.



Rysunek 5.4. Metoda delficka

Źródło: A. Stabryła, Zarządzanie przedsiębiorstwem, Zeszyty Naukowe MWSE w Tarnowie 2011, nr 2(19)

Cechy metody delfickiej:

- niezależność i anonimowość opinii oraz ekspertów,
- eliminacja dominowania określonych osobowości,
- możliwość zdalnej komunikacji,
- statystyczne opracowanie wyników,
- wieloetapowość,
- uzgadnianie i sumowanie opinii kompetentnych osób.

Słabe strony metody delfickiej:

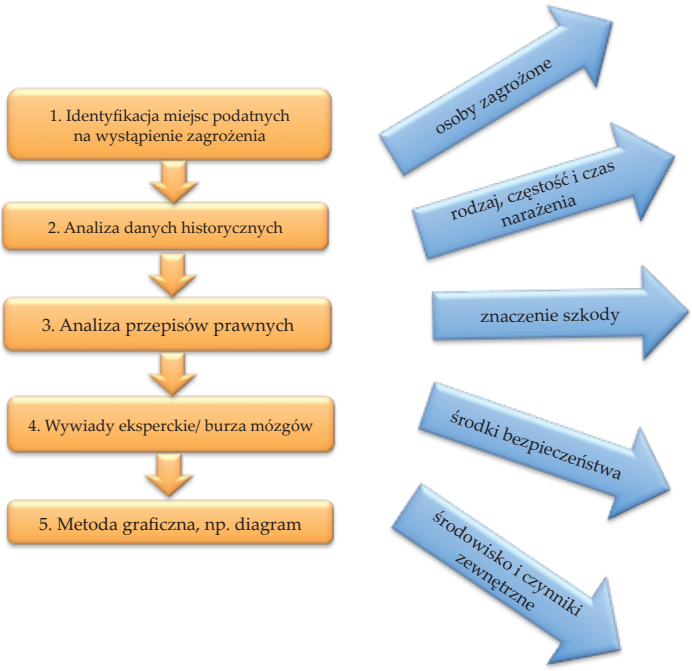
- czasochłonność,
- trudności w doborze grupy ekspertów,
- konieczność zaangażowania dużej liczby osób opracowujących ankiety i odpowiedzi,
- brak bezpośredniej wymiany poglądów,
- przydatna tylko do sporządzania prognoz długookresowych, co utrudnia ich weryfikację.

Identyfikacja ryzyka powinna określać, które zagrożenia mogą mieć wpływ na bezpieczeństwo oraz dokumentować cechy każdego z nich. Rozpoznanie powinno obejmować także ryzyko występowania czynników zarówno wewnętrznych, jak i zewnętrznych. Wybór metody identyfikacji ryzyka zależy od wielu uwarunkowań

(doświadczenia zespołu, dostępności do źródeł informacji o danym zagrożeniu) i nie należy ograniczać się do przeprowadzenia analizy zagrożeń za pomocą wyłącznie jednej z wybranych metod. Znane metody identyfikacji zagrożeń różnią się między sobą co do poziomu zaawansowania i przyjętego stopnia szczegółowości analiz – od technik opartych na prostej liście kontrolnej do szczegółowych diagramów logicznych[25]. Ogólnie rzecz biorąc, odpowiednie techniki powinny wykazywać następujące właściwości:

- powinny być uzasadnione i stosowne do sytuacji lub organizacji,
- efektem powinno być zwiększenie świadomości o danym ryzyku (zagrożeniu),
- metody powinny być powtarzalne i możliwe do zweryfikowania.

Poniżej przedstawiono przykładową propozycję działania w procesie identyfikacji ryzyka.



Rysunek 5.5. Uproszczony schemat identyfikacji zagrożeń

Źródło: opracowanie własne

Powody, dla których decydujemy się na wybór techniki, powinny się odnieść do ich przydatności. Wyniki z różnych badań i zastosowanych technik powinny być porównywalne. Podejmując próbę analizy metod identyfikacji ryzyka pod kątem możliwości ich wykorzystania w procesie oceny ryzyka, warto przypomnieć, iż składa się on z elementów:

[25] Identyfikacja źródeł zagrożenia: Poradnik metod ocen ryzyka związanego z niebezpiecznymi instalacjami procesowymi, WIOŚ, Warszawa 2008.

1) Identyfikacji ryzyka (proces wyszukiwania, rozpoznawania i opisywania ryzyka)[26].
2) Analizy ryzyka (proces złożony z identyfikacji ryzyka, opisu ryzyka oraz pomiaru ryzyka w odniesieniu do jego oddziaływania, jeśli ryzyko wystąpi oraz prawdopodobieństwa wystąpienia tego ryzyka)[27].
3) Ewaluacji ryzyka (proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane)[28].

Przed przystąpieniem do oceny ryzyka powinno się jasno określić:

- cele i zakres,
- potrzeby decydentów (w niektórych wypadkach wymaga się wysokiego poziomu szczegółowości, aby wynik był wiarygodny, w innych wystarczająca jest bardziej ogólna ocena),
- rodzaj i zakres analizowanych ryzyk,
- potencjalna wielkość skutków,
- umiejętności i doświadczenia zespołu prowadzącego ocenę ryzyka,
- dostępność informacji i danych,
- budżet, jeśli wymagane są zasoby zewnętrzne,
- wymogi prawne,
- aktualną sytuację,
- ograniczenia dotyczące czasu.

Część z zaprezentowanych metod można zastosować podczas procesu oceny ryzyka. Możliwe jest także ich łączenie w zależności od badanego obszaru lub etapu. Wykorzystując na przykład metodę burzy mózgów, za pomocą której członkowie zespołu analizują obiekt, proces lub stanowisko, odpowiadając na pytania i wzajemnie dyskutując, zwiększa się szansa na wytypowanie zagrożeń, które nie były wcześniej brane pod uwagę. W połączeniu z metodą wstępnej analizy zagrożeń, która umożliwia zestawienie zagrożeń, które są już znane oraz dodatkowo wykorzystując technikę diagramu przyczynowo-skutkowego, który graficznie przedstawia działanie całego obiektu, procesu i jego otoczenia, możliwe będzie przeprowadzenie oceny ryzyka.

Narzędziem, które można wykorzystać podczas obu etapów, jest także technika HRA charakteryzująca zasoby i zdolności systemu, rodzaj i stopień niepewności oraz stopień skomplikowania procesu, możliwe jest jednak przy zastosowaniu tej techniki otrzymanie ilościowego wyniku. Jednocześnie treść normy ISO 31010:2009 wskazuje, że technika ta jest odpowiednia do identyfikacji ryzyka, analizy skutków, określenia prawdopodobieństwa i poziomu ryzyka, a także do oceny ryzyka.

Analiza z zastosowaniem list kontrolnych, czyli zestawów pytań, które dotyczą istotnych ze względu na bezpieczeństwo właściwości układu człowiek–obiekt techniczny–środowisko, mogą być opracowywane na podstawie wymagań obowiązu-

[26] PN-ISO 31000:2012, *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN Warszawa 2012; s. 21.

[27] Załącznik do zarządzenia nr 92/2011 Wojewody Łódzkiego z dnia 29 marca 2011 r. w sprawie zarządzania ryzykiem w Łódzkim Urzędzie Wojewódzkim w Łodzi.

[28] PN-ISO 31000:2012, *Zarządzanie ryzykiem – Zasady i wytyczne,* PKN Warszawa 2012, s. 25.

jących przepisów lub dokumentów planistycznych, a zidentyfikowane problemy charakterystyczne dla danego obiektu/procesu mogą zostać wykorzystane w procesie oceny ryzyka.

Kolejną metodą jest HAZOP – systematyczna analiza możliwych odchyleń od zamierzonego przebiegu procesu (każde z tych odchyleń może być zagrożeniem dla bezpieczeństwa, jakości produktu, czy środowiska) oraz metoda FMEA – wykorzystywana do analizy ryzyka związanego z obiektami technicznymi, w której analizowany obiekt dzieli się na elementy i każdy z nich jest analizowany oddzielnie.

Inne metody, które mogą zostać zastosowane zarówno na etapie identyfikacji ryzyka, jak i w całym procesie oceny ryzyka. Zgodnie z normą ISO 31010:2009, to:

- szacowanie eksperckie,
- modelowanie matematyczne,
- analiza danych z systemów monitorowania zagrożeń,
- badanie przypadków,
- diagram sekwencji działań (przyczynowo-skutkowy),
- analiza przyczyn i skutków (PHA),
- burza mózgów,
- *flowchart*,
- metody scenariuszowe,
- metoda delficka.

5.2. Szacowanie ryzyka

Jedną z często stosowanych metod oceny ryzyka jest metoda Monte Carlo. Nazwa metody miała wskazywać na losowy (przypadkowy, hazardowy) charakter zjawisk. Sama nazwa metody – Monte Carlo – została ukuta przez N. Metropolisa i nawiązuje oczywiście do stolicy gier hazardowych – Monako. Często podkreśla się tu również związek *ducha* metody z zainteresowaniem S. Ulama gra w pokera i stawianiem pasjansa [29].

Historia metody Monte Carlo sięga XVIII wieku, kiedy to francuski matematyk Georges-Louis Leclerc próbował zastosować próbkowanie losowe do obliczania całki przez rzucanie igły na poziomą płaszczyznę pokrytą równoległymi liniami prostymi. W XX wieku z rachunków na liczbach losowych korzystali m.in. Enrico Fermi przy eksperymentach dotyczących dyfuzji i transportu neutronów w reaktorach jądrowych oraz polski matematyk Stanisław Ulam wraz z Richardem Feynmanem i Nicholasem Metropolisem podczas prac nad projektem bomby jądrowej *Manhattan*.

Pojawienie się szybkich komputerów przeliczających olbrzymie ilości danych w bardzo krótkim czasie przyczyniło się do zwiększenia zainteresowania tą metodą. Dziś wachlarz jej zastosowań jest bardzo szeroki. Zaczynając od socjologii, poprzez nauki przyrodnicze i techniczne, a kończąc na ekonomii i finansach. Największe

[29] *The beginning of the Monte Carlo Method*, Metropolis. N, Los Alamos Science, Numer 15, 1987, s. 126-127.

sukcesy odnosi jednak w działach matematyki numerycznej[30]. Służy do matematycznego modelowania procesów zbyt złożonych (obliczenia całek, łańcuchów procesów statystycznych), aby można było przewidzieć ich wyniki za pomocą podejścia analitycznego[31]. Istotą w metodzie Monte Carlo jest losowanie przypadkowe wielkości charakteryzujących proces, dotyczy to rozkładów procesów prostych lub złożonych. Składa się ona z następujących głównych części: sformułowanie modeli stochastycznych badanych procesów realnych, modelowania zmiennych losowych o danym rozkładzie prawdopodobieństwa, rozwiązywania problemu statystycznego z zakresu teorii estymacji[32].

Monte Carlo zaliczane jest do metod statystycznych, ponieważ wielkości wyznaczane są w postaci wartości oczekiwanych pewnych rozkładów prawdopodobieństwa. W celu zobrazowania metody został wykorzystany arkusz kalkulacyjny przygotowany przez Krzysztofa Czobę[33], wykorzystujący normalny rozkład prawdopodobieństwa.

Pierwszy arkusz zawiera tabelę zwaną macierzą kwantyfikacji ryzyk. Zawiera ona dwanaście ryzyk oraz cztery szanse, na jakie narażeni mogą być obywatele w założonym scenariuszu. Scenariuszem może być np: powódź, pożar, karambol czy groźny wypadek samochodowy. Każdemu zagrożeniu z danego scenariusza przypisane jest prawdopodobieństwo wystąpienia zagrożenia, ewentualny skutek jego wystąpienia, oraz poziom zagrożenia, czyli iloczyn prawdopodobieństwa i skutku. Wszystkie uporządkowane wartości przedstawia poniższa tabela.

Tabela 5.4. Macierz kwalifikacji ryzyka i szans

RBS	Opis ryzyka	Prawdop.	Skutek (Koszt)	Poziom	LOS()	SKUTEK
Z-1	Zagrożenie nr 1	0,10	200	**20**	0,595213	
Z-2	Zagrożenie nr 2	0,05	300	**15**	0,707888	
Z-3	Zagrożenie nr 3	0,10	50	**5**	0,425584	
Z-4	Zagrożenie nr 4	0,50	10	**5**	0,157022	**10**
Z-5	Zagrożenie nr 5	0,20	20	**4**	0,215453	
Z-6	Zagrożenie nr 6	0,30	100	**30**	0,268335	**100**
Z-7	Zagrożenie nr 7	0,08	600	**48**	0,821064	
Z-8	Zagrożenie nr 8	0,50	25	**12,5**	0,351598	**25**
Z-9	Zagrożenie nr 9	0,60	5	**3**	0,968542	
Z-10	Zagrożenie nr 10	0,37	42	**15,54**	0,46431	
Z-11	Zagrożenie nr 11	0,70	45	**31,5**	0,211827	**45**
Z-12	Zagrożenie nr 12	0,80	80	**64**	0,912578	

[30] K. Ziętek-Kwaśniewska, *Symulacje Monte Carlo jako metoda wyceny opcji.*
[31] A. Chyliński, *Metoda Monte Carlo w bankowości,* s. 148.
[32] Tamże, s. 149.
[33] Arkusz można pobrać ze strony: http://dotproject.net.pl/node/227.

RBS	Opis ryzyka	Prawdop.	Skutek (Koszt)	Poziom	LOS()	SKUTEK
S-1	Szansa nr 1	0,05	-50	**-2,5**	0,849958	
S-2	Szansa nr 2	0,10	-150	**-15**	0,239693	
S-3	Szansa nr 3	0,30	-15	**-4,5**	0,048584	**-15**
S-4	Szansa nr 4	0,66	-5	**-3,3**	0,91442	

Gdzie :
RBS – oznacza kod ryzyka (*Risk Breakdown Structure*);
Opis ryzyka – hasłowy opis ryzyka;
Prawdop. – prawdopodobieństwo wystąpienia, np. 0,10 oznacza 10%,
Skutek (koszt) – wpływ ryzyka, skutek, jeśli ryzyko się ziści, ujemne, gdy konsekwencje są pozytywne
Poziom = prawdop. * skutek - oczekiwana wartość ryzyka
Źródo: opracowanie własne

Kolejne dwie kolumny zostały wprowadzone, aby można było zastosować metodę Monte Carlo. Pierwsza z nich LOS() generuje dowolną liczbę losową z przedziału od 0 do 0,99. Nowe liczby generowane są przy wprowadzaniu jakiejkolwiek zmiany w arkuszu lub przy odświeżaniu (F9). Każdorazowe odświeżenie utożsamiane jest z wprowadzeniem nowego scenariusza dla wymienionych zagrożeń.

Natomiast ostatnia kolumna *SKUTEK* jest zapełniana, gdy spełniony będzie warunek prawdopodobieństwa dla danego zagrożenia. Pola tej kolumny korzystają z funkcji JEŻELI, która sprawdza, czy wartość z poprzedniej kolumny jest mniejsza od prawdopodobieństwa ryzyka, jeśli tak, to przepisuję kwotę z pola Skutek (Koszt).

Generując nowe scenariusze (F9), można zauważyć, że prawdopodobieństwo przepisania kwoty z kolumny *Skutek (Koszt)* do *SKUTEK* jest takie, jak wartość prawdopodobieństwa dla ryzyka podana w kolumnie *Prawdopodobieństwo*. Wynika to z faktu liniowego rozkładu gęstości prawdopodobieństwa funkcji LOS().

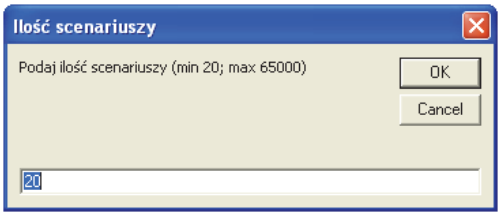
W powyższej tabeli widać, że scenariusz obejmuje Zagrożenie nr 4, Zagrożenie nr 6, Zagrożenie nr 8, Zagrożenie nr 11 oraz Szansę nr 3 (wartość *LOS()* jest mniejsza niż wartość *Prawdopodobieństwo*). Wartość oczekiwana ryzyka wynosi 228,24 i jest sumą Poziomu wszystkich ryzyk w projekcie. W powyższym przykładzie wynosi więc 228,24 PLN. Jest to najprostszy sposób wyliczenia budżetu rezerwowego dla zakładanego scenariusza, czyli kwoty, którą należy wydać, aby zabezpieczyć się przed zagrożeniami.

Oczywiście przy wystąpieniu wszystkich zagrożeń budżet rezerwowy będzie niewystarczający. Jedyną pewną metodą zabezpieczenia budżetu byłoby zgromadzenie kwoty równej sumie poziomu wszystkich ryzyk w projekcie, ale w takim wypadku bufor finansowy znacznie przekroczyłby wysokość budżetu całego scenariusza.

Na podstawie pojedynczego scenariusza nie da się określić budżetu rezerwowego. Inaczej jest w przypadku, gdy scenariuszy jest o wiele więcej. Za pomocą Makr w programie Excel można wygenerować 100, 1000, 20000 lub 50000 scenariusz, a następnie zapisać ich wyniki, a także przedstawić w postaci wykresu sku-

mulowanego prawdopodobieństwa – dystrybuanty. Im większa jest liczba scenariuszy, tym dokładniejsze jest uśrednienie wszystkich kwot[34].

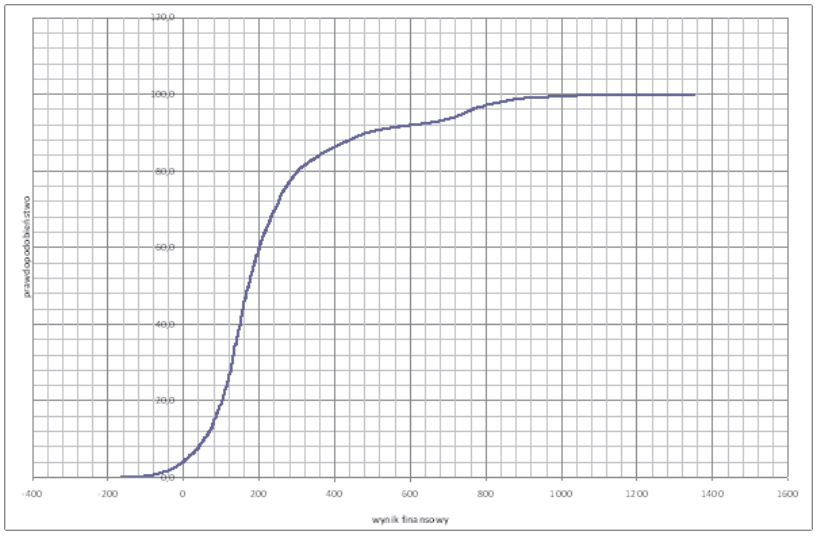
Program po wciśnięciu przycisku *Licz* wyświetli formatkę, do której należy wpisać, ile scenariuszy zostanie policzonych w poleceniu Makro. Wyniki obliczeń zostaną wyświetlone w kolejnym arkuszu.



Rysunek 5.6. Liczba scenariuszy, jaką należy wpisać w formatce
Źródło: dotproject.net.pl/node/227

Kolejny arkusz *Wyniki* przedstawia koszty, jakie należy ponieść, aby zagwarantować bezpieczeństwo scenariusza na danym poziomie (procentowym) prawdopodobieństwa. Dla różnej liczby wygenerowanych scenariuszy przypisywana jest inna kwota dla każdego poziomu prawdopodobieństwa.

Trzeci arkusz zatytułowany *Wykres* przedstawia skumulowany wykres prawdopodobieństwa, czyli dystrybuantę. Jest to graficzne przedstawienie wyników z arkusza *Wyniki*.



Rysunek 5.7. Wykres dystrybuanty dla 32 000 scenariuszy dla prawdopodobieństw z tabeli
Źródło: dotproject.net.pl/node/227

[34] Raport ze szkolenia BSI z 11–15 listopada 2013 r.

Wyniki powyższego wykresu można interpretować w następujący sposób:

- Na wykresie na osi x znajdują się koszty ryzyka dla poszczególnych scenariuszy. Oś y to liczebność populacji scenariuszy, liczona w procencie (udziale) wszystkich możliwych sytuacji. Dla najkorzystniejszego scenariusza koszt ryzyka będzie ujemny i wyniku szansy przy uda się zarobić 180 PLN, a w najmniej korzystnym wariancie straty wyniosą 1360 PLN.
- Przy gwarancji nieprzekroczenia na poziomie 25% trzeba założyć kwotę na ryzyko w wysokości 120 PLN. Gdy gwarancja wzrośnie do 75%, kwota na ryzyko wzrośnie do 280 PLN. Dla 95% koszt będzie wynosić aż 800 PLN.
- W 5% koszty wydane na ryzyko nie przekroczą 0 PLN. Jest to spowodowane tym, że oprócz zagrożeń występuje Szansa.

Otrzymany w drodze symulacji wynik jest jedynie wynikiem przybliżonym. Jednakże w wielu sytuacjach, gdy zastosowanie podejścia analitycznego jest niemożliwe, bądź mogłoby się okazać zbyt czasochłonne, metody Monte Carlo są nieocenione[35].

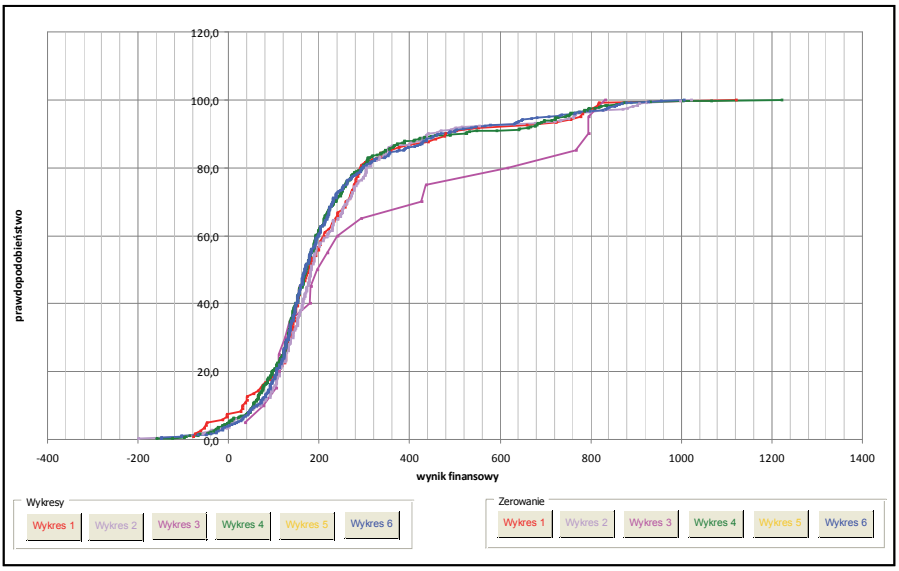
Ostatni arkusz *Porównanie wyników* daje użytkownikowi możliwość porównania kosztów oraz gwarancji nieprzekroczenia budżetu w pięciu różnych wariantach. Wariantem może być różna ilość zagrożeń i szans, różna liczba scenariuszy lub też różne wartości prawdopodobieństwa oraz skutków. Do zapamiętania aktualnie wygenerowanego scenariusza wykresu służy prawe menu z numerami wykresów od 1 do 6. Aby do istniejącego już wykresu dodać nowy wariant scenariusza, należy stworzyć w *arkuszu 1* nową macierz kwantyfikacji ryzyk. Może ona zostać wypełniona według dowolnie wybranych kryteriów. Po naciśnięciu przycisku *Licz* i wygenerowaniu przez program nowych wyników, można dodać nowy wykres w zakładce *Porównanie wyników*. Należy jednak uważać, aby nie nadpisać nowego wykresu na poprzednim. Aby uniknąć ewentualnej pomyłki, każdy wariant scenariusza oraz przyciski do tworzenia wykresów zostały zaznaczone innym kolorem. Jednorazowo program pozwala na porównanie pięciu różnych wariantów jednocześnie. Jeżeli porównywanych jest pięć wariantów, a istnieje potrzeba dodania kolejnego wariantu, należy usunąć najgorszy z istniejących wariantów, po czym dodać nowy. Do tego celu służą przyciski po prawej stronie wykresu. One również zaznaczone są tym samym kolorem co narysowany wykres, aby uniknąć skasowania niezamierzonego wykresu. Powyższy opis zilustrowany jest na rysunku 5.8. przedstawiającym wykres z arkusza kalkulacyjnego.

Wykorzystując metodę Monte Carlo, można tworzyć i porównywać różne warianty scenariuszy zagrożeń. Dzięki temu możliwe jest:

- skalkulowanie wpływu ryzyka na bezpieczeństwo powszechne w danym scenariuszu zagrożenia,
- utworzenie budżetu rezerwowego związanego z wydatkami powstałymi wskutek wystąpienia zagrożeń,

[35] K. Ziętek-Kwaśniewska, *Symulacje Monte Carlo jako metoda wyceny opcji*, Lublin 2006.

- przybliżenie buforu budżetu potrzebnego do zagwarantowania na ustalonym poziomie (wyrażonym w %) niewystąpienia danego zagrożenia.



Rysunek 5.8. Wykres umożliwiający porównanie pięciu różnych wariantów scenariuszy
Źródło: dotproject.net.pl/node/227

5.3. Akceptowalność

Ostatnim etapem szacowania ryzyka jest prezentacja ryzyk na matrycy. Wskazuje się na możliwość ich hierarchizacji w formie listy ryzyk od najistotniejszych (o najwyższych wartościach) do najmniej istotnych (o najniższych wartościach). Dokonuje się tego zgodnie z wartościami określonymi w matrycy ryzyka, a następnie wyznacza sposoby postępowania z ryzykiem.

Etap ten łączy się również z koniecznością określenia poziomu akceptowalności zidentyfikowanego ryzyka. W literaturze przedmiotu przyjmuje się, że ryzyko akceptowalne (apetyt na ryzyko) jest poziomem ryzyka uznanym za bezpieczny do realizacji celu lub zadania[36]. W innym ujęciu za akceptowalny poziom ryzyka uznaje się poziom istotności, przy którym nie wymaga się podjęcia dodatkowych działań przeciwdziałających ryzyku, a jedynie monitorowanie ryzyk w ramach istniejących mechanizmów kontrolnych[37]. Z kolei w normie PKN-ISO Guide 73:2012 akceptację ryzyka definiuje się jako świadomą decyzję o podjęciu danego ryzyka. Oprócz wskazania, że zaakceptowane ryzyka podle-

[36] Zasady zarządzania ryzykiem w Politechnice Warszawskiej, Załącznik do Zarządzenia nr 5/2012 Rektora PW z dnia 13 stycznia 2012 r.

[37] Polityka zarządzania ryzykiem w Ministerstwie Infrastruktury. Warszawa, październik 2011 r.

gają monitorowaniu oraz przeglądowi przyjmuje się, że sama akceptacja ryzyka może wystąpić bez postępowania z ryzykiem lub w trakcie postępowania z ryzykiem[38].

Kategoria *akceptacji ryzyka* definiowana w dokumentach planistycznych systemu zarządzania kryzysowego odnosi się do konieczności określenia poziomu ryzyka akceptowalnego dla scenariusza w ramach określonego obszaru zadaniowego (kompetencyjnego) realizowanego przez właściwego ministra kierującego działami administracji rządowej, kierownika urzędu centralnego lub wojewody[39]. Na potrzeby jego wyznaczenia wprowadzono cztery kategorie kryteriów akceptacji ryzyka, tj. ryzyko akceptowane, ryzyko tolerowane, ryzyko warunkowo tolerowane oraz nieakceptowane. Istotą wyboru poszczególnych kategorii jest określenie, czy wymagane są dodatkowe środki bezpieczeństwa, czy akceptowane są aktualne rozwiązania i przypisane im siły i środki, wskazanie, czy konieczne wydaje się wprowadzenie zmian organizacyjnych, prawnych i funkcjonalnych, jak również podjęcie ewentualnej decyzji o ulepszeniu stosowanych rozwiązań. Dodatkowo wymaga się od osób zarządzających bezpieczeństwem w ramach określonego obszaru zadaniowego/kompetencyjnego, uzasadnienia akceptacji, co stanowić ma ich subiektywną ocenę.

Przyjęte w ramach procedury rozwiązanie odnosi się do sfery administracji, w tym ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów. W tym względzie nie rozważa się, czy dane ryzyko jest akceptowalne przez społeczeństwo. Ponadto w tym ujęciu akceptowalności nie rozpatruje się pod kątem kosztów działań obniżających to ryzyko.

Obecnie nie istnieje jedna, uniwersalna metoda możliwa do wykorzystania na potrzeby określenia poziomu akceptowalności zidentyfikowanego ryzyka. Niemniej jednak analiza literatury przedmiotu oraz normy IEC/FDIS 31010 *Risk management – Risk assessment techniques* wykazała, że w tym celu można wykorzystać szereg metod i technik wspierających proces analizy ryzyka[40]. Rozważania te prowadzą do konstatacji, że metoda określenia poziomu akceptowalności zidentyfikowanego ryzyka może być oparta na modelach scenariuszowych oraz analizy przypadku.

Metody scenariuszowe stanowią jedno z narzędzi planowania strategicznego. Ich istotą jest opis zjawisk oraz wskazanie ich logicznego oraz spójnego następstwa, a w konsekwencji ustalenie, w jaki sposób będą się one rozwijały w przyszłości. W literaturze przedmiotu przyjmuje się ich podział na grupy scenariuszy możliwych zdarzeń, scenariusze symulacyjne, scenariusze stanów otoczenia oraz scenariusze procesów w otoczeniu[41].

Scenariusze analizuje się pod kątem różnych rodzajów ryzyk mogących wystąpić w ramach każdego z nich. W metodach tych za punkt wyjścia przyjmuje się

---

38 PKN-ISO Guide 73, *Zarządzanie ryzykiem – Terminologia*, marzec 2012.

39 Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Warszawa 2010, s. 17.

40 IEC/FDIS 31010 *Risk management – Risk assessment techniques.*

41 M. Lisiński, Metody planowania strategicznego, Wyd. Polskie Wydawnictwo Ekonomiczne, Warszawa 2004, s. 105.

stan interesującego nas zjawiska, w ramach którego konstruuje się przyszły, alternatywny ciąg zdarzeń. W tym kontekście scenariusze są więc układem zdarzeń, które są ze sobą powiązane w logiczną sekwencję (zazwyczaj w porządku chronologicznym). Ponadto wskazuje się, że powinny one być one istotne dla zjawiska, dla którego opracowuje się scenariusz, umiejscowione w określonym czasie, jak również powiązane ze sobą za pomocą różnego rodzaju relacji (w tym m.in. formalnoprawnych, przyczynowo-skutkowych czy też czasowego następstwa). Rozwijając scenariusze, rozważa się zarówno *najlepszy przypadek*, *najgorszy przypadek*, jak również *spodziewany przypadek*[42].

Wśród metod scenariuszowych możliwych do wykorzystania w przedmiotowym zakresie, za szczególnie przydatną uznać można analizę scenariuszy możliwych zdarzeń. Zaletą metody jest możliwość rozpatrywania różnych wariantów incydentów, biorąc pod uwagę takie czynniki, jak: przyczyny wystąpienia zdarzenia, jego intensywność, czas trwania, rozwój, czy też rozmiar konsekwencji dla osób poszkodowanych. o jej przydatności na potrzeby określenia akceptowalności zidentyfikowanego ryzyka decyduje fakt, że dzięki posiadaniu szczegółowych informacji m.in. na temat skali skutków danego zdarzenia oraz wiedzy na temat posiadanych środków bezpieczeństwa oraz dostępnych sił i środków, możliwe jest podjęcie decyzji o akceptacji bądź braku akceptacji ryzyka, a w konsekwencji o wyborze odpowiedniej opcji postępowania z ryzykiem. Należy jednak pamiętać, iż ograniczeniem metody jest fakt, że opracowane scenariusze mogą okazać się nierealne, bądź mogą nie uwzględniać zdarzeń, które faktycznie wystąpią w przyszłości.

Metoda scenariuszy możliwych zdarzeń może posłużyć jako punkt wyjścia do analizy mającej na celu określenie poziomu akceptowalności zidentyfikowanego ryzyka. Wydaje się, że w uzupełnieniu do niej można by wykorzystać szereg technik i metod ujętych w normie IEC/FDIS 31010[43].

Metody te to:

- analiza SWOT,
- ETA,
- FTA,
- Bow-tie,
- *Co jeśli?*,
- BIA,
- Analizy kosztów/korzyści,
- *Case study* (analiza przypadku).

Analiza SWOT pozwala na zdefiniowanie słabych i mocnych stron organizacji, biorąc pod uwagę m.in. posiadane zasoby. Dzięki temu możliwe jest określenie, z jakiego rodzaju ryzykiem będzie ona mogła sobie poradzić lub nie, w przypadku *zrealizowania się* danego scenariusza możliwych zdarzeń, warunkując tym samym podjęcie decyzji o tym, czy dane ryzyko może zaakceptować czy nie oraz czy po-

[42] Tamże.
[43] IEC/FDIS 31010 *Risk management – Risk assessment techniques*.

winna podjąć działania mające na celu zapobieżenie mu lub jego redukcję (przyczyn lub skutków).

Metoda ETA jest przydatna przy *rozwijaniu* scenariuszy możliwych zdarzeń obejmujących *efekt domina*. ETA pozwala bowiem na wskazanie, czy zabezpieczenie dedykowane reakcji na wystąpienie kolejnego zdarzenia rozgałęziającego zadziałało lub nie. Dzięki jej zastosowaniu możliwe byłoby precyzyjne określenie łącznej skali i rozmiaru skutków danego zdarzenia, w tym poniesionych strat. Natomiast FTA podobnie jak analiza drzewa zdarzeń pozwala rozpatrzeć scenariusze o dużym stopniu skomplikowania, ale podążając w stronę przyczyn (błędów) odnoszących się do zdarzenia początkowego. Dzięki jej wykorzystaniu możliwe byłoby wskazanie, czy ich uniknięcie (biorąc pod uwagę koszty podjętych działań zapobiegawczych) jest bardziej korzystne, niż powstrzymanie się od jakichkolwiek działań i podjęcie decyzji o akceptacji zidentyfikowanego ryzyka.

Metoda Bow-tie stanowi połączenie dwóch powyżej wskazanych metod, stąd też podobnie jak one mogłaby zostać wykorzystana w omawianym zakresie. Kładzie ona nacisk na określenie *barier*, tj. istniejących środków kontrolnych w kontekście działań mających na celu niedopuszczenie do zainicjowania się danego ryzyka oraz *barier*, które nie pozwolą na eskalację zdarzenia do najgorszych możliwych skutków. Innymi słowy, byłaby pomocna przy wskazaniu, czy posiadane środki bezpieczeństwa, zabezpieczenia byłyby wystarczające w obliczu wystąpienia danego scenariusza zdarzeń, jak również przy określeniu kosztów oraz korzyści z działań związanych z zapobieganiem lub redukcją ryzyka do poziomu uznanego za akceptowalny.

Metoda *Co jeśli?* jest oparta na zbudowanym katalogu pytań, które w trakcie badania są zadawane ekspertom. Pytania powinny być wcześniej ustalone i zadawane w określonej kolejności członkom zespołu specjalistów. Pytania te mogą być zarówno pytaniami otwartymi, jak i zamkniętymi. Głównym założeniem jest odpowiedź na pytanie: *Co mogłoby się stać?* W ramach rozpatrywania *najgorszych możliwych scenariuszy*. Chodzi o sytuację, w której np. rozmiar skutków danego zdarzenia w zderzeniu z brakiem lub niewystarczającą ilością zasobów/brakiem zabezpieczeń może doprowadzić do przekroczenia poziomu ryzyka akceptowalnego.

Metoda BIA kładzie nacisk na ustalenie i ocenę kluczowych procesów danej organizacji oraz wskazanie finansowych i niefinansowych strat w przypadku ich przerwania lub zakłócenia, a zatem pozwala na wskazanie, jak długo organizacja może bez nich funkcjonować. Mogłaby być więc przydatna w odniesieniu do określenia poziomu akceptowalności ryzyk, które można postrzegać w ujęciu procesowym, tj. odnoszących się do systemów zaopatrywania w wodę, prąd, energię cieplną.

Istotnym elementem w ramach określenia poziomu akceptowalności zidentyfikowanego ryzyka wydaje się też wyliczenie kosztów i korzyści z działań mających na celu zapobieganie lub redukcję zidentyfikowanego ryzyka. Przydatną metodą do ich określenia byłaby metoda analizy kosztów i korzyści.

Jest to metoda oceny efektywności inwestycji i projektów, przy uwzględnieniu kosztów zewnętrznych (np. środowiskowych, społecznych). Zarówno dla korzyści, jak i strat przyporządkowuje się ich wartość finansową, biorąc pod uwagę zmiany w czasie (wartość bieżąca w netto)[44]. Metoda ta znajduje swoje zastosowanie w kontekście podjęcia decyzji co do postępowania z zidentyfikowanym ryzykiem, dokonania rozróżnienia pomiędzy jego formami oraz wyboru najlepszej opcji postępowania z ryzykiem.

W kontekście określenia akceptowalności zidentyfikowanego ryzyka byłaby użyteczna pod kątem wyliczenia kosztów/korzyści z podjęcia działań ukierunkowanych na zapobieganie (w stosunku do przyczyn wystąpienia zdarzenia) oraz redukcję ryzyka (w odniesieniu do skutków zdarzenia) w stosunku do możliwości jego akceptacji, biorąc pod uwagę aspekt finansowy. Za przykład można podać dyskusję na temat wprowadzenia w Polsce systemu ubezpieczeń obowiązkowych od skutków powodzi[45].

Pojęcie *case study* funkcjonuje w literaturze przedmiotu jako analiza przypadku. Badacze tej problematyki zwracają uwagę na konieczność rozróżnienia terminów przypadku (*case*), analizy przypadku (*case study*) oraz metody analizy przypadku (*case study method*). Pierwsze z wymienionych pojęć oznacza zjawisko badane lub analizowane, niezależnie od dyscypliny naukowej, w ramach której jest ono rozpatrywane. Z kolei analiza przypadku stanowi analizę zjawiska, opis zjawiska lub analizę opisu. Ostatni z terminów, tj. metodę analizy przypadku definiuje się jako metodę służącą do konstrukcji sposobu analizowania przypadku. Polega ona przede wszystkim na analizowaniu i omawianiu prawdziwych sytuacji[46].

Wyróżnia się następujące rodzaje case'ów: epizody bez zakończenia, eseje, cases oparte o dokumenty, pamiętniki, kroniki, zeznania świadków, dokumentacja sądowa, opisy oraz winietki. Wskazane typy przypadków mogą mieć charakter eksploracyjny (*case study*, badanie terenowe oraz zbieranie danych poprzedzone są zdefiniowaniem pytań i hipotez badawczych), opisowy (pokrywają cały zakres przypadku poddanego analizie, w tym wypadku badacz rozpoczyna swoją pracę od zaprezentowania teorii lub wskazania, że rozważony zostanie interesujący go problem) oraz wyjaśniający (stosuje się do analiz przyczynowo-skutkowych). Każdy z nich może funkcjonować w postaci pojedynczej (*single-case*) lub wielokrotnej (*multiple-case*)[47].

Wskazuje się, że pierwsze z nich znajdują zastosowanie w sytuacji, gdy dany przypadek jest krytyczny (z punktu widzenia teorii), ekstremalny, typowy lub też

---

[44] Witryna internetowa http://www.governica.com/Analiza_koszt%C3%B3w_i_korzy%C5%9Bci, z dnia 30.09.2014 r.

[45] A. Łasut, *Koszty i korzyści z wprowadzenia w Polsce systemu ubezpieczeń obowiązkowych od skutków powodzi*, Kraków 2006.

[46] Ż. Ptak-Kostecka, *Analiza przypadku, czyli metoda case study,* Rozdział 4 pracy doktorskiej pt. *Efektywność pełnienia ról menedżerskich* (2000).

[47] Tamże.

odkrywczy, jak również gdy zjawisko ma charakter długotrwały. Używane są również wtedy, gdy ich celem jest falsyfikacja teorii. W takiej sytuacji bierze się pod uwagę przypadek ekstremalny, tj. tzw. czarnego łabędzia. Mogą być również wykorzystane jako badanie pilotażowe, którego przeznaczeniem jest stworzenie *wstępnej teorii* (zakładając, że teoria na ten temat nie istnieje)[48].

Wielokrotne studium przypadku z kolei koncentruje się wokół doboru odmiennych lub podobnych przypadków (wtedy celem jest porównanie ich między sobą). Przyjmuje się, że ich liczba powinna oscylować w granicach od 4 do 10 przypadków. Analizę za pomocą studiów wielokrotnych przypadków uważa się za rzetelniejszą, niż w przypadku s*ingle-case*[49].

Przygotowanie case'ów składa się z trzech etapów (tj. określenia celów przypadku), odpowiedniego doboru materiałów (wraz ze wskazaniem stopnia skomplikowania materiałów pod względem zawartych w nim informacji, zawartości oraz języka) oraz przygotowania się do omawiania case'u. Ostatni z etapów obejmuje przygotowanie serii pytań dotyczących wyjaśnienia opisanych zdarzeń czy też konsekwencji zjawisk zaprezentowanych w analizowanym przypadku. Pomimo faktu, że nie istnieją sztywne reguły analizowania case'ów, wśród kroków służących do jego omawiania wskazuje się kolejno na: dokładne przeczytanie tekstu i refleksję, ocenę informacji, zdefiniowanie problemu, proces generowania tematycznych rozwiązań, poszukiwanie skutków decyzji (zanim dokonana zostanie ocena alternatyw rozwiązań), ocenę alternatyw rozwiązań oraz sporządzenie listy rozwiązań wraz ze wszystkimi argumentami *za* oraz *przeciw* tym rozwiązaniom[50].

Metody analizy przypadku mogą się okazać przydatne na potrzeby określenia akceptowalności zidentyfikowanego ryzyka w oparciu o analizę niepożądanych zdarzeń z przeszłości. Analiza danych historycznych stanowi jedno z głównych źródeł informacji niezbędnych do identyfikacji zagrożeń. Skupienie uwagi na doświadczeniach związanych z wystąpieniem zdarzeń niepożądanych w przeszłości, w tym ich przyczyn, skutków, posiadanych na ten czas zasobów – wystarczających lub nie do przeciwdziałania tym zdarzeniom, może pozwolić na przeprowadzenie wnikliwej analizy dostępnych sił i środków oraz skuteczności działań podejmowanych z ich udziałem. Może również uwidocznić potrzebę wprowadzenia dodatkowych zabezpieczeń i środków bezpieczeństwa oraz przeprowadzenia analizy wszelkich ewentualnych kosztów i korzyści z tym związanych.

Oparcie się tylko i wyłącznie na zdarzeniach historycznych może niewątpliwie stanowić istotne ograniczenie w zastosowaniu tej metody. Dopuszcza się jednak możliwość wprowadzenia do opisu danego przypadku elementów fikcyjnych. Z kolei problem generalizacji wniosków wynikających z przeprowadzonej analizy pojedynczego case'u (najczęściej ekstremalnego lub typowego) można rozwiązać

---

[48] P. Wójcik, *Znaczenie studium przypadku jako metody badawczej w naukach o zarządzaniu*, luty 2013, s. 20.

[49] Tamże.

[50] Ż. Ptak-Kostecka, *Analiza przypadku, czyli metoda case study*, Rozdział 4 pracy doktorskiej pt. *Efektywność pełnienia ról menedżerskich* (2000).

przez zastosowanie analizy wielokrotnych przypadków. Umożliwiłaby ona porównanie różnych wersji danego incydentu (przez dokonanie modyfikacji opisu faktycznego zdarzenia, przez pryzmat np. rozmiaru jego skutków) i refleksję czy w rozpatrywanych przypadkach bardziej zasadne byłoby podjęcie dodatkowych działań mających na celu zapobieganie ryzyku lub jego redukcję.

W założeniu metodę analizy *case study* wykorzystuje się głównie w oparciu o analizę zdarzeń rzeczywistych. W obszarze zarządzania kryzysowego punktem odniesienia mogą więc być dane historyczne związane z wystąpieniem zagrożeń na danym terenie. Powyższe informacje, niezbędne do sporządzenia opisu danego przypadku mogą pochodzić m.in. z raportów sporządzanych przez poszczególne służby po wystąpieniu zagrożenia/sytuacji kryzysowej. W niniejszej części opracowania, w celu sporządzenia opisu przypadku wykorzystano treść raportu po powodzi z maja i czerwca 2010 r. przygotowanego przez Urząd Miasta Kraków[51].

Opis przypadku – Powódź, maj–czerwiec, Kraków 2010

W dniach 14–15 maja 2010 r. Województwo Małopolskie znalazło się w zasięgu ośrodka niżowego znad Polesia, jak również chłodnego frontu atmosferycznego, a jednocześnie z północnego zachodu zaczęła napływać chłodna masa powietrza polarno-morskiego. Co więcej, znad Niziny Węgierskiej i Ukrainy zaczęły napływać wilgotne i ciepłe masy powietrza czarnomorskiego. W związku z tym Instytut Meteorologii i Gospodarki Wodnej w Krakowie wydał ostrzeżenie hydrometeorologiczne, a dwudniowa prognoza przewidywała opady deszczu o wysokości rzędu maksymalnie 100–150 mm. Stanowiło to poważne ostrzeżenie dla służb miejskich oraz zapowiedź znacznego wezbrania, szczególnie na górskich dopływach Wisły powyżej Krakowa. W kolejnych dniach zanotowano obfite opady deszczu. Prognozy potwierdziły się, a w wyniku intensywnych opadów deszczu nastąpił gwałtowny przybór wód we wszystkich prawobrzeżnych karpackich dopływach Wisły (Mała Wisła, Sola, Skawinka). Ponadto wezbrały także lewobrzeżne dopływy. W tej sytuacji Prezydent miasta ogłosił pogotowie przeciwpowodziowe dla miasta Krakowa. Tego samego dnia w związku z pogarszającą się sytuacją hydrologiczną zwołano posiedzenie Powiatowego Zespołu Zarządzania Kryzysowego. Po zapoznaniu się z sytuacją oraz po przeprowadzeniu analizy przepisów prawnych (Ustawa o samorządzie powiatowym) oraz zapisów operacyjnego planu ochrony przed powodzią, Prezydent Krakowa ogłosił alarm przeciwpowodziowy na terenie całego miasta. W kolejnych dniach wydano dyspozycje o montażu rozbieralnych ścianek przeciwpowodziowych na Zakolu pod Wawelem oraz podjęto decyzję o zamknięciu ruchu na Moście Dębnickim i przegrodzenie go specjalistycznymi urządzeniami w celu zapobieżenia przelaniu się wód Wisły. Doszło do podtopień niektórych obszarów miasta. Ich przyczynami były: odcięcie spływu wód w wyniku zamknięcia śluz wałowych, zamknięcie przelewów burzowych kanalizacji ogólnospławnej. Ponadto wystąpiły podtopienia obszarów miasta oddalonych od Wisły. W czasie powodzi podejmowano wiele interwencji związanych z podtopieniami w rejonach około 60 ulic miasta. Ze względu na przesiąki przez obwałowania, zagrożenie przerwaniem wałów oraz przerwanie obwałowania przy jednej z ulic, podjęto działania takie jak uszczelnianie studzienek kanalizacyjnych workami z piaskiem czy odpompowanie wody

[51] Raport po powodzi z maja i czerwca 2010 r., Urząd Miasta Krakowa, Kraków 2010.

z zalanych piwnic. Zarządzono ewakuację kilku ulic, a osoby poszkodowane przewieziono do jednej ze szkół. Akcję przeciwpowodziową prowadzono także w obszarach oddalonych od Wisły. Ponadto wprowadzono wiele ograniczeń i zmian w organizacji komunikacji miejskiej.

