



REDAKCJA NAUKOWA
bryg. dr hab. inż. Dariusz Wróblewski

ZARZĄDZANIE RYZYKIEM

po co?

jak?

PRZEGLĄD WYBRANYCH METODYK

wydanie rozszerzone



REDAKCJA NAUKOWA
bryg. dr hab. inż. Dariusz Wróblewski

ZARZĄDZANIE & RYZYKIEM

po co?

jak?

PRZEGLĄD WYBRANYCH METODYK

wydanie rozszerzone

Redakcja opracowania:
bryg. dr hab. inż. Dariusz Wróblewski

Zespół autorski w składzie:

Grzegorz Abgarowicz
Inga Abgarowicz
Anna Banulska
Jan Gołębiowski
Piotr Guzewski
Maria Kędzierska
Daniel Małozieć
Maciej Napiórkowski
Bartłomiej Połeć
Witold Skomra
Ewa Sobór
Tomasz Sowa
Paweł Stępień
Małgorzata Trzczińska (cz. III)

Aktualizacja wydania:

Maria Kędzierska
Bartłomiej Połeć
Małgorzata Trzczińska (cz. III)
Dariusz Wróblewski

Recenzja:

st. bryg. dr inż. Paweł Janik
nadbryg. dr hab. inż. Paweł Kępka, prof. SGSP
st. bryg. w st. spocz. dr hab. inż. Bogdan Kosowski, prof. UJ
st. bryg. w st. spocz. mgr inż. Dariusz Marczyński

Przygotowanie do wydania:

Anna Golińska
Elżbieta Muszyńska

Projekt okładki:

Julia Pinkiewicz

Grafika na okładce: Freepik.com

ISBN: 978-83-948534-0-2

DOI: 10.17381/2018.1

Skład i wydruk został sfinansowany przez KG PSP

Publikacja powstała w oparciu o wyniki projektu
pt. „Zintegrowany system budowy planów zarządzania kryzysowego
w oparciu o nowoczesne technologie informatyczne” finansowanego przez NCBR

© Copyright by Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego Państwowy Instytut Badawczy, Józefów 2018

Wydawca:

Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego
Państwowy Instytut Badawczy
05-420 Józefów k/Otwocka ul. Nadwiślańska 213
www.cnbop.pl

Przygotowanie do druku: BEL Studio Sp. z o.o.

Druk: Print Group Sp. z o.o.

SPIS TREŚCI

WPROWADZENIE	9
WYKORZYSTANE SPRAWOZDANIA Z BADAŃ	15
SPIS OZNACZEŃ	17

CZĘŚĆ I

PRZEGLĄD WYBRANYCH PRZEPISÓW KRAJOWYCH, ZAGRANICZNYCH ORAZ NORM I STANDARDÓW DOTYCZĄCYCH ZARZĄDZANIA RYZYKIEM

WPROWADZENIE	21
1. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – USTAWY	23
1.1. Ustawa o zarządzaniu kryzysowym	23
1.2. Ustawa – Prawo wodne (akt obowiązujący do 31.12.2017)	24
1.2.1. Ustawa – Prawo wodne (akt obowiązujący od 1.01.2018)	26
1.3. Ustawa o ochronie żeglugi i portów morskich	34
1.4. Ustawa – Prawo ochrony środowiska	36
1.5. Ustawa o Państwowej Inspekcji Sanitarnej	40
1.6. Ustawa o finansach publicznych	41
2. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – ROZPORZĄDZENIA	43
2.1. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej	43
2.2. Rozporządzenie Rady Ministrów w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej	44
2.3. Rozporządzenie Rady Ministrów w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego	44
2.4. Rozporządzenie Ministra Środowiska, Ministra Transportu, Budownictwa i Gospodarki Morskiej, Ministra Administracji i Cyfryzacji oraz Ministra Spraw Wewnętrznych w sprawie opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego	45
3. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – PRZEPISY RESORTOWE	47
3.1. Zarządzenie Ministra Spraw Zagranicznych w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych	48
3.2. Zarządzenie Ministra Administracji i Cyfryzacji w sprawie powołania Zespołu do spraw zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji	49
3.3. Zarządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie systemu kontroli zarządczej w działach administracji rządowej	