W działaniach interwencyjnych brały udział: PSP (31 samochodów, 256 strażaków), sprzęt pływający (3 łodzie), Wojsko (9 samochodów, 136 żołnierzy), Policja (58 samochodów, 146 policjantów), Straż Miejska (4 samochody, 16 strażników) oraz inne służby (11 samochodów, 13 osób).

Niezależnie od prowadzonych działań ratowniczych, tj. niesienia pomocy poszkodowanym przystąpiono także do ustalania szkód i szacowania strat spowodowanych powodzią. W wyniku prac komisji do spraw szacowania strat spowodowanych przez klęski żywiołowe w infrastrukturze komunalnej, komisji do spraw szacowania zakresu szkód w rolnictwie oraz komisji do spraw szacowania szkód w gospodarstwach domowych powołanych przez Prezydenta Miasta ustalono, że:

- *straty w infrastrukturze komunalnej wyniosły 168 mln zł (w tym straty w infrastrukturze drogowej – 60 mln zł, uszkodzenia obiektów mostowych – 6 mln 580 tys. zł, straty w placówkach oświatowych 6 mln 556 tys. zł, inne obiekty komunalne 82 mln 703 tys.); zniszczenia objęły: drogi, mosty, przepusty, kładki, cmentarze, szkoły, budynki mieszkalne, obiekty sportowe, obiekty turystyki itp.),*
- *straty w infrastrukturze przeciwpowodziowej wyniosły 11 320 tys. zł,*
- *straty w rolnictwie (straty wystąpiły na obszarach 900 ha, w okresie maj–lipiec zgłoszono ponad 300 wniosków o pomoc, doszło do zalania obiektów gospodarskich).*

Miejski Ośrodek Pomocy Społecznej w Krakowie udzielił również pomocy osobom dotkniętym powodzią w formie: dyżurów pracowników socjalnych, zasiłku celowego, pomocy rzeczowej oraz wsparcia psychologicznego. Z wnioskiem o udzielenie pomocy zgłosiło się do MOPS 1057 osób poszkodowanych. Łączna kwota wszystkich wniosków o pomoc finansową z budżetu państwa, które zostały złożone przez Gminę Miejską Kraków, a następnie przekazane do Małopolskiego Urzędu Wojewódzkiego, wyniosła 2 318 498,57 zł.

Pomoc poszkodowanym objęła również wydanie przez Powiatową Stację Sanitarno-Epidemiologiczną środków do odkażania studni przydomowych. Zapewniono także pomoc w zakresie oczyszczania terenów zalanych, obejmującą akcje zbierania wszystkich zalanych przedmiotów oraz ich wywóz na składowisko odpadów. Z kolei formą pomocy dla przedsiębiorców, którzy ponieśli szkodę w wyniku powodzi z 2010 r. jest możliwość ubiegania się o udzielnie pożyczki zgodnie z przepisami ustawowymi o wspieraniu przedsiębiorców dotkniętych skutkami powodzi z 2010 r. W stosunku do osób mieszkających na działkach udzielono zaś pomocy w ramach zadań własnych gminy, tj. zasiłków celowych ze względu na wystąpienie zdarzenia losowego. Poszkodowani otrzymali też pomoc rzeczową, tj. środki czystości, odzież, żywność i materiały budowlane, a część z nich została objęta wsparciem psychologicznym[52].

Powyższy opis odnosi się do przypadku opartego na dokumentach (w tym wypadku raportu z powodzi). Ma on charakter pojedynczy (*single-case*). Jego wybór był podyktowany faktem, że stanowi on przykład rzadkich i unikalnych uwarun-

[52] Raport po powodzi z maja i czerwca 2010 r., Urząd Miasta Krakowa, Kraków 2010.

kowań. Powódź z 2010 r. była jedną z największych, jakie wydarzyły się kiedykolwiek w Polsce[53]. Dość powiedzieć, że kulminacja fali wezbraniowej była największa od 160 lat[54]. Co więcej, w wybranych miejscach (w tym w rozpatrywanym przypadku w Krakowie) poziom wody na Wiśle przekroczył poziom odnotowany podczas powodzi tysiąclecia w 1997 r.

Celem analizy rozpatrywanego case'u jest wskazanie poziomu akceptowalności zidentyfikowanego ryzyka (w tym wypadku *zrealizowanego* ryzyka wystąpienia powodzi). Pomocne w tym względzie będzie określenie, czy istniejące zabezpieczenia/środki bezpieczeństwa okazały się wystarczające w obliczu wystąpienia tego zagrożenia, pozwalając na określenie kategorii akceptacji ryzyka.

Do tak określonego problemu sformułowano następujące pytania badawcze:

1) Czy posiadane siły i środki, które zostały wykorzystane w ramach interwencji podejmowanych w czasie powodzi okazały się wystarczające w stosunku do skali zagrożenia?
   - Państwowa Straż Pożarna (ludzie, sprzęt),
   - Wojsko (ludzie, sprzęt),
   - Policja (ludzie, sprzęt),
   - Straż Miejska (ludzie, sprzęt),
   - Inne służby (ludzie, sprzęt).
2) Jeżeli nie, to jakiego rodzaju braki w ramach wymienionych kategorii sił i środków zostały zidentyfikowane w wyniku prac nad raportem z powodzi?
3) Czy posiadane środki ochrony przeciwpowodziowej okazały się wystarczające w obliczu wystąpienia zagrożenia? (biorąc pod uwagę poniższe kategorie):
   - działania prawno-organizacyjne,
   - techniczne środki ochrony przeciwpowodziowej, w tym środki ochrony czynnej oraz środki ochrony biernej.
4) Jeżeli nie, to jakiego rodzaju braki/nieprawidłowości w tym zakresie zidentyfikowano w wyniku prac nad raportem z powodzi?
5) Czy stan techniczny środków ochrony przeciwpowodziowej okazał się zadowalający w obliczu wystąpienia zagrożenia?
6) Jeżeli nie, to środki ochrony przeciwpowodziowej jakiego rodzaju i w jakiej ilości wymagają naprawy/zakupu/doposażenia?
7) Z jakimi kosztami wiązałoby się dokonanie inwestycji w tym zakresie?
8) Czy komunikacja pomiędzy poszczególnymi służbami biorącymi udział w działaniach interwencyjnych przebiegła prawidłowo?
9) Jeżeli nie, to jakiego rodzaju problemy w tym obszarze zidentyfikowano w wyniku prac nad raportem z powodzi?
   - niewłaściwe procedury,
   - brak standardów wymiany informacji,

[53] Witryna internetowa http://www.ekologia.pl/srodowisko/ochrona-srodowiska/najwieksze-powodzie-w-polsce-w-xx-i-xxi-wieku,12426.html, z dnia 11.12.14 r.

[54] Witryna internetowa http://www.polskieradio.pl/5/3/Artykul/198291,Fala-na-Wisle-najwieksza-od-160-lat z dnia 11.12.14 r.

- brak technicznych możliwości wymiany informacji,
- inne.

10) Czy środki przeznaczone na pomoc poszkodowanym przez powódź okazały się wystarczające w stosunku do potrzeb poszkodowanej ludności?
    - pomoc udzielona przez Miejski Ośrodek Pomocy Społecznej,
    - pomoc udzielona przez Powiatową Stację Sanitarno Epidemiologiczną,
    - pomoc w zakresie oczyszczania terenów zielonych,
    - pomoc przedsiębiorcom,
    - pomoc udzielona na rzecz zalanych Rodzinnych Ogródków Działkowych.
11) Jaki łączny koszt poniesiono w związku z podjęciem działań interwencyjnych oraz pomocowych?
12) Jakie korzyści przyniosłoby podjęcie następujących działań naprawczych (biorąc pod uwagę następujące kategorie)?
    - zmiany prawno-organizacyjne,
    - naprawa/zakup/doposażenie środków ochrony przeciwpowodziowej,
    - inne.
13) Czy korzyści wynikające z wprowadzenia dodatkowych środków bezpieczeństwa/zabezpieczeń byłyby większe niż ewentualne koszty z tym związane (w tym w szczególności inwestycje finansowe w tym zakresie)?
14) Czy straty poniesione przez poszkodowanych zostały im zrekompensowane w postaci udzielenia im adekwatnej formy pomocy z punktu widzenia poszkodowanej ludności (innymi słowy, czy do administracji wpłynęły głosy na temat społecznego niezadowolenia z działań służb mających na celu przeciwdziałanie zaistniałemu zagrożeniu)?

Odpowiedzi na powyższe pytania mogą przyczynić się określenia akceptowalnego poziomu zidentyfikowanego ryzyka, zarówno przez administrację, jak i społeczeństwo. Część danych niezbędnych do odpowiedzi na nie znajduje się w przywoływanym raporcie z powodzi. Z kolei inne informacje można by pozyskać w oparciu o wiedzę będącą w gestii poszczególnych służb biorących udział w przeciwdziałaniu zagrożeniu, jakim jest powódź, jak również osób bezpośrednio poszkodowanych w wyniku powodzi (np. badanie ankietowe dotyczące akceptowalności przez społeczeństwo poniesionych strat w stosunku do zaoferowanej oraz udzielonej im pomocy).

Podobnie jak w przypadku modelu scenariuszowego wynikiem analizy rozpatrywanego przypadku będzie wskazanie poziomu akceptowalności zidentyfikowanego ryzyka, w oparciu o wybór jednej z trzech kategorii, tj. ryzyka akceptowanego, ryzyka tolerowanego lub ryzyka nieakceptowanego.

Innymi metodami są metody preferencji ujawnionych i wyrażonych oraz oceny wartości życia ludzkiego. Metody preferencji ujawnionych i wyrażonych wykorzystywane są w ekonomii oraz marketingu i zarządzaniu. W założeniu, dla preferencji ujawnionej miarą akceptowalności ryzyka związanego z danym przedsięwzięciem jest ryzyko, które już istnieje w społeczeństwie. Jako przykład podaje się posiadanie informacji na temat danego ryzyka, tj. np. sytuacja, w której częstość

utraty pieniędzy z konta bankowego wynosi raz na milion, a jednocześnie zjawisko to jest akceptowane przez klientów banku. Ze względu na fakt, że preferencje ujawnione odzwierciedlają rzeczywiste decyzje rynkowe np. konsumentów, do ich analizy wykorzystuje się przede wszystkim dane historyczne (np. dane z przeprowadzonych sondaży odnoszących się do wyborów rynkowych wcześniej dokonanych przez klientów czy też materiałów statystycznych)[55].

Zgodnie z metodą preferencji wyrażonych różne osoby pyta się wprost o akceptowalność danego ryzyka, zakładając, że znane są zarówno korzyści, jak i ryzyka danego przedsięwzięcia. Jako przykład można podać deklarowane (hipotetyczne) zachowania rynkowe konsumentów oparte o dane zgromadzone za pomocą sondaży pośrednich i bezpośrednich, które pozwalają na identyfikację intencji nabywczych konsumentów w czasie przeprowadzanego badania.

Metodę preferencji ujawnionych można by wykorzystać na potrzeby określenia poziomu akceptacji społecznej dla zidentyfikowanego ryzyka, np. zgoda ludzi na zasiedlanie terenów zalewowych ze wszystkimi tego możliwymi konsekwencjami. Z kolei metoda preferencji wyrażonych mogłaby znaleźć swoje zastosowanie w ramach budowy scenariuszy możliwych zdarzeń i wzięcie pod uwagę stopnia akceptacji społecznej na wypadek *zrealizowania się* danego ryzyka, np. biorąc pod uwagę możliwe straty z tym związane oraz rekompensatę, jaka byłaby przyznawana poszkodowanym w ramach usuwania skutków danego zdarzenia.

W literaturze wskazuje się na następujące metody podejścia do wyceny wartości życia ludzkiego:

- życie ludzkie traktowane jako kapitał – wersja netto (w tym przypadku wartość osoby jako wartość straty dla reszty społeczeństwa wylicza się poprzez odjęcie od dyskontowanych zarobków dyskontowanej sumy przyszłej konsumpcji tej osoby, z kolei w wersji brutto w ocenie wartości życia uwzględnia się także przyszłą konsumpcję jednostki, z zastrzeżeniem, że nie odejmuje się jej od dyskontowanej sumy przyszłych zarobków),
- orzeczenie sądowe (sprawy odszkodowań za utratę życia),
- ogólna suma odszkodowania (taka, której zażądaliby członkowie grupy narażonej na ryzyko przy wyrażeniu przez nich zgody na dodatkowe prawdopodobieństwo utraty życia, które wynika z ocenianego przedsięwzięcia,
- metoda *wojskowa* (ilość strat własnych tzw. siła żywa kontra osiągnięte cele)[56].

Metoda ta byłaby użyteczna w przypadku rozpatrywania zdarzeń (historycznych lub przewidywanych), których konsekwencją jest wystąpienie ofiar śmiertelnych, rannych, pod kątem oszacowania związanych z tym strat finansowych.

Możliwość wykorzystania metody określenia akceptowalności zidentyfikowanego ryzyka opartej na modelu scenariuszowym zostanie rozpatrzona na przykła-

[55] A. I. Szymańska, *Badania preferencji konsumentów z wykorzystaniem kompozycyjnej metody badań* MDPREF, s. 1.

[56] Witryna internetowa http://edu.pjwstk.edu.pl/wyklady/psk/scb/index15.html z dnia 30.09. 2014 r.

dzie opracowania modelu scenariusza możliwych zdarzeń związanego z wystąpieniem zagrożenia powodziowego. Został on *rozwinięty* w oparciu o użycie metod wspomagających, w tym metody Bow-tie, metody analizy drzewa zdarzeń (analiza ETA) oraz metody analizy drzewa błędów (analiza FTA).

Punktem wyjścia dla rozpatrywanego modelu scenariusza było określenie zdarzenia głównego, tj. wystąpienia powodzi. W stosunku do niego określone zostały potencjalne przyczyny zdarzenia (za pomocą metody FTA) oraz potencjalne skutki (za pomocą metody ETA). W trakcie budowy *drzewa skutków* wykorzystano założenia metody SWIFT (*Co jeśli?*) polegającej na zadawaniu pytań niejako *prowokujących* do rozpatrzenia wszystkich wariantów możliwych skutków zdarzenia. Bazując na założeniach metody Bow-tie, analizę uzupełniono również o wskazanie barier (zabezpieczeń), które powinny zapobiec jego przyczynom (a tym samym obniżyć prawdopodobieństwo jego wystąpienia) oraz ograniczyć skutki zdarzenia.

Pierwszą część modelu scenariusza możliwych zdarzeń związanych z wystąpieniem powodzi, obejmującą wskazanie przyczyn wystąpienia zagrożenia, zobrazowano na schemacie sporządzonym za pomocą *mapy myśli* (załącznik nr 4).

Na schemacie uwzględniono również bariery (zabezpieczenia) po stronie przyczyn, które mogą wpłynąć na obniżenie prawdopodobieństwa wystąpienia zdarzenia związanego z wystąpieniem powodzi. Zostały one oznaczone liczbami porządkowymi oraz znakiem STOP. Należą do nich:

- dla 4 (przepisy prawne dotyczące warunków technicznych, jakim powinny odpowiadać budowle hydrotechniczne i ich usytuowanie; modernizacja/naprawa wałów przeciwpowodziowych),
- dla 5 (działania prawno-organizacyjne np. ograniczenie zabudowy na terenach szczególnie zagrożonych powodzią, wyznaczenie stref zagrożenia powodziowego, sterowanie pojemnością zbiornika wodnego, system dotacji oraz ubezpieczeń; Techniczne środki ochrony przeciwpowodziowej, w tym środki ochrony czynnej, np. zbiorniki retencyjne, poldery oraz środki ochrony biernej, np. obwałowania, regulacja rzeki),
- dla 6 (dokumenty planistyczne, w tym plan zarządzania kryzysowego, plan operacyjny ochrony przed powodzią; organizacja ćwiczeń; narzędzie informatyczne wspomagające przygotowanie bazy sił i środków).

Drugą część modelu scenariusza możliwych zdarzeń związanych z wystąpieniem powodzi, obejmującą wskazanie skutków wystąpienia zagrożenia oraz określenie zabezpieczeń (barier) ograniczających ich eskalację, podobnie jak w przypadku *drzewa przyczyn* zilustrowano za pomocą *mapy myśli* (załącznik nr 5).

Do wskazanych skutków przyporządkowano następujące bariery (zabezpieczenia):

- Dla 1: Działania ratownicze (procedury, personel, sprzęt ratowniczy), Organizacja usług medycznych dla ludności poszkodowanej (procedura, personel, sprzęt), Plan ewakuacji I, II stopnia, Organizacja usług transportowych dla ludności poszkodowanej (procedura, personel, środki transportowe), Organizacja usług kwaterunkowych dla ludności.

- Dla 2: Odszkodowania dla przedsiębiorców zajmujących się przetwarzaniem oraz sprzedażą żywności oraz dla rolników w związku ze stratami, które ponieśli w swoich gospodarstwach, Zabezpieczenia istniejących budynków, Uruchomienie środków pomocy społecznej, w tym przyznanie zasiłku celowego, pomoc rzeczowa oraz wsparcie psychologiczne.
- Dla 3: Odkażanie zalanych studni i ujęć wodnych; Zabiegi dezynfekcyjne; Przedsięwzięcia przeciwepidemiczne.
- Dla 4: Procedura organizacji dostaw artykułów powszechnego użytku; Procedura organizacji dostaw wody, Dystrybucja wody butelkowanej, System obwoźny, Beczkowozy, Awaryjne ujęcia wody; Procedura organizacji dostaw żywności, Przygotowanie i dystrybucja paczek żywnościowych, punkty żywienia zbiorowego; Agregaty prądotwórcze, Procedura organizacji i przywrócenia dostaw prądu (wskazanie czasu przerwy funkcjonowania danego procesu, tj. przerwy w dostawie prądu oraz czasu odtworzenia, tj. czasu od uszkodzenia linii energetycznej do czasu przywrócenia dostaw prądu stanowi praktyczne zastosowanie metody BIA).
- Dla 5: Akcja informacyjno-instruktażowa dla społeczeństwa, Zabezpieczenie mienia ewakuowanej ludności.

Powyższa analiza potencjalnych przyczyn oraz skutków wystąpienia powodzi jest jedynie przykładem łańcucha zdarzeń, które mogą wystąpić w przypadku pojawienia się zagrożenia powodzi oraz zabezpieczeń (barier) umożliwiających obniżenie prawdopodobieństwa (przyczyn) oraz ograniczenie skutków danego zdarzenia. Może jednak stanowić podstawę do *rozwinięcia* scenariusza możliwych zdarzeń na danym terenie. Jego opracowanie wymaga bowiem znajomości specyfiki funkcjonowania danej organizacji (np. jednostki samorządu terytorialnego), w tym charakterystyki obszaru, w ramach którego funkcjonuje, informacji na temat przyjętych procedur działania w przypadku wystąpienia zagrożenia, posiadanych zasobów czy też trybu uruchamiania niezbędnych sił i środków.

Podsumowując, na potrzeby określenia poziomu akceptowalności zidentyfikowanego ryzyka, zasadne wydaje się odwołanie do specyfiki scenariusza poddanego analizie oraz zwrócenie szczególnej uwagi na:

- dotkliwość skutków zdarzenia ujętego w scenariuszu,
- istniejące zabezpieczenia i ich wpływ na obniżenie prawdopodobieństwa (zapobieganie przyczynom) wystąpienia zdarzenia oraz ograniczenie jego skutków.

W odniesieniu do drugiego ze wskazanych punktów, będzie to kontynuacja rozważań, które rozpoczynają się na etapie analizy ryzyka, gdzie w ramach analizy podatności definiowane są mocne oraz słabe strony organizacji.

W celu określenia akceptowalnego poziomu ryzyka, zasadne wydaje się przeprowadzenie szczegółowej analizy mającej na celu zbadanie relacji pomiędzy tzw. ryzykiem *początkowym* (rozumianym jako poziom ryzyka wraz z zabezpieczeniami istniejącymi *tu i teraz*) a ryzykiem *pożądanym* (rozumianym jako oczekiwany poziom ryzyka przy zastosowaniu dodatkowych zabezpieczeń oraz środków

bezpieczeństwa)[57]. Jej istotą będzie wskazanie, czy i w jakim stopniu dodatkowe zabezpieczenia mogą obniżyć poziom ryzyka początkowego (poprzez obniżenie prawdopodobieństwa jego wystąpienia oraz ograniczenie skutków). Wsparciem w tym względzie będzie analiza kosztów i korzyści, ukierunkowana na rozpatrzenie ewentualnych inwestycji związanych z nowymi zabezpieczeniami pod kątem finansowym. Zastosowanie tej metody pozwoli na ocenę potencjalnego *wkładu* finansowego w poprawę istniejących zabezpieczeń i środków bezpieczeństwa pod kątem racjonalnego gospodarowania. Innymi słowy chodzi o wskazanie, czy powstrzymanie się od podjęcia jakichkolwiek działań zapobiegawczych (i przyjęcia wszelkich konsekwencji z tym związanych) jest korzystniejsze, niż dokonanie inwestycji w przedmiotowym zakresie.

Poniżej przedstawiono przykładowy schemat postępowania w przypadku określenia akceptowalności zidentyfikowanego ryzyka dla scenariusza możliwych zdarzeń związanych z wystąpieniem powodzi. Pierwszym etapem analizy będzie analiza istniejących zabezpieczeń w odniesieniu do tzw. ryzyka początkowego, zgodnie z tabelą 5.5.

Tabela 5.5. Analiza istniejących zabezpieczeń/środków bezpieczeństwa w kontekście poziomu ryzyka *początkowego*

Ryzyko *początkowe* *Nazwa*	
Istniejące zabezpieczenia/ środki bezpieczeństwa	Zasoby materialne (np. rzeczowe, osobowe, finansowe) lub niematerialne (np. informacyjne, prawne)
Wpływ na obniżenie prawdopodobieństwa	Tak/Nie
Uzasadnienie	Jeżeli *Tak* to w jaki sposób istniejące zabezpieczenia wpływają na obniżenie prawdopodobieństwa wystąpienia zdarzenia ujętego w rozpatrywanym scenariuszu? (np. na podstawie analizy danych historycznych, studium przypadku, wniosków z ćwiczeń)
Wpływ na ograniczenie skutków	Tak/Nie
Uzasadnienie	Jeżeli *Tak* to w jaki sposób istniejące zabezpieczenia wpływają na ograniczenie skutków wystąpienia zdarzenia ujętego w rozpatrywanym scenariuszu (np. na podstawie analizy danych historycznych, studium przypadku, wniosków z ćwiczeń)? Dla kategorii skutków: Ludność: np. ograniczenie liczby ofiar, poszkodowanych, osób wymagających udzielenia im pomocy medycznej Gospodarka/mienie/infrastruktura: np. ograniczenie zniszczeń mienia, obiektów IK

[57] Prezentacja: G. Abgarowicz, *Ocena ryzyka zagrożeń transgranicznych, scenariusz powódź – propozycja metodyki*, Rządowe Centrum Bezpieczeństwa, Warszawa 2014 r.

Uzasadnienie	Środowisko: np. niedopuszczenie do powstania epidemii Dostawy: np. kontynuacja dostaw wszelkich usług dla ludności, w tym związanych z IK/sprawne przywrócenie usług dla ludności, które zostały *przerwane* w wyniku wystąpienia zagrożenia Niematerialne: np. niedopuszczenie do wzrostu poziomu niezadowolenia społecznego, utraty wizerunku i reputacji polityków i administracji
Akceptacja obecnie stosowanych rozwiązań *(Czy posiadane zabezpieczenia są wystarczające?)*	TAK/NIE
Uzasadnienie	W przypadku udzielenia odpowiedzi *Nie* należy wskazać dlaczego nie są one wystarczające (np. zbyt mała ilość posiadanych zasobów, złe przepisy, błędne procedury)

Źródło: opracowanie własne

W przypadku podjęcia decyzji o akceptacji obecnie stosowanych rozwiązań, niniejszą analizę można uznać za zakończoną. Przy podjęciu decyzji o konieczności przeprowadzenia zmian w tym zakresie, dodatkowo należałoby przeprowadzić analizę potencjału wprowadzenia dodatkowych zabezpieczeń/środków bezpieczeństwa lub ich poprawy/zmiany, zgodnie z tabelą 5.6.

Tabela 5.6. Analiza potencjału wprowadzenia dodatkowych zabezpieczeń/środków bezpieczeństwa lub ich zmiany/poprawy w kontekście poziomu ryzyka *pożądanego*

Ryzyko *pożądane* *Nazwa*	
Dodatkowe zabezpieczenia/ środki bezpieczeństwa	Zasoby materialne (np. rzeczowy, osobowy, finansowy) lub niematerialne (np. informacyjny, prawny)
Potencjalny wpływ na obniżenie prawdopodobieństwa	Tak/Nie
Uzasadnienie	Jeżeli *Tak*, to w jaki sposób dodatkowe zabezpieczenia mogą wpłynąć na obniżenie prawdopodobieństwa wystąpienia zdarzenia ujętego w rozpatrywanym scenariuszu (np. na podstawie szacowania eksperckiego)?
Potencjalny wpływ na ograniczenie skutków	Tak/Nie
Uzasadnienie	Jeżeli *Tak*, to w jaki sposób dodatkowe zabezpieczenia mogą wpłynąć na ograniczenie skutków wystąpienia zdarzenia ujętego w rozpatrywanym scenariuszu (np. na podstawie szacowania eksperckiego? Dla kategorii skutków: Ludność: ograniczenie liczby ofiar, poszkodowanych, osób wymagających udzielenia im pomocy medycznej Gospodarka: np. ograniczenie zniszczeń mienia, obiektów IK Środowisko: np. niedopuszczenie do powstania epidemii

	Dostawy: np. kontynuacja dostaw wszelkich usług dla ludności, w tym związanych z IK/sprawne przywrócenie usług dla ludności, których świadczenie zostało *przerwane* w wyniku wystąpienia zagrożenia Niematerialne: np. niedopuszczenie do wzrostu poziomu niezadowolenia społecznego, utraty wizerunku i reputacji polityków i administracji
Analiza korzyści i kosztów	Korzyści: np. minimalizacja strat związanych ze zniszczeniami mienia, budynków mieszkalnych, infrastruktury, ograniczenie strat w ludziach (wyrażone w wartości pieniężnej[1]) Koszty: Wysokość wkładu finansowego związanego z inwestycjami odnoszącymi się do poprawy istniejących zabezpieczeń/wprowadzenia dodatkowych zabezpieczeń np. koszt budowy zbiornika retencyjnego
Akceptacja wprowadzenia dodatkowych zabezpieczeń/ środków bezpieczeństwa	TAK/NIE *Tak*, w przypadku gdy korzyści wynikające z wprowadzenia dodatkowych zabezpieczeń/środków bezpieczeństwa przeważają nad ewentualnymi kosztami *Nie*, w przypadku gdy koszty poniesione w wyniku wprowadzenia dodatkowych zabezpieczeń/środków bezpieczeństwa przeważają nad korzyściami wynikającymi z podjęcia tych przedsięwzięć

Źródło: opracowanie własne

W oparciu o powyżej przeprowadzoną analizę można by przyjąć następujące kategorie akceptacji ryzyka:

- ryzyko akceptowane (akceptowane są aktualne rozwiązania, zabezpieczenia, środki bezpieczeństwa),
- ryzyko tolerowane (aktualne rozwiązania, zabezpieczenia wymagają poprawy, należałoby wprowadzić dodatkowe środki bezpieczeństwa, jednakże z analizy kosztów i korzyści wynika, że koszty działań z tym związanych przekroczą spodziewane korzyści, zaleca się więc prowadzenie działań monitorujących),
- ryzyko nieakceptowane (należy podjąć natychmiastowe działania zmierzające do wprowadzenia lub poprawy istniejących zabezpieczeń – dotyczy dodatkowych zabezpieczeń, których wprowadzenie przyniesie organizacji więcej korzyści niż strat).

5.4. Prezentacja ryzyk

Po przeprowadzeniu identyfikacji oraz analizy ryzyka należy przystąpić do jego pomiaru i oceny. Efektem procesu oceny ryzyka powinien być obraz przedstawiający hierarchię ryzyka w organizacji[58]. Aby taka hierarchia mogła powstać, należy najpierw ryzyko skwantyfikować, to znaczy określić prawdopodobieństwo jego wystąpienia oraz wartość potencjalnej straty związanej z jego wystąpieniem.

[58] J. Zawarska, *Identyfikacja i pomiar ryzyka w procesie zarządzania ryzykiem podmiotów gospodarczych*, Zarządzanie i Finanse, nr 1/2012, s. 69.

W literaturze napotykamy prezentacje różnorodnych metod i podejść, zaczynając od najmniej skomplikowanych, opartych bardziej na zwykłej subiektywnej ocenie, po metody korzystające z zaawansowanych nauk matematyczno-statystycznych oraz osiągnięć rachunku prawdopodobieństwa[59]. Za bardziej precyzyjne można uznać metody ilościowe, ale do ich zastosowania należy korzystać z odpowiednich danych, którą muszą być wiarygodne i obejmować zadowalający przedział czasowy. Oczywiście dostęp do danych potrzebnych do oceny może okazać się zbyt kosztowny i wtedy korzysta się z metod jakościowych. Chociaż są one oparte na subiektywnej ocenie, to w większości przypadków jest ocena to eksperta lub grupy ekspertów, którzy w danej dziedzinie posiadają zarówno duże doświadczenie oraz szeroką wiedzę.

Według najczęściej występującej definicji ryzyko jest to iloczyn prawdopodobieństwa wystąpienia ryzyka oraz jego ewentualnych skutków. Najprościej przedstawia to poniższy wzór:

ryzyko = prawdopodobieństwo x wartość skutków

W tym przypadku jako prawdopodobieństwo rozumie się stosunek liczby zrealizowanych ryzyk – czyli zaistniałych wypadków losowych, do ogólnej liczby istniejących ryzyk – czyli wszystkich przedmiotów zagrożonych ryzykiem[60]. Bardzo często dokładne określenie prawdopodobieństwa jest niemożliwe. W takich wypadkach najczęściej stosuje się kategoryzację ryzyka według przyjętych podziałów. Tak jest m.in. w metodzie Richarda Prouty'ego, który klasyfikuje ryzyko na następujące grupy:

- *prawie zerowe* – zdarzenie nie wystąpi,
- *niewielkie* – zdarzenie nie miało miejsca do chwili obecnej i prawdopodobieństwo jego wystąpienia w przyszłości jest małe,
- *umiarkowane* – zdarzenie miało już miejsce i przewiduje się, że w przyszłości również zajdzie,
- *określone* – zdarzenie występowało regularnie i należy przyjąć, że tak będzie również w przyszłości[61].

Powyższe dane można również przedstawić za pomocą tabeli 5.7.

Tabela 5.7. Punktowa mapa prawdopodobieństwa wystąpienia ryzyka

	1	**2**	**3**	**4**	**5**
Opis	Rzadkie	Mało prawdopodobne	średnie	Prawdopodobne	Prawie pewne
Prawdopodobieństwo	0-20%	21-40%	41-60%	61-80%	81-100%

Źródło: Zarządanie ryzykiem w sektorze publicznym, Ministerstwo Finansów RP

[59] J. Zawarska, *Identyfikacja i pomiar ryzyka w procesie zarządzania ryzykiem podmiotów gospodarczych*, Zarządzanie i Finanse, nr 1/2012, s. 69.

[60] A. Liwacz, *Zarządzanie ryzykiem*, Poradnik Samorządowy, grudzień 2004, s. 28.

[61] C.A. Williams Jr., M.L. Smith, P.C. Young, *Zarządzanie ryzykiem a ubezpieczenia,* Wydawnictwo Naukowe PWN, Warszawa 2002, s. 94.

W przypadków szacowania wartości prawdopodobieństwa istotne jest, by dane dotyczące podobnych wypadków w przeszłości pochodziły z dokumentacji danej organizacji. W sytuacji, kiedy nie ma możliwości wykorzystania własnych danych statystycznych, należy wykorzystywać dane zewnętrzne, wliczając literaturę fachowa.

Przy ustalaniu wielkości skutków również można zastosować metodę kategoryzacji, gdy nie są dostępne dane ilościowe, lub gdy nie jest potrzebne dokładne wyznaczenie konkretnej liczby (ustalenie poziomu strat na wysoki średni i niski). Natomiast w przypadku danych ilościowych można stosować jedną z niżej wymienionych metod:

- Probable Maximum Loss (PML) – Prawdopodobna Maksymalna Strata,
- Possible Maximum Loss (PML) – Możliwa Maksymalna Strata,
- Maximum Probable Loss (MPL) – Maksymalna Prawdopodobna Strata,
- Maximum Possible Loss (MPL) – Maksymalna Możliwa Strata,
- Maximum Credible Loss (MCL) – Maksymalna Realna Strata,
- Maximum Foreseeable Loss (MFL) – Maksymalna Przewidywalna Strata,
- Estimated Maximum Loss (EML) – Szacunkowa Maksymalna Strata[62].

Określając wartości zarówno dla prawdopodobieństwa, jak i dla skutków można wyznaczyć mapę ryzyka, zwaną również matrycą ryzyka, modelem ryzyka, charakterystyką ryzyka. Mapa ryzyka to graficzna prezentacja oceny zidentyfikowanego ryzyka, powstała dzięki sprowadzeniu wszystkich ocen do punktu pozwalającego porównać ze sobą analizowane ryzyka[63]. W zależności od dokładności danych dotyczących prawdopodobieństwa oraz skutków można wyznaczyć dowolną mapę ryzyka. Im dane są bardziej szczegółowe, tym mapa ryzyka może zawierać więcej przedziałów, co przełoży się na większą ilość obszarów.

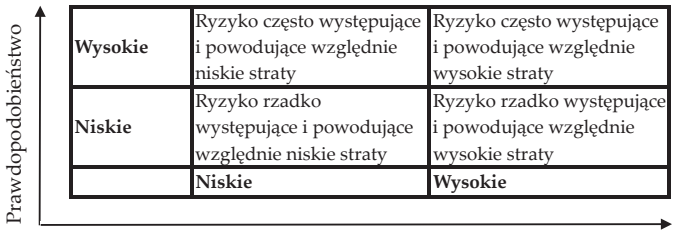
W zależności od potrzeb i możliwości ustalana jest odpowiednia liczba pól matrycy. Pierwszy rysunek przedstawia przykład najprostszej mapy ryzyka. W praktyce wskazane jest jednak stosowanie bardziej rozbudowanej skali map ryzyka, dostosowanej jednocześnie do specyfiki jednostki, ale też przyjętych metod analizy oraz dostępnych danych.

Poniżej przedstawiono mapy ryzyka dla wariantu bardzo ogólnego i trochę bardziej szczegółowego, zawierającego pięć przedziałów dla prawdopodobieństwa oraz pięć przedziałów dla potencjalnych skutków wystąpienia ryzyka:

---

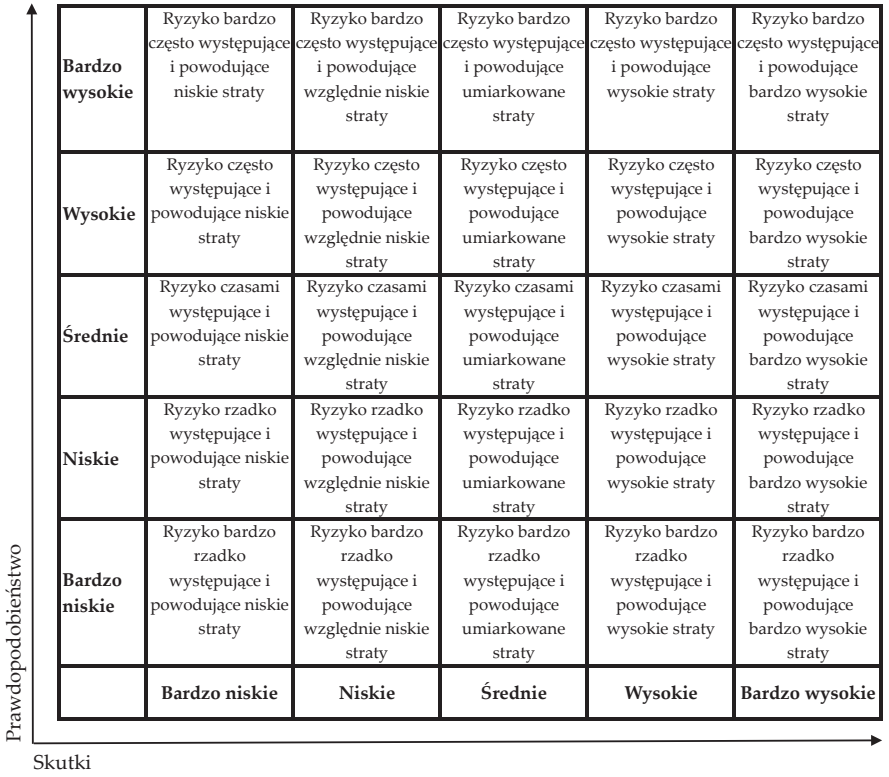
62 A. Liwacz, *Zarządzanie ryzykiem*, Poradnik Samorządowy, grudzień 2004, s. 28.

63 A. Kumpiałowska, *Skuteczne zarządzanie ryzykiem a kontrola zarządcza w sektorze publicznym*, Wydawnictwo C.H. Beck, Warszawa.2011 s. 78.
E. Lorek, *Pomiar ryzyka*, w: *Zarządzanie zintegrowanym ryzykiem przedsiębiorstw w Polsce*, Wolters Kluwers Polska Sp. z o.o., Warszawa 2001, s. 114-115.



Rysunek 5.9. Mapa ryzyka dla dwóch wartości prawdopodobieństwa i dwóch wartości skutków

Źródło: J. Zawarska, Identyfikacja i pomiar ryzyka w procesie zarządzania ryzykiem podmiotów gospodarczych

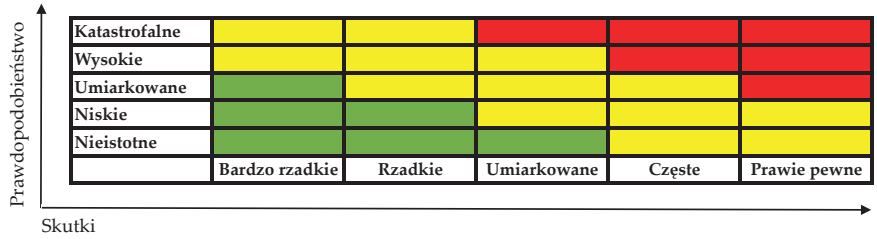


Rysunek 5.10. Mapa ryzyka dla pięciu wartości prawdopodobieństwa i pięciu wartości skutków

Źródło: Prezentacja Zakładu Ochrony Ludności CNBOP–PIB, Szacowanie ryzyka na potrzeby systemu ochrony ludności w Polsce. Stan obecny oraz kierunki przyszłych rozwiązań, materiał konferencyjny, Kraków 2014 r.

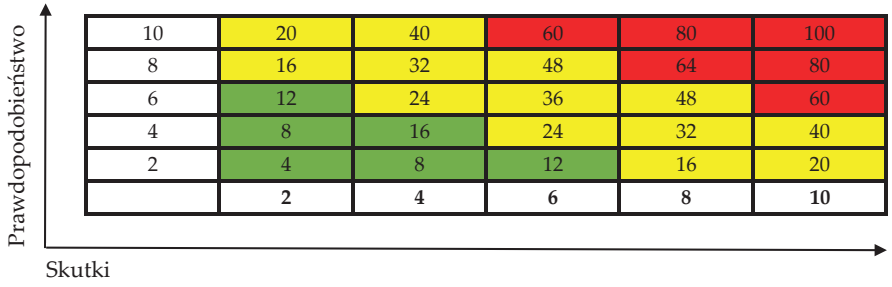
Szczegółowość map ryzyka zależy również od przyjętej metodologii zarządzania ryzykiem. Spotykane są najczęściej dwa rozwiązania: pierwsze, polegające na klasyfikacji ryzyka do deskryptywnych kategorii, określających konsekwencje jego wystąpienia, np. ryzyko nieistotne, niskie, umiarkowane, wysokie, katastrofalne, a także stratę ponoszoną w przypadku jego wystąpienia: prawie pewne (wystę-

pujące często, np. częściej niż raz w roku), częste, umiarkowane, rzadkie, bardzo rzadkie. Innym sposobem jest nadanie omawianym dwóm wymiarom punktacji w skali 1–5[64]. Poniżej przedstawiono obie opcje mapowania ryzyka:



Rysunek 5.11. Mapa ryzyka dla pięciu wartości prawdopodobieństwa i pięciu wartości skutków

Źródło: opracowanie własne na podstawie Procedury oparacowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, s. 17



Rysunek 5.12. Punktowa mapa ryzyka dla pięciu wartości prawdopodobieństwa i pięciu wartości skutków

Źródło: opracowanie własne na podstawie Procedury opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, s. 17

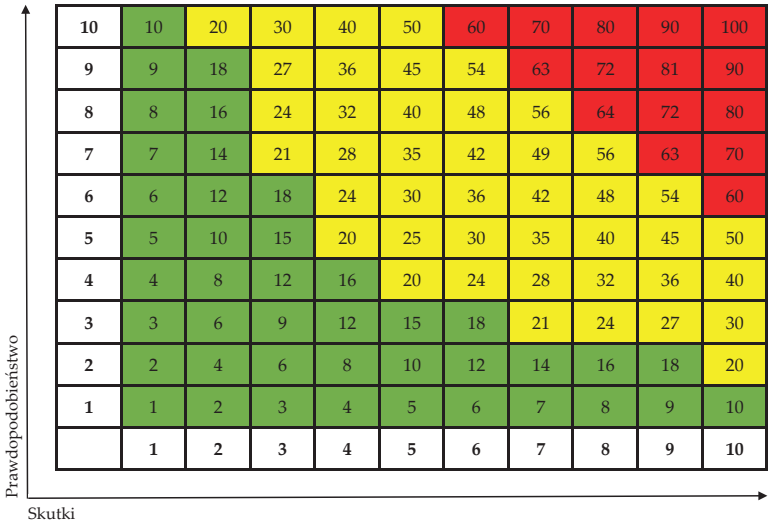
Punktowa ocena ryzyka umożliwia uporządkowanie rodzajów ryzyka i hierarchizację działań podejmowanych w celu zmniejszenia ryzyka:

- ryzyka znajdujące się w prawym, górnym rogu (kolor czerwony) wymagają pilnej uwagi organizacji,
- ryzyka znajdujące się w środku matrycy (kolor żółty) należy omówić i monitorować. W pewnych wypadkach organizacja może podjąć dalsze działania,
- ryzyka znajdujące się w lewym, dolnym rogu (kolor zielony) to najniższe zagrożenie dla organizacji.

Warto tu również zaznaczyć, że często można podjąć łatwo i szybko czynności, aby ryzyko średnie zamienić na niższe. Gorzej sytuacja wygląda z szybkim podjęciem działań dla ryzyk o bardzo wysokiej ocenie punktowej (zaznaczonych na kolor czerwony), gdzie czasami podjęcie jakichkolwiek czynności jest niemożliwe.

[64] R. Gabryelczyk, B. Dessoulavy-Śliwiński, *Mapowanie ryzyka w obszarze Facility Management*, Administrator, nr 4/2014.

Aby zwiększyć dokładność mapy ryzyka, należy zwiększyć liczbę przedziałów prawdopodobieństwa i/lub liczbę przedziałów dla skutków wystąpienia ryzyka.



10	10	20	30	40	50	60	70	80	90	100
9	9	18	27	36	45	54	63	72	81	90
8	8	16	24	32	40	48	56	64	72	80
7	7	14	21	28	35	42	49	56	63	70
6	6	12	18	24	30	36	42	48	54	60
5	5	10	15	20	25	30	35	40	45	50
4	4	8	12	16	20	24	28	32	36	40
3	3	6	9	12	15	18	21	24	27	30
2	2	4	6	8	10	12	14	16	18	20
1	1	2	3	4	5	6	7	8	9	10
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

Rysunek 5.13. Punktowa mapa ryzyka dla 10 wartości prawdopodobieństwa i 10 wartości skutków

Źródło: opracowanie własne na podstawie Procedury oparacowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, s. 17

Sporządzając mapę, należy rozważyć liczbę przedziałów nie tylko pod kątem ich ilości, ale także, czy matryca powinna mieć parzystą, czy nieparzystą ich liczbę. Wybór ma zasadnicze znaczenie dla określania wartości prawdopodobieństwa i skutków ryzyka. Szczególnie przy wykorzystaniu metod jakościowych bardzo często pojawia się pokusa określenia jego *bezpiecznego* poziomu przez wskazanie średnich (środkowych) wartości.

Mapa podatności to bardziej rozbudowana mapa ryzyka. Podatność określa wzajemną zależność, wrażliwość (narażenia) i odporność społeczności lokalnej i środowisk na zagrożenia. Mapy podatności związane są ze współzależnością zagrożeń i ekspozycją społeczności na te zagrożenia oraz gotowością cywilną tej społeczności[65]. Powstaje ona według następującego schematu:

- Dokładnie opisywany jest badany obszar. W charakterystyce zawiera się takie informacje, jak położenie geograficzne, administracyjne i komunikacyjne, liczba ludności, gęstość zaludnienia, systemy transportowe czy warunki klimatyczne.
- W kolejnym kroku identyfikuje się zagrożenia, które mogą wpływać na wcześniej wymienione charakterystyki oraz ich potencjalne skutki.
- Następnie przy użyciu programów modelujących prognozowane jest ryzyko zidentyfikowanych zagrożeń na badany obszar wraz z jego następstwami dla ludzi, mienia i środowiska.

[65] M. Kopczewski, K. Pająk, *Tworzenie map ryzyka i map podatności jako elementu zarządzania kryzysowego*, Zeszyty Naukowe WSOWL, nr 4/2011, s. 301.

- Kolejną procedurą przy tworzeniu mapy podatności jest ułożenie ankiet[66], które pozwolą na określenie podatności. Pierwsza ankieta określa wrażliwość na opisane w pkt. 1 elementy badanego obszaru, np. liczba ludności czy liczba obiektów publicznych. Każdemu kryterium przypisywana jest liczba punktów, które określają wrażliwość dla danego elementu. Oczywiście również jak przypadku map ryzyka im większa liczba kryteriów, tym mapa będzie dokładniejsza.

Liczba obiektów publicznych (szpitale, szkoły itp.)			
kryteria	>5	1-5	brak
punkty	2	4	2

Rysunek 5.14. Ankieta określająca wrażliwość

Źródło: M. Kopczewski, K. Pająk, Tworzenie map ryzyka i map podatności jako elementu zarządzania kryzysowego, Zeszyty Naukowe WSOWL, nr 4/2011, s. 303

Drugą ankietą jest ankieta odporności, gdzie każdej wyznaczonej wcześniej odporności przypisuje się punkty określające jej *siłę*.

Stan zabezpieczeń technicznych			
kryteria	niedostateczny	wystarczający	dobry
punkty	2	4	2

Rysunek 5.15. Ankieta określająca odporność

Źródło: M. Kopczewski, K. Pająk, Tworzenie map ryzyka i map podatności jako elementu zarządzania kryzysowego, Zeszyty Naukowe WSOWL, nr 4/2011, s. 304

Podatność wylicza się ze wzoru matematycznego:

$$podatność = wrażliwość + odporność$$

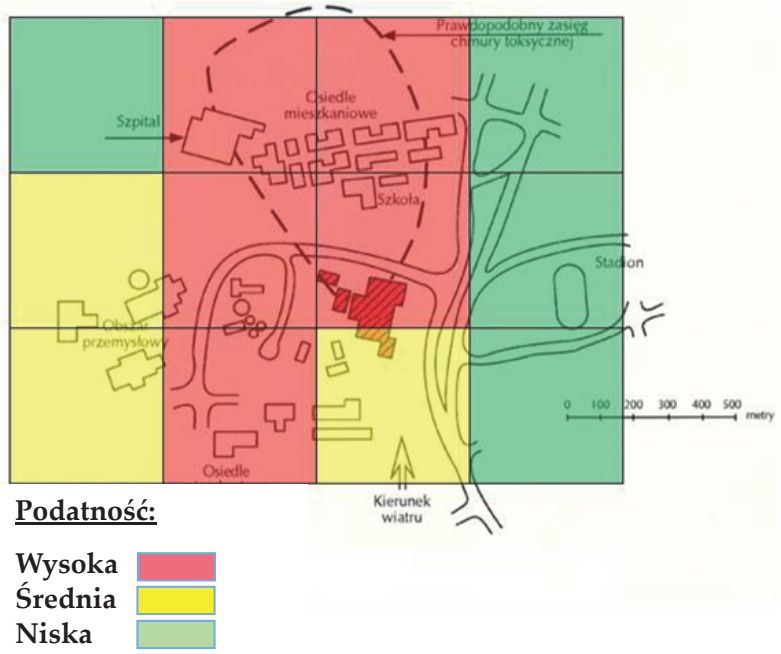
Dla każdej pozycji z ankiety wrażliwości i odporności sumuje się liczbę punktów. W zależności od wymagań dokładności mapy podatności, charakterystyki obszaru i jego zagrożeń tworzy się klasyfikację poziomu podatności. Przykład takiej klasyfikacji zawiera poniższy rysunek:

Poziom podatności	**Przedział punków**	**Kolor**
niski	<12	zielony
średni	12-12	żółty
wysoki	>24	czerwony

Rysunek 5.16. Klasyfikacja poziomu podatności

Źródło: M. Kopczewski, K. Pająk, Tworzenie map ryzyka i map podatności jako elementu zarządzania kryzysowego, Zeszyty Naukowe WSOWL, nr 4/2011, s. 304

[66] Tamże, s. 303-304.



Rysunek 5.17. Mapa podatności

Źródło: M. Kopczewski, K. Pająk, Tworzenie map ryzyka i map podatności jako element systemu zarządzania kryzysowego, Zeszyty Naukowe, WSOWL, nr 4 (162), 2011, s. 305

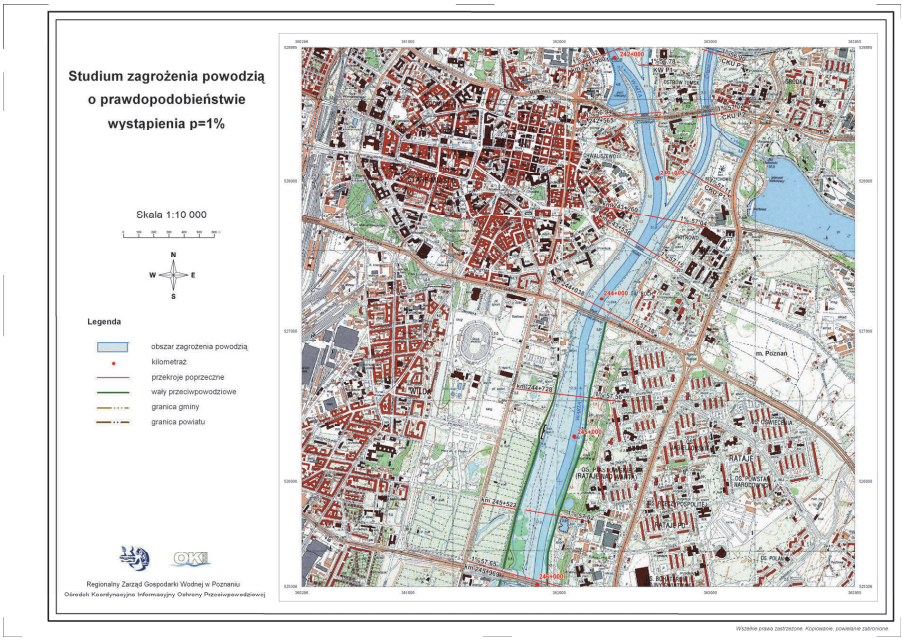
Na mapę ryzyka nakłada się siatkę kwadratów. Każdy kwadrat należy analizować oddzielnie na podstawie ustalonej wcześniej ankiety. Dla każdego pojedynczego kwadratu wylicza się podatność i przypisuje mu kolor z tabeli klasyfikacji poziomu podatności.

Mapa zagrożeń jest dokumentem zawierającym potencjalne zagrożenia dla życia, zdrowia oraz mienia ludzkiego z uwzględnieniem ich rozkładu przestrzennego i czasowego. Ma charakter retrospektywny (dokumentacyjny), ponieważ odzwierciedla zagrożenia już dostrzeżone i zarejestrowane, np. na przełomie ostatnich kilku lat przez służby oraz inspekcje, które uczestniczą w likwidacji zagrożeń[67]. Mapa zagrożeń powinna uwzględniać zagrożenia o różnym charakterze zarówno zewnętrzne, jak i wewnętrzne oraz oddziałujące na procesy i informacje mające wpływ na bezpieczeństwo.

Mapa powinna także identyfikować krytyczne procesy i przewidywać możliwe straty w wyniku ich wystąpienia[68].

[67] Mapa zagrożeń powiatu wrocławskiego, październik 2014 r.

[68] Witryna internetowa http://www.powiatwroclawski.pl/index.php?option=com_content&id=1142:mapa-zagroe-powiatu-wrocawskiego&Itemid=80 z dnia 04.09.2014 r.



Rys. 5.18. Analiza zabezpieczenia przeciwpowodziowego miasta Poznania ze wskazaniem stref zalewowych dla wód o prawdopodobieństwie wystąpienia p=1%;

Źródło: Analiza zabezpieczenia przeciwpowodziowego miasta Poznania ze wskazaniem stref zalewowych dla wód o prawdopodobieństwie wystąpienia p=10% p=1% p=0,5% z wykorzystaniem matematycznego modelu Mike Flood, Regionalny Zarząd Gospodarki Wodnej w Poznaniu Ośrodek Koordynacyjno-Informacyjny Ochrony Przeciwpowodziowej

Wybrane metody opracowane zostały na podstawie *Procedury opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego*, norm zagranicznych oraz dostępnej literatury. Dokument wykazuje szeroką różnorodność metod, które mogą zostać wykorzystane.

Zwykle ryzyko dotyczy możliwości poniesienia szkody lub straty, jednak można je rozpatrywać także pod kątem szansy (pozytywnego rezultatu) lub zagrożenia (negatywnego skutku). Zatem ryzyko należy postrzegać jako determinantę każdego procesu decyzyjnego.

Identyfikację ryzyka można osiągnąć przez identyfikację przyczyn i efektów, a opisy źródeł ryzyka powinny zasadniczo zawierać szacunki:

- prawdopodobieństwa wystąpienia zagrożenia,
- zakres możliwych rezultatów,
- przewidywany czas,
- częstotliwość zdarzeń ryzyka z danego źródła.

Identyfikacja zagrożeń powinna być ściśle związana z określonymi w planie danej działalności organizacji zadaniami oraz determinowana celami, jakie mają być osiągnięte poprzez realizację tych zadań. Ponadto powinna być ona procesem

powtarzalnym (systematycznym), zintegrowanym z procesem planowania działalności. Podczas tej oceny powinny być brane pod uwagę wszelkie możliwe ryzyka, które mogą się pojawić i tym samym wpływać na osiągnięcie zamierzonych celów, a także ich źródła. W procesie identyfikacji zagrożeń konieczna jest dokładna znajomość jednostki, jej otoczenia oraz zrozumienie wspomnianych celów i zadań oraz czynników kluczowych dla osiągnięcia jej sukcesu. Należy zaznaczyć, że proces zarządzania ryzykiem przyniesie wymierne korzyści dla organizacji wtedy, gdy będzie dokonywana rzetelna identyfikacja i ocena ryzyka, a informacje generowane z systemu zarządzania ryzykiem znajdą zastosowanie w codziennym zarządzaniu jednostką. Kluczowym zasobem w procesie identyfikacji ryzyka jest informacja. Zbieranie i przetwarzanie informacji jest warunkiem koniecznym do rozpoznania problemu we wczesnym etapie. Stałe gromadzenie informacji generuje więcej uporządkowanych i wyraźnych dowodów potencjalnych zmian w środowisku zewnętrznym. Ważne jest poszerzenie zakresu dostępnych źródeł oraz dostępu do nich, dzięki czemu wykorzystanie zebranych informacji stanie się bardziej efektywne. Pojawienie się społeczeństwa informacyjnego sprzyja ogromnemu postępowi w dziedzinie technologii informacyjnych i komunikacyjnych i niewątpliwie ułatwia dostęp do ogromnej ilości informacji. Identyfikacja ryzyka powinna być przeprowadzona na wszystkich poziomach administracji publicznej, ze względu na wzrastającą liczbę nowych zagrożeń oraz w celu łatwiejszego określenia ich kategorii. W procesie identyfikacji ryzyka istotne jest wnikliwe przeanalizowanie potencjalnych czynników ryzyka, czyli zdarzeń, które mogą spowodować wystąpienie ryzyka.

Identyfikacja zagrożeń ma fundamentalne znaczenie, ponieważ ryzyka, które nie zostaną rozpoznane na tym etapie, nie będą brane pod uwagę na dalszych etapach zarządzania ryzykiem. Dlatego proces ten powinien być przeprowadzony w sposób jak najbardziej dokładny.

Dobór metody jest kwestią dobrowolną i zależy od przeprowadzającego identyfikację ryzyka. Prosta metoda, odpowiednio przeprowadzona, może zapewnić lepsze wyniki niż bardziej wyrafinowane procedury zrobione źle.

Kolejnymi scharakteryzowanymi metodami były metody pozwalające na określenie poziomu akceptowalności zidentyfikowanego ryzyka oparte na modelu scenariuszowym oraz analizy przypadku. Pierwsza z nich mogłaby zostać użyta w odniesieniu do zidentyfikowanych zagrożeń pod warunkiem opracowywania względnie szczegółowych scenariuszy możliwych zdarzeń, o różnej skali ich intensywności (*najlepszy możliwy przypadek*, *spodziewany przypadek*, *najgorszy możliwy przypadek*). Z kolei druga może znaleźć swoje zastosowanie w odniesieniu do konieczności określenia poziomu akceptowalności ryzyka przy wykorzystaniu do tego celu analizy danych historycznych. W pierwszym modelu wsparcie dla budowy scenariuszy możliwych zdarzeń mogłyby stanowić takie metody, jak: analiza SWOT, BIA, ETA, FTA, Bow-tie czy *Co jeśli?* W obu omawianych modelach należy rozważyć mozliwość przeprowadzenia analizy kosztów i korzyści, która wskazywałaby, czy podjęcie działań mających na celu zapobieganie lub redukcję zidentyfi-

kowanego ryzyka przyniosłoby więcej korzyści i mniejsze koszty, niż powstrzymanie się od wszelkich działań i podjęcie decyzji o akceptacji ryzyka.

Zdaniem autorów kluczowe znaczenie przy podjęciu decyzji o akceptacji zidentyfikowanego ryzyka ma określenie relacji pomiędzy poziomem ryzyka *początkowego* (wyznaczonego przez pryzmat istniejących zabezpieczeń) a poziomem ryzyka *pożądanego*, tj. poziomu oczekiwanego przy wykorzystaniu dodatkowych środków bezpieczeństwa. Wartości te mają charakter umowny. Analiza istniejących oraz potencjalnych rozwiązań w dziedzinie bezpieczeństwa, w odniesieniu do obu zdefiniowanych wskaźników, powinna prowadzić do przeprowadzenia analizy korzyści i strat, będącej decydującym wyznacznikiem akceptacji ryzyka lub jej braku. W proponowanym rozwiązaniu kończy się ona wyborem jednej z trzech kategorii akceptacji ryzyka, tj. ryzyka akceptowanego, ryzyka tolerowanego lub ryzyka nieakceptowanego.

Nie ulega wątpliwości, że działania te są niezwykle istotne z uwagi na potrzebę efektywnego podziału środków finansowych w obszarze zarządzania kryzysowego. Zapobieganie lub przygotowanie się na wszystkie warianty potencjalnych zdarzeń nie jest możliwe. Jednakże właściwie przeprowadzona analiza ryzyka pozwala na wskazanie ryzyk największych, nieakceptowalnych, czyli takich, gdzie skutki mogą być najbardziej dotkliwe, a zatem takich, w stosunku do których należy skierować dodatkowe środki finansowe, prawne czy organizacyjne. Pytaniem otwartym pozostaje, w jaki sposób w omawianym podejściu uwzględnić wartości niepoliczalne w pieniądzu, w tym np. życie ludzkie.

Rozdział prezentuje również obecnie wykorzystywane sposoby prezentacji ryzyka. Biorąc pod uwagę obszar badań, należy wskazać, że pojęcie map można odnieść do trzech kategorii, jakimi są: ryzyko, podatność oraz zagrożenie. Każda z tych kategorii prezentuje inny wymiar przeprowadzanej analizy. Samo ryzyko najczęściej prezentowane jest w postaci dwuwymiarowej matrycy, która odnosi się do wartości skutków i prawdopodobieństwa – przy czym ich skala jest determinowana celami i procesami zachodzącymi w organizacji. Mapa podatności stanowi niejako uzupełnienie map ryzyka i pozwala na odczytanie na mapie (fizycznej lub geograficznej) poziomu odporności terenu na ryzyko pierwotne. Obie te mapy (a więc i wartości w nich ukazane) wzajemnie się uzupełniają i występuje pomiędzy nimi zależność – im większa podatność (suma wrażliwość i odporności), tym ryzyko jest wyższe. Przy analizie ryzyka wystąpienia zagrożeń naturalnych oraz awarii technicznych (które mają swoje odniesienie geograficzne) wrażliwość terenu będzie podnosiła poziom ryzyka, natomiast odporność (np. sposób zorganizowania ochrony przed tymi zagrożeniami) obniżała. Wskazane rodzaje map odnoszą się do potencjalnych niekorzystnych zdarzeń. Natomiast ostatnim trzecim rodzajem map omówionym w badaniu są mapy zagrożeń, które prezentują dane o zdarzeniach mających miejsce w przeszłości.

Tworzenie map jest jednym z ostatnich elementów procesu szacowania ryzyka. Stanowią wizualizację przeprowadzonej analizy i pozwalają w jasny i przejrzysty sposób zaprezentować efekty badań.

6. Zastosowanie metody foresight do identyfikacji zagrożeń bezpieczeństwa narodowego

Metoda foresight jest jednym ze sposobów analizy otoczenia[1], który najtrafniej można opisać przy użyciu terminów proces[2] i perspektywa[3]. Istotą tej metody jest obserwacja, analiza i ewaluacja informacji. Foresight jako proces polega na konfrontacji własnej wiedzy, własnych doświadczeń – z innymi scenariuszami. Metoda ta, niejako wymuszając konieczność spojrzenia na inne punkty widzenia – w pewnym zakresie umożliwia weryfikację dotychczasowych wzorców myślenia[4]. Foresight jako proces tworzenia wizji polega na integracji różnych perspektyw, czy inaczej rzecz ujmując, na swoistym uzgadnianiu preferencji[5], przyczyniając się w ten sposób do tworzenia perspektyw dla przyszłości[6], do rozwoju koncepcji alternatywnych[7].

Foresight jest tylko jedną z możliwości, jednym z narzędzi pozwalających podjąć próbę i to próbę (co szczególnie wyraźnie należy podkreślić) ograniczonego poznania rzeczywistości. Nie daje gotowych odpowiedzi, ani tym bardziej odpowiedzi pewnych, ostatecznych i komplementarnych. Dostarcza raczej nowych punktów widzenia, częściowo poszerza horyzonty i właśnie w ten sposób umożliwia badaczowi, jak się wydaje, lepsze, nieco pełniejsze zrozumienie. Należy w tym miejscu stwierdzić, że to już jest bardzo dużo.

Zatem, projektując badanie, warto przyjąć dwa założenia. Po pierwsze, że rzeczywistość społeczna nie jest, tak jak rzeczywistość materialna, czymś *gotowym*. Rzeczywistość społeczna znajduje się w ciągłym procesie tworzenia, którego charakterystyczną cechą jest zmiana[8]. Po drugie, że nie ma żadnej *obiektywnej*

---

1 *Foresight jako metoda kształtowania przyszłości. Identyfikacja potencjału i zasobów Dolnego Śląska w obszarze nauka i technologie na rzecz poprawy jakości życia,* Safin K. (red.), Uniwersytet Ekonomiczny we Wrocławiu, Katowice 2010, s. 11.

2 K. Borodako, *Foresight w zarządzaniu strategicznym*, Wydawnictwo C.H. Beck, Warszawa 2009, s. 12.

3 Ł. Mamica, P. Kopyciński, *Foresight technologiczny na rzecz zrównoważonego rozwoju Małopolski*, w: *Foresight regionalny i technologiczny. Pierwsze doświadczenia polskich regionów*, A. Klasik, T. Markowski (red.), Komitet Przestrzennego zagospodarowania kraju PAN, Warszawa 2010, s. 107.

4 *Foresight jako metoda kształtowania przyszłości*, dz. cyt., s. 11.

5 Tamże.

6 Ł. Mamica, P. Kopyciński, art. cyt., s. 107.

7 *Foresight jako metoda kształtowania przyszłości*, dz. cyt., s. 11.

8 J. Niżnik, *Przedmiot poznania w naukach społecznych*, Państwowe Wydawnictwo Naukowe, Warszawa 1979, s. 5.

rzeczywistości, którą można by obserwować. Jeśli już, to istnieją subiektywne perspektywy jej oglądu[9]. Takie podejście pozwoli zachować odpowiednią ostrożność wobec znaczenia uzyskanych wyników, a tym samym możliwości ich zastosowania w praktyce życia społecznego. Jednocześnie, co warto zauważyć, może być ono też (i to nie mimo tych ograniczeń, a właśnie ze względu na nie) zachętą do kontynuacji badań, doskonalenia narzędzi, jak i poszukiwania nowych metod. Zapotrzebowanie na wiedzę o rzeczywistości społecznej to właśnie ten moment, w którym ujawnia się słabość nauk społecznych i zarazem sytuacja, która zmusza do intensyfikacji poszukiwań skutecznych sposobów przezwyciężania istniejących słabości[10].

6.1. Możliwości eksploracji obszaru bezpieczeństwa narodowego przy zastosowaniu metody foresight

Poszukiwanie nowych sposobów opisu rzeczywistości w obszarze bezpieczeństwa bierze się z głębokiej potrzeby namysłu nad nim. Ciągłe poszukiwania nowych i bardziej adekwatnych do współczesnego, szybko zmieniającego się świata, metod pozwala zrozumieć, czym bezpieczeństwo jest warunkowane i co go destabilizuje.

Toczący się dyskurs w tym zakresie zakłada, że bezpieczeństwo w przeszłości i obecnie warunkuje możliwości przetrwania ludzi. Jednak przeżycie nie jest w tych rozważaniach jedyną wartością. Bezpieczeństwo nie tylko zapewnia byt jednostki, czy też społeczności, ale zapewnia również odpowiedni komfort życia[11]. Uznać zatem należy, że zakres pojęcia bezpieczeństwa jest zmienny, a tym samym, że wskazanie poziomu, od którego zaczyna się dysfunkcja bezpieczeństwa, uwarunkowane jest m.in. oczekiwaniami, czy dokładniej – obowiązującym standardem. Zmiany w postrzeganiu poziomu życia rozumiane jako polepszenie warunków egzystencjalnych, wzrost oczekiwań, a także towarzyszący im, jak i będący przyczyną wspomnianych zmian – rozwój nauki (badań nad bezpieczeństwem) powodują, że coraz bardziej powiększa się zakres tego, co pewne, przewidywalne. To z kolei powoduje wzrost oczekiwań, potrzeb odnoszących się do poziomu poczucia bezpieczeństwa. Niewątpliwie dążenie do zapewnienia bezpieczeństwa było jedną z głównych sił napędowych w ewolucji społecznej ludzi[12]. Oczywiście z zastrzeżeniem, że człowiek coraz dokładniej poznaje otaczającą go przestrzeń, ale jej znaczna część pozostaje nadal niezbadana. W obszarze rzeczywistości społecznej dodatkowo problemem są narzędzia, które dają dość ograniczone możliwości badania rzeczywistości, oraz są obciążone subiektywizmem.

---

[9] E. Babbie, *Podstawy badań społecznych*, przekł. Betkiewicz W. i in., Wydawnictwo Naukowe PWN, Warszawa 2008, s. 27.

[10] J. Sztumski, *Wstęp do metod i technik badań społecznych*, „Śląsk", Katowice 1999, s. 13.

[11] J. Wolanin, *Zarys teorii bezpieczeństwa obywateli. Ochrona ludności na czas pokoju*, Danmar, Warszawa 2005, s. 13.

[12] Tamże.

Nie ulega jednak wątpliwości, że każdy człowiek chce czuć się bezpiecznie i że to bezpieczeństwo jest jedną z jego najważniejszych potrzeb[13]. Niezależnie od form organizacyjnych, w których przychodzi ludziom funkcjonować, rozwoju cywilizacyjnego czy poziomu edukacji bezpieczeństwo nadal pozostaje fundamentalną potrzebą. Zmianie jednak ulegają wymogi dotyczące bezpieczeństwa, poszerza się liczba płaszczyzn, które mają być chronione. Zmiany dotyczą też dostępnych, względnie możliwych do zastosowania środków. Zmienia się w związku z tym perspektywa bezpieczeństwa.

Z punktu widzenia celu niniejszych rozważań należy przyjąć perspektywę organizacji. Otoczenie zewnętrzne organizacji charakteryzuje się stałą zmiennością, wymuszając konieczność przystosowywania się do niego[14]. Tak samo państwo musi dostosowywać się do zmieniających warunków wewnętrznych i zewnętrznych, realizując m.in. funkcję adaptacyjną, która umożliwia mu zachowanie kontroli, dającej się opisywać w kategoriach sprawności i skuteczności[15]. Biorąc to pod uwagę, organizacje należy zaliczyć do systemów otwartych, ponieważ suma ryzyk wynikająca z poszczególnych szczegółowych scenariuszy, odnoszących się bezpośrednio do elementów struktury danej organizacji, nie równa się ryzyku, dotyczącemu całej organizacji. Dzieje się tak, ponieważ organizacja nie jest prostą sumą jej strukturalnych elementów. Elementy struktury danej organizacji połączone w całość tworzą zupełnie nową jakość, a zatem stosowanie metod z układów zamkniętych (w których suma ryzyk poszczególnych elementów jest ryzykiem całkowitym) do układów otwartych, ma znacznie ograniczony charakter[16]. W związku z powyższym, projektując działania organizacji, jako punkt wyjścia należy przyjmować cały system, a więc wszystkie jego elementy i powiązania oraz uwzględniać następstwa poszczególnych działań dla całości i poszczególnych jego części.

Organizacja (np. państwowa, biznesowa) korzysta z zasobów otoczenia zewnętrznego i przez to jest już od niego zależna. Można wymienić tu m.in. procesy globalizacyjne, które są następstwem wychodzenia organizacji poza dotychczasowe ramy. Procesy te stanowią równocześnie środowisko, do którego organizacja musi się dostosowywać. Zależność tę najprościej opisać można tak, że organizacja zarówno przetwarza zasoby pochodzące z otoczenia, ale też oddaje otoczeniu przetworzone przez nią zasoby[17]. Organizacja zatem jest modyfikowana przez otoczenie i w pewnym zakresie sama oddziałuje na jego kształt.

Skuteczność działania organizacji w określonym środowisku zależy od jej zdolności adaptacyjnych do warunków otoczenia. Te warunki otoczenia charakteryzują: wysoka i zarazem rosnąca niejasność, niepewność, presja czasu, nie-

---

13 Tamże.

14 J.M. Baugier, S. Vuillod, *Strategie zmian w przedsiębiorstwie. Nowoczesna metoda*, przekł. Egeman M., Poltext, Warszawa 1993, s. 11.

15 P. Winczorek, *Wstęp do nauki o państwie*, LIBER, Warszawa 2000, s. 128.

16 J. Wolanin, dz. cyt., s. 31.

17 M. Kukurba, *Miejsce i rola rachunkowości zarządczej w systemie zarządzania przedsiębiorstwem (wybrane zagadnienia)*, Zeszyty Naukowe Wyższej Szkoły Zarządzania 2003, nr 2, s. 5-6.

dostępność i nieprecyzyjność ważnych informacji[18]. Stąd też miarą efektywności organizacji są jej zdolności adaptacyjne[19].

Jest to jednak jeden z modeli funkcjonowania organizacji, ponieważ ze względu na rodzaj relacji organizacji z otoczeniem zewnętrznym wyróżnia się trzy rodzaje systemów: deterministyczne, stochastyczne oraz adaptacyjne[20]. Systemy deterministyczne odznaczają się znaczną łatwością przewidywania zmian. Z kolei systemy stochastyczne charakteryzują się małą przewidywalnością zmian, a znaczny współczynnik błędu prognoz w tych systemach jest następstwem zmiennego i nieprzewidywalnego otoczenia. W systemach tych próbuje się podejmować działania zaradcze, jakimi są planowanie i kontrola elementów mających wpływ na funkcjonowanie systemu[21]. Jednakże trzeba tu mieć na uwadze, że proces planowania w organizacji biznesowej jest zazwyczaj utrudniony. Barierą są już same uwarunkowania, w jakich planowanie jest prowadzone. Podstawowym ograniczeniem jest niepewność co do przyszłego rozwoju. Jeśli spojrzeć na wielość zadań podlegających planowaniu, to widać, że koniecznością staje się każdorazowe uwzględnianie znacznej liczby zmiennych, często wzajemnie od siebie zależnych. Im większa liczba elementów, które należy wziąć pod uwagę, tym większa nieprzewidywalność. Tym większa niepewność, ryzyko. Rozpatrując to w odniesieniu do sytuacji modelowej, zauważyć należy, że zapewne możliwe byłoby uzyskanie takich niezbędnych danych ilościowych. Jednak zazwyczaj dostępne są jedynie dane jakościowe. Znaczenie obserwacji jakościowych jest jednak ograniczone do poszczególnych zdarzeń, w odniesieniu do których je poczyniono. Ze względu na to, że rzeczywistość nie ma charakteru statycznego i charakteryzuje się znacznym stopniem zmienności, zagrożeniem staje się również powielanie działań, planów, które nie uwzględniają zmieniających się warunków[22].

W systemach adaptacyjnych natomiast zdolność stałego dostosowywania się do zmieniającego otoczenia osiągana jest poprzez wdrożenie systemu permanentnego reagowania oraz dostosowywania do zmian systemu jako całości[23]. Adaptacyjność struktur to zdolność przystosowania istniejących struktur do realizowania innych niż dotąd funkcji. Jej utrzymanie wiąże się jednak ze znacznymi kosztami, które wpływać mogą ujemnie na sprawność ekonomiczną organizacji. Ponadto ograniczeniem jest również to, że adaptacyjność jest znacząco ograniczona w dużych, zbiurokratyzowanych organizacjach. W tej sytuacji zabezpieczeniem mogą okazać się elastyczne struktury, lub opóźnienie momentu podjęcia decyzji o dzia-

[18] T. Zaleśkiewicz, *Organizacje wobec niepewności. O naturalistycznym paradygmacie w badaniu decyzji menedżerskich*, w: *Organizacje – wyzwania i zagrożenia. Perspektywa psychologiczna*, Strykowska M. (red.), Wydawnictwo Fundacji Humaniora, Poznań 2002, s. 75.

[19] Tamże, s. 75.

[20] M. Kukurba, art. cyt., s. 5-6.

[21] Tamże.

[22] H. Kreikebaum, *Strategiczne planowanie w przedsiębiorstwie*, przekł. Zawisza W., Wydawnictwo Naukowe PWN, Warszawa 1996, s. 24-25.

[23] M. Kukurba, art. cyt., s. 5-6.

łaniu w stosunku do rozpoczęcia danego działania, a więc realizacja określonych działań w jak najkrótszym czasie od podjęcia decyzji[24].

Złożona i wysoce wyspecjalizowana, zbiurokratyzowana struktura państwowa staje się ze względu na znacznie rozbudowany aparat państwowy ociężała w kwestii reagowania na nietypowe zjawiska, a z drugiej strony ta nieustannie rozwijająca się specjalizacja, pogłębiająca się szczegółowość państwa ma na celu stworzenie warunków dla lepszej ochrony przed niepożądanymi zdarzeniami. Tak jak duża organizacja biznesowa jest silna i odznacza się wysokim stopniem sprawności, ale jednocześnie staje się powolna, tak samo współczesne państwo odznacza się podobnymi właściwościami.

Aby lepiej zrozumieć działanie organizacji państwowej, należy wskazać na wyzwania bezpieczeństwa narodowego. Bezpieczeństwo narodowe to stan uzyskiwany w wyniku odpowiednio zorganizowanej obrony i ochrony przed zagrożeniami zewnętrznymi i wewnętrznymi. Stan ten określa się stosunkiem potencjału obronnego do skali zagrożeń[25]. Należy podkreślić, że bezpieczeństwo narodowe jest nie tylko ochroną narodu i terytorium przed fizyczną napaścią, lecz również (a może przede wszystkim) ochroną, za pomocą różnych środków, żywotnych interesów ekonomicznych i politycznych, których utrata zagroziłaby żywotności i podstawowym wartościom państwa[26]. Pisząc o bezpieczeństwie narodowym, nie można pominąć również aspektu subiektywnego, bezpieczeństwo narodowe bowiem to również stan świadomości społecznej[27]. Tak zdefiniowany wielowymiarowy charakter bezpieczeństwa narodowego warunkuje znacznie rozbudowany zasób instrumentów, działań niezbędnych do jego utrzymania bądź osiągnięcia. Odpowiedzialność organizacji państwowej, niewątpliwie przewyższając zakres odpowiedzialności organizacji biznesowej, ze względu na realizowane zadania niejako wymusza zastosowanie kompleksowych metod analitycznych do zarządzania ryzykiem. Zatem użyteczność metody foresight w sferze biznesu może, przy zachowaniu świadomości tych ograniczeń, stanowić przesłankę do zastosowania jej w badaniu bardziej złożonego obszaru rzeczywistości społecznej, jakim jest bezpieczeństwo narodowe.

W ujęciu systemowym, rozumianym jako sieć powiązanych i wzajemnie oddziałujących na siebie elementów (stanowiących pewien określony zbiór, który obejmuje całość rzeczywistości społecznej, a w jej ramach poszczególne podsystemy), który bezpośrednio wiązać należy ze wspomnianym wyżej rozwojem społecznym, bezpieczeństwo to stan, który umożliwia normalny rozwój państwa, czyli pomyślną realizację wszystkich jego celów. Osiągnięcie tego stanu możliwe jest w wyniku zorganizowanej ochrony i obrony przed wszelkimi zagrożeniami, przy

---

[24] *Zarządzanie strategiczne. Systemowa koncepcja biznesu*, Moszkowicz M. (red.), Polskie Wydawnictwo Ekonomiczne, Warszawa 2005, s. 43.

[25] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Pawłowski J. i in. (opr.), Akademia Obrony Narodowej, Warszawa 2002, s. 16.

[26] Tamże, s. 15.

[27] Tamże.

użyciu sił i środków pochodzących ze wszystkich dziedzin działalności państwa[28]. Na potrzeby niniejszych rozważań przyjęto, że poszczególne obszary bezpieczeństwa (rozpatrywane osobno) nie warunkują bezpieczeństwa w sensie szerokim (bezpieczeństwa narodowego). Możliwość taką stwarza dopiero suma poszczególnych komponentów. Zatem rozpatrywanie bezpieczeństwa musi mieć wymiar systemowy, a jeśli tak, konieczne jest zastosowanie podejścia interdyscyplinarnego.

Patrząc na zmienne konstruujące pojęcie bezpieczeństwa, daje się zaobserwować, że podstawową kategorią bezpieczeństwa są zagrożenia. Zagrożenia jako takie nie stanowią kategorii samoistnej, ponieważ zawsze odnoszą się do danego podmiotu, dla którego mają charakter destrukcyjny[29]. Zależność tego typu znacząco podnosi poziom niepewności, a zarazem utrudnia badanie samych zagrożeń. I to nie tylko ze względu na ich różnorodność, ale także ze względu na brak powtarzalności, regularności i subiektywność ocen.

Nie należy jednak na tej podstawie zakładać, że bezpieczeństwo jest stanem nieosiągalnym. Z pewnością bezpieczeństwo w ujęciu modelowym, idealnym pozostaje poza możliwościami ludzi. Jednak potencjalnie możliwe są stany zbliżone do takich modelowych ujęć. Ponad wszelką wątpliwość zaprojektowanie rzeczywistości idealnej nie przełoży się na budowę takiej rzeczywistości, czyli na stworzenie systemu zabezpieczeń, który całkowicie je wyeliminuje, powstrzyma. Należy zatem stwierdzić, że możliwe jest zbudowanie systemu, który będzie zdolny do reagowania na zagrożenia, ale przy uwzględnieniu jego stałej tendencji do dysfunkcji.

Przyjęcie podejścia systemowego, wskazującego na wielość komponentów tworzących bezpieczeństwo narodowe, prowadzi do kolejnego założenia, zgodnie z którym osiągnięcie bezpieczeństwa jest możliwe w wyniku działań zorganizowanych (zbiorowych) oraz nieprzypadkowych, zaplanowanych, będących następstwem, czy też warunkowanych swoistym zobowiązaniem, jakie leży u podstaw organizacji państwowej. Z tych powodów właściwą do badań nad identyfikacją zagrożeń wydaje się właśnie metoda foresight. Bezpieczeństwo jest bowiem dobrem publicznym[30] i to nie mimo swej różnorodności, ale właśnie ze względu na nią. To państwo ma obowiązek, ale i możliwości poszukiwania optymalnych, najmniej uciążliwych dla obywateli rozwiązań w zakresie bezpieczeństwa. W związku z powyższym, wskazać też należy na postępującą tendencję do zastępowania terminu *foresight technologiczny* terminem *foresight*, ze względu na coraz częstsze zastosowania tej metody w dziedzinach nietechnicznych. Warto również zauważyć, że zadania w obrębie foresight technologii często w równej mierze dotyczą kwestii gospodarczych, społecznych oraz kulturowych i rozwoju technologicznego[31].

---

[28] J. Gierszewski, *Bezpieczeństwo wewnętrzne. Zarys systemu. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2013, s. 12.

[29] Tamże, s. 24.

[30] J. Wolanin, dz. cyt., s. 17.

[31] *Foresight technologiczny. Podręcznik. t. 1. Organizacja i metody*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2007, s. 8.

Patrząc przez pryzmat zagrożeń należy wskazać, że stan bezpieczeństwa to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni. Ze względu na taki sposób klasyfikacji wyróżnia się m.in.: bezpieczeństwo globalne, regionalne, narodowe; bezpieczeństwo militarne, polityczne, społeczne; bezpieczeństwo fizyczne, psychiczne, socjalne; bezpieczeństwo strukturalne i personalne[32]. Kategoria bezpieczeństwa jest więc zasadniczym punktem odniesienia we wszelkich działaniach podejmowanych przez ludzi, którzy dążą do maksymalizacji pewności i przewidywalności. Tak samo każda organizacja przygotowuje swoje przyszłe działania, w okresie kilkuletnim opierając się zazwyczaj na przyjętej przez siebie strategii. Natomiast w horyzoncie co najmniej piętnastoletnim, kiedy nie wszystko da się ustalić i przed wszystkim niepożądanym zabezpieczyć, przygotowuje się, przeprowadzając właśnie badania typu foresight[33].

Ogólna zasada przyjmowana w tego typu badaniach zakłada, że foresight musi odnosić się do okresu dłuższego od normalnego horyzontu planowania[34]. I to właśnie ta potrzeba i chęć przewidywania kierunków zdarzeń w momencie, kiedy są one w odpowiednio wczesnym stadium rozwoju, a czas reagowania jest odpowiednio długi, charakteryzują istotę metody foresight[35].

Foresight zaliczany jest do grupy badań złożonych i niepewnych, ponieważ stara się antycypować przyszłość w odniesieniu do licznych oddziałujących na nią czynników: społecznych, technologicznych, ekonomicznych, ekologicznych i politycznych[36]. Wskazuje się w tym kontekście, że nawet foresight technologiczny nie powinien być zdominowany wyłącznie przez naukę i technologię. Dlatego w przypadku tak zorientowanych badań zwraca się szczególną uwagę na znaczenie czynników społeczno-gospodarczych, które również mają wpływ na kształtowanie innowacji[37], przyjmując w zadaniach foresightu perspektywy zorientowane na takie problemy, jak: zapobieganie przestępczości, edukacja oraz umiejętności, starzejące się społeczeństwa[38].

Badania foresight należą do grupy studiów nad przyszłością[39]. Można w nich wyróżnić trzy powiązane ze sobą elementy: otwarcie na przyszłość z wykorzystaniem wszystkich możliwych środków, rozwój opinii na temat przyszłych wersji przyszłości, a następnie wybór jednej z nich[40]. Jego podstawowym założeniem jest równoczesna realizacja trzech zadań:

1) przemyślenia przyszłości,
2) przeprowadzenia na jej temat specjalistycznej publicznej debaty,

---

32 *Słownik terminów z zakresu bezpieczeństwa narodowego*, s. 13.
33 L.J. Jasiński, *Myślenie perspektywiczne. Uwarunkowania badania przyszłości typu foresight*, Instytut Nauk Ekonomicznych Polskiej Akademii Nauk, Warszawa 2007, s. 9.
34 *Foresight technologiczny. Podręcznik. t. 1*, s. 8.
35 *Foresight jako metoda kształtowania przyszłości*, s. 8.
36 K. Borodako, dz. cyt., s. 11.
37 *Foresight technologiczny. Podręcznik. t. 1*, s. 8.
38 Tamże.
39 L.J. Jasiński, dz. cyt., s. 9.
40 K. Borodako, dz. cyt., s. 11.

3) podjęcia w krótkim czasie działań na rzecz odpowiedniego jej ukształtowania[41].

Należy w tym miejscu wskazać, że foresight jest procesem: systematycznym, partycypacyjnym, pozwalającym na gromadzenie wiedzy dotyczącej przyszłości, polegającym na budowaniu wizji rozwoju w średniookresowej i długookresowej perspektywie, przy równoczesnym zorientowaniu na obecne decyzje i wymuszającym wspólne działania[42]. Analizując specyfikę badań foresight, należy zauważyć, że cały wysiłek badawczy koncentruje się właśnie na budowaniu wizji. Można tu postawić zarzut, że sama wizja jako taka jest dopiero pewnym wyobrażeniem, które niekoniecznie musi być ugruntowane na poziomie danej dyscypliny. Nie musi też się sprawdzać w praktycznym zastosowaniu. Zapewne, ale foresight to nie badanie, które koncentruje się na jednej wizji, ale na różnych punktach widzenia. Stąd też jest procesem, którego istotą jest właśnie ścieranie się ze sobą różnych poglądów.

Dlatego też przyjmuje się, że najbliższym odpowiednikiem pojęcia foresight jest słowo perspektywa. Foresight umożliwia tworzenie perspektyw dla przyszłości. Wyjaśniając istotę tego pojęcia, warto również zwrócić uwagę na dystynkcję zachodzącą miedzy nim a tradycyjnie pojmowaną prognozą badawczą. Nowoczesne przewidywanie oznacza proces systematycznego podejścia do identyfikacji przyszłych zjawisk w sferze nauki, technologii, ekonomii i zjawisk społecznych. Foresight uznaje się w pewnym sensie za proces ciągły[43]. Jakkolwiek w badaniach społecznych szczególnie podkreśla się potrzebę aktualizacji wyników poprzez powtórną falsyfikację i ponowną weryfikację dotychczasowych ustaleń, to w tym przypadku rzecz ma się nieco inaczej. Otóż badanie foresight z założenia odznacza się swego rodzaju ciągłością. Kontynuacja jest w tym przypadku potrzebna po to, aby wyniki, ustalenia miały określoną wartość praktyczną. Ten wymóg kontynuacji badań, ponawiania refleksji nad problematyką znajdującą się w kręgu zainteresowań badacza, jest tym, co przyczynia się w pewnym stopniu do zmniejszenia niepewności. Foresight, będąc reakcją na zmieniające się otoczenie, zabezpiecza się przed tym poprzez wymóg ciągłości. Tak więc, próby spojrzenia na przyszłość, aby móc używać w odniesieniu do nich terminu foresight, muszą być systematyczne, ciągłe, liniowe, w odróżnieniu od tworzenia scenariuszy endogennych[44], czyli punktowych.

Podstawą funkcjonowania procesu foresight jest identyfikowanie kluczowych kierunków rozwoju i ich opisywanie celem stworzenia płaszczyzny dla debaty publicznej, prowadzącej do konsensusu w zakresie celów społecznie pożądanych i sposobów ich osiągnięcia[45]. Tego typu przewidywanie ma być niejako przeciwieństwem wcześniejszych praktyk, kiedy często prognozowanie przyszłych zjawisk

41 L.J. Jasiński, dz. cyt., s. 9.
42 K. Borodako, dz. cyt., s. 12.
43 Ł. Mamica, P. Kopyciński, art. cyt., s. 107.
44 *Foresight technologiczny. Podręcznik. t. 1.*, dz. cyt., s. 8.
45 Ł. Mamica, P. Kopyciński, art. cyt., s. 107-108

odbywało się tylko w wąskim gronie ekspertów[46]. Kolejną cechą badania foresight jest to, że jego rezultaty nie ograniczają się jedynie do schematycznych prezentacji scenariuszy, raportów i zalecanych działań. Ważne jest rozwijanie przyjętych wizji strategicznych poprzez nacisk na powstawanie sieci kooperacji w różnych środowiskach politycznych, gospodarczych i społecznych. Foresight nie jest więc autonomiczną metodą i korzysta z szerokiego zasobu narzędzi badawczych[47].

Należy wskazać na następujące założenia badań foresight:

- foresight to proces, a nie technika prognozowania,
- to analiza interdyscyplinarna,
- obejmuje długoterminowe perspektywy czasowe,
- integruje różne perspektywy, w tym rozwój naukowy, technologiczny, gospodarczy, polityczny i społeczny,
- stanowi narzędzie wspomagające proces decyzyjny, ale nie oferuje gotowych strategii korporacyjnych czy politycznych,
- jest próbą promowania innowacji technologicznych i społecznych w sektorze publicznym i prywatnym,
- optymalnie powinien być realizowany jako proces partycypacyjny z promotorami, którzy muszą zrealizować później decyzje[48].

Najbliższy do foresightu w obszarze zagrożeń bezpieczeństwa narodowego na poziomie konceptualizacji jest foresight regionalny. Foresight regionalny, którego głównymi zasobami są źródła wiedzy oraz partnerzy regionalni, jest procesem konsolidacji różnych grup interesu oraz środowiska. Uczestnikami procesu foresight na poziomie regionalnym są najczęściej przedstawiciele samorządów, uczelni wyższych, biznesu, lokalnych mediów, organizacji pozarządowych. W wymiarze regionalnym poszukiwanie odpowiedniej reprezentacji różnych grup i interesu i zachęcenie do aktywnego udziału w pracach jest szczególnie ważne. Wypracowane wizje i koncepcje rozwoju, jeżeli mają być przełożone na język wdrożeń, muszą być akceptowane przez tych, którzy będą realizować wytyczne polityki gospodarczej (innowacyjnej). Jako instytucje lokalne rozumie się tu zwykle samorząd lokalny, instytucje użyteczności publicznej, lokalne przedstawicielstwa administracji[49].

Zgodnie z przyjętym podejściem systemowym oczekuje się, że foresight regionalny będzie dotyczyć różnych aspektów życia na danym obszarze, a przewidywane kierunki rozwoju powinny odpowiadać na rzeczywiste potrzeby[50]. W ramach realizacji projektu tworzy się listy kluczowych technologii oraz odpowiednie scenariusze rozwoju. Wskazane technologie powinny mieć charakter priorytetowy z punktu widzenia zrównoważonego rozwoju. Zwyczajowo scenariusze te zakładają najróżniejsze możliwości rozwoju danego regionu lub branży. Powinny one

46 Tamże, s. 108.
47 Tamże.
48 *Foresight technologiczny. Podręcznik. t. 2. Foresight technologiczny w praktyce*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2007, s. 197.
49 *Foresight jako metoda kształtowania przyszłości*, s. 18-19.
50 Tamże, s. 18.

uwzględniać zarówno zdarzenia pozytywne, jak i negatywne. Niezaprzeczalną zaletą scenariuszy rozwoju jest ich obrazowość. W nader przystępny sposób pokazują one przyszłość bez potrzeby interpretacji wyników z innych działań kluczowych[51]. Należy pamiętać, że przeprowadzenie badania foresight ma na celu nie tyle dokładne określenie zjawisk, które mają wystąpić, ile raczej lepsze przygotowanie do przyszłości[52], a jeśli tak, to znaczenie badań foresight sprowadza się do zastosowań w zakresie tworzenia systemu bezpieczeństwa, systemu powiązanych ze sobą elementów, które foresight ma za zadanie pomóc usprawnić.

Jednakże tu pojawia się poważne ograniczenie. Jak można porównywać poszczególne rodzaje bezpieczeństwa, przynależne do różnych dyscyplin? W jaki sposób można je badać, jeżeli metodologie szczegółowe są do siebie nieprzystawalne? Rozwiązaniem jest znalezienie wspólnego poziomu objaśniania struktury badanych zjawisk i podjęcie w ramach badań refleksji właśnie nad nią. Czy takie założenie jest uprawnione? Wydaje się, że tak, ponieważ dotychczas analizowana struktura bezpieczeństwa prowadzi do diagnozy, że zagrożenia, jako swego rodzaju efekt, są elementem ryzyka. Ryzyko jest więc kategorią, którą należy uczynić przedmiotem refleksji. Jest ono wszechobecne, ponieważ żyjemy i działamy w przestrzeni ryzyka, zaś przestrzeń ta ma tyle wymiarów, ile aspektów życia da się w ogóle określić. Co więcej, dla wzmocnienia dotychczas poczynionych ustaleń warto przywołać opinię, że w ogóle wątpliwa wydaje się definicja bezpieczeństwa określająca je jako brak zagrożeń. Zagrożenia są elementem ryzyka i występują zawsze. Skoro tak, to nie ma sytuacji braku zagrożeń. Przyjmując, że taka sytuacja występuje, czynimy założenie o charakterze czysto teoretycznym, co w konsekwencji czyni pojęcie bezpieczeństwa konstruktem idealnym. Z drugiej zaś strony nie ulega jednak wątpliwości, że mimo występowania zagrożeń, w wielu przypadkach można mówić o bezpieczeństwie[53].