– administracja publiczna, sprawy wewnętrzne, wyznania religijne oraz mniejszości narodowe i etniczne	50
3.4. Zarządzenie Ministra Cyfryzacji w sprawie systemu kontroli zarządczej w dziale administracji rządowej - informatyzacja- administracja publiczna, sprawy wewnętrzne, wyznania religijne oraz mniejszości narodowe i etniczne	51
3.5. Zarządzenie Ministra Infrastruktury i Budownictwa w sprawie ustalenia opisu systemu kontroli zarządczej w Ministerstwie Infrastruktury i Budownictwa	52
3.6. Komunikat w sprawie szczegółowych wytycznych w zakresie kontroli zarządczej dla Ministerstwa Infrastruktury i Budownictwa oraz działów administracji rządowej - budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, łączność, transport	54
3.7. Zarządzenie Ministra Rozwoju i Finansów w sprawie kontroli zarządczej w Ministerstwie Rozwoju	55
3.8. Zarządzenie Ministra Rozwoju i Finansów w sprawie systemu kontroli zarządczej w Ministerstwie Finansów	57
3.9. Rozporządzenie Ministra Rozwoju i Finansów w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach	58
3.10. Rozporządzenie Ministra Rozwoju i Finansów w sprawie kapitału wewnętrznego, systemu zarządzania ryzykiem, programu oceny nadzorczej oraz badania i oceny nadzorczej, a także polityki wynagrodzeń w domu maklerskim	60
3.11. Zarządzenie Prezesa Wyższego Urzędu Górniczego w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych	61
4. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – PRAWO MIEJSCOWE NA PRZYKŁADZIE WOJEWÓDZTWA MAZOWIECKIEGO	63
4.1. Zarządzenie Wojewody Mazowieckiego w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie	64
4.2. Zarządzenie Prezydenta Miasta Stołecznego Warszawy w sprawie systemu zarządzania ryzykiem w m.st. Warszawie	66
4.3. Zarządzenie Burmistrza Karczewa w sprawie wprowadzenia instrukcji dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej	69
4.4. Zarządzenie Burmistrza Karczewa w sprawie wprowadzenia polityki zarządzania ryzykiem	70
5. PRZEGLĄD WYBRANYCH NORM I STANDARDÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM	73
5.1. ISO/IEC 31010:2009 Risk management – Risk assessment techniques	74
5.2. ISO GUIDE 73:2009 Risk management – Vocabulary	74
5.3. ISO 31000:2009 Zarządzanie ryzykiem – Zasady i wytyczne	75
5.4. BSI-Standard 100-4 Business Continuity Management	75
5.5. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security	77
5.6. PKN-CEN/CWA 15537 Network Enabled Abilities – Service-Oriented Architecture for civilian and military crisis management	80

5.7. CAN/CSA-Q850-97:2009 Risk Management: Guideline for Decision-Makers	81
6. PRZEGLĄD WYBRANYCH PROJEKTÓW NORM Z ZAKRESU ZARZĄDZANIA RYZYKIEM . . .	83
6.1. N 96 ISO 18482 Security Management System – Guidance for use-Security risk assessment	83
6.2. ISO/CD 16125 Security management system	84
PODSUMOWANIE I WNIOSKI	89
LITERATURA	97