Przyjmując w związku z tym, że bezpieczeństwo państwa to rzeczywisty stan stabilności[54], przy równoczesnym założeniu, że bezpieczeństwo jest pojęciem szerszym niż pojęcie zagrożenia[55], należy uznać, że bezpieczeństwo (otoczenia cywilizacyjnego i naturalnego) określane jest przez poziom jego całkowitego ryzyka[56]. Ryzyko, jak już wskazano, związane jest właściwie z całym obszarem działalności człowieka oraz jego funkcjonowaniem zarówno w środowisku naturalnym, jak i cywilizacyjnym, oraz wiąże się z zagrożeniem[57].

Zauważyć należy, że zagrożenie odnosić się może do pojedynczego człowieka, grupy ludzi, społeczności lokalnych, a także całych społeczeństw. Należy pod-

[51] *Foresight województwa mazowieckiego. Krzyżowa analiza wpływów, scenariusze rozwoju, priorytetowe technologie*, Szewczyk R. i in. (opr.), Przemysłowy Instytut Automatyki i Pomiarów PIAP, Warszawa 2008, s. 9.

[52] Ł. Mamica, P. Kopyciński, art. cyt., s. 108.

[53] J. Wolanin, dz. cyt., s. 14.

[54] *Słownik terminów z zakresu bezpieczeństwa narodowego*, s. 16.

[55] J. Wolanin, dz. cyt., s. 14.

[56] Tamże, s. 35.

[57] Tamże, s. 36.

kreślić, że każda z wymienionych grup postrzega ryzyko w sposób właściwy tylko dla niej. Czy jednak tak wysoki stopień subiektywizmu nie stanowi zagrożenia dla procesu foresight? Z pewnością nie, jeżeli weźmie się pod uwagę, że stanowisko, zgodnie z którym przy podejmowaniu wszelkich działań dotyczących obniżania wartości ryzyka nie należy uwzględniać innych oprócz matematycznych metod jego określania, ignoruje fakt, że w pojęciu ryzyka zawarty jest właśnie element społecznego postrzegania, który ma charakter subiektywny[58]. Co więcej, należy zauważyć, że do badania zagrożeń, ze względu na ich dość zróżnicowany charakter, dodatkowo wzmocniony subiektywnym postrzeganiem, zastosowanie znajduje metoda foresight. Foresight, korzystając w większym zakresie z metod jakościowych, pozwala na uwzględnienie tego typu różnorodności, trudnej w pomiarze (i w ogóle trudnej do uchwycenia, oddania ich specyfiki) przy zastosowaniu metod ilościowych. Jako przykład można tu podać gospodarkę, odznaczającą się wysokim stopniem zmienności i elastyczności. Środowisko to niejako burzy użyteczność dotychczasowych metod kreowania przyszłości. Z tego względu w tym obszarze coraz większe znaczenie mają czynniki i metody analizy jakościowej, które znajdują potwierdzenie w różnorodnych, coraz bardziej rozbudowywanych metodologiach studiów prospektywnych. Badania te mają orientację systemową i heurystyczną. Posługują się zarówno osiągniętym poziomem wiedzy i nowymi koncepcjami, jak i miękkimi narzędziami wspierającymi alternatywne myślenie o przyszłości[59].

Uzasadnienia wymaga jeszcze postulat objęcia zainteresowaniem badawczym problematyki ryzyka. Warto w tym kontekście przywołać pogląd, zgodnie z którym pojęcie bezpieczeństwa należy wiązać raczej z pojęciem ryzyka i jego miarą, niż bezpośrednio z pojęciem zagrożenia[60]. Dlatego też w procesie identyfikacji zagrożeń dla bezpieczeństwa narodowego przy zastosowaniu metody foresight kluczową kategorią należy uczynić ryzyko, będące miarą zagrożeń bezpieczeństwa, ponieważ zależność pomiędzy bezpieczeństwem a ryzykiem jest odwrotnie proporcjonalna. Im większe ryzyko, tym mniejsze bezpieczeństwo związane z tym ryzykiem. I odwrotnie, im mniejsze ryzyko, tym większe bezpieczeństwo. Jednak i w tym przypadku trzeba uwzględnić to, że na tak pojmowane bezpieczeństwo nakłada się, jak wyżej wskazano, wcale nie mało istotny czynnik związany z poczuciem bezpieczeństwa. Bezpieczeństwo związane z ryzykiem, dającym się wyliczyć przez ekspertów, to bezpieczeństwo realne, ale trzeba zauważyć, że bezpieczeństwo realne i poczucie bezpieczeństwa wcale nie pokrywają się zarówno co do swojej wielkości, jak i hierarchii[61].

Tak więc realizacja procesu badania identyfikacji zagrożeń bezpieczeństwa narodowego metodą foresight musi uwzględniać złożoną i wielowymiarową typologię celów bezpieczeństwa narodowego. Zastosowanie znajduje tu podejście holistyczne, pozwalające na postrzeganie bezpieczeństwa narodowego jako odrębnej całości. Dodatkowo zastosowanie kryterium kontekstowości umożliwia

[58] Tamże.
[59] A. Klasik, T. Markowski, *Wprowadzenie*, w: *Foresight regionalny i technologiczny*, s. 5.
[60] J. Wolanin, dz. cyt., s. 15.
[61] Tamże.

rozpatrywanie go w szerszym otoczeniu. W przypadku kryterium kontekstowości chodzi o obecność i oddziaływanie innych bytów o charakterze hierarchicznie nadrzędnym, równorzędnym lub podrzędnym. Tym sposobem typologia uwarunkowań bezpieczeństwa narodowego może obejmować uwarunkowania wewnętrzne oraz zewnętrzne, jak też powiązania między nimi. Uwarunkowania wewnętrzne związane są z tym, co dzieje się we wnętrzu bezpieczeństwa narodowego, uwarunkowania zewnętrzne natomiast konsekwentnie stanowią właściwość otoczenia bezpieczeństwa narodowego i oddziałują na nie zarówno bezpośrednio, jak i pośrednio[62].

Projektując badanie foresight, należy odpowiedzieć również na pytanie, jaka jest jego istota w kontekście prognozowania technologicznego oraz zarządzania, w szczególności planowania strategicznego. Należy również wyjaśnić wskazane wcześniej różnice między procesem foresight a ogólnie rozumianym prognozowaniem. Pojęcie prognozowania, w znaczeniu ogólnym, utożsamiane jest głównie z metodami numerycznymi jako pierwotnymi dla prognozowania. Mimo dużego podobieństwa metody foresight do prognozowania w zakresie stosowanej metodyki, nie są to tożsame pojęcia. Dzięki zasadom foresight możliwe jest bowiem badanie przyszłych zjawisk, które mogą wydawać się jedynie *nierealnymi marzeniami*. Nie można jednak również wykluczyć, że po upływie pewnego czasu mogą się zrealizować. Należy w tym miejscu zwrócić uwagę na główną cechę odróżniającą foresight od prognozowania, jaką jest nastawienie wobec przyszłości. Prognozowanie przyjmuje raczej formę pasywną, opisową, a więc bada i analizuje naukowo opracowaną ścieżkę przyszłości. Natomiast foresight ma charakter wyjątkowo aktywny, ponieważ sprawdza do jakich następstw mogą prowadzić poszczególne zmiany i jakie opcje działania doprowadzą do alternatywnego rozwoju pożądanej przyszłości. Istotnym elementem odróżniającym foresight od prognozowania jest obecność w procesie badawczym ekspertów, którzy w końcowych etapach prac dokonują oceny wypracowanych rezultatów, przede wszystkim zaś wyrażają swoje poglądy na temat wypracowanych scenariuszy rozwoju danego obszaru badań. Wreszcie bardzo często foresight odróżnia się od prognozowania przeprowadzeniem konsultacji z głównymi partnerami społecznymi i instytucjonalnymi, co z kolei umożliwia szerszą akceptację wyników prowadzonych badań[63]. Niezależnie jednak od przyjętej metody i zastosowanych narzędzi, w przypadku prowadzenia badań związanych z przyszłością, która jest nieznana, żadna technika nie daje całkowitej pewności wyników. Jednakże zastosowanie zróżnicowanych metod, tak jak w przypadku procesu foresight, może pozwolić na obniżenie poziomu błędnej prognozy[64].

Wielkość ryzyka związana jest ze stopniem zorganizowania społeczności, świadomości, porządku i urządzeń społecznych. Mówiąc o zarządzaniu ryzykiem, z jednej strony mamy do czynienia ze specjalistycznymi obliczeniami, których ce-

[62] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Akademia Obrony Narodowej, Warszawa 2011, s. 101.
[63] K. Borodako, dz. cyt., s. 15.
[64] Tamże.

lem jest określenie wartości ryzyka. Z drugiej z całym kompleksem problemów socjologicznych. Ta złożoność powiązań metod inżynierskich z naukami społecznymi stanowi szczególny wyróżnik zarządzania ryzykiem. Powoduje ona również brak jednoznaczności rozwiązań. Niemożliwe tym samym jest wskazanie klarownych zwięzłych recept zarządzania[65].

Jednakże foresight, mimo oparcia na metodach jakościowych, nie jest *wróżeniem*, chociaż wiedza uzyskana tą drogą ma bardzo specyficzny charakter[66]. Foresight, jak wskazano, jest rodzajem usystematyzowanego myślenia, które pozwala przewidywać przyszłość, zarządzać nią i często również ją kreować. Temu ostatniemu celowi służy jednoczesne uruchomienie procesu komunikacji, koncentracji, koordynacji, budowy konsensusu i partycypacji oraz podjęcie działań już dzisiaj *tworzonych jutro*. Foresight jest więc swego rodzaju *egzotyczną mieszanką* trzech elementów:

- przeczucia,
- pewności,
- prawdopodobieństwa[67].

W tym kontekście należy wskazać, że wiele niepowodzeń kreowania bezpieczeństwa wynika z niedoceniania (sygnalizowanego już) czynnika subiektywnego, przy równoczesnym przecenianiu specjalistycznych rozważań. Przecenianie to polega w głównej mierze na przyjęciu rygorystycznych, nieuwzględniających innych aspektów, wniosków dotyczących stanu bezpieczeństwa, wynikających tylko z analiz statystycznych. Taka sytuacja może doprowadzić do niepotrzebnych nacisków społecznych na zwiększenie bezpieczeństwa, którego realny poziom w rzeczywistości jest dostateczny. To z kolei może prowadzić do ponoszenia nieuzasadnionych kosztów, przez podejmowanie zbędnych działań lub też zaniechanie niezbędnych przedsięwzięć. Problem rozbieżności między bezpieczeństwem realnym a poczuciem bezpieczeństwa należy do bardzo poważnych. Zwłaszcza przy określaniu kierunków polityki bezpieczeństwa. Wzajemne, skomplikowane powiązania między tymi dwoma elementami to istota procesu podejmowania decyzji. Główne dylematy powstają na styku czterech perspektyw:

- polityka, który przy podejmowaniu decyzji jest raczej wyczulony na odbiór społeczny,
- eksperta, który wywiera na tego pierwszego silną presję,
- społeczności, która wie swoje na temat własnego bezpieczeństwa,
- mediów, które oceniają te na ogół konfliktowe relacje[68].

Dominacja różnych rodzajów metod sprawia, że wśród projektów realizowanych metodą foresight generalnie można wyróżnić trzy odmiany:

---

[65] J. Wolanin, dz. cyt., s. 31.

[66] A. Rogut, B. Piasecki, *Foresight: niekonwencjonalny instrument strategicznego zarządzania rozwojem regionu (doświadczenia woj. łódzkiego)*, w: *Foresight regionalny i technologiczny*, dz. cyt., s. 12.

[67] Tamże.

[68] J. Wolanin, dz. cyt., s. 16.

1) Foresight oparty na metodach ilościowych, czyli taki rodzaj badania, w którym dominują metody ilościowe (np. analizy statystyczne, rachunek prawdopodobieństwa, modele matematyczne). Jednak takie podejście stosuje się bardzo rzadko z uwagi na istotę procesu foresight odnoszącą się do metod partycypacyjnych (eksperckich).
2) Foresihgt oparty na metodach jakościowych, który wykorzystuje w badaniu metody jakościowe (np. panele eksperckie, metodę delficką, budowę scenariuszy), przy czym nie wyklucza też zastosowania w tym wariancie metod ilościowych.
3) Foresight oparty na metodach normatywnych, gdzie punktem wyjścia badań jest określenie pożądanej przyszłości, jej formy i kształtu[69].

Jak widać z powyższej klasyfikacji, w metodzie foresight zastosowanie mają:

- techniki analityczne (umożliwiające analizę problemu),
- społeczne (obejmujące praktyki ułatwiające interakcje między uczestnikami, czy grupami uczestników),
- techniki skupiające się na ekspertach (wykorzystujące ekspertów do stworzenia poglądów, opinii na temat przyszłości, wyznaczenia trendów, celów, najważniejszych priorytetów i strategii), a także techniki oparte na założeniach (wykorzystujące do stworzenia wizji publicznie dostępną wiedzę, np. dostępne statystyki, analizy raporty)[70].

Z punktu widzenia podejścia systemowego obiecujące może być sięgnięcie po myślenie antycypacyjne. Zasadę tego kierunku stanowi uznanie, że elementy pewnej całości same w sobie funkcjonują inaczej, niż gdy pozostają w określonym zespole i z tego właśnie powodu wypada analizować cały system, kładąc nacisk na wzajemne zależności jego komponentów. Myślenie systemowe jest podejściem holistycznym. Każdy system ujęty jako całość pozostaje otwarty na oddziaływanie ze strony swojego otoczenia. Podobnie pozostają uzależnione od niego części składowe systemu. Stały przepływ informacji między komponentami systemu i między nimi a otoczeniem wpływa na zewnętrzny kształt systemu. Przede wszystkim zaś na sposób jego postrzegania. Z tego powodu wypada traktować go jako konstrukcję dynamiczną, zmienną w czasie. W przypadku badania przyszłości podejście holistyczne (stosowane wobec zjawisk minionych i współczesnych) zostaje przeniesione na wydarzenia i sytuacje jeszcze nie zrealizowane, czyli takie, które nie wystąpiły[71].

Skonstruowana zgodnie z zasadami myślenia antycypacyjnego jest metoda delficka[72]. Wydaje się ona szczególnie przydatna do identyfikacji zagrożeń bezpieczeństwa narodowego. W wersji klasycznej metoda delficka oznaczała wymianę informacji między anonimowymi ekspertami mającą na celu maksymalne zbliżenie opinii, dokonywaną za pośrednictwem ankiety pocztowej. W każdej kolejnej rundzie eksperci mieli do dyspozycji rezultaty poprzedniej rundy (kontrolowany przepływ informacji zwrotnej), dające im możliwości rewizji swojego stanowiska

[69] K. Borodako, dz. cyt., s. 38.
[70] A. Rogut, B. Piasecki, art. cyt., s. 13.
[71] L.J. Jasiński, dz. cyt., s. 17.
[72] Tamże.

(podtrzymanie dotychczasowego lub jego zmian). Cały proces powtarzany był tak często, jak to było potrzebne (choć większość badań nie wychodziła poza dwie rundy). Zakładano przy tym, że każda kolejna runda zwiększała prawdopodobieństwo osiągnięcia konsensusu[73]. Obecnie tradycyjna ankieta pocztowa jest zastępowana ankietą elektroniczną lub instrumentami on-line. Te ostatnie stwarzają możliwość odejścia od tradycyjnych rund i przejścia do ciągłej wymiany informacji w rzeczywistym czasie. Alternatywą dla klasycznej metody delfickiej staje się także kontakt bezpośredni. W takim przypadku rezygnuje się nawet z wymogu anonimowości, a celem staje się po prostu gromadzenie argumentów, a nie budowa konsensusu. Dlatego współcześnie metoda delficka traktowana jest przede wszystkim jako proces ustrukturyzowanej komunikacji między grupą osób/ekspertów dzielących się wiedzą (skodyfikowaną, ukrytą, nieujawnioną), w ramach którego dostarczany jest wartościowy wkład (argumenty, dowody, uzasadnienia) w rozwiązywanie jakiegoś kompleksowego problemu[74]. Jednak wskazuje się też w tym kontekście, że proces foresight ma ułatwić przeprowadzenie rozpoznania rzeczywistości, a nie kształtować opinie odpowiednio do własnych przekonań[75]. Anonimowość odpowiedzi uwalnia wyniki otrzymane metodą delficką od wpływu na nie ze strony osób dysponujących władzą lub autorytetem środowiskowym[76].

Metoda delficka musi spełniać cztery następujące kryteria:

- Proces musi być powtarzany, czyli eksperci muszą być co najmniej dwukrotnie pytani o opinię dotyczącą tej samej hipotezy badawczej.
- Utrzymywana jest anonimowość, a odpowiedzi uczestników badań znane są bezpośrednio wyłącznie koordynującemu badania.
- Komunikacja z ekspertami ma charakter kontrolowanego sprzężenia zwrotnego, co oznacza, że wymiana informacji między ekspertami następuje za pośrednictwem koordynatora, dzięki czemu można wyeliminować wszystkie nieistotne informacje.
- Odpowiedzi są formułowane w sposób pozwalający na ich przetworzenie ilościowe i statystyczne[77], a kiedy brane są pod uwagę informacje prezentowane w formie jakościowej, nie odgrywają już one dużego znaczenia w przypadku weryfikowania przyjętej hipotezy[78].

Ponadto, aby oddać *nieznaną naturę przyszłości*, analizy ilościowe muszą być wzbogacone o czynniki z otoczenia, w jakim zachodzą. Muszą być także prowadzone zgodnie z przyjętymi założeniami związanymi z oczekiwaną i pożądaną przyszłością[79]. Dodatkowo jednym z najważniejszych aspektów badań jest dobór właściwych metod badawczych, który musi być:

---

73 A. Rogut, B. Piasecki, art. cyt., s. 17-18.
74 Tamże, s. 18.
75 L.J. Jasiński, dz. cyt., s. 17-18.
76 Tamże, s. 18.
77 A. Rogut, B. Piasecki, art. cyt., s. 17.
78 K. Borodako, dz. cyt., s. 15-16.
79 Tamże, s. 16.

- odpowiednio wkomponowany w zakres badań, postawione cele i charakter badanych dziedzin,
- zrozumiały dla uczestniczących w pracy ekspertów oraz przedstawicieli wiodących instytucji[80].

Trzeba też wskazać, że wiedza foresight jest nieweryfikowalna, ponieważ nie opisuje realnej rzeczywistości. A jeśli tak, to może być oceniana wyłącznie z punktu widzenia prawdopodobieństwa zdarzeń, zjawisk, procesów, ale w żadnym razie nie przez pryzmat ich przewidywalności. Badania foresight mają charakter eksploracyjny, a nie prognostyczny. Wiedza foresight obarczona jest dużym ryzykiem niepewności, zwłaszcza jeśli chodzi o związki przyczynowo-skutkowe między rozpatrywanymi zdarzeniami, zjawiskami, procesami. Jakość wiedzy foresiht weryfikowana jest poprzez:

- dopasowanie do celu (chodzi tu o związek między informacją, wiedzą a założonym celem, gdzie kluczowe znaczenie mają: zgodność, znaczenie, trafność, kompleksowość),
- wiarygodność (źródeł informacji/wiedzy, metod pozyskiwania, informatorów, rzetelności analizy),
- możliwości wykorzystania (osiągalność, dostępność, zrozumiałość, przydatność)[81].

Uzyskanie maksymalnych korzyści z organizacji procesu foresight związane jest z występowaniem takich atrybutów, jak:

- antycypacja, czyli wykorzystywanie w prowadzonych aktualnie działaniach i podejmowanych decyzjach dotyczących przyszłości wiedzy o potencjalnych zjawiskach oraz zdarzeniach mogących zajść w przyszłości, przyjęcie takiej postawy pozwala partnerom instytucjonalnym oraz firmom na zwiększenie swojego przekonania o możliwości kreowania i ukierunkowywania przyszłości swojej organizacji i bliższego otoczenia, a tym samym tworzenia ich przyszłości,
- partycypacja, a więc udział w projekcie wielu różnorodnych partnerów reprezentujących odmienne grupy interesu, a także inne obszary wiedzy specjalistycznej,
- konsensus społeczny, który oznacza, że wypracowane rezultaty projektu muszą być uzgodnione ze wszystkimi uczestniczącymi w przedsięwzięciu partnerami i przez nich zatwierdzone, co gwarantuje większą identyfikację z osiągniętymi wynikami,
- sieci partnerskie, które warunkują, aby prace prowadzone w trakcie trwania projektu umożliwiły nawiązywanie nowych kontaktów, stanowiących punkt wyjścia tworzenia się sieci współpracy i budowania klastrów w danym obszarze,
- długookresowa perspektywa, wyrażająca się poszukiwaniem pożądanej przyszłości dla danej jednostki terytorialnej, która musi uwzględniać ewentualne reakcje na bieżące wydarzenia w danej jednostce oraz poza nią (w skali kraju i na świecie) i jednoczesne utrzymywanie długookresowej perspektywy,

[80] Tamże, s. 38.
[81] A. Rogut, B. Piasecki, art. cyt., s. 13.

- kultura myślenia o przyszłości, warunkująca to, że projekt foresight musi być impulsem dla interesariuszy do prowadzenia wszystkich kluczowych działań z myślą o ich skutkach w średniookresowej i długookresowej perspektywie[82].

Foresight wymusza na partnerach zaangażowanie się w działanie związane z wprowadzeniem w życie uzyskanych wyników. Należy też podkreślić, że już sam proces współpracy wielu osób i instytucji jest w wielu wypadkach ważniejszy niż lista priorytetów, która jest rezultatem prac zespołów. Proces ten zwiększa poczucie współtworzenia wyników i angażuje do wspólnej ich implementacji. Wykorzystane w projektach metody muszą zachęcać uczestników do bezpośredniej współpracy. Ważne jest przygotowanie takich, metod jak: panele, warsztaty, sympozja, seminaria, aby zwiększyć efektywność komunikacji między uczestnikami. Przekazy w metodzie foresight powinno się również obudować informacjami dotyczącymi mocnych i słabych stron rozpatrywanych dziedzin. Decydując się na pilotażowe badania opinii społecznej lub wybranej grupy, należy pamiętać, że powinny one stanowić jedynie podstawę do dyskusji i wymiany poglądów różnych osób, a tym samym nie pochłaniać za dużo środków przeznaczonych na sam proces foresight[83]. Badanie foresight zakończy się sukcesem, jeśli przez cały czas będzie prowadzony z zaangażowaniem. Wyznacznikiem sukcesu w długiej perspektywie jest z pewnością ciągłość tego procesu[84]. Ponadto należy pamiętać, że foresight z definicji jest procesem strategicznym i w sytuacji, gdy nie ma bieżących decyzji i działań wdrażających wyniki, przestaje nim być[85].

6.2. Charakterystyka narzędzia zastosowanego w badaniu foresight

Celem badania zaprezentowanego poniżej było odtworzenie i porównanie wizji, perspektyw w zakresie identyfikacji zagrożeń bezpieczeństwa narodowego, czyli sposobów identyfikowania i szacowania ryzyka w poszczególnych obszarach bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Badanie miało charakter ekspercki. Zakwalifikowano do niego dwanaście osób zajmujących się zawodowo problematyką bezpieczeństwa. Zaprojektowano trzy etapy badania. Każdy z etapów był realizowany za pomocą ankiety opracowanej w edytorze tekstu, wysyłanej do respondentów pocztą elektroniczną. W badaniu przestrzegano zasady anonimowości. Odpowiedzi ekspertów były kodowane. Dostęp do danych pozwalających na identyfikację respondentów mieli wyłącznie koordynatorzy badania.

W pierwszym etapie respondenci mieli za zadanie udzielić odpowiedzi na trzydzieści dwa pytania kwestionariusza. W drugim etapie zadaniem ankietowanych było odniesienie się do zbiorczego zestawienia wszystkich uzyskanych odpowiedzi.

---

82 K. Borodako, dz. cyt., s. 27-28.

83 Tamże.

84 Tamże.

85 *Foresight w praktyce zarządzania przedsiębiorstwem. Analizy i studia przypadków*, K. Borodako, M. Nowosielski (red.), Instytut Zachodni, Poznań 2012, s. 10.

W celu prawidłowej realizacji drugiej części badania, oprócz zestawienia, respondenci otrzymali również zestaw pytań pomocniczych. W trzecim etapie eksperci otrzymali kolejne zestawienie wraz z zadaniami przewidzianymi dla tego etapu.

Ankiety składały się z pytań typu otwartego, aby nie sugerować możliwych odpowiedzi, nie narzucać ekspertom określonych sposobów opisu rzeczywistości. Sugestie co do kierunku, kształtu odpowiedzi ograniczono do niezbędnego minimum i to wyłącznie w przypadkach, w których konieczne było zagwarantowanie poprawnego zrozumienia zadań przez ekspertów. W instrukcji do badania podkreślono, że nie ma ono na celu przeprowadzenia weryfikacji wiedzy respondentów. To bardzo ważne założenie, nie chodziło w nim bowiem o to, aby respondenci przedstawili ogólnie dostępną wiedzę. Należało w związku z tym przekonać ekspertów, żeby podzielili się swoimi subiektywnymi przemyśleniami, uwagami, wątpliwościami, czy przypuszczeniami. Względnie, żeby takie przemyślenia nasunęły im się w trakcie opracowywania odpowiedzi. Badanie było próbą zrekonstruowania subiektywnych perspektyw ankietowanych. Udzielone odpowiedzi miały być w założeniu odzwierciedleniem punktów widzenia respondentów w obszarze, w obszarach ich kompetencji. Każdy z ekspertów miał za zadanie przedstawić to jak on postrzega, jak widzi daną problematykę. Chodziło niejako o uwolnienie respondentów od swoistego ograniczenia, jakim mogły być obowiązujące, prawomocne punkty widzenia, narracje. Należało zatem przekonać ekspertów do tego, aby ich narracje nie były w przeważającej części zbudowane na dyskursie dostępnym w fachowej literaturze, czy aktach prawnych. Należy przez to rozumieć nie to, że respondenci mieliby konsekwentnie odrzucić dotychczasowy dorobek w danej dziedzinie jako podstawę do formułowania swoich stanowisk i szukać zupełnie innych, nowych narracji, ale żeby unikali nadmiernych zapożyczeń, aby nie byli skrępowani szablonami. Należało ich zachęcić, żeby wykraczali poza nie. Miała to być zachęta do krytycznej analizy, przeglądu dotychczasowej wiedzy, ujawnienia swoich przypuszczeń, obaw, innowacyjnych myśli.

Przeszkodą w badaniu była jego korespondencyjna formuła. Przyjęty sposób realizacji dawał ograniczone możliwości skłonienia ekspertów do udzielenia rozbudowanych, złożonych odpowiedzi. Wyzwaniem było również skłonienie respondentów w kolejnych dwóch etapach do podjęcia ponownej refleksji nad odpowiedziami udzielonymi przez nich w pierwszej ankiecie i odpowiedziami innych respondentów. To była dość poważna bariera ograniczająca znacząco wymianę myśli. Poza tym respondenci, którzy wypełniali ankiety w zróżnicowanych warunkach (na które koordynator nie miał zupełnie wpływu), mogli uznać, że udzielili już wyczerpujących odpowiedzi. Z pewnością łatwiej byłoby osiągnąć te cele w bezpośrednim kontakcie z respondentami, w badaniu fokusowym, czy poprzez indywidualne wywiady pogłębione, podczas których moderator ma dość duże możliwości wpływania na efektywność badania, przez wdrażanie określonych działań: korygowanie tego procesu, konfrontowanie ze sobą różnych punktów widzenia, inicjowanie sporów. W przyjętej dla przedmiotowego badania formule koordynator poza samym etapem przygotowania kwestionariuszy, nie miał w za-

sadzie żadnych możliwości ingerowania w przebieg badania. Ponadto słabością ankiety korespondencyjnej było również to, że respondent miał możliwość zapoznania się z całym scenariuszem badania przed przystąpieniem do wypełniania ankiety, mógł udzielać odpowiedzi w dowolnej kolejności, wracać do wcześniejszych pytań, zmieniać odpowiedzi. Cały ten proces wypełniania kwestionariuszy był niestety niedostępny dla koordynatora, a wiedza ta mogłaby zostać wykorzystana do ulepszenia narzędzia. Jednak mimo tych trudności zdecydowano się na ankietę korespondencyjną, ponieważ w badaniu fokusowym nie dałoby się zachować anonimowości ekspertów. Brak anonimowości mógłby wytworzyć u części ankietowanych obawę przed ujawnieniem własnego stanowiska ze względu na pozycję, autorytet pozostałych ekspertów.

W pierwszym etapie każdy z respondentów otrzymał kwestionariusz składający się z trzydziestu dwóch pytań. Dodatkowo zwrócono się do ankietowanych z prośbą o udzielanie obszernych, szczegółowych wypowiedzi. Zdecydowano się przygotować taką rozbudowaną ankietę ze świadomością, że może ona wywołać zniechęcenie, zmęczenie u ekspertów, co z kolei mogło się przełożyć na jakość udzielanych odpowiedzi. Jednak decydując się na taki krok uznano, że badana problematyka, ze względu na swoją złożoność i wielowymiarowość, nie może zostać zredukowana do kilku ogólnych pytań, ponieważ ich szeroki zakres interpretacyjny może przełożyć się negatywnie jeszcze w większym stopniu na jakość i poprawność odpowiedzi (rozpatrywaną z punktu widzenia efektu, jaki poprzez pytania badacz stara się osiągnąć).

W pytaniu nr 1 zwrócono się do ekspertów, aby określili jedną, główną dziedzinę bezpieczeństwa mieszczącą się w zakresie ich kompetencji. W pytaniu tym podano możliwe warianty odpowiedzi, np.: bezpieczeństwo polityczne, bezpieczeństwo społeczne, bezpieczeństwo kulturowe, bezpieczeństwo militarne, bezpieczeństwo ekonomiczne, bezpieczeństwo ekologiczne, bezpieczeństwo informacyjne i telekomunikacyjne. Każdy z respondentów, dokonując wyboru, musiał w związku z tym zredukować, dookreślić obszar swoich zainteresowań, umiejscowić go, przyporządkować do rodzaju bezpieczeństwa szczegółowego. Następnie w pytaniu nr 2 poproszono ekspertów o dokończenie następującego zdania: *Bezpieczeństwo… (tu respondenci musieli uzupełnić puste miejsce zgodnie z odpowiedzią udzieloną na pierwsze pytanie)*, a następnie przedstawić tę dziedzinę bezpieczeństwa, którą wskazali. Celowo nie poproszono respondentów o podanie definicji, tylko o dokończenie zdania, aby w ten sposób zmniejszyć możliwość szablonowego podejścia do tego pytania. W kolejnym pytaniu – nr 3 – respondenci mieli za zadanie określić obszar (względnie obszary szczegółowe), którymi się zajmują. Chodziło tu o wskazanie takich obszarów, które pozwoliłyby na dokładniejszą charakterystykę wskazanej w odpowiedzi na pierwsze pytanie dziedziny bezpieczeństwa. W tym pytaniu również wymieniono kilka przykładowych odpowiedzi, np. bezpieczeństwo polityczne: partie polityczne; bezpieczeństwo społeczne: demografia; bezpieczeństwo ekonomiczne: system podatkowy. W odpowiedzi na pytanie nr 4 należało scharakteryzować i uszczegółowić wymienione w odpowiedzi na pytanie nr 3 obszary.

Należy wskazać, że odpowiedzi na pytania 1–4 dały możliwość poznania znaczeń, jakie ankietowani przypisali poszczególnym pojęciom. Podczas analizy okazało się, że ten sam termin jest używany przez respondentów w odmiennych znaczeniach (ujawniono więc deficyty w zakresach stosowanych pojęć).

W drugim etapie badania przy tworzeniu zbiorczych zestawień odpowiedzi posługiwano się kategoriami, które respondenci wyznaczyli w pytaniu nr 1 do opisania swoich zakresów kompetencji:

E[86]-1 – bezpieczeństwo społeczne *rozumiane jednak inaczej niż zabezpieczenie społeczne. (…) nie chodzi o prostą kalkę zabezpieczenia społecznego, które jest elementem polityki społecznej, lecz o sferę bezpieczeństwa stanowiącą część szerszej koncepcji*,

E-2 – bezpieczeństwo państwa,

E-3 – bezpieczeństwo ekologiczne, środowiskowe, bezpieczeństwo ekologiczne technologii środowiskowych,

E-4 – bezpieczeństwo kulturowe,

E-5 – bezpieczeństwo społeczne, bezpieczeństwo publiczne, bezpieczeństwo społeczności lokalnej,

E-6 – bezpieczeństwo społeczne,

E-7 – bezpieczeństwo wewnętrzne/porządek publiczny,

E-8 – bezpieczeństwo hydrologiczne,

E-9 – bezpieczeństwo militarne,

E-10 – bezpieczeństwo militarne,

E-11 – zarządzanie kryzysowe *które stanowi element kierowania bezpieczeństwem narodowym, w ramach podsystemów ochronnych państwa i ludności (bezpieczeństwa cywilnego, pozamilitarnego) – przeznaczonych do redukowania ryzyk i przeciwdziałania zagrożeniom*,

E-12 – bezpieczeństwo kulturowe, bezpieczeństwo etniczne.

W trzecim etapie natomiast na podstawie odpowiedzi uzyskanych w pytaniach 1–4 wyróżniono sześć dziedzin bezpieczeństwa, do których przyporządkowano poszczególnych ekspertów:

1) bezpieczeństwo społeczne (E-1, E-6),
2) bezpieczeństwo państwa (E-2, E-7, E-11),
3) bezpieczeństwo ekologiczne (E-3),
4) bezpieczeństwo kulturowe (E-4, E-12),
5) bezpieczeństwo hydrologiczne (E-5, E-8),
6) bezpieczeństwo militarne (E-9, E-10).

Kwalifikacja ta została narzucona przez koordynatora. Miała ułatwić przeprowadzenie dalszych analiz porównawczych, ale przede wszystkim pozwoliła zmienić układ zestawienia zbiorczego, aby w ten sposób wyeliminować możliwość rutynowego podejścia przez ankietowanych do zadań.

[86] E – ze względu na anonimowy charakter badań ekspertom przypisano kolejne (od 1 do 12) numery.

W pytaniu nr 5 ankietowani poproszeni zostali o wskazanie organizacji (nazwy instytucji, komórki organizacyjnej), w ramach której zajmują się (względnie zajmowali) problematyką wskazaną w odpowiedziach na pytania nr 1 i 3, a następnie w pytaniu nr 6 o wskazanie zajmowanego stanowiska, głównych zadań, które wykonują lub wykonywali w organizacji wymienionej w odpowiedzi na pytanie nr 5. Przy czym należało wymienić tu tylko te zadania, które mieściły się w obszarach wskazanych wcześniej odpowiedziach na pytania nr 1 i 3.

Kolejnych pięć pytań dotyczyło systemów bezpieczeństwa. W zadaniu nr 7 respondenci mieli dokończyć następujące zdanie: *System bezpieczeństwa… (tu respondenci musieli uzupełnić puste miejsce zgodnie z odpowiedzią udzieloną na pytania nr 1 i 3) w Rzeczypospolitej Polskiej tworzą obecnie….* W pytaniu nr 8 zadaniem respondentów było wskazanie znanych im działań służących zapewnieniu bezpieczeństwa w obszarze, który określili w pytaniu nr 1 i 3. W tym celu poproszono ankietowanych o dokończenie następującego zdania: *Działania w zakresie zapewnienia bezpieczeństwa… w Rzeczypospolitej Polskiej obejmują…* W kolejnym zadaniu – nr 9 – zwrócono się do ekspertów, aby zidentyfikowali braki w systemie bezpieczeństwa RP. Respondenci mieli dokończyć następujące zdanie: *Działania w zakresie zapewnienia bezpieczeństwa…, system zapobiegania zjawiskom zagrażającym bezpieczeństwu w Rzeczypospolitej Polskiej należałoby uzupełnić o…* W pytaniu nr 10 przyjęto założenie, że bezpieczeństwo jest produktem podmiotów odpowiedzialnych za bezpieczeństwo[87], a więc takich podmiotów, które muszą być zarówno przygotowane, jak i zdolne (chodzi tu o zdolność rozumianą jako siły, środki dostępne w zasięgu społeczeństwa, organizacji, mogących zredukować poziom ryzyka zagrożenia/zagrożeń) do działania w sposób ciągły. Następnie poproszono respondentów, aby określili i ocenili stopień gotowości, zdolności podmiotów odpowiedzialnych za dziedzinę bezpieczeństwa określoną przez nich w odpowiedziach na pytania nr 1 i 3. Zadanie nr 11 było modyfikacją pytania nr 9. Eksperci mieli dokończyć następujące zdanie: *W systemie bezpieczeństwa … w Rzeczypospolitej Polskiej warto zastanowić się nad wprowadzeniem zmiany/zmian w…* Powtórzenie zadania miało skłonić ankietowanych do ponownej refleksji nad budową systemu bezpieczeństwa. Liczono się bowiem z tym, że ankietowani mogą wskazać w odpowiedzi na pytanie nr 9, iż system nie wymaga uzupełnień. Dodatkowo w pytaniu nr 11 zadanie celowo zostało sformułowane w sposób mniej kategoryczny niż w pytaniu nr 9 (zadanie nr 9: *należałoby uzupełnić o*, zadanie nr 11: *warto zastanowić się nad wprowadzeniem zmian/zmiany*). Zastosowano więc dwa podobne komunikaty, ale o różnej sile przekazu. Oba zadania miały zachęcić respondentów do wskazania, czego w systemie ich zdaniem brakuje, a różnica polegała na tym, że w pytaniu nr 9 założono istnienie luk w systemie, a w pytaniu nr 11 jedynie

[87] E. Nowak, *Bezpieczeństwo narodowe – istota, zakres, uwarunkowania*, w: *Bezpieczeństwo narodowe i zarządzanie kryzysowe w Polsce w XXI wieku*, Jemioło T., Rajchel K. (red.), Wyższa Szkoła Informatyki, Zarządzania i Administracji w Warszawie, Wydział Strategiczno-Obrony Akademii Obrony Narodowej w Warszawie, Towarzystwo Naukowe Powszechne, Warszawa 2009, s. 65.

zasugerowano, że można by dokonać ewentualnych zmian, o ile eksperci dostrzegaliby taką konieczność.

W pytaniach nr 12, 18 i 19 odwołano się do koncepcji postrzegania bezpieczeństwa autorstwa Daniela Freia[88]. D. Frei wyróżnił cztery perspektywy:

- stan braku bezpieczeństwa – gdy występuje duże rzeczywiste zagrożenie, a postrzeganie tego zagrożenia jest prawidłowe,
- stan obsesji – gdy nieznaczne zagrożenie jest postrzegane jako duże,
- stan fałszywego bezpieczeństwa – kiedy zagrożenie jest poważne, a postrzegane jest jako niewielkie,
- stan bezpieczeństwa – gdy zagrożenie zewnętrzne jest nieznaczne i postrzegane jest prawidłowo.

Zdecydowano się na wykorzystanie tej klasyfikacji do budowy kwestionariusza, ponieważ ukazuje ona dość wyczerpująco istotę zróżnicowania (pojemności) kategorii bezpieczeństwa.

W zadaniu nr 12 poproszono ankietowanych, aby wymienili w punktach i krótko scharakteryzowali elementy, które ich zdaniem oddziałują na obiektywny, faktyczny stan bezpieczeństwa (w odniesieniu do dziedzin wskazanych w odpowiedziach na pytania nr 1 i 3). Nie umieszczono w tym zadaniu dodatkowych wyjaśnień, ponieważ funkcję tę spełnić miały kolejne pytania nr 13–17. W zadaniu nr 13 należało wskazać, a następnie opisać zależności między elementami, które zostały wymienione w odpowiedzi na poprzednie pytanie (nr 12). W pytaniu nr 14 poproszono respondentów, aby opisali znane im metody (a w przypadku ich braku, żeby przedstawili propozycje takich metod) umożliwiające ocenę stanu bezpieczeństwa w odniesieniu do tych elementów, które wymienili w odpowiedzi na pytanie nr 12. Następnym zadaniem w pytaniu nr 15 było opisanie skal (względnie przedstawienie propozycji takich skal) umożliwiających ocenę ryzyka w odniesieniu do elementów wymienionych w odpowiedzi na pytanie nr 12. W zadaniu nr 16 respondenci mieli wskazać przyjęte, uznane punkty graniczne, punkty krańcowe stanu stabilności państwa (lub spróbować określić takie punkty) na opisanych, zaproponowanych w odpowiedzi na pytanie nr 15 skalach. Chodziło tu o punkty, po przekroczeniu których wystąpi stan niestabilności. Natomiast w zadaniu nr 17 zwrócono się do ankietowanych, aby określili kryteria, czynniki, które pozwoliły dokonać wyboru punktów granicznych wskazanych w odpowiedzi na pytanie nr 16.

W zadaniu nr 18 respondenci mieli scharakteryzować potencjalny stan braku bezpieczeństwa. W tym celu poproszono ich o rozwinięcie następującego zdania: *Stan braku bezpieczeństwa…, czyli sytuacji, w której występuje duże rzeczywiste zagrożenie, a postrzeganie tego zagrożenia jest prawidłowe, występuje wtedy, gdy…* Podobną konstrukcję przyjęto w pytaniu nr 19. Tu ankietowani mieli z kolei opisać stan fałszywego bezpieczeństwa: *Stan fałszywego bezpieczeństwa…, czyli sytuacji, w której zagrożenie jest poważne, a postrzegane jest jako niewielkie, występuje wtedy, gdy…*

[88] J. Gierszewski, dz. cyt., s. 23.

Pytania nr 20, 21 i 22 stanowiły próbę rozwinięcia perspektyw wyznaczonych przez Freia w oparciu o dychotomię obiektywnych i subiektywnych zagrożeń[89]. Pytanie nr 20 dotyczyło uwarunkowań, przyczyn subiektywnego, indywidualnego postrzegania bezpieczeństwa. Tu zadaniem respondentów było dokończenie następującego zdania: *Na poczucie braku bezpieczeństwa…, jego subiektywny, indywidualny odbiór, swoiste poczucie braku pewności wpływa/wpływają:…* Z kolei w pytaniu nr 21 ankietowani mieli określić, z czego wynikają, jakie są przyczyny rozbieżności między bezpieczeństwem realnym w obszarze bezpieczeństwa wskazanym przez nich w pytaniach 1 i 3 a poczuciem, indywidualnym odbiorem bezpieczeństwa. W zadaniu nr 22 zapytano o to, czy i w jakim zakresie wyeliminowanie wymienionych przez ankietowanych w odpowiedzi na pytanie nr 20 czynników kształtujących subiektywne poczucie braku bezpieczeństwa spowoduje w ich ocenie zmianę tego subiektywnego poczucia braku bezpieczeństwa na uwarunkowane obiektywnie poczucie pewności.

Pytania nr 23–28 odwoływały się również do dwudzielnej koncepcji zagrożeń: wewnętrzne/zewnętrzne, indywidualne/grupowe, abstrakcyjne/konkretne, potencjalne/aktywne[90]. W pytaniu nr 23 poproszono respondentów, aby wymienili w punktach, a następnie scharakteryzowali wewnętrzne (wewnątrzpaństwowe) zagrożenia dla dziedziny bezpieczeństwa określonej przez nich w odpowiedziach na pytania nr 1 i 3. W pytaniu nr 24 z kolei należało wymienić w punktach i scharakteryzować zewnętrzne (ulokowane na zewnątrz państwa) zagrożenia dla wybranej dziedziny bezpieczeństwa. Podobnie skonstruowane pytanie nr 25 dotyczyło zagrożeń indywidualnych (w odniesieniu do jednostki), a pytanie nr 26 zagrożeń grupowych (w odniesieniu do społeczności). W pytaniu nr 27 poproszono respondentów, aby wymienili i opisali zdarzenia niepożądane/sytuacje kryzysowe w odniesieniu do wskazanej przez nich dziedziny bezpieczeństwa. Zadanie nr 28 polegało na wskazaniu potencjalnych zagrożeń dla bezpieczeństwa.

Następnie w pytaniu nr 29 poproszono respondentów, aby dokonali selekcji zagrożeń wymienionych w odpowiedziach na pytania nr 23–28, a następnie wskazali 3–5 zagrożeń, które w ich ocenie charakteryzują się największym prawdopodobieństwem wystąpienia. Dodatkowo poproszono ankietowanych o uszeregowanie tych zagrożeń – rozpoczynając od najbardziej prawdopodobnego. W zadaniu nr 30 respondenci mieli dla każdego z zagrożeń wskazanych w odpowiedzi na poprzednie opisać sposób szacowania prawdopodobieństwa jego wystąpienia, a w pytaniu nr 31 sposób szacowania skutków ich wystąpienia. Ostatnim zadaniem nr 32 (z pierwszego etapu) było opracowanie przez ekspertów na podstawie dotychczasowych odpowiedzi hierarchicznie uporządkowanej listy zagrożeń dla wybranej przez nich dziedziny bezpieczeństwa. Poproszono, aby ankietowani wymienili maksymalnie dziesięć zagrożeń, zaczynając od najważniejszego.

W drugim etapie badania ekspertów proszono o:

[89] Tamże, s. 27.
[90] Tamże.

- zapoznanie się ze zbiorczym zestawieniem odpowiedzi na pytania 2 i 7–32,
- wskazanie, w jakim zakresie informacje, punkty widzenia przedstawione przez pozostałych respondentów mogą mieć zastosowanie, mogą zostać zaadaptowane, posłużyć do rekonstrukcji, zmiany ich odpowiedzi.

Kwestionariusz był zbudowany w taki sposób, że pod każdym z pytań zostały umieszczone odpowiedzi dwunastu ekspertów. Odpowiedzi, jak już wcześniej wskazano, dla ułatwienia identyfikacji oznaczono numerami. Obok numerycznych identyfikatorów podano dodatkowo wskazaną przez każdego z ekspertów w odpowiedzi na pytanie nr 1 – dziedzinę bezpieczeństwa mieszczącą się w zakresie jego kompetencji. Na końcu takich zbiorów odpowiedzi (dla każdego pytania) pozostawiono puste miejsce na uwagi do odpowiedzi. Poproszono respondentów, aby ci, jeśli uznają, że udzieloną przez nich na dane pytanie odpowiedź warto (po zapoznaniu się z zestawieniami odpowiedzi innych ankietowanych) uzupełnić, zmodyfikować, zmienić:

- wpisali numer eksperta (numery ekspertów), którego odpowiedź stanowiła dla nich inspirację do uzupełnienia, zmiany własnej odpowiedzi,
- syntetycznie opisali, czego i w jakim zakresie zmiana dotyczy,
- krótko uzasadnili wprowadzoną modyfikację.

W trzecim etapie w pierwszej części zestawiono obszary szczegółowe (wraz z charakterystykami), wskazane przez ekspertów w pierwszym etapie w pytaniu nr 4. Następnie poproszono ankietowanych, żeby wykorzystując to zestawienie dokonali rozbudowy, zmian szczegółowych obszarów oraz opisów, które wyróżnili w ramach dziedziny bezpieczeństwa znajdującej się w ich kompetencji. W drugiej części przygotowano zestawienia uwag z drugiego etapu do odpowiedzi na pytania 2 i 7–32. Ponieważ w drugim etapie część respondentów przedstawiła także swoje zastrzeżenia do odpowiedzi sformułowanych przez innych ekspertów, w ostatnim etapie poproszono ankietowanych o dokonanie rekonstrukcji własnych odpowiedzi, a także podjęcie polemiki z tymi uwagami.

6.3. Syntetyczne omówienie wyników badania

Zastosowane w badaniu foresight narzędzie wstępnie umożliwiło zidentyfikowanie zagrożeń charakterystycznych dla następujących dziedzin bezpieczeństwa: państwa, społecznego, kulturowego, militarnego, ekologicznego oraz hydrologicznego. Zastrzec jednak należy, że są to kategorie wskazane przez poszczególnych ekspertów i dodatkowo w trzecim etapie zmodyfikowane przez koordynatora na potrzeby badania. Ich znaczenia nie były w zasadzie negocjowane przez uczestników badania – nie stanowiły przedmiotu uzgodnień. Kategorie te spełniały przede wszystkim funkcję porządkującą. Większość z nich jest przy tym bardzo pojemna, przez co ich granice stają się trudne do wytyczenia, zaś one same nakładają się na siebie. Z tych powodów zbiory zagrożeń wyróżnione w ramach tych dziedzin należy traktować raczej jako jeden nieuporządkowany zbiór zagrożeń w obszarze bezpieczeństwa narodowego.

Tababela 6.1. Wskazane przez ekspertów hierarchicznie uporządkowane zbiory zagrożeń (rozpoczynając od najważniejszego) według podziału na dziedziny bezpieczeństwa wyróżnione w trzecim etapie badania

BEZPIECZEŃSTWO PAŃSTWA
E-7: (1.) Zbiorowe zakłócenia porządku publicznego, (2.) Nielegalne zgromadzenia i protesty społeczne, (3.) Cyberzagrożenia, (4.) Przestępczość zorganizowana o charakterze ekonomicznym, (5.) Zorganizowana przestępczość narkotykowa, (6.) Przestępczość nieletnich, (7.) Przestępczość kryminalna, (8.) Katastrofy i wypadki w ruchu drogowym, (9.) Katastrofy naturalne, (10.) Patologie społeczne.
BEZPIECZEŃSTWO PAŃSTWA
E-11: (1.) Często fakultatywne zapisy zawarte w ustawie o zarządzaniu kryzysowym wpływające na kształt organizacyjny systemu zarządzania kryzysowego, (2.) Poważnie zaniżone znaczenie omawianego obszaru, rzutujące na sprawność i skuteczność działania struktur administracji publicznej, (3.) Nieadekwatność organizacyjna i merytoryczna struktur systemu zarządzania kryzysowego w stosunku do zakresu i rodzaju ciążących zadań, a w tym brak wsparcia finansowego ze strony budżetu państwa, (4.) Nie w pełni realizowane zadania ustawowe przez jednostki samorządu terytorialnego, mające pośredni lub bezpośredni wpływ na skuteczność działania elementów systemu zarządzania, reagowania kryzysowego, np. prowadzone przez Wydziały Bezpieczeństwa i Zarządzania Kryzysowego kontrole stanu utrzymania melioracji szczegółowej, stanu przygotowania do potencjalnej awarii energetycznej – wykazały niski poziom utrzymania bądź przygotowania, (5.) Klęski żywiołowe (katastrofy, awarie techniczne), które mogą spowodować bardzo duże straty w zasobach ludzkich oraz infrastrukturze systemu zarządzania kryzysowego, (6.) Ograniczenia zasobów ratowniczych systemu zarządzania kryzysowego ze względów ekonomicznych, (7.) Nieskuteczność informowania, ostrzegania i alarmowania o możliwości wystąpienia lub wystąpieniu sytuacji kryzysowych, ze względu na brak odpowiednich w tym zakresie narzędzi, (8.) Deficyt sił i środków na likwidację powstałych szkód i strat oraz odbudowę.
BEZPIECZEŃSTWO SPOŁECZNE
E-1: (1.) Zagrożenie stabilności porządku geopolitycznego i reperkusje światowego kryzysu, zwłaszcza dla krajów i grup biedniejszych, mających mniejsze możliwości do radzenia sobie z jego niekorzystnymi następstwami, (2.) Brak autonomicznej polityki społecznej wobec zjawiska wzrostu nierówności społecznych. Podejmowane działania są niewystarczające bądź nieudolnie kopiowane,

(3.) Wadliwe mechanizmy rekrutacji elit politycznych. Problemami bezpieczeństwa społecznego zajmują się często osoby wyłonione z naruszeniem kryteriów merytokratycznych, (4.) Brak warunków instytucjonalnych do powstawania adekwatnych analiz eksperckich dotyczących najistotniejszych problemów społecznych, brak odbiorców takich analiz, (5.) Uwiąd dyskusji merytorycznych (uwzględniających także dyskusję o metodach badania i konstruowania analiz dotyczących bezpieczeństwa społecznego), co prowadzi do powstawania analiz uproszczonych, wręcz banalnych, o przypadkowej konstrukcji i małym kręgu oddziaływania, (6.) Brak rozwoju inicjatyw i struktur społeczeństwa obywatelskiego w obszarze bezpieczeństwa społecznego. Większość zadań i problemów przerzuca się na państwo lub po prostu stara się ich nie dostrzegać.
BEZPIECZEŃSTWO SPOŁECZNE
E-6: (1.) Kryzys ekonomiczny w efekcie rosnącego zadłużenia – kryzysu fiskalnego, (2.) Załamanie systemu świadczeń socjalnych (zwłaszcza emerytalnego), (3.) Rozwój kultury nieufności względem państwa, instytucji, innych ludzi – skutkujący wytwarzaniem się enklaw społecznych, (4.) Załamanie systemów infrastrukturalnych (*gwałtowne* lub *pełzające*).
BEZPIECZEŃSTWO KULTUROWE
E-4: (1.) Wojna, w tym wojny domowe i zamieszki na tle religijnym i etnicznym, (2.) Klęski żywiołowe, w tym globalne ocieplenie, (3.) Grabieże, kradzieże, dewastacja, przemyt, (4.) Niespójny system ochrony dóbr kultury, (5.) Polityka rządu, (6.) Niekompetentni ludzie zajmujący się ochroną dziedzictwa kulturowego, (7.) Wzrost ekspansji kultury masowej, (8.) Rozpad więzi społecznych i wartości rodzinnych, (9.) Globalizacja, (10.) Obojętność.
BEZPIECZEŃSTWO KULTUROWE
E-12: (1.) Osłabienie świadomości przynależności do różnego rodzaju wspólnot, ze wspólnotą narodową na czele, anomia społeczna, (2.) Osłabianie więzi międzyludzkich, chęci stowarzyszania się, wspólnego działania w celu realizacji interesów grupowych, zanik etosu współpracy i kompromisu, (3.) Brak spójnej polityki tożsamościowej i historycznej, (4.) Radykalizacja nastrojów, skłonność do postrzegania zjawisk społecznych w kategoriach dwóch skrajności, bez uwzględnienia złożoności sytuacji, (5.) Spadek jakości wykształcenia na różnych szczeblach edukacji, (6.) Wzrastająca presja ze strony różnego rodzaju separatyzmów (w tym śląskiego), (7.) Osłabienie świadomości religijnej – laicyzacja życia społecznego.

BEZPIECZEŃSTWO MILITARNE
E-9: (1.) Zagrożenie dotyczące zawleczenia choroby (czynnika) wysoce zakaźnego na terytorium kraju, (2.) Poszukiwanie oszczędności dla budżetu państwa w sferze obronnej, (3.) Zagrożenie dotyczące aktów terrorystycznych z udziałem czynnika biologicznego, (4.) Zagrożenie dotyczące nieintencjonalnego uwolnienia czynnika biologicznego z firmy farmaceutycznej wykorzystującej ww. czynnik, (5.) Zagrożenie dotyczące nieintencjonalnego uwolnienia czynnika biologicznego z placówki naukowo-badawczej wykorzystującej ww. czynnik.
BEZPIECZEŃSTWO MILITARNE
E-10: (1.) Lekceważenie problematyki bezpieczeństwa militarnego przez polityków, (2.) Poszukiwanie oszczędności dla budżetu państwa w sferze obronnej, (3.) Polityka mocarstwowa Federacji Rosyjskiej, (4.) Cyberatak, (5.) Rozpad lub ograniczenie możliwości działania NATO.
BEZPIECZEŃSTWO EKOLOGICZNE
E-3: (1.) Przekroczenie standardów emisyjnych do powietrza w wyniku awarii technologicznej, (2.) Ciągłe przekroczenie standardów emisyjnych do środowiska w wyniku np. transportu lub nieprawidłowo działającej instalacji, (3.) Niekontrolowany zrzut ścieków do środowiska (wód lub gleb), (4.) Brak dostępu do czystej wody użytkowej.
BEZPIECZEŃSTWO HYDROLOGICZNE
E-5: (1.) Uszkodzenia wałów przeciwpowodziowych spowodowane przez zwierzęta (bobry, nornice), (2.) Wystąpienie powodzi w trakcie prowadzonych inwestycji na wałach przeciwpowodziowych. Rozkopany wał przeciwpowodziowy nie spełni swojej roli. Woda bez kontroli zaleje obszary chronione, (3.) Wzrastające ryzyko powodzi zatorowych i utrudnienia w prowadzeniu akcji lodołamania wynikające ze zmian w profilu podłużnym i poprzecznym koryta rzeki, (4.) Problem zbyt małej świadomości społecznej w zakresie zagrożenia powodziowego oraz metod ograniczania ryzyka powodziowego na etapie przygotowania się do powodzi oraz na etapie prowadzenia akcji przeciwpowodziowej i usuwania skutków powodzi.
BEZPIECZEŃSTWO HYDROLOGICZNE
E-8: (1.) Powódź, (2.) Susza, (3.) Zanieczyszczenie rzek, (4.) Nieodpowiednie przepływy wymagane ekologicznie, (5.) Brak odpowiedniego impulsu wezbraniowego dla obszarów mokradłowych (pożądana powódź).

Źródło: opracowanie własne

Analiza materiału badawczego pokazała, że problematyka bezpieczeństwa (m.in. zagrożenia), znajdująca się w obszarze zainteresowania ekspertów, może być rozpatrywana z różnych, odmiennie uwarunkowanych perspektyw. Następstwem takiego zróżnicowania punktów wyjściowych są niejednakowe obrazy, różne konfiguracje zmiennych wyodrębniane w ramach tych samych dziedzin. Dodatkowo należy wskazać, że poszczególne zmienne i ich właściwości też nie są precyzyjnie określone. Eksperci wykorzystują bowiem do analizy zastanej rzeczywistości kategorie nieostre, trudne do skwantyfikowania, dające się zobrazować przy użyciu opisu, a jeśli tak, to te charakterystyki nie są zobiektywizowane. Z tych powodów znacznie utrudnione staje się prowadzenie analiz porównawczych.

Obserwacja powyższa potwierdza, że zagrożenia mają strukturę niejednorodną, zmienną i złożoną, co powoduje, że eksploracja ich jest dość ograniczona i zarazem podatna na zakłócenia. Nie oznacza to jednak, że badanie ukazało wyłącznie same rozbieżności w postrzeganiu zagrożeń przez respondentów. Przykładowo, po zanalizowaniu odpowiedzi na pytanie o kryteria, które pozwoliły dokonać wyboru punktów krańcowych stanu stabilności państwa – można stwierdzić, że o ile eksperci mieli raczej problem z dość dokładnym ukazaniem takich punktów, nie będąc, co trzeba mocno podkreślić, jednocześnie do końca przekonanymi, że każdorazowo niepożądane zjawiska wystąpią w takiej samej konfiguracji i natężeniu oraz o sile oddziaływania poszczególnych elementów, to już w przypadku kryteriów, które naprowadzać mają badacza na te newralgiczne obszary – w odpowiedziach wskazywano z dużą dokładnością na takie uwarunkowania, a zatem problemem jest określenie samego momentu krytycznego, co może świadczyć również i o tym, że ten punkt graniczny nie jest być może tak istotny, ponieważ każdorazowo znajdować się będzie w zasadzie w innym miejscu.

Bardzo ważne dla procesu identyfikacji zagrożeń, co potwierdzają uzyskane odpowiedzi, jest postrzeganie uwarunkowań zdarzeń niepożądanych zakłócających stan bezpieczeństwa w danej dziedzinie. Jak można wywnioskować z odpowiedzi, dopiero obserwacja tych wzajemnych oddziaływań czynników i ich następstw, oraz doświadczenie w zakresie dotychczasowych zdarzeń niepożądanych – stwarzają możliwości formułowania prognoz w przedmiotowym zakresie. Natomiast jeśli chodzi o zadanie polegające na zdefiniowaniu przez ekspertów stanu braku bezpieczeństwa, czyli sytuacji, w której występuje duże rzeczywiste zagrożenie, a postrzeganie tego zagrożenia jest prawidłowe – wskazywano, jako na istotne czynniki, głównie na zasięg oddziaływania oraz natężenie poszczególnych zjawisk.

W przypadku próby określenia subiektywnego poczucia braku bezpieczeństwa zazwyczaj odwoływano się tu do pojedynczych dysfunkcji systemu, niemających szerszego oddziaływania, ale przez swój negatywny wpływ na jednostkę – przyczyniających się do wytwarzania się u niej błędnego wyobrażenia o ich zasięgu, znaczeniu. Ponadto wskazywano w odniesieniu do tej problematyki również na zaniedbania ze strony państwa, które powodują pogłębianie się dystansu między zobiektywizowanym stanem rzeczy a indywidualnym oglądem, jak i na znaczenie

przekazów medialnych, które na tyle skutecznie oddziałują na odbiorcę, że skłonny jest on przyjmować za obowiązujące przedstawiane w tych komunikatach obrazy. Na podstawie zgromadzonych danych można wyprowadzić wniosek, że eksperci przypisują dość istotną funkcję subiektywnemu poczuciu braku bezpieczeństwa, które stanowi, jak się wydaje, ważną determinantę zachowań.

W pierwszej części niniejszego tekstu wskazano, że foresight jest procesem ciągłym. Mając to na uwadze, należy stwierdzić, że badania nie można uznać za zakończone. Zrealizowane trzy etapy miały charakter pilotażowy. Analiza odpowiedzi udzielonych przez dwunastu ekspertów reprezentujących raczej odmienne dziedziny bezpieczeństwa, mających przy tym różne instytucjonalne afiliacje, a tym samym inny rodzaj styczności z zagrożeniami, czyli odmienne perspektywy – pozwoliła co prawda na poszukiwanie wspólnego poziomu opisu adekwatnego dla tych perspektyw, ale już rozpoznanie w zakresie identyfikacji zagrożeń miało dość ograniczony charakter. Nie można zatem uznać, że uzyskane wyniki mają wartość praktyczną, jeśli przyjąć, że miałyby one być zastosowane społecznie w aktualnym stanie, a nie tylko do dalszej kontynuacji badania i doskonalenia narzędzia. Jednym z podstawowych wyzwań, które powinny zostać w pierwszej kolejności podjęte w następnym z etapów badania, jest przeprowadzenie prób uzgodnień w zakresie struktury i zawartości siatki pojęciowej z zakresu bezpieczeństwa. Deficyt, który ujawnił się w tym obszarze, jest znaczny i stanowił utrudnienie przy prowadzeniu porównań, stwarzając znaczne możliwości odchyleń poprzez konieczność odwoływania się do interpretacji. Oczywiście zdawać sobie trzeba sprawę również i z tego, że stworzenie uniwersalnych tabel zmiennych i wartości nie jest możliwe, jednak podjęcie prób w tym zakresie z pewnością zwiększy zakres zjawisk dających się zmierzyć.

Na koniec warto także zauważyć, że te różne perspektywy zaprezentowane przez ekspertów, w ramach wskazanych przez nich dziedzin bezpieczeństwa, nie stwarzają bariery uniemożliwiających prowadzenie analiz. Nawet w odległych od siebie obszarach udawało się znaleźć wspólny poziom opisu poprzez możliwość zastosowania tych samych kategorii porządkujących. Niewątpliwie dla badań w zakresie identyfikacji zagrożeń bezpieczeństwa narodowego, ale także szerzej – dla nauk o bezpieczeństwie, jest to swoiste wyzwanie. Tym wyzwaniem jest dążenie do podejmowania działań zintegrowanych. Co prawda, nie można w tym kontekście pominąć, że specjalizacja umożliwia koncentrację badań nad wąskimi fragmentami rzeczywistości, ale trzeba też zauważyć, że jej negatywnym następstwem jest niebezpieczeństwo *jednostronności poznania*. Obrazują ją dwie tendencje: oderwanie od otaczających zjawisk oraz ograniczanie w zastosowaniu posiadanej wiedzy. Ponadto ubocznym skutkiem specjalizacji, czyli swoistej izolacji od pokrewnych dziedzin, jest nadmierna hermetyczność, a więc brak zainteresowania zjawiskami z pogranicza dyscyplin, czy dublowanie badań[91]. Postulat integracji wyraża się natomiast

[91] B. Krauz-Mozer, W. Szostak, *Teoria polityki. Podstawy metodologiczne politologii empirycznej*, Uniwersytet Jagielloński, Kraków 1993, s. 9.

konieczności takiej organizacji procesu badawczego, która umożliwi połączenie wysiłków przedstawicieli różnych dyscyplin[92]. W naukach o bezpieczeństwie, co potwierdziło przeprowadzone badanie foresight, sam przedmiot badań tworzy już podstawowe warunki sprzyjające integracji, co może mieć zasadnicze znaczenie dla efektywności procesu identyfikacji zagrożeń bezpieczeństwa narodowego.

[92] Tamże, s. 10.

7. Metodyka zarządzania ryzykiem na potrzeby systemu zarządzania kryzysowego

Definiowanie zdarzeń niepożądanych poprzez wskazanie korelacji pomiędzy *konsekwencjami* i *częstotliwością* weszło na stałe do praktyki zarządzania organizacją. Możliwość weryfikacji celów i strategii w oparciu o zjawisko niepewności podnosi niewątpliwie skuteczność organizacji. Pozwala to nie tylko przygotować się na sytuacje krytyczne, ale wręcz kreować zdarzenia w sposób przybliżający organizację do osiągnięcia zamierzonego celu.

Zarządzanie ryzykiem można wykorzystywać w różnych obszarach działalności organizacji. Przedmiotowo można je odnieść do pojedynczych procesów, mniej lub bardziej złożonych projektów, czy wręcz pełnej sfery jej aktywności. Zakres podmiotowy może być komplementarny i odnosić się jedynie do wybranych elementów organizacji. Z tego punktu widzenia zarządzanie ryzykiem staje się coraz częściej pożądanym lub wręcz niezbędnym elementem procesu definiowania celów, czy też kreowania strategii długofalowego działania.

Do sfery zarządzania kryzysowego elementy zarządzania ryzykiem zostały wprowadzone przy nowelizacji ustawy o zarządzaniu kryzysowym w 2009 r. Nowe przepisy nie tylko wprowadziły do polskiego prawa pojęcia ryzyka, oceny ryzyka i mapy ryzyka, ale także uzupełniły planowanie cywilne o dwa dokumenty strategiczne, w procesie przygotowania których niezbędne jest odwołanie się bezpośrednio do elementów procesu zarządzania ryzykiem. Dokumenty te to: Raport o zagrożeniach bezpieczeństwa narodowego oraz Narodowy Program Ochrony Infrastruktury Krytycznej. Pierwszy z dokumentów stanowi kluczowy element pozwalający zdefiniować ryzyka dla poszczególnych zagrożeń ujętych w planach zarządzania kryzysowego, drugi określa ogólne dyrektywy na potrzeby planów ochrony infrastruktury krytycznej sporządzanych przez ich właścicieli.

Na podstawie delegacji ustawowej, w 2009 r. Rządowe Centrum Bezpieczeństwa rozpoczęło przygotowywanie Raportu o zagrożeniach bezpieczeństwa narodowego. Dokument został sporządzony w 2010 r. i przyjęty przez Radę Ministrów w 2011 r. Pierwszą iterację dokumentu przeprowadzono, zgodnie z wymogiem ustawowym, w 2013 r.

Na potrzeby dokonania oceny ryzyka do *Raportu o zagrożeniach bezpieczeństwa narodowego* Rządowe Centrum Bezpieczeństwa przygotowało w 2010 r. *Procedurę opracowania raportu cząstkowego* (wraz z arkuszem kalkulacyjnym) *do Raportu o zagrożeniach bezpieczeństwa narodowego*.

Biorąc pod uwagę konieczność ciągłej weryfikacji jakości procesu oraz podnoszenia poziomu zarządzania ryzykiem, a także doświadczenia wyniesione w trak-

cie prac nad Raportem (…) przystąpiono do sporządzenia nowej *Procedury opracowywania Raportu*.

Podstawę do jej przygotowania stanowiły z jednej strony ramy ustawy o zarządzaniu kryzysowym oraz rozporządzenia w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego, a z drugiej dyrektywy norm ISO 31000 i 31010.

Zgodnie z przepisami:

§ 4. *Raport (…) jest dokumentem obejmującym następujące elementy:*

1) *wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka, o której mowa w art.3 pkt 10 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, obejmującej wyszczególnienie rodzajów i charakterystyki zagrożeń:*
   a) *o istotnym wpływie na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego,*
   b) *których skutki mogą:*
      – *godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, a w szczególności w suwerenność, niepodległość i nienaruszalność terytorium,*
      – *zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach, albo środowisku na znacznych obszarach,*
      – *oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa,*
      – *dotyczyć terytorium Rzeczpospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie,*
   c) *występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych,*
   d) *związanych z międzynarodowym terroryzmem godzącym w istotne interesy Rzeczypospolitej Polskiej, w tym w funkcjonowanie infrastruktury krytycznej oraz życie i zdrowie jej obywateli;*
2) *określenie celów strategicznych, w szczególności:*
   a) *wskazanie celów, jakie należy osiągnąć, aby zminimalizować możliwość wystąpienia zagrożenia lub jego skutków,*
   b) *hierarchizację celów według kryterium ważności lub wskazanie celów priorytetowych;*
3) *wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych, a szczególnie tych, których realizacja wymaga działań wykraczających poza posiadane kompetencje;*
4) *wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych;*
5) *programowanie zadań w zakresie poprawy bezpieczeństwa państwa przez wskazywanie określonych regionalnych i lokalnych inicjatyw, w szczególności:*
   a) *wyszczególnienie programów krajowych, wojewódzkich, powiatowych i gminnych,*
   b) *wskazanie realizatorów programów:*

– *rządowych,*
– *samorządowych,*
– *pozarządowych,*

c) *sposoby finansowania programów,*
d) *okresy trwania programów;*

6) *określenie priorytetów w reagowaniu na określone zagrożenia, w tym ich wpływ na:*
a) *zasady reagowania w przypadku wystąpienia zagrożenia,*
b) *hierarchizację działań;*

7) inne informacje, które zdaniem wykonawcy mogą być przydatne przy tworzeniu Krajowego Planu Zarządzania Kryzysowego.

Od 1 stycznia 2014 r. obowiązuje nowy dokument, który rozszerza obszar objęty Procedurą. Dokumentem tym jest Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności. Zgodnie z nią państwa członkowskie mają *posiadać zdolność do zarządzania ryzykiem*, czyli *umiejętność zmniejszania, dostosowania się lub ograniczania ryzyka, w szczególności skutków lub prawdopodobieństwa klęsk żywiołowych lub katastrof*.

Dlatego na państwa członkowskie nałożono obowiązek prowadzenia cyklicznej oceny ryzyka. Ocena ryzyka jest rozumiana jako całościowy, przekrojowy proces:

- identyfikacji ryzyka wystąpienia klęsk żywiołowych i katastrof (rozumianych jako sytuacje, które mogą mieć poważne skutki dla ludzi, środowiska naturalnego lub mienia, w tym dziedzictwa kulturowego),
- jego analizy (w szczególności w zakresie potencjalnych skutków oraz prawdopodobieństwa ich wystąpienia),
- oraz szacowania (określenie, do jakiego stopnia dane ryzyko jest dla państwa członkowskiego/lub władz regionalnych akceptowalne).

W zakresie zarządzania ryzykiem, państwa członkowskie powinny również posiadać odpowiedni proces planowania mający na celu:

- zapobieganie ryzyku (działanie mające na celu ograniczanie ryzyka lub łagodzenie negatywnych skutków klęsk żywiołowych i katastrof dla ludzi, środowiska naturalnego oraz mienia, w tym dziedzictwa kulturowego),
- przygotowanie się na wypadek zaistnienia klęski lub katastrofy (w szczególności odpowiedni stan zasobów ludzkich, środków materialnych, struktur, społeczności i organizacji).

Państwa powinny być również zdolne do podejmowania działań mających na celu zapobieganie ryzyku oraz przygotowania się do skutecznego i szybkiego reagowania w przypadku klęsk lub katastrof.

7.1. Definicje pojęć użytych w metodyce

Ryzyko – prawdopodobieństwo wystąpienia zdarzenia wraz z jego niekorzystnymi skutkami dla realizacji celów organizacji określonych zakresem zarządzania ryzykiem (w określonym czasie).

Ryzyko bazowe – ryzyko określone na podstawie prawdopodobieństwa i skutków zdarzeń będące podstawą dla określenia ryzyka właściwego.

Ryzyko właściwe – określone na podstawie ryzyka bazowego ryzyko w kontekście podatności organizacji i stopnia, w jakim oddziałują na nie inne ryzyka.

Podatność organizacji na ryzyko – właściwość organizacji określona przez próg wytrzymałości na oddziałujące na nią ryzyko.

Szacowanie ryzyka – podproces zarządzania ryzykiem niezbędny do podjęcia decyzji o sposobie postępowania z ryzykiem polegający na identyfikacji, analizie i ocenie ryzyk.

Identyfikacja ryzyka – pierwszy etap szacowania ryzyka pozwalający na wyłonienie zdarzeń negatywnie oddziałujących na cele taktyczne oraz wynikające z nich procesy.

Analiza ryzyka – drugi etap szacowania ryzyka pozwalający na dokonanie jego oceny oraz przygotowanie organizacji do podjęcia działań ograniczających ryzyka nieakceptowalne, w trakcie którego należy dla zidentyfikowanych ryzyk określić prawdopodobieństwo i konsekwencje ich wystąpienia oraz stopień niepewności analizy.

Niepewność analizy ryzyka – tolerowany poziom błędu wartości skutku i prawdopodobieństwa ryzyka wynikający z zastosowanych narzędzi i technik (ilościowe, jakościowe lub mieszane) lub stopnia pewności danych wejściowych wykorzystywanych w procesie analizy ryzyka.

Ocena ryzyka – ostatni, trzeci etap szacowania ryzyka polegający na zestawieniu na matrycy ryzyka i porównaniu wszystkich zidentyfikowanych i przeanalizowanych ryzyk oraz podjęciu decyzji odnośnie do sposobów postępowania z nimi.

Hierarchizacja ryzyk – etap szacowania ryzyka polegający na rangowaniu zidentyfikowanych ryzyk oraz wskazaniu zbioru tych, w stosunku do których organizacja powinna określić sposoby postępowania.

Rangowanie ryzyk – kwalifikacja oszacowanych ryzyk według wartości ich rang od najmniejszego do największego.

Zakres zarządzania ryzykiem – obszar i granice zarządzania ryzykiem związane z osiągnięciem celów określonych ustawą, takich jak: rozwój, bezpieczeństwo itd.

Organizacja – podmiot mający realizować określone cele i z tego powodu dokonujący szacowania i zarządzania ryzykiem na potrzeby raportu o zagrożeniach bezpieczeństwa narodowego na odpowiednim poziomie (państwo polskie, ministrowie, kierownicy urzędów centralnych, wojewodowie).

Koordynator – organizacja odpowiedzialna za koordynację szacowania i zarządzania ryzykiem poprzez wskazanie metodyki zarządzania ryzykiem, edukację organizacji, uzgadnianie i zapewnienie spójności wyników szacowania ryzyka, kompilowanie raportów cząstkowych (RCB, ABW – w zakresie zagrożeń terrorystycznych).

Sytuacja kryzysowa – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.

Zagrożenie – przyczyny zdarzenia, które może wpływać niekorzystnie na życie, zdrowie, mienie lub środowisko.

Mapa ryzyka – należy przez to rozumieć mapę lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę.

Mapa zagrożenia – należy przez to rozumieć mapę przedstawiającą obszar geograficzny objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń.

Zdarzenie – wystąpienie okoliczności, które wpływają niekorzystnie na osiągnięcie celów.

Efekt domino – określa sytuację, w której jedno zdarzenie niekorzystne powoduje szereg następujących po sobie, wynikających jedno z drugiego zdarzeń niekorzystnych. Sformułowania tego używa się zazwyczaj w odniesieniu do procesów gwałtownych, destrukcyjnych, niemożliwych do opanowania, gdy już zostaną zainicjowane.

Infrastruktura krytyczna – systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Skutek – następstwo zidentyfikowanego ryzyka, potencjalne konsekwencje prowadzące do zmiany poziomu ryzyka, następstwo oddziaływania zagrożenia na ludzi, mienie, środowisko, infrastrukturę lub zdefiniowane przez organizację cele.

Scenariusz – zapisany w dowolnej notacji katalog potencjalnych przyczyn oraz możliwy do zaistnienia ciąg następujących po sobie zdarzeń będących następstwem wystąpienia ryzyka, prezentujący możliwie szeroki katalog skutków.

Profil ryzyka – zbiór cech pozwalających jednoznacznie scharakteryzować ryzyko, uwzględniając jego istotność oraz sposób postępowania z ryzykiem.

Kontekst – sparametryzowany zbiór informacji, które są niezbędne do wskazania właściwego poziomu ryzyka oraz zasad postępowania z nim, pozwalające na scharakteryzowanie samej organizacji (kontekst wewnętrzny) i środowiska, w którym organizacja realizuje swoje cele (kontekst zewnętrzny).

Monitorowanie – proces polegający na ciągłej weryfikacji stanu: ryzyka oraz procesu zarządzania nim, uwzględniający konieczność ciągłego doskonalenia struktury odpowiedzialnej za ten proces oraz weryfikacji poprawności oraz skuteczności przyjętej metodyki.

Cel – określony przez organizacje, pożądany stan lub efekt intencjonalnego działania.

Proces – zdefiniowany na poziomie strategicznym, taktycznym i operacyjnym ciąg podejmowany przez organizację działań zmierzających do osiągnięcia założonych celów.

Proces krytyczny – proces, którego trwałe lub czasowe przerwanie wpłynie negatywnie na osiągnięcie celu strategicznego.

Proces zarządzania ryzykiem – uporządkowane w czasie stosowane oraz przyjęte w organizacji procedury: ustalania kontekstu, oceny ryzyka i postępowania z ryzykiem.

Polityka zarządzania ryzykiem – wdrożone w organizacji ogólnie respektowane i stosowane zasady odnoszące się do funkcjonującej struktury zarządzania ryzykiem wraz z przypisanymi jej odpowiedzialnościami.

Skuteczność – miara określająca stopień osiągnięcia zamierzonego celu.

Efektywność – miara określająca wartość dodaną (netto) celowego działania organizacji.

Interesariusz – osoba lub organizacja, która posiada zdolność oddziaływania na ryzyko bądź proces zarządzania ryzykiem, lub na którą to ryzyko może oddziaływać.

Właściciel ryzyka – organ władzy, komórka organizacyjna urzędu bądź inna osoba, która posiada największe kompetencje w zakresie redukcji ryzyk (władzę umożliwiającą wydawanie wiążących decyzji, budżet, zasoby).

Podatność – cecha organizacji determinowana przez jej słabe punkty lub luki w zabezpieczeniach określająca stopień, w jakim oddziałujące na nią ryzyka mogą prowadzić do niepożądanych zdarzeń.

Zabezpieczenie – zasób materialny (np. rzeczowy, osobowy, finansowy) lub niematerialny (np. informacyjny, prawny), który organizacja wykorzystuje lub może wykorzystać do obniżenia podatności na ryzyko.

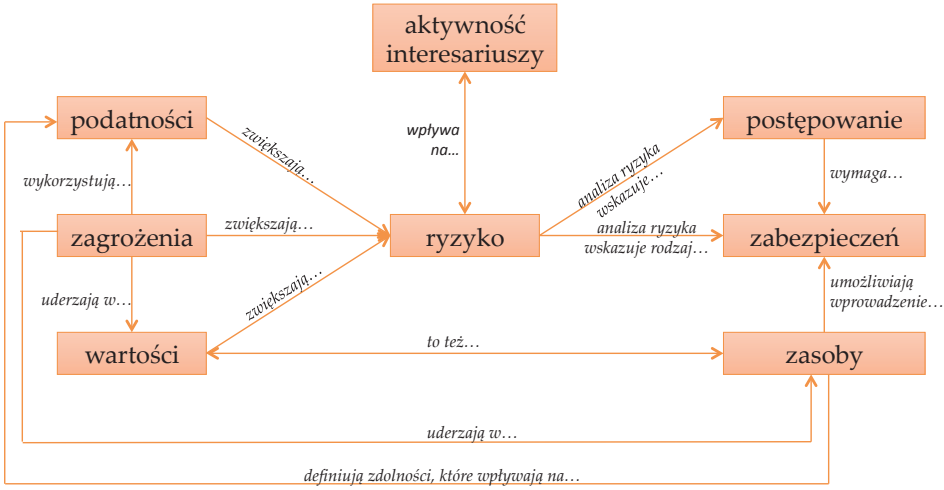
Akceptacja – postrzeganie ryzyka jako nieistotnego z punktu widzenia organiza-

cji, będące podstawą dla decyzji o braku podejmowania działań zmierzających do mityzacji ryzyka.

Wprowadzenie zabezpieczeń – działanie zmierzające do mityzacji ryzyka poprzez podnoszenie odporności organizacji oraz jej środowiska zewnętrznego; działanie bezpośrednio wpływające na prawdopodobieństwo.

Zapewnienie ciągłości działania – działanie zmierzające do ograniczenia skutków ryzyka dla organizacji, a w szczególności do zapewnienia realizacji przez nią krytycznych procesów (pozwalających na wypełnienie jej polityki i celów).

Zależności pomiędzy podstawowymi pojęciami przedstawia rysunek 7.1.



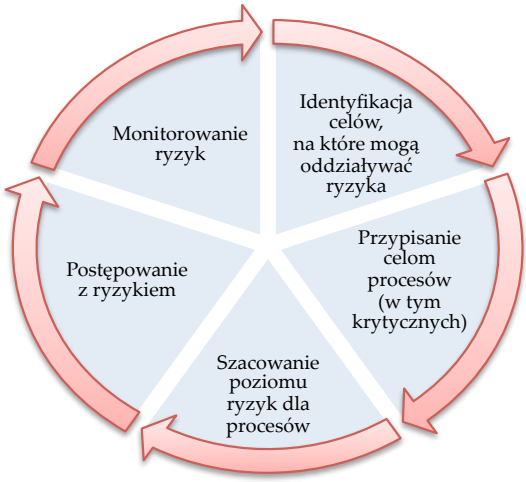
Rysunek 7.1. Zależności pomiędzy podstawowymi kategoriami, którymi posługuje się metodyka

Źródło: opracowanie własne

7.2. Przygotowanie organizacji do wdrożenia systemu zarządzania ryzykiem

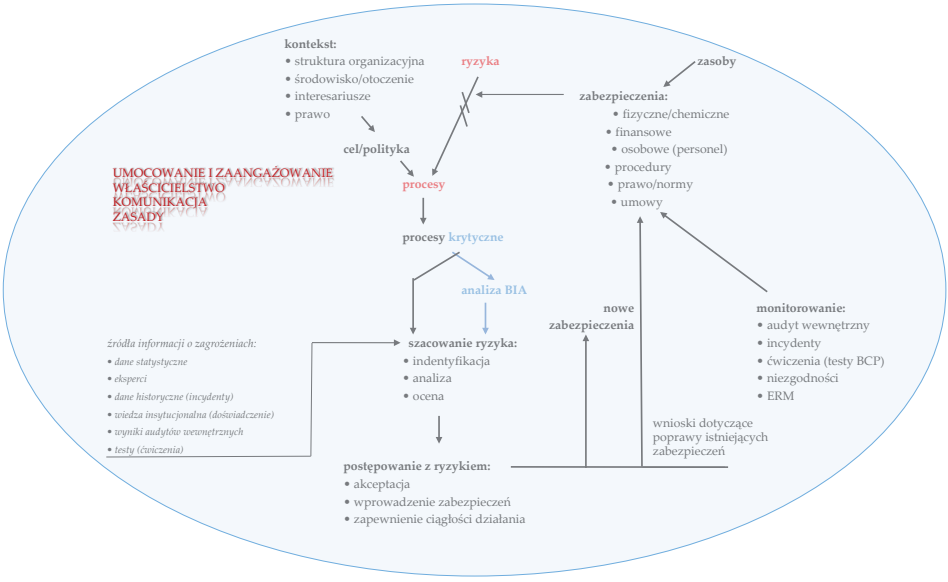
Główne podprocesy zarządzania ryzykiem

Niezbędne jest, aby w celu uzyskania porównywalnych wyników dla wszystkich szacowanych ryzyk, które zostaną zaprezentowane w Raporcie o zagrożeniach bezpieczeństwa narodowego, wytwórcy raportów cząstkowych ujednolicili sposoby ich sporządzania. Proces sporządzania raportów cząstkowych (przedstawiony na rysunku 7.2.) został oparty na ogólnym cyklu zarządzania ryzykiem: identyfikacji celów organizacji, określenia procesów niezbędnych do ich osiągnięcia, oszacowania poziomu ryzyk dla procesów, wskazanie sposobów zarządzania ryzykiem oraz monitorowanie efektów postępowania z ryzykiem.



Rysunek 7.2. Ogólny cykl zarządzania ryzykiem

Źródło: opracowanie własne



Rysunek 7.3. Główne podprocesy zarządzania ryzykiem właściwe do sporządzenia raportów cząstkowych i Raportu o zagrożeniach bezpieczeństwa narodowego – zależności pomiędzy głównymi kategoriami

Źródło: opracowanie własne

Zasady zarządzania ryzykiem

Proces zarządzania ryzykiem opiera się na czterech ogólnych i odwołujących się do każdego podprocesu regułach:

1) niezbędne jest, aby każdy podmiot sporządzający raport cząstkowy przyjął i respektował **zasady zarządzania ryzykiem**,
2) każdy podmiot sporządzający raport cząstkowy powinien w jasny i precyzyjny sposób określić **umocowanie** wykonawców poszczególnych podprocesów i decydentów w procesie (uprawnienia i odpowiedzialności) oraz obszar ich **zaangażowania** (zakres realizowanych zadań, w tym: sporządzanie analiz, ich przedkładanie decydentom oraz zatwierdzanie),
3) podmiot sporządzający raport cząstkowy powinien mieć wiedzę co do właściwych dla siebie ryzyk, akceptować swoje **właścicielstwo** w stosunku do nich oraz znać właścicieli innych ryzyk (szczególnie, jeśli zidentyfikował je w swoim urzędzie),
4) niezbędne jest zapewnienie kanałów komunikacji i ciągłe **komunikowanie się** w trakcie całego procesu zarządzania ryzykiem pomiędzy poszczególnymi elementami struktury podmiotu sporządzającego raport cząstkowy.

Zarządzanie ryzykiem definiuje się jako *logicznie uporządkowany zbiór reguł i zasad, który w sposób jednolity i stały jest stosowany w odniesieniu do ryzyka* związanego z działaniem organizacji. o skuteczności procesu decyduje więc nie tylko wybór metody oceny ryzyka, poprawność jego przeprowadzenia, czy odpowiednio wpisane w strukturę organizacyjną upoważnienia oraz kompetencje, ale również zbiór ogólnie akceptowalnych i rozumianych w ten sam sposób (przez wszystkich uczestników procesu) zasad.

Biorąc pod uwagę złożoną strukturę systemu zarządzania kryzysowego oraz interdyscyplinarny charakter dokumentów planistycznych, wskazane zasady przyczynią się do zwiększenia poprawności uzyskanych w trakcie oceny ryzyka wyników.

Przyjęcie jednolitych zasad pozwoli z jednej strony na standaryzację sporządzania raportów cząstkowych przez ich wykonawców, a z drugiej na stworzenie spójnego modelu weryfikacji ich poprawności.

Zarządzanie ryzykiem:
1) Kreuje i chroni wartości
Zarządzanie ryzykiem pozwala na zdefiniowanie bądź zredefiniowanie celów oraz poprawę skuteczności ich osiągnięcia. Jednym z głównych celów raportów cząstkowych oraz sporządzanego na ich podstawie Raportu o zagrożeniach bezpieczeństwa narodowego jest ochrona ważnych dla bezpieczeństwa narodowego wartości:

- międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego,
- bezpieczeństwa państwa, jego porządku konstytucyjnego, a w szczególności w suwerenności, niepodległości i nienaruszalności terytorium,
- życia lub zdrowia dużej liczby osób, mienia w znacznych rozmiarach, a także środowiska na znacznych obszarach.

2) Jest zintegrowane z procesami organizacji i ze strukturą zarządzania
Przygotowanie Raportu (…) jest jednym z elementów szerszego procesu planowania cywilnego. Zgodnie z ustawą o zarządzaniu kryzysowym jego wyniki powinny

służyć za podstawę do sporządzenia planu zarządzania kryzysowego. Natomiast do jego sporządzenia niezbędne jest z kolei pozyskanie informacji o składowych ryzyk (prawdopodobieństwo, skutki, podatność) zidentyfikowanych dla infrastruktury krytycznej.

Funkcjonalnie, Raport (…) stanowi element wspomagający proces podejmowania decyzji pośrednio poprzez wpływ na procedury zawarte w planach zarządzania kryzysowego i bezpośrednio przez wskazanie w nim działań i programów redukujących ryzyka. W konsekwencji wpływa zarówno na minimalizację skutków (faza reagowania), jak i oddziałuje na całe ryzyko w fazie zapobiegania.

Biorąc pod uwagę zadania poszczególnych organów administracji rządowej wynikających z ustawy o wojewodzie oraz ustawy o działach w administracji rządowej, a także potencjalnie uzyskiwaną w trakcie zarządzania ryzykiem użyteczność (efektywność) należy przyjąć, że zarządzanie ryzykiem nie powinno być traktowane jako odrębny proces, ale jako element każdego działania mogącego mieć wpływ na realizację tych zadań.

3) Jest istotnym elementem procesu decyzyjnego

Zarządzanie ryzykiem skoncentrowane jest na działaniach długofalowych o strategicznym znaczeniu dla organizacji. W konsekwencji oszacowanie ryzyka powinno skutkować wyłonieniem ryzyk, na które organizacja będzie oddziaływać (znajdą się one w planie postępowania z ryzykiem) poprzez wprowadzenie nowych lub poprawę skuteczności już istniejących zabezpieczeń. Mając na uwadze efektywność wykorzystania środków publicznych niezbędnych do zmniejszenia podatności, decyzje odnośnie do ich alokacji powinny zostać poprzedzone oceną ryzyka.

4) Uwzględnia niepewność

Ze względu na ograniczone zasoby baz danych (lub ich brak dla niektórych zagrożeń), gromadzone w trakcie monitorowania ryzyka informacje, będące danymi wejściowymi dla kolejnych etapów zarządzania ryzykiem, nie powinny stanowić jedynego źródła wiedzy zespołów odpowiedzialnych za przygotowanie raportów cząstkowych. Należy dążyć do dywersyfikacji sposobów pozyskiwania danych o ryzykach, wykorzystując między innymi wiedzę ekspercką lub wynikającą z przeprowadzonych audytów i kontroli.

Należy założyć, że każdy rodzaj informacji (bez względu na źródło jej pochodzenia) obarczony jest pewnym stopniem niepewności. Niepewność ta powinna zostać zaprezentowana, szczególnie w trakcie procesu podejmowania decyzji. Określenie granicy błędu dla wyników oceny ryzyka może w istotny sposób wpłynąć na istotę decyzji.

5) Jest systemowe (według reguł), uporządkowane i realizowane zgodnie z założonym harmonogramem

Zarządzanie ryzykiem powinno odbywać się według udokumentowanych zasad, a proces powinien zapewnić uzyskanie możliwie rzeczywistych wyników. Rezultaty analizy ryzyka powinny (bez zbędnej zwłoki) zostać zaimplementowane do planów zarządzania ryzykiem oraz stanowić podstawę do podejmowanych decyzji. Czas, który upłynie od momentu oszacowania poziomu ryzyka do podjęcia nie-

zbędnych decyzji odnoszących się do jego mitygacji powinien być możliwie krótki. Przedłużanie procesu decyzyjnego, przy zmiennym ryzyku, może skutkować podjęciem nieadekwatnej, w stosunku do zidentyfikowanego ryzyka, decyzji.

6) Opiera się na najlepszych dostępnych informacjach

Przed rozpoczęciem szacowania ryzyka należy zinwentaryzować wszystkie istotne i dostępne źródła wiedzy na temat ryzyk. Źródłami tymi mogą być między innymi wyniki:

- analizy danych statystycznych,
- analizy danych historycznych,
- szacowania eksperckiego,
- oceny sytuacji międzynarodowej,
- modelowania matematycznego,
- analizy danych z systemów monitorowania zagrożeń,
- badania przypadków (*case study*),
- oraz innych metod wskazanych w normie ISO 31010.

Przy wykorzystaniu eksperckiej metody szacowania ryzyka należy wziąć pod uwagę, że jej poprawność należy zweryfikować w oparciu o rzetelne uzasadnienie wyników lub wskazanie dowodów przemawiającymi na ich rzecz.

Za ekspertów należy uznać przede wszystkim pracowników instytucji posiadających niezbędną wiedzę z różnych szczebli hierarchii organizacyjnej.

7) Wymaga ciągłej komunikacji

W całym procesie zarządzania ryzykiem powinna zostać zapewniona ciągła komunikacja między interesariuszami wewnętrznymi i zewnętrznymi oraz właścicielami poszczególnych ryzyk w celu osiągnięcia bardziej wiarygodnych i spójnych wyników szacowania i zarządzania ryzykiem.

Pozostałe zasady:

8) Należy decentralizować proces szacowania ryzykiem

W celu zwiększenia odpowiedzialności i świadomości uczestników etapu szacowania ryzyka niezbędne jest włączenie właścicieli ryzyk oraz pracowników na każdym szczeblu organizacji do szacowania ryzyka. Ich wiedza odnosząca się do kontekstu wewnętrznego i zewnętrznego organizacji jest niezbędna do prawidłowego przeprowadzenia etapu.

9) Niezbędne jest wdrożenie mechanizmu komentowania i uzasadniania

Wszelkie decyzje podjęte w trakcie szacowania ryzyka (np. jakie scenariusze będą analizowane, dlaczego wyceniono skutek na taką wartość) neleży pisemnie komentować i uzasadniać. Zachowanie tej zasady pozwala na zapewnienie powtarzalności i spójność przy kolejnej iteracji szacowania ryzyka.

10) Należy zapewnić powtarzalność metodyki szacowania ryzyka

Należy dążyć do sytuacji, w której kolejne iteracje szacowania ryzyka będą przeprowadzane w oparciu o taką samą lub zbliżoną metodę. Powtarzalność można osiągnąć poprzez zastosowanie mechanizmu komentowania i uzasadniania, jasną i czytelną metodykę szacowania i dobrze opisane skale (uniwersalność, jasne

i obiektywne kryteria zaliczania ryzyk do poszczególnych stopni skali). Powtórne szacowanie tego samego ryzyka (przy niezmienionych okolicznościach) dokonane przez inny zespół (albo nawet przez ten sam, ale w odstępie czasu) i dysponujący podobną wiedzą powinno doprowadzić do zbieżnych wyników.