CZĘŚĆ II

ZAGADNIENIA OGÓLNE Z ZAKRESU ZARZĄDZANIA RYZYKIEM

WPROWADZENIE	103
1. ZARZĄDZANIE RYZYKIEM WEDŁUG NORMY ISO 31000	105
1.1. Norma ISO 31000:2009 – zakres i przeznaczenie	106
1.2. Zasady zarządzania ryzykiem	108
1.3. Struktura ramowa zarządzania ryzykiem	110
1.4. Proces zarządzania ryzykiem	114
1.4.1. Komunikacja i konsultacje	117
1.4.2. Ustalenie kontekstu	117
1.4.3. Ocena ryzyka	118
1.4.4. Postępowanie z ryzykiem	121
1.4.5. Monitorowanie i przegląd	123
1.5. Dokumentowanie zarządzania ryzykiem	124
2. METODY WYKORZYSTYWANE W OCENIE RYZYKA	127
2.1. Metoda, metodyka, metodologia	128
2.2. Analiza przyczyn i konsekwencji (<i>cause and consequence analysis</i>)	134
2.3. Analiza przyczynowo – skutkowa (<i>cause and effect analysis</i>)	136
2.4. Analiza warstw ochrony – LOPA (<i>layer protection analysis</i>)	138
2.5. Analiza drzewa decyzji (<i>decision tree analysis</i>)	140
2.6. Analiza drzewa błędów (<i>fault tree analysis</i>)	142
2.7. Analiza drzewa zdarzeń (<i>event tree analysis</i>)	143
2.8. Ocena niezawodności człowieka (<i>human reliability analysis</i>)	144
2.9. Analiza muchy (<i>bow tie analysis</i>)	146
2.10. Metoda konserwacji ukierunkowana na niezawodność – RCM (<i>reliability centred maintenance</i>)	148
2.11. Zapowiedź analizy – SA (<i>sneak analysis</i>) i zapowiedź analizy obwodu – SCA (<i>sneak circuit analysis</i>)	150
2.12. Metoda SWIFT – co jeśli? (<i>structured „what if?” technique</i>)	151
2.13. Analiza scenariuszowa (<i>scenario analysis</i>)	151
2.14. Analiza wpływu na działalność – BIA (<i>business impact analysis</i>)	153
2.15. Matryca skutek/prawdopodobieństwo (<i>consequence/probability matrix</i>) . .	154
PODSUMOWANIE I WNIOSKI	159
LITERATURA	162

CZĘŚĆ III ZARZĄDZANIE RYZYKIEM NA SZCZEBLU UNII EUROPEJSKIEJ

WPROWADZENIE	167
1. ZARZĄDZANIE RYZYKIEM W UNII EUROPEJSKIEJ	171
2. POJĘCIE ZARZĄDZANIA RYZYKIEM W UNII EUROPEJSKIEJ	173
3. ANALIZA PRZEPISÓW UNIJNYCH ZWIĄZANYCH Z ZARZĄDZANIEM RYZYKIEM	177
3.1. Rozporządzenia	177
3.2. Dyrektywy	177
3.3. Decyzje	178
4. ROLA INSTYTUCJI UNIJNYCH W ZAKRESIE ZARZĄDZANIA RYZYKIEM	179
5. ZARZĄDZANIE RYZYKIEM W OBSZARZE BEZPIECZEŃSTWA WEWNĘTRZNEGO UNII EUROPEJSKIEJ	183
5.1. Zarządzanie ryzykiem powodziowym	186
5.1.1. Wstępna ocena ryzyka powodziowego	189
5.1.2. Mapy zagrożenia powodziowego i mapy ryzyka	191
5.1.3. Plany zarządzania ryzykiem powodziowym	192
5.2. Kontrola zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi – SEVESO III	193
5.3. Zarządzanie ryzykiem związanym z elektrowniami jądrowymi – testy wytrzymałościowe	196
5.4. Zarządzanie ryzykiem w dziedzinie zdrowia Unii Europejskiej	200
5.5. Zarządzanie ryzykiem na wypadek kryzysów związanych z żywnością	206
5.6. Zarządzanie ryzykiem nielegalnej imigracji – FRONTEx	208
5.7. Mechanizm Ochrony Ludności	212
6. ZARZĄDZANIE RYZYKIEM W OBSZARZE BEZPIECZEŃSTWA ZEWNĘTRZNEGO UNII EUROPEJSKIEJ	215
7. PRZYKŁADOWE PROJEKTY BADAWCZE Z ZAKRESU OCENY RYZYKA	219
7.1. KULTURisk	219
7.2. MATRIX	220
7.3. Catalyst	222
PODSUMOWANIE I WNIOSKI	223
LITERATURA	230