11) Należy zapewnić porównywalność metodyk szacowania ryzyka

Organizacja powinna być w stanie:

- porównać ryzyka między sobą w czasie (określić, jak zmieniło się to samo ryzyko w stosunku do poprzedniej iteracji),
- porównać wszystkie ryzyka zidentyfikowane w organizacji podczas jednego szacowania (w celu podjęcia decyzji co do hierarchizacji ryzyk i określenia postępowania z ryzykami, np. poprzez alokację środków finansowych).

Niezbędne jest stosowanie jednolitej metodyki w całej organizacji, a w sytuacji, gdy metodyka ulega zmianie, przygotować tabele przejściowe.

12) Należy zachować kolejność *od ogółu do szczegółu*

Przystępując do szacowania ryzyka, na wstępie należy ująć je syntetycznie i na dużym poziomie ogólności (najczęściej jakościowo). Po wskazaniu listy ryzyk krytycznych (istotnych) należy dokonać ich szczegółowej analizy (o ile to możliwe – ilościowo).

13) Należy zachować kolejność od skutku do przyczyny

Przystępując do szacowania ryzyka, należy na wstępie określić katalog skutków (w przypadku wykorzystania metody Bow-tie). Dopiero w następnym kroku (dla ryzyk o najbardziej dotkliwych skutkach) przystępujemy do szacowania przyczyn. Analogicznie w przypadku wykorzystania metod *drzew* zaczynamy od metody ETA (*Event Tree Analysis* – analiza drzewa zdarzeń), a w drugim kroku dla ryzyk krytycznych dokonujemy analizy FTA (*Fault Tree Analysis* – analiza drzewa błędów).

14) Należy racjonalnie określić katalog rozważanych scenariuszy

Ze względu na ograniczone zdolności organizacji co do możliwości przeanalizowania wszystkich, wskazanych w trakcie identyfikacji ryzyk, scenariuszy powinno się dążyć do redukcji ich katalogu. Należy koncentrować się na ryzykach, których skutki mogą oddziaływać na cele operacyjne i strategiczne, istotne z punktu widzenia zarządzania ryzykiem.

Umocowanie i zaangażowanie

Skuteczne i efektywne zarządzanie ryzykiem musi mieć swoje oparcie w strukturze organizacji, która powinna jasno zdefiniować uczestników całego procesu oraz ich odpowiedzialności. Niezbędne jest wskazanie ról i właściwości poszczególnych osób w każdym z etapów:

- polityki zarządzania ryzykiem,
- projektowania całego procesu wraz z określeniem odpowiedzialności,
- przeprowadzenia procesu lub uczestnictwa w nim,
- akceptacji wyników szacowania ryzyka,
- podejmowania decyzji w zakresie działań zmierzających do mityzacji ryzyka.

Ponieważ przepisy ustawy o zarządzaniu kryzysowym w sposób formalny definiują całą strukturę ramową, nie ma potrzeby definiowania jej na nowo przez każdy podmiot przygotowujący raport cząstkowy.

Zgodnie z tymi przepisami: ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie, zgodnie ze swoimi kompetencjami, sporządzają Raport o zagrożeniach bezpieczeństwa narodowego. Koordynację przygotowania raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, a w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego. Raport przyjmuje Rada Ministrów w drodze uchwały.

Natomiast na potrzeby sporządzenia raportów cząstkowych konieczne jest wpisanie tego procesu w działalność struktury organizacyjnej (umocowanie) oraz wskazanie wykonawców i decydentów (zaangażowanie).

W konsekwencji tego działania organizacja powinna powołać zespół ds. zarządzania ryzykiem, w którego skład powinni wchodzić przedstawiciele wszystkich komórek organizacyjnych zaangażowanych w zarządzanie ryzykiem. Do zadań zespołu należy koordynacja procesu zarządzania ryzykiem poprzez:

- moderację dyskusji w organizacji w trakcie realizacji poszczególnych etapów procesu,
- przestrzeganie zasad zarządzania ryzykiem,
- redukcję pojawiających się (zwłaszcza przy wykorzystaniu metod eksperckich) propozycji *granicznych* scenariuszy, czy znacznych odchyleń w wynikach wartości ryzyk,
- omawianie i rozstrzyganie właścicielstwa ryzyka przy ryzykach **krosowych** (pojawiające się to samo ryzyko w kilku obszarach działania organizacji),
- przedkładanie do akceptacji propozycji wyników szacowania ryzyka oraz decyzji w sprawie postępowania z ryzykiem.

Należy dążyć do sformalizowania funkcjonowania zespołu, np. w drodze zarządzenia organu, w którym należy podać m.in.: jego skład, stanowiska w organizacji i role w procesie zarządzania ryzykiem.

Wynikiem tego podprocesu powinno być również naniesienie na strukturę organizacyjną (będącą elementem podprocesu ustalania kontekstu wewnętrznego) strukturę zarządzania ryzykiem wraz ze wskazaniem ról i zadań poszczególnych uczestników/komórek organizacyjnych zaangażowanych w proces.

Właścicielstwo

Poza wskazaniem uczestników procesu i przypisaniem im ról, które pozwoli na określenie struktury zarządzania ryzykiem w urzędzie oraz zdefiniowanie i udział poszczególnych komórek organizacyjnych i pracowników w procesie szacowania ryzyka niezbędne jest zdefiniowane właścicielstwa dla poszczególnych ryzyk. Właścicielstwo jako reguła odwołuje się do podprocesu postępowania z ryzykiem i powinno zostać przypisane organowi władzy (lub innej osobie), która ma największy wpływ na skuteczne oddziaływanie na ryzyko.

Właściciel ryzyka powinien zostać wyłoniony na dwóch poziomach. W raporcie cząstkowym w komórce organizacyjnej, która jest merytorycznie właściwa w zakresie monitorowania ryzyka, komunikowania o nim (zarówno wewnątrz organizacji, jak i na zewnątrz) oraz przygotowania planu zarządzania nim. Natomiast drugi poziom to określenia właściciela ryzyka (organu władzy właściwego zgodnie z ustawą o działach) w Raporcie o zagrożeniach bezpieczeństwa narodowego.

Prezentacja właścicieli ryzyk powinna zostać przedstawiona w tabeli, która będzie zawierać: podmiot, nazwę ryzyka oraz podstawę uznania właścicielstwa.

Tabela 7.1. Tabela prezentująca właścicielstwo ryzyk sporządzana na potrzeby raportu cząstkowego

lp.	nazwa ryzyka	komórka organizacyjna urzędu/właściciel	formalna podstawa uznania właścicielstwa (regulamin organizacyjny urzędu)
…	…	…	…

Źródło: opracowanie własne

Tabela 7.2. Tabela prezentująca właścicielstwo ryzyk sporządzana na potrzeby Raportu o zagrożeniach bezpieczeństwa narodowego

lp.	nazwa ryzyka	organ władzy/właściciel	formalna podstawa uznania właścicielstwa (ustawa o działach)
…	…	…	…

Źródło: opracowanie własne

Komunikacja o ryzykach (wewnętrzna i zewnętrzna)

Należy przygotować i realizować w każdej fazie zarządzania ryzykiem plan komunikowania zarówno wewnątrz organizacji, jak i na jej zewnątrz. Komunikacja zewnętrzna obejmuje również element raportowania (przedłożenia raz na dwa lata dyrektorowi Rządowego Centrum Bezpieczeństwa raportu cząstkowego).

Przy określaniu zasad i kanałów komunikacji należy uwzględnić potrzebę zachowania przepisów o ochronie informacji niejawnych.

1) Komunikacja wewnętrzna

Plan komunikacji wewnętrznej powinien uwzględniać:

- już istniejące i wykorzystywane w organizacji metody zarządzania ryzykiem i skoordynować sposób wymiany informacji o ich wynikach, np. wynikające z konieczności przeprowadzania kontroli zarządczej. Elementami kontroli zarządczej są m.in.: określanie celów na poszczególnych poziomach organizacji i szacowanie ryzyk związanych z nieosiągnięciem tych celów,
- zapewnienie kanałów komunikacji wewnętrznej pomiędzy poszczególnymi obszarami organizacji posiadającymi wiedzę na temat ryzyk, np. w sytuacji identyfikacji dwóch podobnych ryzyk w różnych obszarach organizacji tak, aby można

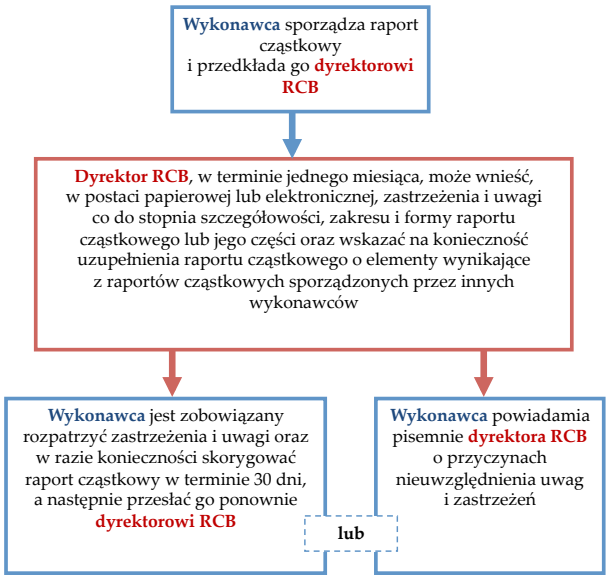
było podjąć wspólne działania zmierzające do ich lub jego (w przypadku redukcji ich do jednego ryzyka) mityzacji,
- wymianę oraz dokumentowanie wymagań i oczekiwań zainteresowanych podmiotów i włączenie tych danych do szacowania ryzyka,
- możliwość zapewnienia kanału informacyjnego umożliwiającego zgłaszanie ryzyk przez każdego pracownika organizacji,
- potrzebę konsultacji z podległymi pracownikami i innymi komórkami organizacyjnymi odpowiedzialnymi za szacowanie ryzyka, umożliwiającą pozyskanie wiedzy na temat ryzyk,
- konieczność przekazywania informacji (potwierdzającej lub falsyfikującej) zwrotnej osobom lub podmiotom zgłaszającym zidentyfikowane nowe ryzyka lub zmiany odnośnie do ryzyk uprzednio już zidentyfikowanych.

2) Komunikacja zewnętrzna i raportowanie

Komunikacja zewnętrzna odbywa się na ogólnie przyjętych przez system zarządzania kryzysowego zasadach wymiany informacji i powinna uwzględniać formalne zasady zwierzchnictwa i podległości wykonawców raportów cząstkowych.

Za raportowanie uznaje się przedłożenie dyrektorowi Rządowego Centrum Bezpieczeństwa, po uprzednim dokonaniu przeglądu ryzyk i formalnej aktualizacji, raportu cząstkowego. Zgodnie z wymogiem *rozporządzenia w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego* raportowanie odbywa się raz na dwa lata.

Komunikacja zewnętrzna powinna uwzględniać ponadto procedurę wskazaną w § 7 ww. rozporządzenia, która reguluje kwestie uzgadniania raportu cząstkowego pomiędzy jego wykonawcą a dyrektorem RCB.

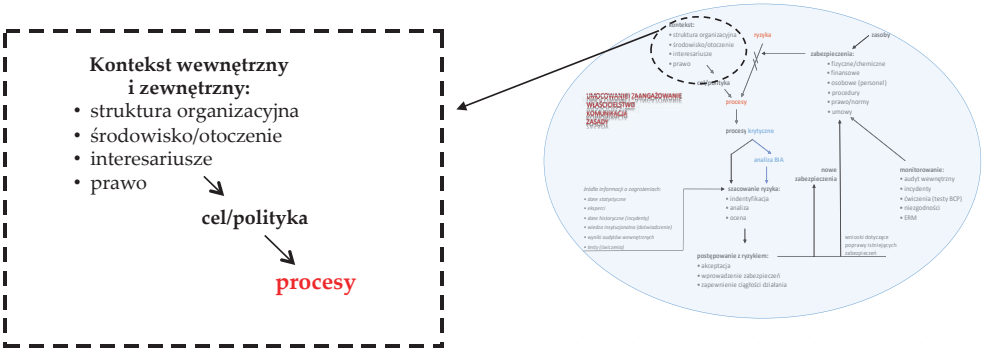


Rysunek 7.4. Sposób uzgadniania raportów cząstkowych w kontekście komunikacji zewnętrznej

Źródło: opracowanie własne

W wypadku, gdy na potrzeby szacowania ryzyka wykonawca raportu cząstkowego wykorzystuje inną metodykę – szacujący powinien dostarczyć dane dotyczące metodyki i zastosowanych skal, tak aby możliwe było przygotowanie tabeli przejściowej w celu ujednolicenia parametrów ryzyk oraz ich prezentacji na wspólnej (dla wszystkich ryzyk) matrycy ryzyka.

7.3. Proces zarządzania ryzykiem



Kontekst wewnętrzny i zewnętrzny

Dane wejściowe:

- wiedza o organizacji (zadania wynikające z przepisów polskiego prawa, funkcja w systemie bezpieczeństwa państwa/zarządzania kryzysowego, struktura organizacji wraz z właściwościami poszczególnych jej elementów),
- wiedza o otoczeniu (zagrożenia, interesariusze, prawo determinujące sposób realizacji zadań).

Dane wyjściowe:

- zdefiniowane zdolności organizacji,
- charakterystyka środowiska organizacji,
- podatność organizacji.

Określenie istotnych z punktu widzenia organizacji wewnętrznych i zewnętrznych parametrów oddziałujących na ryzyko pozwala na zrozumienie tła dla identyfikowanych zagrożeń oraz zdolności organizacji.

1) Określenie kontekstu wewnętrznego

Kontekst wewnętrzny to charakterystyka organizacji uwzględniająca zależne od niej elementy (na które ma ona wpływ i może je kreować lub dowolnie zmieniać) elementy pozwalające na określenie podatności organizacji na ryzyka oraz determinujące możliwości oddziaływania na ryzyko (zarządzania nim).

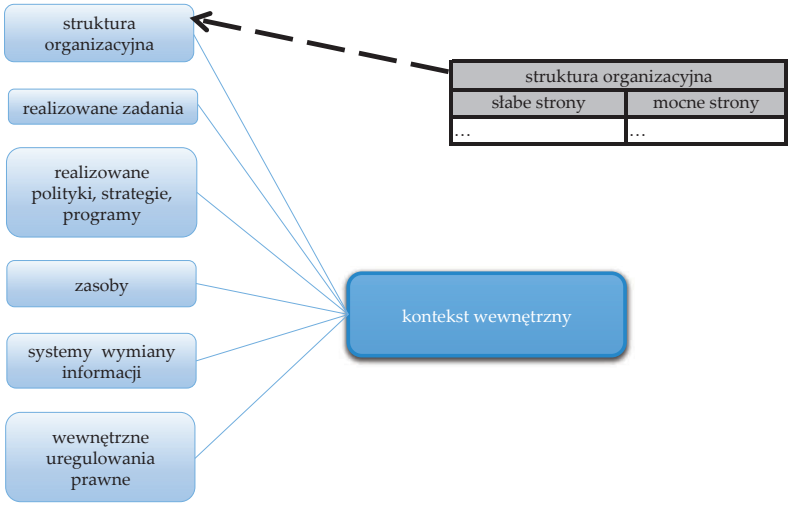
Podczas jego określania należy wskazać m.in.:

- strukturę organizacyjną oraz przypisane do niej zadania,
- realizowane już polityki, strategie, programy wpływające na podatność organizacji,

- posiadane zasoby,
- systemy wymiany informacji,
- wewnętrzne uregulowania prawne.

Ponadto należy określić wpływ tych elementów na realizację zamierzonych/zdefiniowanych celów (podatność) oraz wskazać, na ile możliwe jest oddziaływanie na tę podatność (zmniejszenie jej) poprzez ich zmianę.

W celu określenia podatności należy wskazać słabe i mocne strony organizacji, opierając się na założeniach metodologicznych analizy SWOT. Celem analizy jest odpowiedź na pytanie: *Na ile każdy z elementów charakteryzujący kontekst wewnętrzny (struktura organizacyjna oraz przypisane do niej zadania, realizowane już polityki, strategie, programy wpływające na podatność organizacji, posiadane zasoby, systemy wymiany informacji oraz wewnętrzne uregulowania prawne) obniża lub podnosi podatność organizacji?*



Rysunek 7.5. Obszary kontekstu wewnętrznego będące podstawą do określenia podatności
Źródło: opracowanie własne

Przy czym należy pamiętać, że wraz ze zwiększaniem się podatności organizacji wzrastają prawdopodobieństwo i skutki występujących/zidentyfikowanych ryzyk.

2) Określenie kontekstu zewnętrznego

Kontekst zewnętrzny to charakterystyka środowiska organizacji (w tym oddziałujące na nią zagrożenia), w którym realizuje ona swoje zadania. Prawidłowe scharakteryzowanie zewnętrza pozwala organizacji określić, na ile niezależne od niej czynniki mogą determinować jej zachowanie się w trakcie postępowania z ryzykiem. Kontekst zewnętrzny stanowi również punkt wyjścia dla etapów identyfikacji ryzyk, szacowania ich wartości oraz ewaluacji.

Podczas jego określania należy wskazać m.in.:

- środowisko naturalne, technologiczne, prawne uwzględniające czynniki lokalne, narodowe i międzynarodowe,

- interesariuszy wpływających na organizację, jej cele bądź ryzyka, na które jest ona narażona,
- możliwe do zdefiniowania trendy wpływające na zmianę celów i zadań organizacji,
- otoczenie prawne.

Do właściwego określenia kontekstu wewnętrznego należy dokonać szczegółowej analizy interesariuszy, którzy z jednej strony aktywnie mogą wpływać na proces zarządzania ryzykiem (w tym jego szacowania), a z drugiej, w przypadku już zaistniałego ryzyka, mogą być narażeni na jego skutki.

Charakterystyka interesariuszy

Na potrzeby charakterystyki interesariuszy należy:

- zidentyfikować interesariuszy,
- wskazać ich wpływ na organizację,
- wskazać wpływ organizacji na interesariuszy,
- określić wspólne i rozbieżne potrzeby organizacji i interesariuszy w odniesieniu do zarządzania ryzykiem.

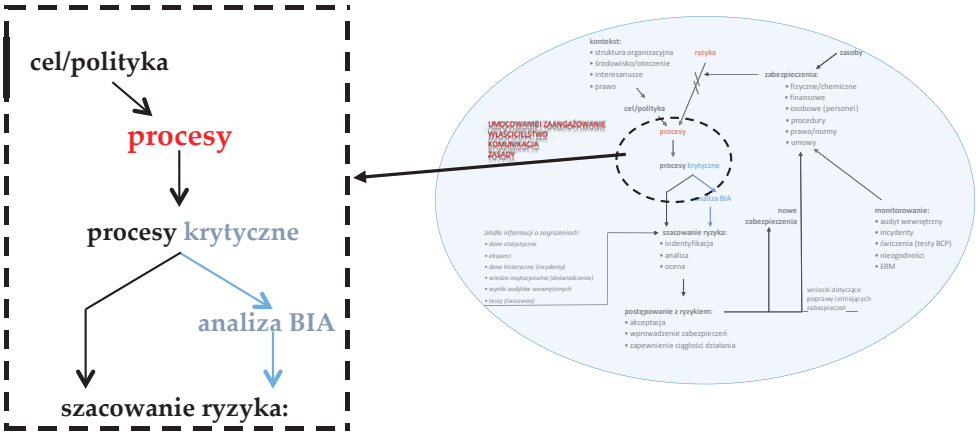
Dane te można prezentować w tabeli.

Tabela 7.3. Sposób prezentacji zależności pomiędzy organizacją a interesariuszami

interesariusz	wpływ interesariusza na organizację	interesy i potrzeby interesariusza	wpływ organizacji na interesariusza (potrzeby organizacji)	wpływ ryzyka na interesariusza
…	…	…	…	…

Źródło: opracowanie własne

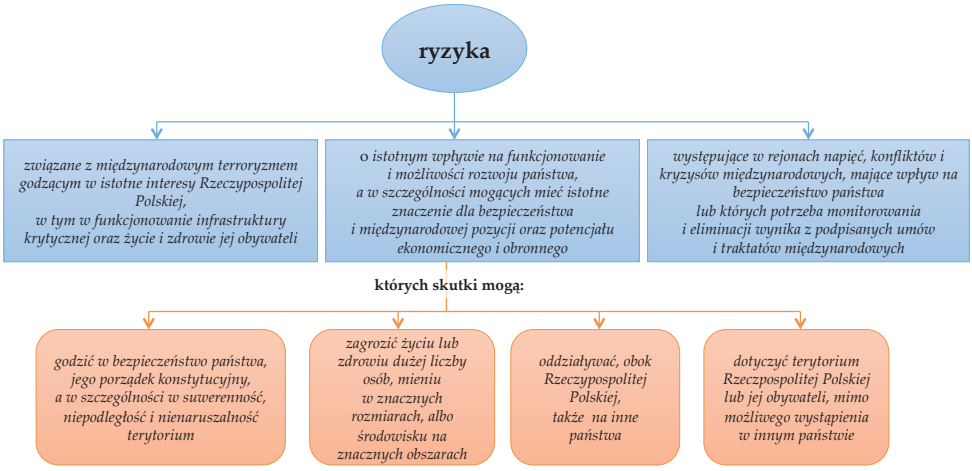
Dekompozycja celów oraz klasyfikacja procesów



Dane wejściowe:
- zdefiniowane zdolności organizacji,
- charakterystyka środowiska organizacji,
- podatność organizacji.

Dane wyjściowe:
- cele strategiczne, taktyczne i operacyjne organizacji,
- procesy zachodzące w organizacji,
- procesy krytyczne zachodzące w organizacji,
- wyniki analizy wpływu na organizację procesów krytycznych.

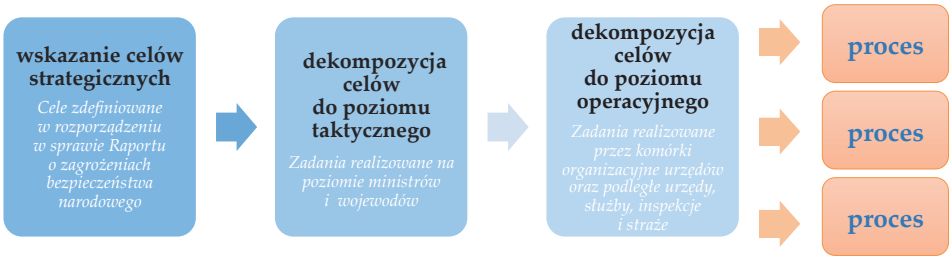
Po przeprowadzeniu analizy wnętrza organizacji i środowiska, w którym realizuje ona swoje zadania, kolejnym krokiem jest wskazanie celów i procesów, które powinny zostać objęte zarządzaniem ryzyka. W przypadku Raportu (…) cele zostały zdefiniowane w rozporządzeniu w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (rysunek 7.6.). Rozporządzenie, definiując ryzyka istotne z punktu widzenia bezpieczeństwa narodowego, definiuje cele z poziomu strategicznego.



Rysunek 7.6. Główne cele państwa w zakresie bezpieczeństwa narodowego zdefiniowane w rozporządzeniu w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego

Źródło: opracowanie własne

Ze względu na brak możliwości dokonania oceny ryzyka na poziomie strategicznym niezbędne jest przeprowadzenie dekompozycji celów strategicznych do poziomu operacyjnego, a następnie przypisanie im procesów, które zostaną objęte procesem zarządzania ryzykiem. Podproces ten powinien przebiegać w czterech etapach:



Rysunek 7.7. Etapy dekompozycji celów i definiowania procesów
Źródło: opracowanie własne

Ze względu na dużą liczbę podmiotów sporządzających raporty cząstkowe, właściwie przeprowadzony podproces dekompozycji celów oraz identyfikacji procesów, poprzez zagregowanie celów na trzech wskazanych poziomach oraz przypisanie do poziomu operacyjnego procesów zachodzących w organizacji, zapewni porównywalność procesów, a tym samym pozwoli na zestawienie wszystkich szacowanych ryzyk na jednej matrycy ryzyka.

Należy wskazać procesy, które:
- bezpośrednio wpływają na cel,
- organizacja jest właścicielem procesu (posiada możliwości prawne i finansowe do jego przeprowadzenia,
- są wykonywane przez komórkę organizacyjną,
- są koordynowane przez komórkę organizacyjną, a wykonywane przez inne komórki urzędu lub służby, inspekcje, straże.

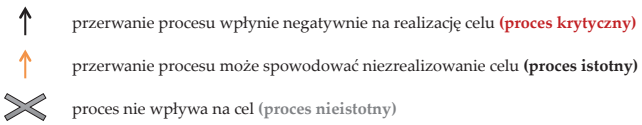
!!!

Ministrowie oraz podporządkowani im kierownicy urzędów centralnych planując zakres swoich raportów (w przypadku kiedy raporty cząstkowe są sporządzanie przez każdego z nich samodzielnie) powinni wziąć pod uwagę zakresy dekomponowanych celów wskazanych na rysunku 7.6.

Klasyfikacja procesów

Klasyfikacja zidentyfikowanych procesów powinna prowadzić do wyodrębnienia, z ogólnego katalogu, procesów istotnych i krytycznych.

Zgodnie ze wskazaną na rysunku 7.3. ogólną ideą zarządzania ryzykiem w obszarze bezpieczeństwa narodowego należy przyjąć, że bazową kategorią poddawaną ocenie ryzyka jest proces. Procesy zachodzące w organizacji można podzielić na trzy kategorie:
- procesy niewpływające na realizację celów,
- procesy, których przerwanie wpływa negatywnie na realizowane cele,
- procesy, których przerwanie może spowodować niezrealizowanie celów.



cele: / procesy:	cel taktyczny 1	cel taktyczny 2	cel taktyczny 3	cel taktyczny 4
proces 1	↑	↑	↑	✕
proces 2	↑	↑	↑	↑
proces 3	✕	↑	✕	↑
proces 4	↑	↑	↑	↑

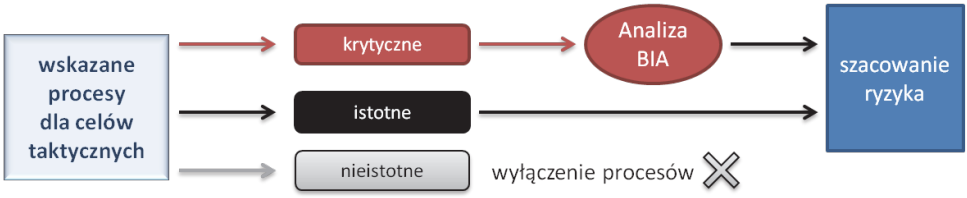
Rysunek 7.8. Tabela zależności pomiędzy procesami a celami

Źródło: opracowanie własne

Dokonanie kategoryzacji procesów należy przeprowadzić w odniesieniu do celów taktycznych, a więc takich, za realizację których odpowiadają ministrowie oraz wojewodowie.

Przypisanie procesom atrybutów: krytyczne, istotne, nieistotne pozwoli na podjęcie decyzji odnośnie do dalszych kroków postępowania w stosunku do zidentyfikowanych procesów. Odwołując się do jednej z zasad zarządzania ryzykiem (postulat ograniczania analizowanych procesów/scenariuszy), należy dążyć do wyłączenia z dalszej analizy procesów, których wpływ na cele są minimalne bądź żadne.

Pozostałe procesy należy poddać procesowi szacowania ryzyka poprzedzonego, w przypadku procesów krytycznych, analizie BIA.



Rysunek 7.9. Postępowanie ze zidentyfikowanymi procesami

Źródło: opracowanie własne

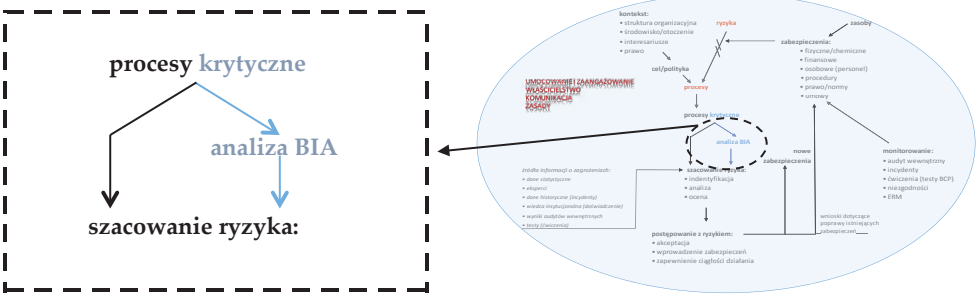
Wynikiem tego etapu powinna być tabela zidentyfikowanych procesów wraz ze wskazanymi atrybutami procesów:

Tabela 7.4. Dekompozycja celów wraz z przypisanymi im procesami

lp.	cel strategiczny	cel taktyczny	cel operacyjny	proces celu taktycznego	atrybut
…	…	…	…	…	…

Źródło: opracowanie własne

Analiza wpływu na organizację (BIA)



Dane wejściowe:
- procesy krytyczne zachodzące w organizacji**.**

Dane wyjściowe:
- wpływ procesów krytycznych na realizację celów,
- zabezpieczenia wraz z oceną ich skuteczności,
- maksymalny tolerowany czas przerwania procesu (MTPoD),
- docelowy czas wznowienia procesu (RTO).

W wyniku analizy BIA proces zarządzania ryzykiem zostanie uzupełniony o informacje dotyczące potencjalnych strat, które mogłyby powstać na skutek przerwania kluczowych procesów.

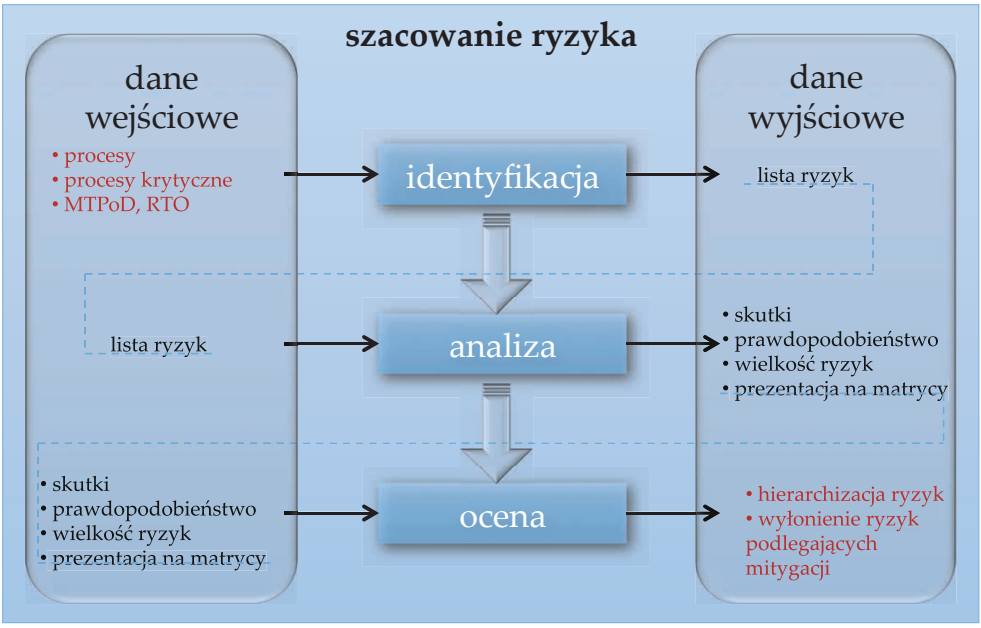
Szacowanie ryzyka

Dane wejściowe:
- procesy zachodzące w organizacji,
- procesy krytyczne zachodzące w organizacji,
- wyniki analizy wpływu na organizację procesów krytycznych.

Dane wyjściowe:
- ryzyka dla procesów organizacji,
- skutki i prawdopodobieństwo wystąpienia ryzyk,
- wielkość ryzyk,
- hierarchizacja ryzyk.

Pośrednie dane wejściowe i wyjściowe pomiędzy etapami identyfikacji, analizy oraz oceny prezentuje rysunek 7.10.

Szacowanie ryzyka jest generalnym procesem w stosunku do: identyfikacji ryzyka, dokonania jego analizy i oceny. Celem podejmowanych czynności jest porównanie wszystkich zidentyfikowanych ryzyk oraz ich prezentacja na wspólnej matrycy ryzyka.



Rysunek 7.10. Pośrednie dane wejściowe i wyjściowe dla etapów szacowania ryzyka
Źródło: opracowanie własne

1) Identyfikacja ryzyka

Zaleca się, aby w kolejnym kroku organizacja zidentyfikowała ryzyka, które mogą negatywnie wpływać na realizowane procesy bez względu na to, czy pozostają one, czy też są poza jej kontrolą. Źródłami informacji o ryzykach mogą być:
- plany zarządzania kryzysowego,

- dane statystyczne,
- eksperci,
- dane historyczne (incydenty),
- wiedza instytucjonalna (doświadczenie),
- wyniki audytów wewnętrznych,
- testy (ćwiczenia).

Identyfikacja ryzyka to etap, podczas którego należy odpowiedzieć na pytanie: *Co złego i gdzie może się stać?* w raporcie cząstkowym identyfikacji podlegają wszystkie bez wyjątku rodzaje negatywnych zdarzeń potencjalnie podnoszących podatność organizacji. W konsekwencji, jeśli do kompetencji danego ministra, kierownika urzędu centralnego lub wojewody należy przeciwdziałanie lub zwalczanie kilku rodzajów zagrożeń (wpływających negatywnie na realizację celów strategicznych), to należy wskazać je wszystkie. Zagrożenia te mają odpowiadać kryteriom wskazanym w rozporządzeniu w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego.

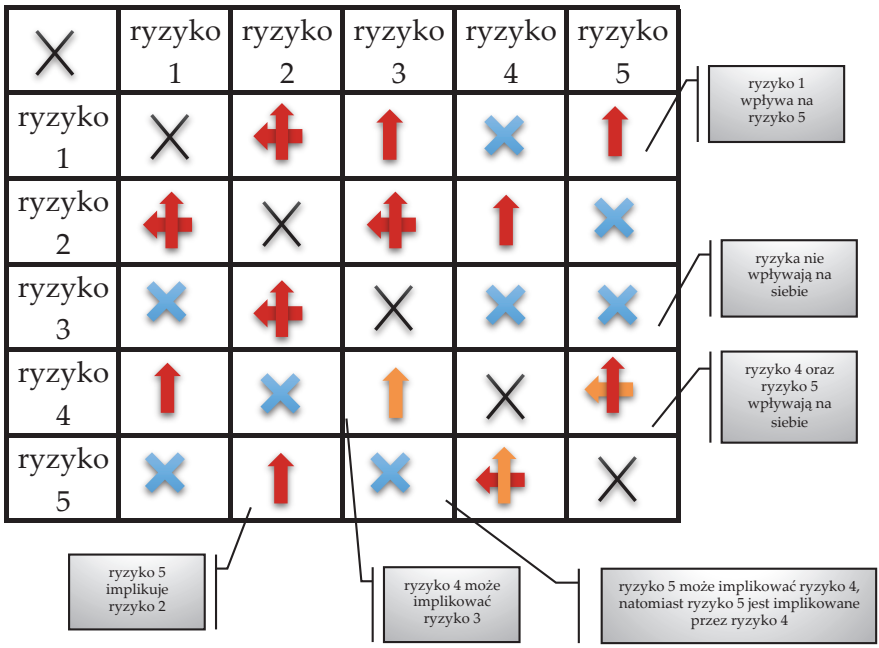
Podczas tego etapu niezbędne jest także odniesienie się do potencjalnych skutków procesów, które nie są jeszcze odczuwalne społecznie, ale których wystąpienie jest prawdopodobne. Procesami tymi mogą być np.:

- zmiany demograficzne (w tym zmiany struktury demograficznej w kontekście starzenia się społeczeństwa),
- zmiany klimatyczne,
- postępujący rozwój technologiczny (w tym, w kontekście stopniowej, rezygnacja z posługiwania się pieniądzem materialnym na rzecz wirtualnego czy używania środka płatniczego bitcoin),
- aktywność ruchów ekstremistycznych i separatystycznych,
- zmiany w światowej gospodarce (w tym także konieczność ograniczenia emisji spalin, stopniowy wzrost wymagań w zakresie ochrony środowiska naturalnego).

Wynikiem tego etapu powinna być lista zidentyfikowanych ryzyk wraz z uzasadnieniem, a także zestawienie ich w tabeli zależności. Tabela powinna przedstawiać wzajemne oddziaływanie na siebie ryzyk wraz z poziomem tego wpływu. Sposób prezentacji pokazuje rysunek 7.11.

Wypełniając tabelę, należy kierować się następującymi wskazówkami:

1) tabelę należy uzupełniać, wychodząc od ryzyk wskazanych w kolumnie (od lewej do prawej strony, a nie w pionie od góry do dołu).
2) pojedyncze strzałki mają zawsze groty skierowane do góry,
3) wskaźniki (strzałki) informują o:
   a) kierunku oddziaływania (ryzyko 5 wpływa na ryzyko 2),
   b) wadze wpływu:
      – ryzyko 5 implikuje ryzyko 2 – pojawienie się ryzyka 5 zawsze wzbudzi ryzyko 2,
      – ryzyko 4 może implikować ryzyko 3 – pojawienia się ryzyka 4 może wzbudzić ryzyko 3 w sytuacji wystąpienia określonych okoliczności.



Rysunek 7.11. Tabela zależności pomiędzy ryzykami

Źródło: opracowanie własne

Tabela powinna zostać uzupełniona o wskazanie okoliczności (dla strzałek warunkowego wpływu), których wystąpienie może doprowadzić do implikacji ryzyka:

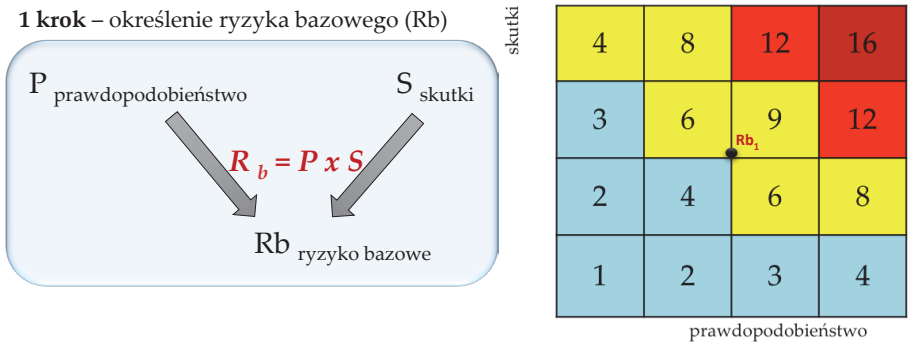
Tabela 7.5. Warunki oddziaływania ryzyk

lp.	ryzyko z kolumny/ryzyko z wiersza	okoliczności wzbudzenia ryzyka
1.	r4/r3	…
2.	r5/r4	…

Źródło: opracowanie własne

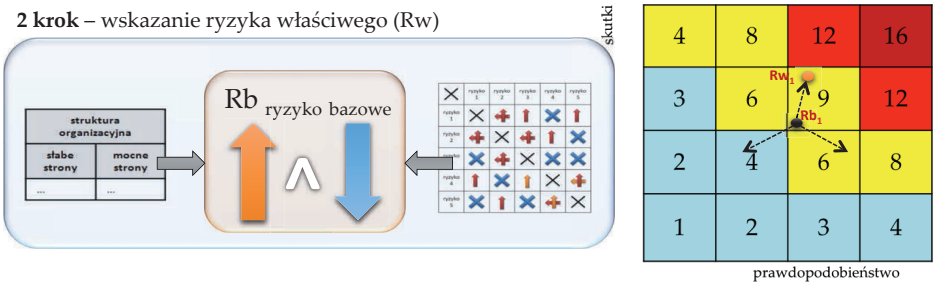
2) Analiza ryzyka

Przeprowadzając analizę ryzyka, można wykorzystać każdą metodę (podstawę do wyboru metody może stanowić norma IEC/FDIS 31010), pozwalającą na dokonanie oceny prawdopodobieństw i skutków ryzyk oraz prezentację w czterostopniowych skalach uwspólnionych wag (matryca ryzyka).



Rysunek 7.12. Sposób określania ryzyka bazowego
Źródło: opracowanie własne

Etap ten powinien zawierać również weryfikację poziomu ryzyka bazowego w kontekście podatności (opartą o analizę mocnych i słabych stron elementów kontekstu wewnętrznego) oraz wpływu na niego innych ryzyk.



Rysunek 7.13. Sposób określania ryzyka właściwego
Źródło: opracowanie własne

Podstawę dla analizy ryzyka stanowi scenariusz. Scenariusz, bez względu na wykorzystywaną metodę służącą jego budowie, powinien wskazywać przyczyny, które mogą doprowadzić do zaistnienia ryzyka oraz jego potencjalne konsekwencje.

Wskazanie przyczyn i konsekwencji stanowi punkt wyjścia do określenia ryzyka bazowego.

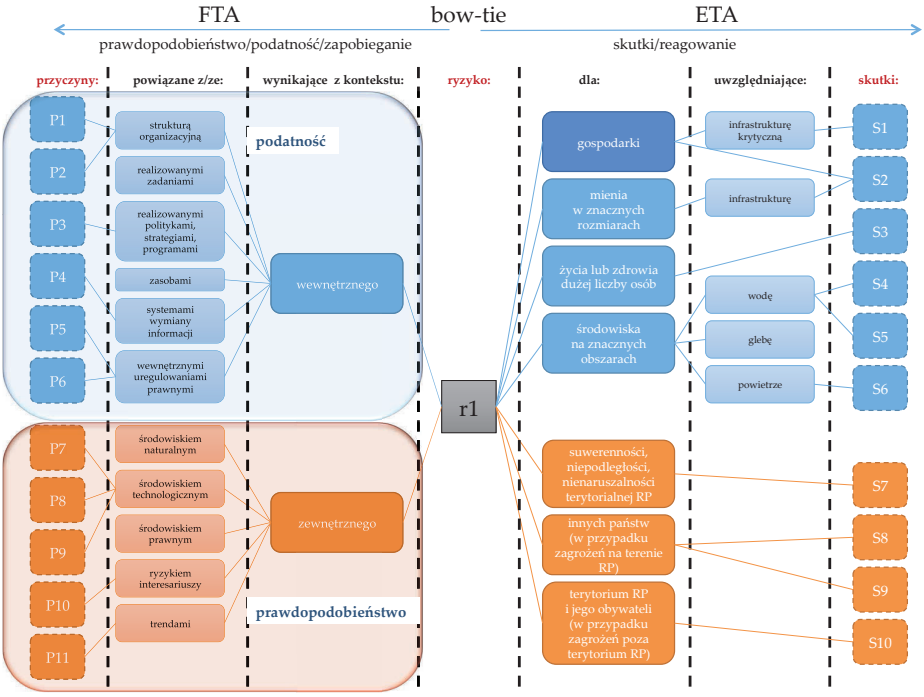
1 krok – określenie ryzyka bazowego

Dla każdego zidentyfikowanego ryzyka należy wskazać (o ile jest to możliwe):

- przyczyny:
  - wewnętrzne (zgodnie z charakterystyką kontekstu wewnętrznego),
  - środowiskowe (zgodnie z charakterystyką kontekstu zewnętrznego),
- skutki dla:
  - suwerenności, niepodległości i nienaruszalności terytorium RP,
  - życia lub zdrowia dużej liczby osób,
  - mienia w znacznych rozmiarach,

- środowiska na znacznych obszarach,
- innych państw (w sytuacji wystąpienia ryzyka w RP),
- terytorium RP lub jej obywateli (w sytuacji wystąpienia ryzyka poza granicami RP).

Scenariusz może zostać zapisany w notacji graficznej lub opisowej, powinien jednak uwzględniać elementy wskazane na poniższym rysunku.



Rysunek 7.14. Scenariusz ryzyka. Elementy niezbędne do przeprowadzenia analizy ryzyka (określenia przyczyn i skutków)

Źródło: opracowanie własne

Wynikiem analizy powinna być tabela zawierająca przypisane do poszczególnych ryzyk katalogi przyczyn oraz skutków.

Tabela 7.6. Tabela przyczyn i skutków zidentyfikowanych ryzyk

nr ryzyka	nazwa ryzyka	przyczyny	skutki
r1	…	*P1 ….* *P2 ….* *Pn ….*	*S1 ….* *S2 ….* *Sn ….*
r2	…	*P1 ….* *P2 ….* *Pn ….*	*S1 ….* *S2 ….* *Sn ….*

Źródło: opracowanie własne

Kolejnym krokiem analizy ryzyka powinno być określenie wielkości ryzyk przez wskazanie wag dla przyczyn (prawdopodobieństwo) oraz skutków.

Prawdopodobieństwo należy rozpatrywać w wartościach od 0 do 1, gdzie 0 to brak występowania ryzyka, a 1 to pewność jego wystąpienia. Należy przyjąć, że prawdopodobieństwo na potrzeby raportu cząstkowego zostanie określone przy wykorzystaniu informacji o częstości powtórzeń zagrożeń (ryzyk).

Tabela 7.7. Określanie wartości prawdopodobieństwa ryzyka na podstawie częstości wystąpienia zagrożeń

wartość	opis	charakterystyka
1	bardzo rzadkie	zdarzenie zakłócające proces może wystąpić jedynie w wyjątkowych okolicznościach, a prawdopodobnie w ogóle nie zaistnieje; nie wystąpiło dotychczas lub dotyczy jednostkowych zdarzeń (przedział częstości powyżej 100 lat; **r > 100**)
2	rzadkie	istnieje małe prawdopodobieństwo wystąpienia zdarzenia zakłócającego proces (pomiędzy 20 a 100 lat; **100 > r > 20**)
3	prawdopodobne	istnieje prawdopodobieństwo wystąpienia zdarzenia zakłócającego proces (pomiędzy 5 a 20 lat; **20 > r > 5**)
4	bardzo prawdopodobne	wystąpienie zdarzenia zakłócającego proces jest prawdopodobne lub pewne (pomiędzy 1 a 5 lat; **1 > r > 5**)

Źródło: opracowanie własne

Tabela 7.8. Określanie wartości skutków ryzyk

wartość	opis	kryteria:			
		finansowe	wpływ na proces	życie, zdrowie	reputacja
1	małe	brak lub małe koszty poniesione w trakcie reagowania oraz odbudowy niewymagające uruchomienia rezerw celowych samorządu, możliwe uruchomienie środków pomocy społecznej, brak konieczności uruchomienia środków przeznaczonych na usuwanie skutków klęsk żywiołowych (BUSKŻ MAiC)	krótkotrwałe zakłócenia w działalności	brak lub mała liczba osób rannych	krytyczne informacje w mediach lokalnych

wartość	opis	kryteria:			
		finansowe	wpływ na proces	życie, zdrowie	reputacja
2	znaczne	koszty poniesione w trakcie reagowania i odbudowy wymagają uruchomienia rezerw celowych samorządu oraz środków pomocy społecznej, możliwość uruchomienia środków przeznaczonych na usuwanie skutków klęsk żywiołowych (BUSKŻ MAiC)	zakłócenia kluczowych procesów niepowodujące ich przerwania	znaczna liczba osób poszkodowanych niewymagająca jednak koordynacji ze strony lekarza koordynatora	krytyczne informacje w mediach regionalnych
3	duże	koszty poniesione w trakcie reagowania i odbudowy wymagają uruchomienia rezerw celowych samorządu, środków pomocy społecznej, środków przeznaczonych na usuwanie skutków klęsk żywiołowych (BUSKŻ MAiC) oraz środków budżetowych (państwa) z rezerwy celowej	przerywa kluczowe procesy, a ich odtworzenie jest możliwe w czasie gwarantującym osiągnięcie celu	duża liczba osób poszkodowanych wymagająca interwencji lekarza koordynatora lub podwyższenie gotowości szpitali	krytyczne informacje w mediach krajowych, w tym także elektronicznych, na portalach społecznościowych, pojawiające się liczne *memy* i komentarze
4	katastrofalne	koszty poniesione w trakcie reagowania i odbudowy wymagają uruchomienia rezerw celowych samorządu, środków pomocy społecznej, środków przeznaczonych na usuwanie skutków klęsk żywiołowych (BUSKŻ MAiC) oraz środków budżetowych (państwa) z rezerwy celowej, a także zwrócenie się o pomoc międzynarodową (np. z Funduszu Solidarności UE)	przerywa kluczowe procesy, uniemożliwiając osiągnięcie celów	duża liczba osób poszkodowanych wymagająca podwyższenia gotowości szpitali oraz skorzystania z pomocy innych państw	krytyczne informacje w mediach krajowych i zagranicznych, w tym także elektronicznych, na portalach społecznościowych, pojawiające się liczne memy i nieprzychylne komentarze internautów

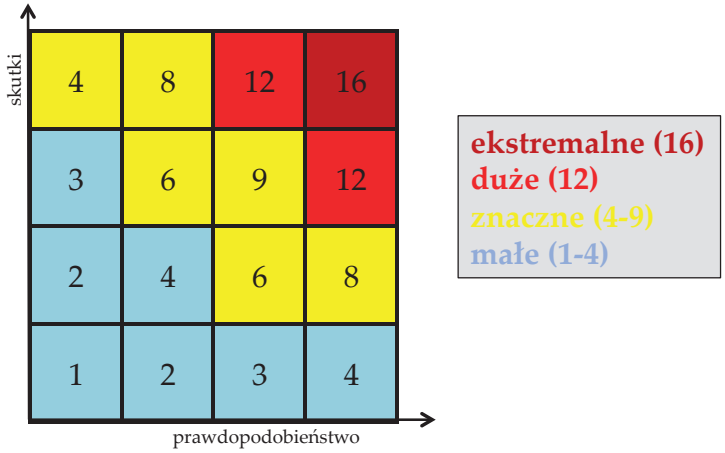
Źródło: opracowanie własne

W przypadku braku danych historycznych przy określaniu wartości prawdopodobieństwa i skutków można posłużyć się metodami analiz scenariuszowych lub *Co jeśli?*

Prezentacja ryzyka polega na wskazaniu jego wartości (iloczyn wartości prawdopodobieństwa i skutków), gdzie:

$$R = P \times S$$

oraz zobrazowanie otrzymanej wartości na matrycy ryzyka.



Rysunek 7.15. Matryca ryzyka oraz nazwy wartości ryzyka

Źródło: opracowanie własne

2 krok – określenie ryzyka właściwego

W celu określenia właściwego poziomu ryzyka niezbędne jest zweryfikowanie wartości ryzyka bazowego poprzez wskazanie: *czy, a jeśli tak, to w jaki sposób wpływają na ryzyko bazowe czynniki organizacyjne (kontekst wewnętrzny) oraz inne ryzyka (tabela zależności pomiędzy ryzykami)?*

Kontekst wewnętrzny pozwala na określenie podatności organizacji. Analiza zdolności reakcji organizacji na ryzyko powinna zostać przeprowadzona dla każdego zidentyfikowanego ryzyka zgodnie z poniższą tabelą:

Tabela 7.9. Analiza podatności organizacji

ryzyko:	**r1**	**r2**	**r3**	**r4**	**r_n**
słabe strony:	x	x	x	x	x
…	↑	–	–	–	–
…	–	↑	↑	–	↑
mocne strony:	x	x	x	x	x
…	–	↓	–	–	↓
…	↓	↓	–	↓	–

↑ - zwiększa podatność

↓ - zmniejsza podatność

– - nie wpływa na podatność

Źródło: opracowanie własne

Analiza podatności decyduje o podniesieniu bądź obniżeniu ryzyka w obszarze skutków. Należy przyjąć, że:

- nie wpływa na zmianę wartości skutków (braku zmiany podatności):
  - brak występowania słabych i mocnych stron,
  - wartość ich oddziaływania jest niska,
  - wartości ich oddziaływania równoważą się.
- wartość skutków można obniżyć (zmniejszenie podatności), jeśli:
  - występują wyłącznie mocne strony,
  - słabe strony mają małą wagę, a mocne dużą wagę.
- wartość skutków podwyższa się (zwiększa się podatność):
  - występują wyłącznie słabe strony,
  - słabe strony mają dużą wagę, a mocne małą wagę.

Pod pojęciem „wagi strony" należy rozumieć stopień oddziaływania na organizację „słabej lub mocnej strony" w kontekście zidentyfikowanego pojedynczego ryzyka

wartość skutków	opis
1	małe
2	znaczne
3	duże
4	katastrofalne

Rysunek 7.16. Kierunki i wartości wpływu podatności na ryzyko właściwe
Źródło: opracowanie własne

Zależność pomiędzy ryzykami może wpływać na zwiększenie podatności ryzyka. Analizując tabelę zależności pomiędzy ryzykami (rys. 7.11.), należy przyjąć, że:

- na zmianę prawdopodobieństwa nie wpływa:
  - brak lub mała liczba ryzyk wpływająca na zidentyfikowane ryzyko,
- zwiększa prawdopodobieństwo:
  - duża liczba ryzyk oddziałujących na zidentyfikowane ryzyko,
  - ryzyka oddziałujące na ryzyko zostały wskazane jako ryzyko prawdopodobne lub bardzo prawdopodobne.

Zależność pomiędzy ryzykami nie wpływa na obniżenie prawdopodobieństwa

wartość prawdopodobieństwa	opis
1	bardzo rzadkie
2	rzadkie
3	prawdopodobne
4	bardzo prawdopodobne

Rysunek 7.17. Kierunki i wartości wpływu innych ryzyk na zidentyfikowane ryzyko właściwe

Źródło: opracowanie własne

Biorąc pod uwagę podatność i zależności pomiędzy ryzykami przy określaniu ryzyka właściwego, możliwe jest podniesienie lub obniżenie wartości ryzyka (oddzielnie dla skutków lub prawdopodobieństwa) jedynie o jedną wagę.

W wyniku powyższych analiz można dokonać zmiany wartości ryzyka bazowego i określić końcową wartość ryzyka właściwego.

3) Ocena ryzyka

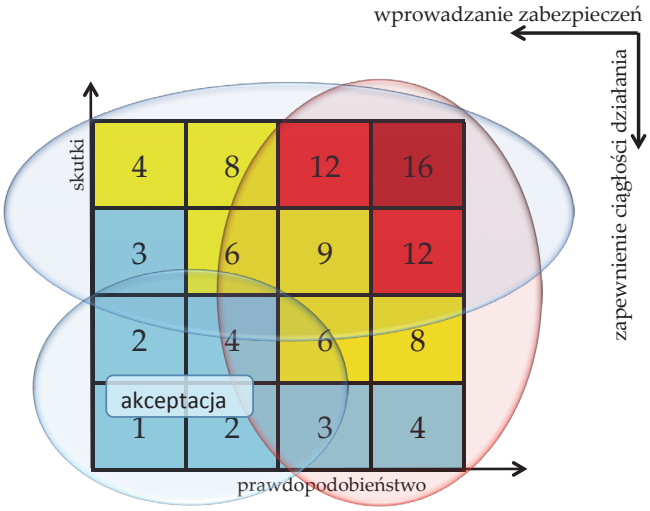
Ostatnim etapem szacowania ryzyka powinna być prezentacja ryzyk właściwych na matrycy oraz ich hierarchizacja (lista ryzyk ułożona od najistotniejszych (o najwyższych wartościach) do najmniej istotnych (o najniższych wartościach)) zgodnie z wartościami wskazanymi w matrycy ryzyk (rys. 7.15) oraz wskazanie sposobów postępowania z ryzykiem.

Tabela 7.10. Sposób prezentacji hierarchizacji ryzyk

wartość ryzyka właściwego	nazwa ryzyka
16	…
12	…
9	…
8	…
6	…
4 (znaczne)	…
4 (małe)	…
3	…
2	…
1	…

Źródło: opracowanie własne

Przypisanie wartości ryzykom i ich zhierarchizowanie pozwala na określenie sposobów postępowania z ryzykiem. Zgodnie z przyjętą metodyką każdemu ryzyku należy przypisać sposób, w jaki będziemy z nim postępować (lub zaniechamy podejmowania jakichkolwiek działań).

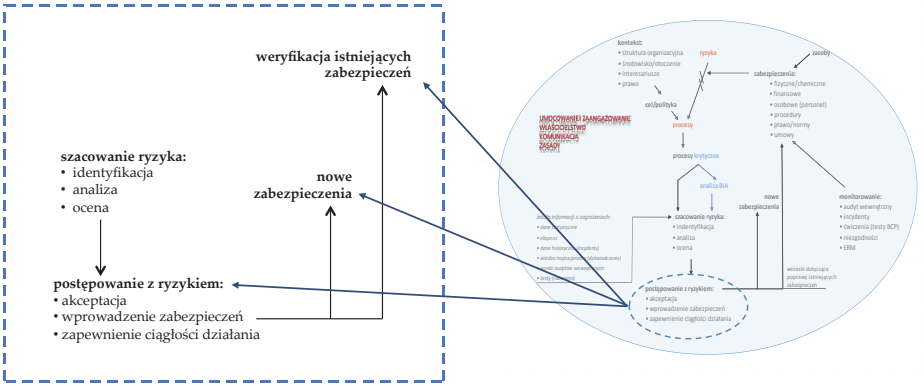


Rysunek 7.18. Możliwe do podjęcia kroki postępowania z ryzykiem
Źródło: opracowanie własne

Ogólne dyrektywy przyjęte dla metody w zakresie postępowania z ryzykiem wskazują, że:

- w stosunku do ryzyka obarczonego dużym prawdopodobieństwem należy podejmować działania zmierzające do wprowadzenia lub poprawy istniejących zabezpieczeń,
- w stosunku do ryzyka obarczonego dużymi skutkami należy podejmować działania zmierzające do zapewnienia organizacji utrzymania (w czasie kryzysu) realizacji przynajmniej krytycznych procesów,
- w stosunku do ryzyka o niskim prawdopodobieństwie i małych skutkach należy rozważyć możliwość podjęcia decyzji o zaniechaniu działań zmierzających do mityzacji ryzyka.

Postępowanie z ryzykiem

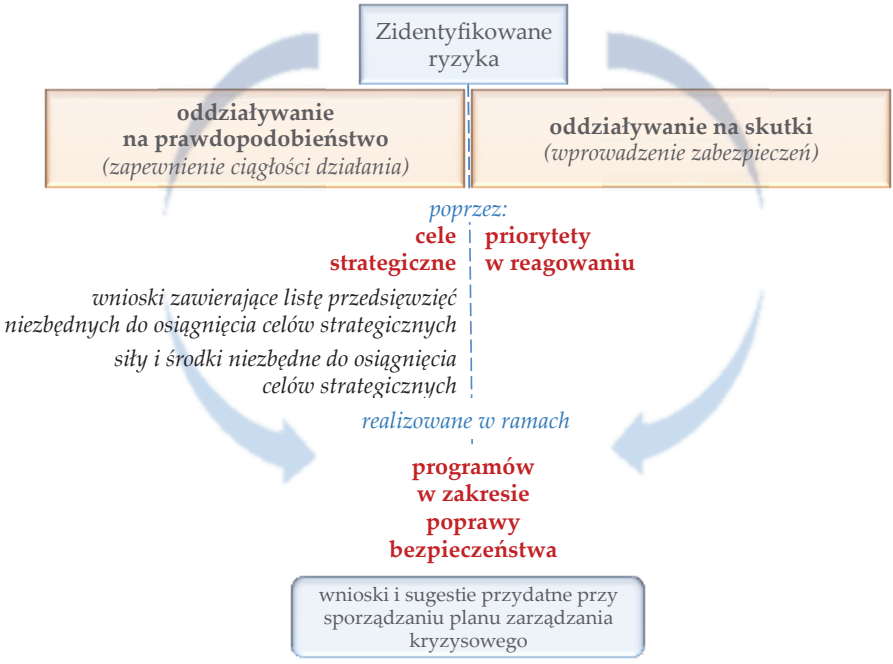


Zgodnie z ustawą o zarządzaniu kryzysowym ostatnim etapem przygotowania raportu cząstkowego jest:

- określenie celów strategicznych,
- określenie priorytetów w reagowaniu na określone zagrożenia,
- wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych,
- zaprogramowanie zadań w zakresie poprawy bezpieczeństwa przez uwzględnianie regionalnych i lokalnych inicjatyw,
- wskazanie wniosków zawierających hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych.

Biorąc pod uwagę powyższe wymogi oraz wskazane sposoby postępowania z ryzykiem, można wskazać generalne dyrektywy dla procesu mitygacji ryzyka.

Efektem tego etapu powinno być zdefiniowanie programów oddziałujących na ryzyko (skutek i prawdopodobieństwo) poprzez określenie celów strategicznych oraz priorytetów w reagowaniu. Poniższy rysunek przedstawia przyporządkowane do ogólnych strategii postępowania z ryzykiem wymagane ustawą o zarządzaniu kryzysowym elementy raportu cząstkowego.



Rysunek 7.19. Planowanie procesu postępowania z ryzykiem

Źródło: opracowanie własne

W celu określenia programów poprawy bezpieczeństwa należy dokonać podziału możliwych do podjęcia działań na obszary:

- oddziaływania na prawdopodobieństwa – działania strategiczne (zapobieganie),
- oddziaływania na skutki – działania operacyjne (reagowanie).

Projektowane działania należy odnieść do istniejących już zabezpieczeń na poziomie strategicznym (cele strategiczne) i operacyjnym (priorytety w reagowaniu).

1. Cele strategiczne

W pierwszym kroku należy wykazać już realizowane cele strategiczne i dokonać ich oceny, a w przypadku wskazania braku ich skuteczności określić nowe cele strategiczne (lub zredefiniować stare) oraz wskazać (zapewnić) dla nich niezbędne zasoby (przedsięwzięcia, siły i środki):

Tabela 7.11. Określenie celów strategicznych wraz zasobami niezbędnymi do ich osiągnięcia

lp.	nazwa ryzyka	realizowany dotąd cel strategiczny	**ocena jego wspływu na ryzyko**	**nowy lub zredefiniowany** (w przypadku oceny „niewystarczający) **cel strategiczny**	**przedsięwzięcia niezbędne dla realizacji celów**	**siły i środku niezbędne dla realizacji celów**
1	r1…	…	wystarczający/ niewystarczający	…	…	…
2	r2…	…	wystarczający/ niewystarczający	…	…	…

Źródło: opracowanie własne

Należy także dokonać priorytetyzacji tych celów:

Tabela 7.12. Priorytetyzacja celów strategicznych

lp.	**nowy** (lub zredefiniowany) **cel strategiczny /realizowany cel strategiczny** (określony jako wystarczający)	wartość ryzyka dla którego został zdefiniowany cel strategiczny	priorytet celu strategicznego	termin realizacji celu
1	…	…	**M** v **S** v **C**	…
2	…	…	**M** v **S** v **C**	…

Źródło: opracowanie własne

Priorytety należy przypisać zgodnie ze skróconą skalą *MoSCoW* (Must, Should, Could, Won't) gdzie:

- **M (must, musi być)** – priorytet o wartości **krytycznej** dla mitygacji ryzyka, cel musi zostać osiągnięty, aby obniżyć wartość ryzyka,
- **S (should, powinien być)** – priorytet o **wysokiej** wartości, cel powinien zostać osiągnięty (jeśli jest to możliwe), aby obniżyć wartość ryzyka,
- **C (could, może być)** – priorytet o **pożądanej** wartości, cel powinien zostać spełniony, jeśli pozwolą na to zasoby lub czas, nie jest konieczny do obniżenia wartości ryzyka (a jedynie wspiera ten proces).

2. Priorytety w reagowaniu
W drugiej kolejności należy określić priorytety w reagowaniu.

Tabela 7.13. Określenie priorytetów w reagowaniu

lp.	nazwa ryzyka	realizowany dotąd priorytet w reagowaniu	ocena jego wpływu na ryzyko	**nowy lub zredefiniowany** (w przypadku oceny „niewystarczający) **priorytet w reagowaniu**
1	r1….	1)… 2)… 3)…	wystarczający/ niewystarczający	
2	r2….	1)… 2)… 3)…	wystarczający/ niewystarczający	

Źródło: opracowanie własne

Priorytety w reagowaniu powinny wskazywać już realizowane/stosowane priorytety, a w przypadku wskazania braku ich skuteczności:
- nowe (niezdefiniowane dotąd w planach służb, inspekcji, straży lub planach zarządzania kryzysowego),
- lub zredefiniowane na nowo.

Ponadto należy określić wpływ priorytetów na:

Tabela 7.14. Wpływ priorytetów na zasady reagowania i hierarchizację działań

lp.	nazwa priorytetu	jego wpływ na:	
		zasady reagowania	hierarchizację działań
1	…	…	…
2	…	…	…

Źródło: opracowanie własne

3. Programy w zakresie poprawy bezpieczeństwa
Ostatnim krokiem etapu postępowania z ryzykiem jest wskazanie programów mających na celu realizację postulowanych celów strategicznych i priorytetów w reagowaniu. W tym celu należy przyporządkować do:
- celów strategicznych realizowanych dotąd (i ocenionych pozytywnie),
- zredefiniowanych realizowanych celów strategicznych (ocenionych negatywnie),
- nowych celów strategicznych,
- priorytetów w reagowaniu realizowanych dotąd (i ocenionych pozytywnie),
- zredefiniowanych realizowanych priorytetów w reagowaniu (ocenionych negatywnie),
- nowych priorytetów w reagowaniu.

realizowane lub przygotowywane programy poprawy bezpieczeństwa:

Tabela 7.15. Programy w zakresie poprawy bezpieczeństwa będące wypełnieniem celów strategicznych i priorytetów w reagowaniu

lp.	nazwa ryzyka	nazwa programu w zakresie poprawy bezpieczeństwa	realizowany w jego ramach cel strategiczny	realizowany w jego ramach priorytet w reagowaniu
1	r1	…	…	…
2	r2	…	…	…

Źródło: opracowanie własne

oraz dokonać charakterystyki tych programów:

Tabela 7.16. Charakterystyka programów w zakresie poprawy bezpieczeństwa

lp.	nazwa programu	obszar realizacji krajowy/ wojewódzki/ powiatowy/ gminny	realizator programu rządowy/ samorządowy/ pozarządowy	sposób finansowania programu	okres trwania programu
1	…	…	…	…	…
2	…	…	…	…	…

Źródło: opracowanie własne

Formułowanie wniosków i sugestii przydatnych przy sporządzaniu planu zarządzania kryzysowego

Przepisy ustawy o zarządzaniu kryzysowym oraz rozporządzenia Rady Ministrów w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego wskazują, że:

- *kierunki działania wynikające z wniosków z Raportu stanowią element Krajowego Planu Zarządzania Kryzysowego oraz są uwzględniane w planach zarządzania kryzysowego* (art. 5a pkt 5 ustawy),
- raport cząstkowy jest dokumentem obejmującym (…) informacje, które zdaniem wykonawcy mogą być przydatne przy tworzeniu Krajowego Planu Zarządzania Kryzysowego (§ 4 pkt 7 rozporządzenia).

Należy przyjąć, że katalog wniosków powinien być budowany w oparciu o informacje zawarte w tabelach 7.12, 7.14 oraz 7.16.

Tabela 7.12

lp.	**nowy** (lub zredefiniowany) **cel strategiczny /realizowany cel strategiczny** (określony jako wystarczający)	**wartość ryzyka dla którego został zdefiniowany cel strategiczny**	**priorytet celu strategicznego**	**termin realizacji celu**
1	…	…	**M** v **S** v **C**	…
2	…	…	**M** v **S** v **C**	…

Tabela 7.14

lp.	nazwa priorytetu	jego wpływ na:	
		zasady reagowania	hierarchizację działań
1	...	...	...
2	...	...	...

Tabela 7.16

lp.	nazwa programu	obszar realizacji krajowy/ wojewódzki/ powiatowy/ gminny	realizator programu rządowy/ samorządowy/ pozarządowy	sposób finansowania programu	okres trwania programu
1	...	...	...	...	...
2	...	...	...	...	...

Rysunek 7.20. Informacje z zakresu działań na poziomie operacyjnym i strategicznym będące podstawą dla określenia wniosków z raportu cząstkowego

Źródło: opracowanie własne

Bazując na powyższych informacjach, należy zgodnie z tabelą wskazać:

Tabela 7.17. Określenie wniosków dla planów zarządzania kryzysowego

lp.	**działanie**	**czy działanie zostało ujęte dotychczas w planie zarządzania kryzysowego?**	**jeśli *tak*, to czy zapis jest wystarczający?**	**jeśli *nie*** (w kolumnie c lub d), **to proszę wskazać część planu, która powinna zostać uzupełniona**	**czy uzupełniony powinien zostać plan urzędu czy KPZK**	**uzasadnienie dla części *d*, *e* i f**
a	**b**	**c**	**d**	**e**	**f**	**g**
I.	**cele strategiczne:**					
I.1.	…	tak/nie	tak/nie	…		
i.2.	…	tak/nie	tak/nie	…		

lp.	**działanie**	**czy działanie zostało ujęte dotychczas w planie zarządzania kryzysowego?**	**jeśli *tak*, to czy zapis jest wystarczający?**	**jeśli *nie*** (w kolumnie c lub d), **to proszę wskazać część planu, która powinna zostać uzupełniona**	**czy uzupełniony powinien zostać plan urzędu czy KPZK**	**uzasadnienie dla części *d*, *e* i f**
a	**b**	**c**	**d**	**e**	**f**	**g**
II.	**priorytety w reagowaniu**					
II.1.	…	tak/nie	tak/nie	…		
II.2.	…	tak/nie	tak/nie	…		

Źródło: opracowanie własne

Zakończenie

Przedstawiliśmy Państwu monografię, która powstała w wyniku pracy zespołu osób, dla których płaszczyznę i odniesienie do dyskursu o sprawach bezpieczeństwa państwa i jego obywateli stanowi pojęcie ryzyka. Podczas pracy nad nią towarzyszyły nam słowa często powtarzane w gronie tych, którzy zajmują się zarządzaniem ryzykiem: *Nie musisz zarządzać ryzykiem. Przetrwanie nie jest obowiązkowe!* Niemniej w przypadku państwa i jego administracji dbałość o bezpieczeństwo jest obowiązkiem. Niniejsza pozycja kierowana jest do osób, które w swojej pracy zawodowej podejmują problemy planowania cywilnego oraz zarządzania ryzykiem, a także które dopiero chcą zapoznać się z tą problematyką. Zakres rozdziałów został wybrany tak, aby poprowadzić czytelnika przez najważniejsze aspekty zarządzania ryzykiem w kontekście aktywności podejmowanych przez system zarządzania kryzysowego. Struktura książki posiada spójną narrację. Wychodząc od zadań administracji publicznej (rozdział 1), w tym także tych odnoszących się do kwestii zarządzania ryzykiem (rozdział 2) poprzez możliwe stosowane i zweryfikowane rozwiązania oparte na normach (rozdział 3) i metodykach stosowanych w innych państwach (rozdział 4), a także starając się pokazać szczegółowe propozycje metod i narzędzi badawczych (rozdziały 5 i 6) książka w podsumowaniu, który stanowi ostatni rozdział (7), pokazuje, bazując na zaprezentowanej wiedzy, komplementarną propozycję metodyki zarządzania (a nie wyłącznie analizy) ryzykiem.

Zgodnie z pierwotnym założeniem, aby we właściwy sposób móc zarządzać ryzykiem, konieczne jest przyjęcie i respektowanie poniższych reguł:

- Każdy powinien respektować jednolite zasady, ponieważ pozwalają one nie tylko na ujednolicenie sposobów definiowania problemu, ale i sposobów jego rozwiązania.
- Każdy powinien w jasny i precyzyjny sposób określić wykonawców poszczególnych procesów i decydentów w procesie oraz wskazać obszar ich zaangażowania.
- Każdy powinien akceptować swoje właścicielstwo w stosunku do zidentyfikowanych i wynikających z przepisów prawa ryzyk w obszarze bezpieczeństwa państwa oraz znać właścicieli ryzyk pozostałych.

Mając na uwadze sprawność i efektywność systemu, niezbędne jest zapewnienie kanałów komunikacji i ciągłe komunikowanie się w trakcie całego procesu zarządzania ryzykiem pomiędzy wszystkimi jego uczestnikami.

Reguły wprowadzają ład organizacyjny i determinują zachowanie wszystkich podmiotów zarówno na zewnątrz w kontaktach z innymi, jak i wewnątrz poprzez

ustanowienie struktury ramowej, adekwatnej do roli w całym procesie, gotowej do podjęcia zarządzania ryzykiem. Jednak samo wprowadzenie, a nawet zaimplementowanie reguł nie buduje jednolitego i transparentnego systemu. O jego przejrzystości decyduje przyjęcie zasad, w wyniku przyjęcia których każdy zaangażowany podmiot uznaje, że zarządzanie ryzykiem: Kreuje i chroni wartości (1), Jest zintegrowane z procesami organizacji i ze strukturą zarządzania (2), Jest istotnym elementem procesu decyzyjnego (3), Uwzględnia niepewność (4), Jest systemowe (według reguł), uporządkowane i realizowane zgodnie z założonym harmonogramem (5), Opiera się na najlepszych dostępnych informacjach (6), Wymaga ciągłej komunikacji (7). Ponadto: Należy decentralizować proces szacowania ryzykiem (8), Niezbędne jest wdrożenie mechanizmu komentowania i uzasadniania (9), Należy zapewnić powtarzalność metodyki szacowania ryzyka (10), Należy zapewnić porównywalność metodyk szacowania ryzyka (11), Należy zachować kolejność *od ogółu do szczegółu* (12), Należy zachować kolejność *od skutku do przyczyny* (13) oraz Należy racjonalnie określić katalog rozważanych scenariuszy (14).

O skuteczności procesu nie decydują więc wyłącznie wybrane metody oceny ryzyka, poprawność jej przeprowadzenia czy adekwatne do zagrożeń/ryzyk wpisane w strukturę organizacyjną upoważnienia oraz kompetencje. To, co determinuje i wpływa na jakość zarządzania, to środowisko analityczne, w którym każdy posługuje się tymi samymi regułami, uznaje tożsame zasady i definiuje jednakowo pojęcia. To właśnie te czynniki – w opinii zespołu autorskiego – decydują o powodzeniu realizacji zarządzania ryzykiem. Współpraca i jednolite postrzeganie problemu są kluczowe dla procesu, reszta stanowi mniej lub bardziej złożone technicznie zabiegi, wykonywane zgodnie z przyjętą metodyką.

Czy udało się nam w książce wyczerpać tematykę odwołującą się do ryzyka oraz zarządzania nim? Z pewnością nie. Monografia stanowi jedynie wstęp do dalszych badań, dyskusji i wniosków. W zmieniającym się otoczeniu ciągła weryfikacja poprawności systemu jest jednym z kluczowych wymiarów sukcesu.

Wszystkim Czytelnikom, którzy dotarli z nami do ostatnich stron książki, dedykujemy słowa George'a Washingtona: *Zrób co możesz, tam gdzie jesteś, z tym co masz i nigdy nie bądź zadowolony!*

Grzegorz Abgarowicz

Bibliografia

Publikacje

Babbie E., Podstawy badań społecznych, przekł. Betkiewicz W. i in., Wydawnictwo Naukowe PWN, Warszawa 2008.

Baugier J. M., Vuillod S., Strategie zmian w przedsiębiorstwie. Nowoczesna metoda, przekł. Egeman M., Poltext, Warszawa 1993.

Borodako K., Foresight w zarządzaniu strategicznym, Wydawnictwo C.H. Beck, Warszawa 2009.

Borodako K., Nowosielski M. (red.), Foresight w praktyce zarządzania przedsiębiorstwem. Analizy i studia przypadków, Instytut Zachodni, Poznań 2012.

Chyliński A., Metoda Monte Carlo w bankowości, Warszawa 1999.

Gabryelczyk R., Dessoulavy-Śliwiński B., Mapowanie ryzyka w obszarze Facility Management, Administrator, nr 4/2014.

Gierszewski J., Bezpieczeństwo wewnętrzne. Zarys systemu. Zarządzanie bezpieczeństwem, Difin, Warszawa 2013.

Jakubczak R., Obrona narodowa w tworzeniu bezpieczeństwa III RP, Dom Wydawniczy BELLONA, Warszawa 2003, załącznik 32 wg Przeworskiego K.

Jasiński L. J., Myślenie perspektywiczne. Uwarunkowania badania przyszłości typu foresight, Instytut Nauk Ekonomicznych Polskiej Akademii Nauk, Warszawa 2007.

Kaszubski R. W., Romańczuk D. (red.), Księga dobrych praktyk w zakresie zarządzania ciągłością działania (Business Continuity Management), Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2011.

Kitler W., Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System, Akademia Obrony Narodowej, Warszawa 2011.

Klasik A, Markowski T., Wprowadzenie, w: Foresight regionalny i technologiczny. Warszawa 2003.

Kopczewski M., Pająk K., Tworzenie map ryzyka i map podatności jako elementu zarządzania kryzysowego, Zeszyty Naukowe WSOWL, nr 4/2011.

Krauz-Mozer B., Szostak W., Teoria polityki. Podstawy metodologiczne politologii empirycznej, Uniwersytet Jagielloński, Kraków 1993.

Kreikebaum H., Strategiczne planowanie w przedsiębiorstwie, przekł. Zawisza W., Wydawnictwo Naukowe PWN, Warszawa 1996.

Kubala A., Efekty termiczne przy odwadnianiu etanolu w cyklicznym procesie adsorpcyjno-desorpcyjnym zmiennociśnieniowym, Rozprawa doktorska, Politechnika Krakowska. Kraków 2010.

Kukurba M., Miejsce i rola rachunkowości zarządczej w systemie zarządzania przedsiębiorstwem (wybrane zagadnienia), Zeszyty Naukowe Wyższej Szkoły Zarządzania 2003, nr 2.

Kumpiałowska A., Skuteczne zarządzanie ryzykiem a kontrola zarządcza w sektorze publicznym, Wydawnictwo C.H. Beck, Warszawa 2010.

Leduchowska D., Zarządzanie ryzykiem w ramach unijnego mechanizmu ochrony ludności, Biuletyn Wydziału Analiz RCB, październik 2014 r.

Lisiński M., Metody planowania strategicznego, Polskie Wydawnictwo Ekonomiczne, Warszawa 2004.

Liwacz A., Zarządzanie ryzykiem, Poradnik Samorządowy grudzień 2004.

Lorek E., Pomiar ryzyka, w: Zarządzanie zintegrowanym ryzykiem przedsiębiorstw w Polsce, Wolters Kluwers Polska Sp. z o.o., Warszawa 2001.

Łasut A., Koszty i korzyści z wprowadzenia w Polsce systemu ubezpieczeń obowiązkowych od skutków powodzi, Kraków 2006.

Łuczak J., Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001, zeszyty naukowe Akademia Morska w Szczecinie 2009,19(91).

Magruk A., Słabe Sygnały i Dzikie Karty – Innowacyjne Metody Antycypacyjne, Economy and Management – 4/2010.

Mamica Ł., Kopyciński P., Foresight technologiczny na rzecz zrównoważonego rozwoju Małopolski, w: Foresight regionalny i technologiczny. Pierwsze doświadczenia polskich regionów, A. Klasik, T. Markowski (red.), Komitet Przestrzennego zagospodarowania kraju PAN, Warszawa 2010.

Moszkowicz M. (red.), Zarządzanie strategiczne. Systemowa koncepcja biznesu, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.

Niżnik J., Przedmiot poznania w naukach społecznych, Państwowe Wydawnictwo Naukowe, Warszawa 1979.

Nowak E., Bezpieczeństwo narodowe – istota, zakres, uwarunkowania, w: Bezpieczeństwo narodowe i zarządzanie kryzysowe w Polsce w XXI wieku, Jemioło T., Rajchel K. (red.), Wyższa Szkoła Informatyki, Zarządzania i Administracji w Warszawie, Wydział Strategiczno-Obrony Akademii Obrony Narodowej w Warszawie, Towarzystwo Naukowe Powszechne, Warszawa 2009.

Okoń W., Nowy słownik pedagogiczny, wyd. Żak, Warszawa 1996.

Orzeł J. Ilościowe metody pomiaru ryzyka operacyjnego BiK V 2005.

Pawłowski J. i in. (opr.), Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej, Warszawa 2002.

Pieter J., Ogólna metodologia pracy naukowej, Ossolineum, Wrocław 1967.

Ptak-Kostecka Ż., Analiza przypadku, czyli metoda case study, Rozdział 4 pracy doktorskiej pt. Efektywność pełnienia ról menedżerskich (2000).

Rogut A., Piasecki B., Foresight: niekonwencjonalny instrument strategicznego zarządzania rozwojem regionu (doświadczenia woj. łódzkiego), w: Foresight regionalny i technologiczny.

Romańczuk D., Analiza wpływu zdarzenia na biznes, NetApp Data Center Fitness, 20 czerwca 2013 r.

Safin K., (red.), Foresight jako metoda kształtowania przyszłości. Identyfikacja potencjału i zasobów Dolnego Śląska w obszarze nauka i technologie na rzecz poprawy jakości życia, Uniwersytet Ekonomiczny we Wrocławiu, Katowice 2010.

Skomra W., Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy, wyd. PRESSCOM, Wrocław 2010.

Stabryła A., Zarządzanie przedsiębiorstwem, Zeszyty Naukowe MWSE w Tarnowie 2011, nr 2(19).

Stemplewska-Żakowicz K., Metody jakościowe, metody ilościowe: hamletowski dylemat czy różnorodność do wyboru?; Roczniki Psychologiczne, tom XIII, nr 1-2010.
Szewczuk W., Encyklopedia psychologii, wyd. Fundacja Innowacja, Wyższa Szkoła Społeczno-Ekonomiczna, Warszawa 1998.
Szewczyk R. i in. (opr.), Foresight województwa mazowieckiego. Krzyżowa analiza wpływów, scenariusze rozwoju, priorytetowe technologie, Przemysłowy Instytut Automatyki i Pomiarów PIAP, Warszawa 2008.
Sztumski J., Wstęp do metod i technik badań społecznych, „Śląsk", Katowice 1999.
Szymańska A. I., Badania preferencji konsumentów z wykorzystaniem kompozycyjnej metody badań MDPREF. Kraków 2013.
Thlon M., Przegląd ilościowych metod szacowania ryzyka operacyjnego, styczeń 2007.
Wawiernia A., Ryzyko jako szansa i zagrożenie dla działalności przedsiębiorstwa. Gdańsk 2013.
Williams C. A. Jr., Smith M. L., P. C. Young, Zarządzanie ryzykiem a ubezpieczenia, Wydawnictwo Naukowe PWN, Warszawa 2002.
Winczorek P., Wstęp do nauki o państwie, LIBER, Warszawa 2000.
Wolanin J., Zarys teorii bezpieczeństwa obywateli. Ochrona ludności na czas pokoju, Danmar, Warszawa 2005.
Wójcik P., Znaczenie studium przypadku jako metody badawczej w naukach o zarządzaniu, luty 2013.
Zaleśkiewicz T., Organizacje wobec niepewności. O naturalistycznym paradygmacie w badaniu decyzji menedżerskich, w: Organizacje – wyzwania i zagrożenia. Perspektywa psychologiczna, Strykowska M. (red.), Wydawnictwo Fundacji Humaniora, Poznań 2002.
Zawarska J., Identyfikacja i pomiar ryzyka w procesie zarządzania ryzykiem podmiotów gospodarczych, Zarządzanie i Finanse, nr 1/2012.
Ziętek-Kwaśniewska K., Symulacje Monte Carlo jako metoda wyceny opcji. Lublin 2006.
Foresight technologiczny. Podręcznik. t. 1. Organizacja i metody, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2007.
Foresight technologiczny. Podręcznik. t. 2. Foresight technologiczny w praktyce, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2007.

Dyrektywy

Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim.
Ramowa Dyrektywa Wodna 2000/60/WE (RDW) z dnia 23 października 2000 r. ustanawiająca ramy wspólnotowego działania w dziedzinie polityki wodnej.

Decyzje

Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

Normy

IEC/FDIS 31010 Risk management — Risk assessment techniques.
ISO 31010 – Zarządzanie ryzykiem – Techniki oceny ryzyka (Risk management – Risk assessment techniques).

Norma BS ISO 22301:2012 Bezpieczeństwo powszechne – Systemy Zarządzania Ciągłością Działania.
Norma BS 11200:2014 Zarządzanie kryzysowe – Wytyczne i dobre praktyki.
Norma PKN-ISO Guide 73 Zarządzanie ryzykiem – Terminologia.
PKN-ISO Guide 73, Zarządzanie ryzykiem – Terminologia, marzec 2012.
PN-ISO 31000:2012 – Wytyczne w zakresie zarządzania ryzykiem korporacyjnym.
PN-ISO 31000:2012, Zarządzanie ryzykiem, zasady i wytyczne, PKN Warszawa 2012.

Ustawy

Ustawa z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. 2009 nr 131, poz. 1076).
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, (Dz.U. z 2013, poz. 1166).
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89, poz. 590, ze zm).
Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska, (Dz.U. z 2013, poz. 1232).
Ustawa z dnia 18 lipca 2001 r. Prawo Wodne (Dz.U. z 2015, poz. 469).
Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2013 r., poz. 885).
Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2013, poz 594).
Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz.U. z 2015, poz 460).
Ustawa z dnia 16 grudnia 2010 r. o publicznym transporcie drogowym (Dz.U z 2011 nr 5, poz. 13).
Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków. (Dz.U. z 2015, poz. 139).
Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. z 2012, poz. 1059).
Ustawa z dnia 21 marca 2014 r. o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz niektórych innych ustaw (Dz.U. 2014, poz. 1138).
Ustawa z 12 marca 2004 r. o pomocy społecznej (Dz.U. z 2015, poz. 163).
Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U. z 2009 r. nr 174, poz. 1380).
Ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz.U. z 2013 r., poz. 595).
Ustawa z dnia 13 października 1998 r. Przepisy wprowadzające ustawy reformujące administrację publiczną (Dz.U. 1998 nr 133, poz. 872).
Ustawa z dnia 5 czerwca 1998 roku o samorządzie województwa (Dz.U. z 2013 r., poz. 596).
Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2015, poz. 827).

Rozporządzenia

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.U. 2010 nr 83, poz. 540).
Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. 2010 nr 83, poz. 542).
Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. 2010 nr 83, poz. 541).
Rozporządzenie Ministra Środowiska, Ministra Transportu, Budownictwa i Gospodarki Morskiej, Ministra Administracji i Cyfryzacji oraz Ministra Spraw Wewnętrznych z dnia 21 grudnia 2012 r. w sprawie opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego (Dz.U. z 2013, poz. 104).

Rozporządzenie Prezesa Rady Ministrów z dnia 22 czerwca 2001 r. w sprawie wykazu samodzielnych publicznych zakładów opieki zdrowotnej, które zostały przejęte przez gminy, powiaty i samorządy województw (Dz.U. 2001 nr 65, poz. 659).

Procedury

Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2010.

Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej.

Strony internetowe

http://www.kzgw.gov.pl/Dyrektywa-Powodziowa.html

http://www.samorzad.lex.pl/czytaj/-/artykul/podstawowa-opieka-zdrowotna-nalezy-do-zadan-wlasnych-gminy

http://www.szydlowiecpowiat.pl/wydzial_rolnictwa_ochrony_srodowiska_gospodarki_wodnej_i_lesnictwa.php

http://www2.mz.gov.pl

http://www.wios.szczecin.pl/bip/chapter_16037.asp

www.mazowieckie.pl

http://www.iso.org.pl/iso-22301

http://www.uwm.edu.pl/mkzk/download/wprowadzenie.pdf

http://www.almamer.pl/aa%20materialy.%20dydaktyczne/E_Zarzadzanie_projektami_biznesowymi_Duczkowska-Piasecka.pdf

http://www.eduteka.pl/doc/metoda-badan-terenowych-i-odpowiadajace-jej-techniki-badan

http://www.fuw.edu.pl/~jarekz/MODELOWANIE/M1_wstep_dyskretne.pdf

http://www.retsat1.com.pl/michauer/chemia/inne/modelowanie.pdf

http://www.powiatwroclawski.pl/index.php?option=com_content&id=1142:mapa-zagroe-powiatu-wrocawskiego&Itemid=8,0

http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego

http://dotproject.net.pl/node/227

http://www.governica.com/Analiza_koszt%C3%B3w_i_korzy%C5%9Bci

http://www.ekologia.pl/srodowisko/ochrona-srodowiska/najwieksze-powodzie-w-polsce-w-xx-i-xxi-wieku,12426.html

http://www.polskieradio.pl/5/3/Artykul/198291,Fala-na-Wisle-najwieksza-od-160-lat

http://edu.pjwstk.edu.pl/wyklady/psk/scb/index15.html

Prezentacje

Abgarowicz G., Ocena ryzyka zagrożeń transgranicznych, scenariusz powódź – propozycja metodyki, Rządowe Centrum Bezpieczeństwa, Warszawa 2014 r.

Skomra W., Zdolność zarządzania ryzykiem jako nowe wyzwanie dla systemu zarządzania kryzysowego, Prezentacja z Konferencji Naukowej Zarządzanie Kryzysowe na poziomie województwa i w jednostkach samorządu terytorialnego, AON, 12–13 maja 2014 r.

Prezentacja Zakładu Ochrony Ludności CNBOP–PIB, Szacowanie ryzyka na potrzeby systemu ochrony ludności w Polsce. Stan obecny oraz kierunki przyszłych rozwiązań, materiał konferencyjny, Kraków 2014 r.
Zbieżność krajowych dokumentów planistycznych z wymogami Mechanizmu, Rządowe Centrum Bezpieczeństwa, wrzesień 2014.

Inne

All Hazards Risk Assessment Methodology Guidelines 2012/2013.
A Framework for Major Emergency Management, A Guide to Risk Assessment in Major Emergency Management, January 2010.
A National Risk Assessment for Ireland, December 2012.
Guide to Risk and vulnerability analyses; Swedish Civil Contingencies Agency; 2012.
Analiza ryzyka – Eksperckie metody analizy ryzyka w zarządzaniu bezpieczeństwem Kołodziński E.
Based on the PHA Waterfall Model Beyond FMEA: The structured what-if technique (SWIFT) © 2012 American Society for Healthcare VOLUME 31, NUMBER 4 23 By Alan J. Card, MPH, CPH, CPHQ James R.Ward, BEng, CEng,PhD, MIET, and P. John Clarkson, PhD, BA(Eng).
Identyfikacja źródeł zagrożenia: Poradnik metod ocen ryzyka związanego z niebezpiecznymi instalacjami procesowymi, WIOŚ, Warszawa 2008.
Komunikat nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (Dz.Urz. MF z 2012 r., poz. 56).
Materiał zgromadzony w toku realizacji projektu: Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. PE.VII.6. Opracowanie metodyki analizy ryzyka możliwej do zastosowania na różnych poziomach zarządzania kryzysowego, w tym opracowanie procedury tworzenia map ryzyka i map zagrożeń. 2014.
Materiał zgromadzony w toku realizacji projektu: Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. PK.1. Projekt dokumentu opisującego wytyczne dla jednostek samorządu terytorialnego. 2015.
Method of Risk Analysis for Civil Protection 2011; Federal Office of Civil Protection and Disaster Assistance 2011.
Metodyka oceny ryzyka do przygotowania sprawozdania za rok 2014, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014r.
Mitkowski P., Ocena ilościowa ryzyka: analiza drzewa błędów (konsekwencji), materiały dydaktyczne.
Mitkowski P., Ocena ilościowa ryzyka: analiza drzewa zdarzeń, materiały dydaktyczne.
Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2013 r.
National Risk Register 2008.
National Security Programme National Risk Assessment Method Guide, 2008.
Ocena ryzyka na potrzeby zarządzania kryzysowego, Raport o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.
Polityka zarządzania ryzykiem w Ministerstwie Infrastruktury, Warszawa październik 2011 r.
Raport ze szkolenia BSI z 11 – 15 listopada 2013 r.
Raport po powodzi z maja i czerwca 2010 r., Urząd Miasta Krakowa, Kraków 2010.

Risk Management Capability Assessment Guidelines – Draft, Bruksela 2014.
Sprawozdanie (projekt) podsumowujące wyniki oceny ryzyka za rok 2014 i lata kolejne, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014.
Swedish National Risk Assessment; Swedish Civil Contingencies Agency; 2012 r.
The beginning of the Monte Carlo Method, Metropolis. N, Los Alamos Science, Numer 15, 1987.
The National Risk Register of Civil Emergencies (NRR) 2010.
Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands.
Zalecenia do powiatowych planów zarządzania kryzysowego. Wydział bezpieczeństwa i zarządzania kryzysowego Mazowieckiego Urzędu Wojewódzkiego w Warszawie. Warszawa, marzec 2014 r.
Załącznik do zarządzenia nr 92/2011 Wojewody Łódzkiego z dnia 29 marca 2011 r. w sprawie zarządzania ryzykiem w Łódzkim Urzędzie Wojewódzkim w Łodzi.
Zasady zarządzania ryzykiem w Politechnice Warszawskiej, Załącznik do Zarządzenia nr 5/2012 Rektora PW z dnia 13 stycznia 2012 r.
Zarządzanie ryzykiem w sektorze publicznym, Ministerstwo finansów RP.