CZĘŚĆ IV ZARZĄDZANIE RYZYKIEM W WYBRANYCH PAŃSTWACH

WPROWADZENIE	235
1. Zarządzanie ryzykiem w Australii	237
1.1. Narodowe ramy oceny ryzyka	238
1.2. Opis procesu zarządzania ryzykiem	245
2. ZARZĄDZANIE RYZYKIEM W IRLANDII	257
2.1. Ramy zarządzania poważnymi sytuacjami kryzysowymi	257
2.2. Narodowa ocena ryzyka Irlandii	260
3. ZARZĄDZANIE RYZYKIEM W REPUBLICE FEDERALNEJ NIEMIEC	269
3.1. Metoda analizy ryzyka dla ochrony ludności	269

4. ZARZĄDZANIE RYZYKIEM W SZWECJI	279
4.1. Przewodnik po analizie ryzyka i podatności	279
4.2. Szwedzka narodowa ocena ryzyka 2012	292
5. ZARZĄDZANIE RYZYKIEM W WIELKIEJ BRYTANII	303
5.1. Krajowy rejestr ryzyka	303
5.2. Standard zarządzania ryzykiem FERMA	308
PODSUMOWANIE I WNIOSKI	318
LITERATURA	326

CZĘŚĆ V ZARZĄDZANIE RYZYKIEM W POLSCE

WPROWADZENIE	331
1. ZARZĄDZANIE RYZYKIEM W PLANOWANIU CYWILNYM	333
1.1. Plany zarządzania kryzysowego	335
1.2. Raport o zagrożeniach bezpieczeństwa narodowego	337
1.3. Ochrona infrastruktury krytycznej	342
2. METODA WDROŻENIA ZARZĄDZANIA RYZYKIEM W PROCES PLANOWANIA CYWILNEGO	345
2.1. Metoda wykorzystania norm ISO w zakresie zarządzania ryzykiem w planowaniu cywilnym	346
2.2. Szczegółowy opis procesu z uwzględnieniem istniejących ograniczeń formalno-prawnych	349
3. ZARZĄDZANIE RYZYKIEM POWODZIOWYM	365
3.1. Implementacja dyrektywy do polskiego systemu prawnego	365
3.2. Proces wdrażania polityki zarządzania ryzykiem	368
3.3. Plany zarządzania ryzykiem powodziowym	375
4. ZARZĄDZANIE RYZYKIEM W KONTROLI ZARZĄDCZEJ	379
4.1. Zarządzanie ryzykiem na szczeblu centralnym	380
4.2. Zarządzanie ryzykiem w województwie, powiecie i gminie	392
5. METODYKA DIAGNOZOWANIA SYSTEMÓW REAGOWANIA POMRISC – ELEMENTY ZARZĄDZANIA RYZYKIEM	403
5.1. Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego (RZSR WP)	404
5.2. Metody badawcze wykorzystane na potrzeby analizy oceny ryzyka – PomRisc	405
5.2.1. Zarys systemu bezpieczeństwa w województwie pomorskim	407
5.2.2. Diagnoza stanu bezpieczeństwa w województwie pomorskim	409
5.3. Identyfikacja i ocena wielkości ryzyka	411
5.4. Diagnoza systemu reagowania jako komponentu zarządzania ryzykiem . .	421
5.4.1. Diagnoza kluczowych elementów systemu RZSR WP	423
5.4.2. Analiza systemu	426
5.4.3. Docelowa (całościowa) wizja RZSR WP na podstawie dotychczasowych wniosków	428
6. NARZĘDZIA TELEINFORMATYCZNE WSPOMAGAJĄCE OCENĘ RYZYKA NA PRZYKŁADZIE OPROGRAMOWANIA RYSKO	433
6.1. Oprogramowanie RYSKO	433

6.2. Katalog zagrożeń – moduł oceny ryzyka „skrojony na miarę”	435
7. MOŻLIWOŚCI WYKORZYSTANIA BADAŃ PRZYCZYN POŻARÓW W ZARZĄDZANIU RYZYKIEM POŻAROWYM W POLSCE	441
7.1. Społeczno-ekonomiczne koszty pożarów jako bodziec rozwoju zarządzania ryzykiem pożarowym	443
7.2. Zarządzanie ryzykiem pożarowym w aspekcie teoretycznym i praktycznym	447
PODSUMOWANIE I WNIOSKI	452
LITERATURA	462

CZĘŚĆ VI

SŁOWNIK WYBRANYCH POJĘĆ Z ZAKRESU ZARZĄDZANIA RYZYKIEM

WPROWADZENIE	467
------------------------	-----

Szanowni Czytelnicy,

Od momentu ukazania się *Zarządzania ryzykiem. Przegląd wybranych metodyk* minęły już ponad dwa lata, w trakcie których obserwowaliśmy zmiany w systemie prawnym RP, który spowodował wzrost zainteresowania tą tematyką. Istotne znaczenie miała tutaj aktualizacja normy PN-EN ISO 9001 z wersji 2009 na 2015, w której położono znaczący nacisk na wdrożenie do systemów zarządzania jakością podejścia opartego na ryzyku. W punkcie 5.1.1 normy jednoznacznie nałożono ten obowiązek na najwyższe kierownictwo organizacji, które: „powinno wykazywać przywództwo i zaangażowanie [...] poprzez: [...] promowanie podejścia procesowego oraz opartego na ryzyku przez najwyższe kierownictwo”. Zobowiązanie najwyższego kierownictwa organizacji oznacza, że wszystkie organizacje posiadające certyfikat ISO i ubiegające się o uzyskanie takiego certyfikatu na zgodność z normą 9001:2015 będą zobowiązane do wdrożenia takiego podejścia. Warto w tym miejscu zauważyć, że przywołana norma nie podaje formalnych metod ani sposobów dokumentowania procesów zarządzania ryzykiem. Nie podaje również szczegółowych zaleceń, w jaki sposób ma być realizowane podejście oparte na ryzyku, pozostawiając te kwestie najwyższemu kierownictwu. W związku z powyższym należy przyjąć, że rekomendowanymi dokumentami wspomagającymi ten proces powinny być następujące normy i wytyczne:

1. PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*,
2. ISO Guide 73:2009 *Risk Management – Vocabulary*,
3. SO/IEC 31010:2009 *Risk Management – Risk Assessment Techniques*.

Wymienione dokumenty normalizacyjne zostały szczegółowo opisane w części II niniejszej publikacji.

Zgodnie ze statystykami prezentowanymi przez Międzynarodową Organizację Normalizacyjną¹ w Polsce w grudniu 2016 roku było 12152 organizacje posiadających certyfikat ISO 9001. Oznacza to, że jeżeli te organizacje zdecydują się utrzymać certyfikat, to w kolejnych latach będą one zobowiązane do promowania podejścia opartego na ryzyku.

Wyżej opisane okoliczności potwierdzają, że zagadnienia związane z zarządzaniem ryzykiem są obecnie aktualne i stają się coraz bardziej powszechne zarówno w organizacjach finansów publicznych (za sprawą m.in. kontroli zarządczej), jak i organizacjach biznesowych (m.in. za sprawą PN-EN ISO 9001:2015, jeżeli te organizacje zechcą utrzymać lub ubiegać się o uzyskanie certyfikatu na zgodność

¹ ISO 9001 – data per country and sector – 1993 to 2016; <http://isotc.iso.org/livelink/livelink?file=11&objId=18808772&objAction=browse&viewType=1>, [dostęp: listopad 2017].

z tą normą) oraz organizacjach, które zobowiązane są do tego przepisami prawa krajowego i UE. Najprawdopodobniej są to również przyczyny wysokiego zainteresowania czytelników problematyką zarządzania