Spis rysunków

Spis rysunków

Spis tabel

Spis wykresów

Noty biograficzne

dr Grzegorz Abgarowicz – doktor nauk społecznych w zakresie nauk o bezpieczeństwie. Adiunkt Zakładu Polityki Bezpieczeństwa w Instytucie Politologii Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, pracownik Rządowego Centrum Bezpieczeństwa. Zajmuje się problematyką bezpieczeństwa powszechnego, zarządzania kryzysowego, ochrony ludności oraz Kaukazu. Autor licznych publikacji naukowych, promotor i recenzent prac naukowych, uczestnik projektów badawczych m.in. z zakresu ochrony ludności (Anvil – Analysis of civil security systems in Europe), metodyki oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP, zintegrowanych systemów budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne. Członek Krakowskiego Oddziału Polskiego Towarzystwa Ludoznawczego, armenolog.

dr Krzysztof Cebul – politolog i socjolog, adiunkt, kierownik Zakładu Polityki Bezpieczeństwa w Katedrze Polityk Publicznych Instytutu Politologii Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Autor analiz dla Urzędu Komitetu Integracji Europejskiej. W swojej pracy badawczej zajmuje się problematyką organizacji władzy, bezpieczeństwa państwa, procesem integracji europejskiej oraz znaczeniami i funkcjami tekstu/wypowiedzi w rzeczywistości politycznej.

mgr Inga Abgarowicz – absolwentka Wydziału Prawa i Administracji Wyższej Szkoły Menedżerskiej w Warszawie, oraz Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej. Kierownik Działu Ochrony Ludności w Centrum Naukowo-Badawczym Ochrony Przeciwpożarowej – Państwowym Instytucie Badawczym. Jako kierownik zespołu ze strony konsorcjanta, prowadzi projekt pt. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP". Jest zastępcą kierownika w projekcie „Emergency Management in Social Media Generation" po stronie CNBOP-PIB. Autorka wystąpień i publikacji z zakresu ochrony ludności, zarządzania kryzysowego i zarządzania ryzykiem. Uczestniczy w projektach naukowych finansowanych przez instytucje krajowe oraz europejskie.

mgr inż. Maciej Napiórkowski – ukończył Wydział Inżynierii Środowiska na Politechnice Warszawskiej. Obecnie doktorant w Zakładzie Informatyki i Badań Jakości Środowiska na wydziale Politechniki Warszawskiej. Pracownik Działu Ochrony Ludności w CNBOP-PIB. Wykonawca zadań w projektach naukowo-badawczych realizowanych przez CNBOP-PIB we współpracy z innymi instytucjami. Pełni funkcję kierownika w projekcie finansowanym z 7 PR UE pt. „Emergency Mana-

gement is Social Media Generation". Ponadto bierze udział w licznych projektach realizowanych na rzecz bezpieczeństwa i obronności.

mgr Tomasz PLASOTA – absolwent Uniwersytetu Warszawskiego na Wydziale Dziennikarstwa i Nauk Politycznych (kierunek: Bezpieczeństwo wewnętrzne). Młodszy specjalista w Dziale Ochrony Ludności w Centrum Naukowo-Badawczym Ochrony Przeciwpożarowej – Państwowym Instytucie Badawczym. Zastępca kierownika zespołu ze strony konsorcjanta w projekcie „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP". Kierownik w projekcie „Emergency Management in Social Media Generation" po stronie CNBOP-PIB. Autor wystąpień i publikacji z zakresu ochrony ludności, zarządzania kryzysowego i zarządzania ryzykiem.

mgr Bartłomiej Połeć – absolwent Akademii Obrony Narodowej na Wydziale Bezpieczeństwa Narodowego. Autor licznych publikacji z zakresu bezpieczeństwa i techniki pożarniczej. Uczestnik projektów badawczo-rozwojowych realizowanych przez CNBOP-PIB we współpracy z innymi instytucjami.

mgr Monika Wachnik – absolwentka Wyższej Szkoły Gospodarki Euroregionalnej, kierunek Bezpieczeństwo Wewnętrzne. Pracownik Działu Ochrony Ludności Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej – Państwowego Instytutu Badawczego. Posiada doświadczenie w przygotowaniu dokumentacji niezbędnej do realizacji wniosków o dofinansowanie z Funduszy Europejskich i programu Innowacyjna Gospodarka. Pełni funkcję zastępcy kierownika w projekcie finansowanym z Narodowego Centrum Badań i Rozwoju pt. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP". Bierze udział w licznych projektach realizowanych na rzecz bezpieczeństwa i obronności oraz w międzynarodowym projekcie EmerGent finansowanym z 7 PR UE. Autorka publikacji z zakresu zarządzania kryzysowego oraz edukacji dla bezpieczeństwa.

Załącznik 1

I. Kwestionariusz ankiety:
określenie potrzeb organów zarządzania kryzysowego administracji rządowej
(Ankieta do badań rozdziału drugiego)

Ankieta skierowana jest do wykonawców raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego, tj. ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych, wojewodów oraz RCB jako koordynatora prac nad dokumentem.

Celem badania jest poznanie opinii ekspertów dotyczących obecnego stanu rozwiązań formalno-prawnych oraz określenie potrzeb organów zarządzania kryzysowego wszystkich szczebli systemu w zakresie oceny ryzyka na potrzeby realizacji zadań z zakresu planowania cywilnego.

Wyniki badań uzyskane tą drogą wzbogacą wiedzę zespołu projektowego Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej, Państwowego Instytutu Badawczego z powyższego zakresu. Rozpatrywane w projekcie *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP* zagadnienia stanowić będą podstawę dla określenia potrzeb jednostek samorządu terytorialnego i administracji rządowej w zakresie identyfikacji zagrożeń oraz procesu szacowania ryzyka.

Uzyskane tą drogą wyniki będą wykorzystane wyłącznie do celów naukowych w postaci zależności statystycznych i zestawień ilościowych. Pytania mają charakter zamknięty i półotwarty.

1. Czy zdaniem Pani/Pana zapisy ustawy o zarządzaniu kryzysowym:
   a) w stopniu wystarczającym odnoszą się do problematyki szacowania ryzyka
   b) należy rozszerzyć o cały proces zarządzania ryzykiem (identyfikacja ryzyka, analiza i jego ocena oraz propozycja postępowania z ryzykiem)

2. Czy definicja mapy ryzyka zawarta w art. 3 pkt. 10 ustawy o zarządzaniu kryzysowym jest dla Pani/Pana zrozumiała? *mapa ryzyka - należy przez to rozumieć mapę lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę*.
   a) TAK
   b) NIE

3. Czy zdaniem Pani/Pana wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka jest niezbędnym elementem raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego?
   a) TAK
   b) NIE

4. Czy zdaniem Pani/Pana wskazane w § 5 .1 Rozporządzenia w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego sposoby przedstawienia mapy ryzyka pozwalają na prezentację danych dotyczących oceny ryzyka? *Mapę ryzyka, (..) przedstawia się w formie: 1) mapy topograficznej, a w postaci elektronicznej - mapy wektorowej lub rastrowej, przedstawiającej zasięg geograficzny zagrożeń z przypisanym prawdopodobieństwem wystąpienia i oceną skutków wystąpienia dla ludności, gospodarki lub środowiska; 2) tabeli opisującej parametry zagrożeń oraz ich prognozowane skutki; 3) opisowej, jeżeli charakter zagrożenia uniemożliwia przedstawienie informacji w sposób określony w pkt 1 i 2*.
   a) TAK
   b) NIE

5. Jeżeli TAK, to który ze wskazanych w Rozporządzeniu sposobów przedstawienia mapy ryzyka uważa Pani/Pan za najbardziej czytelny?
   a) mapa topograficzna
   b) tabela opisująca parametry zagrożeń oraz ich prognozowane skutki
   c) mapa opisowa

6. Jeżeli NIE, to w jaki sposób zdaniem Pani/Pana należałoby przedstawiać mapę ryzyka? Mapę ryzyka należałoby przedstawiać w formie….....

7. Czy zdaniem Pani/Pana określony w §4 pkt.1 Rozporządzenia w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego wykaz rodzajów zagrożeń (zamieszczonych poniżej) został zdefiniowany właściwie?

a) istotnym wpływie na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego,
b) których skutki mogą: - godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, a w szczególności w suwerenność, niepodległość i nienaruszalność terytorium, – zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach, – oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa, – dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie,
c) występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych,

d) o charakterze terrorystycznym mogących doprowadzić do sytuacji kryzysowej;
   a) TAK
   b) NIE

8. Jeżeli NIE, to co zdaniem Pani/Pana należałoby w nim zmienić (można zaznaczyć kilka odpowiedzi)?
   a) rozszerzenie katalogu zagrożeń ujętych w mapie ryzyka
   b) zawężenie katalogu zagrożeń ujętych w mapie ryzyka
   c) inne:

9. Które z wymienionych działań podejmuje się w Pani/Pana instytucji w celu zdobycia danych do zidentyfikowania zagrożeń na potrzeby opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego? (można zaznaczyć kilka odpowiedzi)
   a) analiza danych statystycznych
   b) analiza danych historycznych
   c) szacowanie eksperckie
   d) badania terenowe
   e) ocena sytuacji międzynarodowej
   f) modelowanie matematyczne
   g) analiza danych z systemów monitorowania zagrożeń
   h) analiza trendów
   i) badania przypadków („case study")
   j) rozpoznanie środowiskowe
   k) inne:

10. Czy sposób wykorzystania powyższych działań na potrzeby zdobycia informacji do zidentyfikowania zagrożeń jest dla Pani/Pana zrozumiały?
   a) TAK
   b) NIE

11. Jeżeli NIE to sposób wykorzystania którego z nich należałoby doprecyzować w procedurze opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego? (można zaznaczyć kilka metod)
   Na potrzeby zdobycia danych niezbędnych do zidentyfikowania zagrożeń należałoby doprecyzować sposób wykorzystania:
   a) analiza danych statystycznych
   b) analiza danych historycznych
   c) szacowanie eksperckie
   d) badania terenowe
   e) ocena sytuacji międzynarodowej
   f) modelowanie matematyczne
   g) analiza danych z systemów monitorowania zagrożeń

h) analiza trendów
i) badania przypadków („case study")
j) rozpoznanie środowiskowe
k) inne:

12. Czy uważa Pani/Pan, że podjęcie któregoś z powyższych działań na potrzeby zdobycia informacji do zidentyfikowania zagrożeń wykracza poza kompetencje Pani/Pana instytucji?
a) TAK
b) NIE

13. Jeżeli TAK to podjęcie którego z powyższych działań wymaga wykorzystania zasobów i źródeł informacji spoza Pani/Pana instytucji?
a) analiza danych statystycznych
b) analiza danych historycznych
c) szacowanie eksperckie
d) badania terenowe
e) ocena sytuacji międzynarodowej
f) modelowanie matematyczne
g) analiza danych z systemów monitorowania zagrożeń
h) analiza trendów
i) badania przypadków (*case study*)
j) rozpoznanie środowiskowe

14. Czy zbierając dane niezbędne do opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego czerpie Pani/Pan informacje z poziomu poszczególnych powiatów?
a) TAK
b) NIE

15. Które komórki organizacyjne Pani/Pana instytucji biorą udział w procesie oceny ryzyka na potrzeby opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego?
a) właściwe centrum zarządzania kryzysowego
b) inne:

16. Czy zawarty w procedurze opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego opis opracowania scenariuszy zdarzeń w ramach zagrożeń został zdefiniowany właściwie (czy jest zrozumiały)?
a) TAK
b) NIE

17. Jeżeli NIE, to jakie zmiany w części procedury dotyczącej określenia scenariuszy dla zidentyfikowanych zagrożeń należałoby wprowadzić? (można zaznaczyć kilka odpowiedzi):
   a) zawężenie zakresu informacji niezbędnego do określenia scenariuszy dla zidentyfikowanych zagrożeń
   b) rozszerzenie zakresu informacji niezbędnego do określenia scenariuszy dla zidentyfikowanych zagrożeń
   c) wprowadzenie opisu metody opracowania scenariuszy wystąpienia zagrożeń
   d) inne:

18. Czy zdaniem Pani/Pana przyjęta w procedurze opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego metoda oceny ryzyka pozwala na właściwie jego oszacowanie?
   a) TAK
   b) NIE

19. Jeżeli NIE to co sprawiło Pani/Panu największą trudność w procesie szacowania ryzyka (można zaznaczyć kilka odpowiedzi)?
   a) określenie parametrów skali prawdopodobieństwa wystąpienia zagrożenia (konkretnego scenariusza)niezbędnego do określenia scenariuszy dla zidentyfikowanych zagrożeń
   b) określenie parametrów skali skutków (konsekwencji) zagrożenia (konkretnego scenariusza)
   c) określenie parametrów wartości ryzyka
   d) określenie poziomu akceptacji ryzyka
   e) zastosowanie technik możliwych do wykorzystania przy szacowaniu ryzyka
   f) inne:

20. Czy zdaniem Pani/Pana należałoby wprowadzić zmiany w procedurze opracowania raportów cząstkowych w części odnoszącej się do procesu szacowania ryzyka?
   a) TAK
   b) NIE

21. Jeżeli TAK to zdaniem Pani/Pana, które z wymienionych zmian należałoby wprowadzić (można zaznaczyć kilka odpowiedzi)?
   a) zmiana parametrów oraz opisów skali prawdopodobieństwa
   b) zmiana parametrów oraz opisów skali skutków
   c) zmiana parametrów kategorii wartości ryzyka
   d) zmiana parametrów oraz opisów kategorii akceptacji ryzyka
   e) zmiana parametrów oceny ryzyka
   f) wprowadzenie opisu technik możliwych do wykorzystania przy szacowaniu ryzyka
   g) inne:

22. Czy zdaniem Pani/Pana należy stworzyć system informatyczny wspomagający proces oceny ryzyka na potrzeby opracowania raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego RP?
   a) TAK
   b) NIE

23. Jeżeli TAK, to jakie rozwiązania powinien zawierać projektowany system (można zaznaczyć kilka odpowiedzi)?
   a) prezentować dane wprowadzone przez użytkowników z zakresu identyfikacji zagrożeń na potrzeby oceny ryzyka wraz ze scenariuszami ich wystąpienia
   b) prezentować dane z zakresu szacowania prawdopodobieństwa wystąpienia zagrożeń
   c) prezentować mapy ryzyka
   d) prezentować zależności pomiędzy danymi wprowadzonymi przez użytkowników
   e) umożliwić przepływ informacji pomiędzy poszczególnymi wykonawcami raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego
   f) inne:

24. Czy odczuwa Pani/Pan potrzebę udziału w przedsięwzięciach szkoleniowo-edukacyjnych wzbogacających wiedzę z zakresu zagadnień związanych z dokonywaniem oceny ryzyka na potrzeby opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego?
   a) TAK
   b) NIE

25. Jeżeli TAK to w których przedsięwzięciach wziąłby Pani/Pan udział (można zaznaczyć kilka odpowiedzi):
   a) szkolenie dotyczące metodologii opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej oceny ryzyka zagrożeń
   b) warsztaty dotyczące metod identyfikacji oraz szacowania ryzyka wystąpienia ryzyka zagrożeń na potrzeby opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego
   c) możliwość skorzystania ze specjalnie przygotowanego podręcznika *Analiza ryzyka dla zarządzania kryzysowego* wzbogacającego wiedzę z zakresu oceny ryzyka na potrzeby opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego
   d) inne:

Instytucja w której Pan/Pani pracuje:

Stanowisko:

Czy w ramach zadań służbowych wykonuje Pani/Pan pracę z zakresu planowania cywilnego:
a) TAK
b) NIE

Czy w ramach zadań służbowych wykonuje Pani/Pan pracę z zakresu szacowania ryzyka?
a) TAK
b) NIE

Załącznik 2

II. Kwestionariusz ankiety:
określenie potrzeb organów zarządzania kryzysowego
jednostek samorządu terytorialnego
(Ankieta do badań rozdziału drugiego)

Ankieta skierowana jest do starostów, wójtów/burmistrzów/prezydentów miast

Celem badania jest poznanie opinii ekspertów dotyczących obecnego stanu rozwiązań formalnoprawnych oraz określenie potrzeb organów zarządzania kryzysowego wszystkich szczebli systemu w zakresie oceny ryzyka na potrzeby realizacji zadań z zakresu planowania cywilnego.

Wyniki badań uzyskane tą drogą wzbogacą wiedzę zespołu projektowego Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej, Państwowego Instytutu Badawczego z powyższego zakresu. Rozpatrywane w projekcie *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP* zagadnienia stanowić będą podstawę do określenia potrzeb jednostek samorządu terytorialnego i administracji rządowej w zakresie identyfikacji zagrożeń oraz procesu szacowania ryzyka.

Uzyskane tą drogą wyniki będą wykorzystane wyłącznie do celów naukowych w postaci zależności statystycznych i zestawień ilościowych. Pytania mają charakter zamknięty i półotwarty.

1. Czy zdaniem Pani/Pana zapisy ustawy o zarządzaniu kryzysowym: a) w stopniu wystarczającym odnoszą się do problematyki szacowania ryzyka
   b) należy rozszerzyć o cały proces zarządzania ryzykiem (identyfikacja ryzyka, jego szacowanie, ewaluację oraz zarządzanie nim)

2. Czy definicja mapy ryzyka zawarta w art. 3 pkt. 10 ustawy o zarządzaniu kryzysowym jest dla Pani/Pana zrozumiała?
   a) TAK
   b) NIE

3. Czy uważa Pani/Pan ocenę ryzyka wystąpienia zagrożeń oraz mapy ryzyka za niezbędny element i części planu zarządzania kryzysowego, tj. planu głównego?
   a) TAK
   b) NIE

4. Czy wydane przez właściwy organ wytyczne/zalecenia do planów zarządzania kryzysowego odnoszą się do zagadnień identyfikacji i szacowania ryzyka?
   a) TAK
   b) NIE

5. Jeśli TAK, to czy są one dla Pani/Pana zrozumiałe?
   a) TAK
   b) NIE

6. Jeżeli NIE to które z wymienionych zmian w wytycznych/zaleceniach do planów zarządzania kryzysowego w zakresie identyfikacji i szacowania ryzyka należałoby wprowadzić? (można zaznaczyć kilka odpowiedzi)?
   a) uszczegółowienie części dotyczącej wskazania zagrożeń oraz źródeł informacji niezbędnych do ich zidentyfikowania
   b) uszczegółowienie części dotyczącej metod szacowania prawdopodobieństwa wystąpienia oraz skutków zagrożeń
   c) uszczegółowienie części dotyczącej sposobu przedstawienia mapy ryzyka
   d) inne:

7. Które z wymienionych działań podejmuje się w Pani/Pana instytucji w celu zdobycia danych do zidentyfikowania zagrożeń na potrzeby opracowania planu zarządzania kryzysowego? (można zaznaczyć kilka odpowiedzi)
   a) analiza danych statystycznych
   b) analiza danych historycznych
   c) szacowanie eksperckie
   d) badania terenowe
   e) ocena sytuacji międzynarodowej
   f) modelowanie matematyczne
   g) analiza danych z systemów monitorowania zagrożeń
   h) analiza trendów
   i) badania przypadków (case study)
   j) rozpoznanie środowiskowe
   k) inne:

8. Czy zbierając dane niezbędne do opracowania planu zarządzania kryzysowego w części dotyczącej oceny ryzyka wystąpienia zagrożeń czerpie Pani/Pan informacje z sąsiednich powiatów?**pytanie skierowane do starostów
   a) TAK
   b) NIE

9. Czy zbierając dane niezbędne do opracowania planu zarządzania kryzysowego w części dotyczącej oceny ryzyka wystąpienia zagrożeń czerpie Pani/Pan informacje z poszczególnych gmin wchodzących w skład powiatu?**pytanie skierowane do starostów
   a) TAK
   b) NIE

10. Czy zbierając dane niezbędne do opracowania planu zarządzania kryzysowego w części dotyczącej oceny ryzyka wystąpienia zagrożeń czerpie Pani/Pan informacje z sąsiednich gmin?****pytanie skierowane do wójtów/burmistrzów/prezydentów miast
   a) TAK
   b) NIE

11. Które komórki organizacyjne Pani/Pana instytucji biorą udział w procesie oceny ryzyka na potrzeby opracowania planu zarządzania kryzysowego?
   a) właściwe centrum zarządzania kryzysowego
   b) inne:

12. Czy zdaniem Pani/Pana współpraca z podmiotami biorącymi udział w uzgadnianiu oraz zatwierdzaniu planów zarządzania kryzysowego w części planu głównego dotyczącej oceny ryzyka wystąpienia zagrożeń jest wystarczająca?
   a) TAK
   b) NIE

13. Czy zdaniem Pani/Pana należy stworzyć system informatyczny wspomagający proces oceny ryzyka na potrzeby opracowania planów zarządzania kryzysowego?
   a) TAK
   b) NIE

14. Jeżeli TAK, to jakie rozwiązania powinien zawierać projektowany system (można zaznaczyć kilka odpowiedzi):
   a) prezentować dane wprowadzone przez użytkowników z zakresu identyfikacji zagrożeń na potrzeby opracowania planu zarządzania kryzysowego w części dotyczącej oceny ryzyka zagrożeń
   b) prezentować dane wprowadzone przez użytkowników z zakresu szacowania prawdopodobieństwa wystąpienia zagrożeń
   c) prezentować dane wprowadzone przez użytkowników z zakresu mapowania ryzyka
   d) prezentować zależności pomiędzy danymi wprowadzonymi przez użytkowników

e) umożliwić przepływ informacji pomiędzy podmiotami opracowującymi plany zarządzania kryzysowego
f) inne:

15. Czy odczuwa Pani/Pan potrzebę udziału w przedsięwzięciach szkoleniowo-edukacyjnych wzbogacających wiedzę z zakresu zagadnień związanych z dokonywaniem oceny ryzyka na potrzeby opracowania planów zarządzania kryzysowego?
a) TAK
b) NIE

16. Jeżeli TAK, to w których przedsięwzięciach chciałaby Pani/Pan wziąć udział? (można zaznaczyć kilka odpowiedzi)
a) szkolenie dotyczące metodyki opracowania planu zarządzania kryzysowego w części dotyczącej oceny ryzyka zagrożeń
b) warsztaty dotyczące metod identyfikacji oraz szacowania ryzyka wystąpienia ryzyka zagrożeń na potrzeby opracowania planu zarządzania kryzysowego
c) możliwość skorzystania ze specjalnie przygotowanego podręcznika „Analiza ryzyka dla zarządzania kryzysowego" wzbogacającego wiedzę z zakresu oceny ryzyka na potrzeby opracowania planu zarządzania kryzysowego
d) inne:

17. Czy zdaniem Pani/Pana środki finansowe przeznaczone na realizację zadań własnych z zakresu zarządzania kryzysowego w ramach części budżetu Pani/Pana jednostki samorządu terytorialnego są:
a) wystarczające na potrzeby realizacji zadań obowiązkowych
b) wystarczające na potrzeby realizacji zadań obowiązkowych i dobrowolnych
c) niewystarczające

18. Czy zdaniem Pani/Pana wysokość stworzonej w ramach budżetu Pani/Pana jednostki samorządu terytorialnego rezerwy celowej przeznaczonej na realizację zadań własnych z zakresu zarządzania kryzysowego jest wystarczająca?
a) TAK
b) NIE

19. Czy kiedykolwiek Pani/Pana jednostka samorządu terytorialnego ubiegała się o dofinansowanie zadań własnych z zakresu zarządzania kryzysowego w ramach dotacji celowych z budżetu państwa?
a) TAK
b) NIE

20. Jeżeli TAK, to czy wysokość dofinansowania zadań własnych z zakresu zarządzania kryzysowego w formie dotacji celowych okazała się wystarczająca?
    a) TAK
    b) NIE

21. Czy zasady otrzymywania i rozliczania dotacji celowych na dofinansowanie zadań własnych z zakresu zarządzania kryzysowego są dla Pani/Pana zrozumiałe?
    a) TAK
    b) NIE

Instytucja, w której Pan/Pani pracuje:
……

Stanowisko:
……
Czy w ramach zadań służbowych wykonuje Pani/Pan pracę z zakresu planowania cywilnego:
a) TAK
b) NIE

Czy w ramach zadań służbowych wykonuje Pani/Pan pracę z zakresu szacowania ryzyka?
a) TAK
b) NIE

Załącznik 3

Badanie:

IDENTYFIKACJA ZAGROŻEŃ BEZPIECZEŃSTWA NARODOWEGO

(Badanie realizowane w ramach projektu: *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*)

Typ kwestionariusza:
Kwestionariusz do samodzielnego wypełnienia

Etap:
1/3

Instrukcja:

Szanowni Państwo,

dziękujemy, że przyjęli Państwo zaproszenie do udziału w badaniu: *Identyfikacja zagrożeń bezpieczeństwa narodowego*. Przekazujemy Państwu kwestionariusz, przeznaczony do samodzielnego wypełnienia. Badanie składa się z trzech etapów. W obecnie realizowanym etapie badania **oczekujemy od Państwa udzielenia rozbudowanych odpowiedzi** na pytania kwestionariusza. Są to pytania typu otwartego. Prosimy o odesłanie odpowiedzi w formacie elektronicznym (Word) z adresu mailowego umożliwiającego Państwa identyfikację (zawierającego nazwisko). Udzielone przez Państwa odpowiedzi posłużą do opracowania raportu końcowego z badania. Raport ten zostanie upubliczniony.
Celem badania nie jest weryfikacja i ocena Państwa wiedzy. Prosimy o komentarz ekspercki, mieszczący się w obszarze Państwa kompetencji. W ankiecie samodzielnie określają Państwo dziedzinę bezpieczeństwa narodowego, w odniesieniu do której w dalszej części będą Państwo udzielać odpowiedzi. **Prosimy Państwa o podzielenie się posiadanymi wiedzą i doświadczeniem**, o przedstawienie własnego punktu widzenia w zakresie problematyki, o którą pytamy. Celem badania jest stworzenie wizji, perspektyw w zakresie identyfikacji zagrożeń bezpieczeństwa narodowego. Poprzez badanie **chcemy uzyskać aktualne informacje odnośnie do sposobów identyfikowania i szacowania ryzyka w poszczególnych obszarach bezpieczeństwa narodowego Rzeczypospolitej Polskiej**.
Badanie jest realizowane metodą foresight. Metoda ta jest jednym ze sposobów analizy otoczenia, który najlepiej opisać można przy użyciu terminów *proces* i *per-*

spektywa. Jego istotą jest obserwacja, analiza i ewaluacja informacji. **Foresight**, jako proces, **polega na konfrontacji własnej wiedzy, własnych doświadczeń z innymi scenariuszami**. Rezultatem tej konfrontacji jest weryfikacja dotychczasowych wzorców myślenia, uwzględnianie innych punktów widzenia, rozwój koncepcji alternatywnych. Foresight, jako proces tworzenia wizji, polega na integracji różnych perspektyw, czy inaczej rzecz ujmując, na swoistym *uzgadnianiu preferencji*, umożliwiając tworzenie perspektyw dla przyszłości.

W **pierwszym etapie** badania udzielacie Państwo odpowiedzi na poniżej przedstawione pytania kwestionariusza. W **drugim etapie** zadaniem Państwa będzie odniesienie się do raportu powstałego na podstawie analizy ankiet wytworzonych w pierwszym etapie. W tym celu, oprócz raportu, otrzymacie Państwo także zestaw pytań pomocniczych. Na podstawie Państwa odpowiedzi, udzielonych w drugim etapie badania, opracowany zostanie następny raport. **Trzeci i ostatni etap** badania polegać będzie na przygotowaniu przez Państwa odpowiedzi, tym razem w odniesieniu do drugiego raportu, i tak jak poprzednio, w oparciu o pytania pomocnicze. Odpowiedzi należy umieszczać w pustych miejscach pod pytaniami. **Pozostawione pod pytaniami miejsca nie stanowią sugestii co do objętości Państwa wypowiedzi**. Prosimy o, w miarę możliwości, rozbudowane odpowiedzi, ponieważ zależy nam na uzyskaniu obszernego i zarazem szczegółowego materiału badawczego.

KWESTIONARIUSZ
1.
Proszę określić jedną, główną dziedzinę bezpieczeństwa mieszczącą się w zakresie Pani/Pana kompetencji *(np. bezpieczeństwo polityczne, bezpieczeństwo społeczne, bezpieczeństwo kulturowe, bezpieczeństwo militarne, bezpieczeństwo ekonomiczne, bezpieczeństwo ekologiczne, bezpieczeństwo informacyjne i telekomunikacyjne)*:
2.
Proszę dokończyć następujące zdanie: *Bezpieczeństwo* [proszę uzupełnić zgodnie z odpowiedzią na pytanie nr 1] *to…*

3.
Proszę określić obszar/obszary szczegółowe, którymi Pani/Pan się zajmuje, pozwalające na dokładniejszą charakterystykę wskazanej w odpowiedzi na pytanie nr 1 – dziedziny bezpieczeństwa *(np. bezpieczeństwo polityczne: partie polityczne; bezpieczeństwo społeczne: demografia; bezpieczeństwo ekonomiczne: system podatkowy)*:
4.
Proszę w syntetyczny sposób scharakteryzować i uszczegółowić wymieniony/wymienione w odpowiedzi na pytanie nr 3 – obszar/obszary:
5.
Proszę wskazać organizację/organizacje, w ramach której/których Pani/Pan zajmuje się i/lub zajmowała/zajmował problematyką wskazaną w odpowiedziach na pytania nr 1 i 3 (nazwa instytucji, komórki organizacyjnej):
6.
Proszę wskazać zajmowane stanowisko, główne zadania, które wykonuje i/lub wykonywała/wykonywał Pani/Pan w organizacji/organizacjach wymienionych w odpowiedzi na pytanie nr 5 (chodzi tylko o te zadania, które bezpośrednio odnoszą się do obszarów wymienionych w odpowiedziach na pytania nr 1 i 3):
7.
Proszę dokończyć następujące zdanie: *System bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3] *w Rzeczypospolitej Polskiej tworzą obecnie …* *Proszę o udzielenie rozbudowanej odpowiedzi*

8.
Proszę dokończyć następujące zdanie: *Działania w zakresie zapewnienia bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3] *w Rzeczypospolitej Polskiej obejmują …* *Proszę o udzielenie rozbudowanej odpowiedzi*
9.
Proszę dokończyć następujące zdanie: *Działania w zakresie zapewnienia bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3], *system zapobiegania zjawiskom zagrażającym bezpieczeństwu w Rzeczypospolitej Polskiej należałoby uzupełnić o …* *Proszę o udzielenie rozbudowanej odpowiedzi*
10.
Zakładając, że bezpieczeństwo jest produktem podmiotów odpowiedzialnych za bezpieczeństwo, podmiotów które muszą być przygotowane i zdolne (chodzi tu o zdolność rozumianą jako siły, środki dostępne w zasięgu społeczeństwa, organizacji, mogących zredukować poziom ryzyka zagrożenia/zagrożeń) do działania w sposób ciągły, proszę określić i ocenić stopień gotowości, zdolności podmiotów odpowiedzialnych za dziedzinę bezpieczeństwa określoną przez Panią/Pana w odpowiedziach na pytania nr 1 i 3: *Proszę o udzielenie rozbudowanej odpowiedzi*
11.
Proszę dokończyć następujące zdanie: *W systemie bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3] *w Rzeczypospolitej Polskiej warto zastanowić się nad wprowadzeniem zmiany/zmian w …* *Proszę o udzielenie rozbudowanej odpowiedzi*

12.
Proszę wymienić w punktach i krótko scharakteryzować elementy, które według Pani/Pana oddziałują na obiektywny, faktyczny stan bezpieczeństwa, w obszarze dziedzin wskazanych w odpowiedziach na pytania nr 1 i 3:
13.
Proszę wskazać i opisać zależności między elementami, które zostały wymienione w odpowiedzi na pytanie nr 12: *Proszę o udzielenie rozbudowanej odpowiedzi*
14.
Proszę opisać znane Pani/Panu metody umożliwiające ocenę stanu bezpieczeństwa w odniesieniu do elementów wymienionych w odpowiedzi na pytanie nr 12, i/lub proszę przedstawić propozycje takich metod: *Proszę o udzielenie rozbudowanej odpowiedzi*
15.
Proszę opisać znane Pani/Panu skale umożliwiające ocenę ryzyka w odniesieniu do elementów wymienionych w odpowiedzi na pytanie nr 12, i/lub proszę przedstawić propozycje takich skal: *Proszę o udzielenie rozbudowanej odpowiedzi*
16.
Proszę wskazać przyjęte i/lub spróbować określić możliwe Pani/Pana zdaniem punkty graniczne, punkty krańcowe stanu stabilności państwa na opisanych/zaproponowanych w odpowiedzi na pytanie nr 15 – skalach, po przekroczeniu których wystąpi stan niestabilności": *Proszę o udzielenie rozbudowanej odpowiedzi*

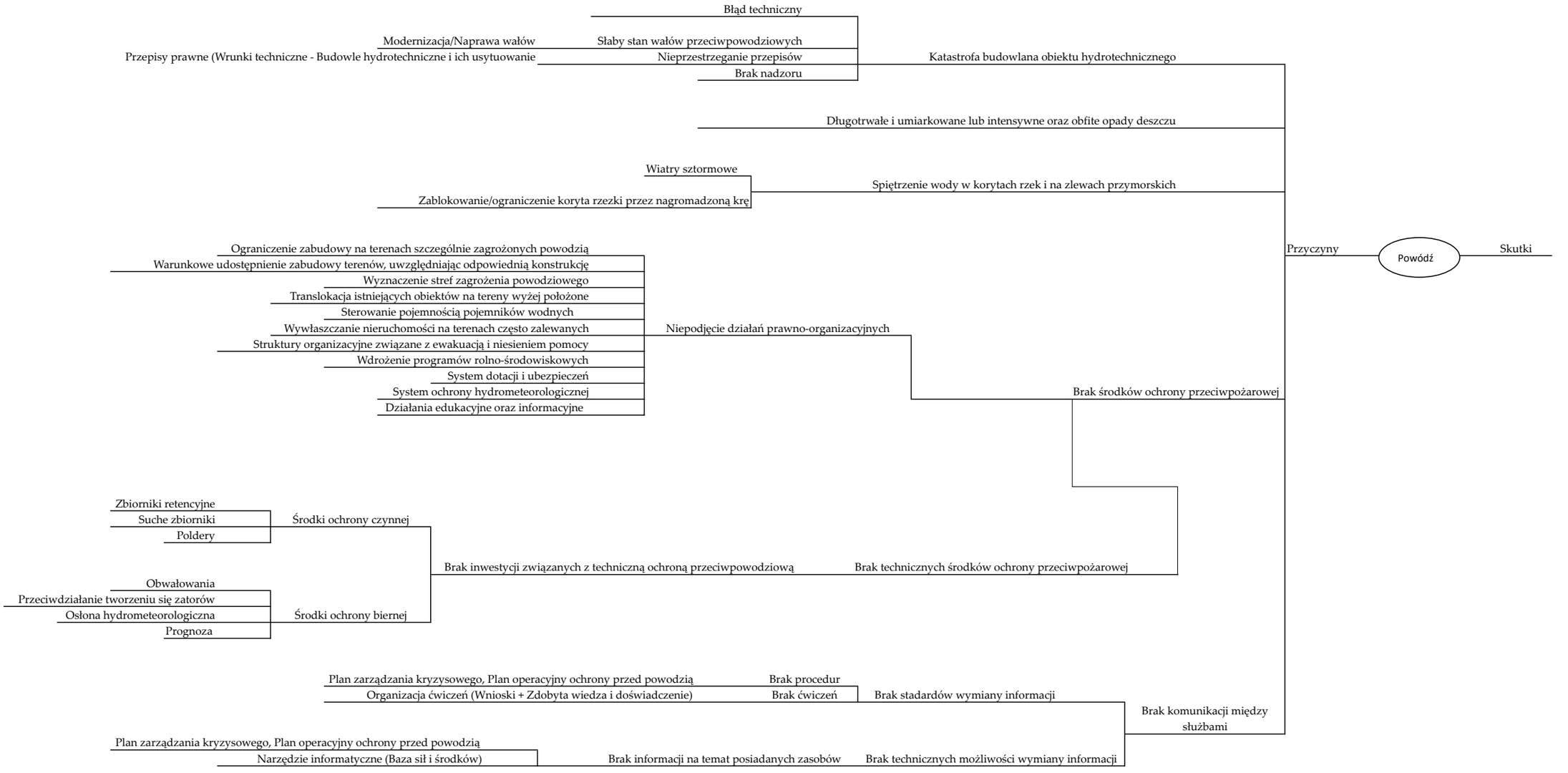
17.
Proszę określić kryteria, czynniki, które pozwoliły dokonać wyboru punktów granicznych wskazanych w odpowiedzi na pytanie nr 16: *Proszę o udzielenie rozbudowanej odpowiedzi*
18.
Proszę dokończyć następujące zdanie: *Stan braku bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3], *czyli sytuacji, w której występuje duże rzeczywiste zagrożenie, a postrzeganie tego zagrożenia jest prawidłowe, występuje wtedy gdy* [proszę scharakteryzować taki potencjalny stan braku bezpieczeństwa]: *Proszę o udzielenie rozbudowanej odpowiedzi*
19.
Proszę dokończyć następujące zdanie: *Stan fałszywego bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3], *czyli sytuacji, w której zagrożenie jest poważne, a postrzegane jest jako niewielkie, występuje wtedy gdy* [proszę scharakteryzować taki potencjalny stan fałszywego bezpieczeństwa]: *Proszę o udzielenie rozbudowanej odpowiedzi*
20.
Proszę dokończyć następujące zdanie: *Na poczucie braku bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3], *jego subiektywny, indywidualny odbiór, swoiste poczucie braku pewności wpływa/wpływają:* *Proszę o udzielenie rozbudowanej odpowiedzi*

21.
Proszę dokończyć następujące zdanie: *Rozbieżności między bezpieczeństwem realnym w obszarze bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3]*a poczuciem, indywidualnym odbiorem bezpieczeństwa* [proszę uzupełnić zgodnie z odpowiedzią na pytania nr 1 i 3] *wynikają z …* *Proszę o udzielenie rozbudowanej odpowiedzi*
22.
Czy i w jakim zakresie wyeliminowanie wymienionych w odpowiedzi na pytanie nr 20 czynników kształtujących subiektywne poczucie braku bezpieczeństwa spowoduje w Pani/Pana ocenie jego zmianę na poczucie pewności uwarunkowane obiektywnie? *Proszę o szczegółowe uzasadnienie wybranej odpowiedzi*
23.
Proszę wymienić w punktach i scharakteryzować wewnętrzne (wewnątrzpaństwowe) zagrożenia dla dziedziny bezpieczeństwa określonej przez Panią/Pana w odpowiedziach na pytania nr 1 i 3:
24.
Proszę wymienić w punktach i scharakteryzować zewnętrzne (ulokowane na zewnątrz państwa) zagrożenia dla dziedziny bezpieczeństwa określonej przez Panią/Pana w odpowiedziach na pytania nr 1 i 3:
25.
Proszę wymienić w punktach i scharakteryzować indywidualne (w odniesieniu do jednostki) zagrożenia dla dziedziny bezpieczeństwa określonej przez Panią/Pana w odpowiedziach na pytania nr 1 i 3:

26.
Proszę wymienić w punktach i scharakteryzować grupowe (w odniesieniu do społeczności) zagrożenia dla dziedziny bezpieczeństwa określonej przez Panią/Pana w odpowiedziach na pytania nr 1 i 3:
27.
Proszę wymienić w punktach i scharakteryzować zdarzenia niepożądane/sytuacje kryzysowe dla dziedziny bezpieczeństwa określonej przez Panią/Pana w odpowiedziach na pytania nr 1 i 3:
28.
Proszę wymienić w punktach i scharakteryzować zagrożenia (potencjalne) dla dziedziny bezpieczeństwa określonej przez Panią/Pana w odpowiedziach na pytania nr 1 i 3:
29.
Spośród zagrożeń wymienionych w odpowiedziach na pytania nr 23–28 proszę wskazać 3–5 zagrożeń, które w Pani/Pana ocenie charakteryzują się największym prawdopodobieństwem wystąpienia (zagrożenia te proszę uszeregować, rozpoczynając od najbardziej w Pani/Pana ocenie prawdopodobnego):
30.
Proszę dla każdego z zagrożeń wymienionych w odpowiedzi na pytanie nr 29 opisać sposób szacowania prawdopodobieństwa ich wystąpienia: *Proszę o udzielenie rozbudowanej odpowiedzi*

31.
Proszę dla każdego z zagrożeń wymienionych w odpowiedzi na pytanie nr 29 opisać sposób szacowania skutków ich wystąpienia: *Proszę o udzielenie rozbudowanej odpowiedzi*
32.
Biorąc pod uwagę dotychczasowe odpowiedzi, proszę stworzyć hierarchicznie uporządkowaną listę zagrożeń (maksymalnie 10; zaczynając od najważniejszego) dla dziedziny bezpieczeństwa określonej przez Panią/Pana w odpowiedziach na pytania nr 1 i 3:

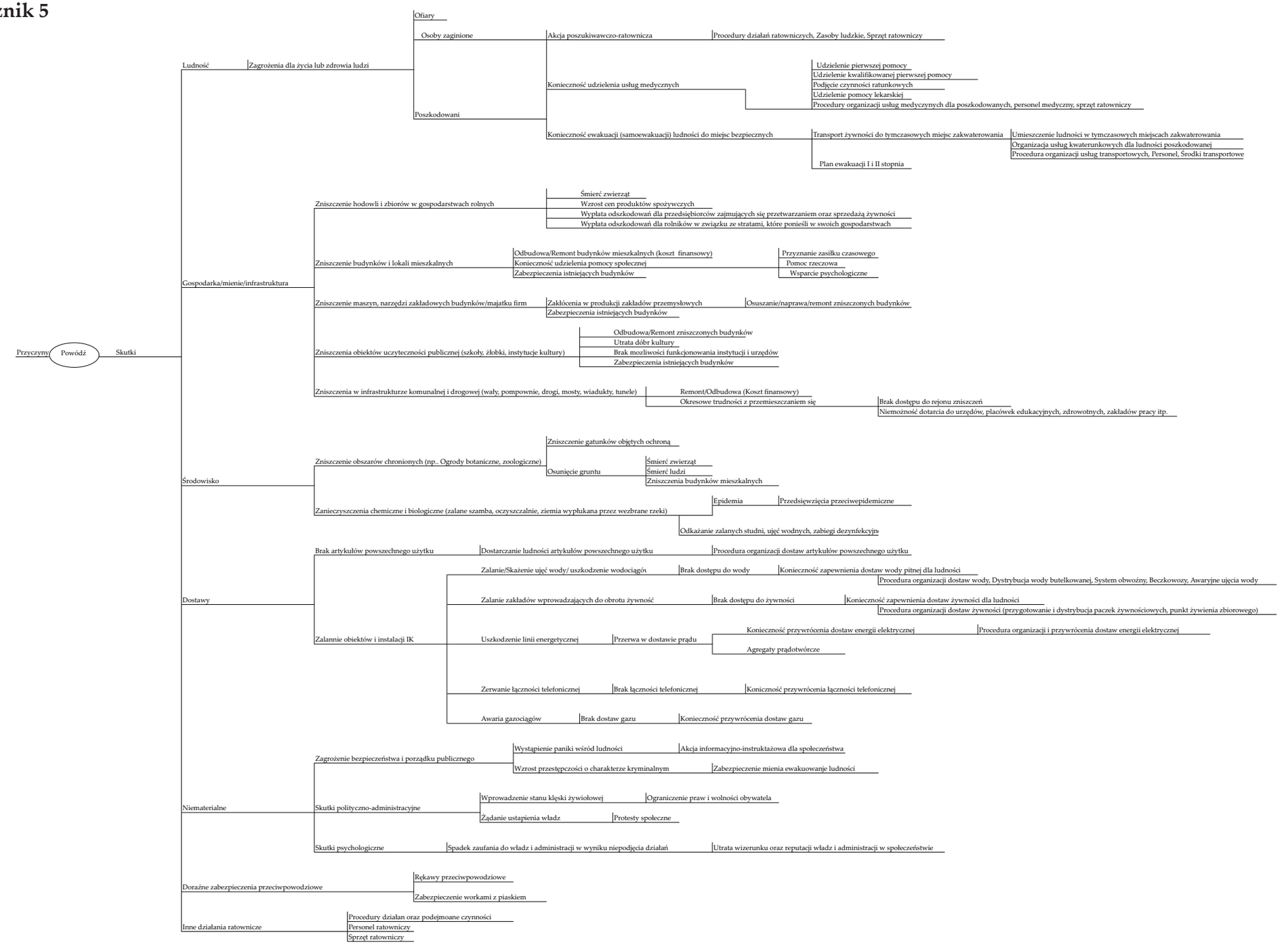
Załącznik 4



Model scenariusza możliwych zdarzeń związanych z wystąpieniem powodzi – przyczyny

Źródło: Opracowanie własne, na podstawie: Krajowy Plan Zarządzania Kryzysowego 2013; Doraźne metody ochrony stosowane podczas powodzi ze szczególnym uwzględnieniem rękawów przeciwpowodziowych (praca zbiorowa pod red. D. Riegert), monografia CNBOP-PIB 2012, Nowak E., Logistyka w sytuacjach kryzysowych, Akademia Obrony Narodowej, 2009.

Załącznik 5



Model scenariusza możliwych zdarzeń związanych z wystąpieniem powodzi – skutki

Źródło: Opracowanie własne, na podstawie: Krajowy Plan Zarządzania Kryzysowego 2013; Doraźne metody ochrony stosowane podczas powodzi ze szczególnym uwzględnieniem rękawów przeciwpowodziowych (praca zbiorowa pod red. D. Riegert), monografia CNBOP-PIB 2012; Nowak E., Logistyka w sytuacjach kryzysowych, Akademia Obrony Narodowej, 2009.

Czy udało się nam w książce wyczerpać tematykę odwołującą się do ryzyka oraz zarządzania nim? Z pewnością nie. Monografia stanowi jedynie wstęp do dalszych badań, dyskusji oraz wniosków. W zmieniającym się otoczeniu ciągła weryfikacja poprawności systemu jest jednym z kluczowych wymiarów sukcesu.

Wszystkim czytelnikom, którzy dotarli z nami do ostatnich stron książki, dedykujemy słowa George'a Washingtona:

Zrób, co możesz, tam gdzie jesteś, z tym co masz i nigdy nie bądź zadowolony!

Z zakończenia

Merytorycznie publikacja wyczerpuje w zasadniczej mierze treści zakreślone jej tematem i może stanowić istotną wartość twórczą w procesie dydaktycznym wyższych uczelni w Polsce oraz być pomocna przy usprawnianiu funkcjonowania administracji regionalnej i lokalnej.

Praca ma wszelkie podstawy, aby stać się przedmiotem zainteresowania instytucji zajmujących się obecnie kreowaniem i zarządzaniem bezpieczeństwem państwa, a także kształceniem kadr w zakresie zarządzania kryzysowego.

Spełnia także wymogi do tego, aby stała się wydawnictwem powszechnie dostępnym dla szerokich kręgów tej części społeczeństwa, która interesuje się sprawami zarządzania kryzysowego w Polsce. Tym samym spełnia ona wymogi, aby mogła być opublikowana, a wiedza w niej zawarta – powszechnie dostępna.

Z recenzji prof. dr. hab. Ryszarda Jakubczaka

Problematyka zarządzania ryzykiem nie jest nowa. Niemal od zawsze ludzie, szczególnie doświadczeni przez życie, zastanawiali się, jak skutecznie zrealizować swoje zamiary. Rozważali przy tym różne scenariusze sprzyjające i niesprzyjające realizacji wyznaczonych celów. Przy budowie strategii i planu działania uwzględniali wcześniejsze przemyślenia tak, aby jak najbardziej redukować negatywny wpływ zidentyfikowanych zagrożeń. Jednakże w przeszłości nie dysponowali odpowiednim aparatem matematycznym i możliwościami obliczeniowymi, aby miarę zagrożeń określić w sposób wystarczająco obiektywny i przekonywający. Nie sposób wyobrazić sobie jakiejkolwiek formy kierowania bez analizy ryzyka. Jednakże w przeszłości oparta ona była na intuicji i doświadczeniu podejmujących decyzje. Była zatem rodzajem sztuki.

W czasach obecnych dysponujemy ogromną ilością informacji zapisanych w wirtualnym świecie. Dysponujemy również aparaturą (komputery) i narzędziami (programy komputerowe, teorie matematyczne) do analizy tych informacji. Powoduje to, że w ocenie sytuacji możemy posługiwać się bardzo obiektywnymi danymi (dostarczonymi przez wielu niezależnych obserwatorów). To wszystko skłania do wykorzystania bogatego aparatu matematycznego przy podejmowaniu decyzji.

Z recenzji dr. hab. inż. Jarosława Prońko

ISBN 978-83-61520-30-6

DOI: 10.17381/2015.3

Wydawnictwo CNBOP-PIB
www.cnbop.pl

Publikacja finansowana ze środków NCBR w ramach projektu nr DOBR/0077/R/ID3/2013/3 pn. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP"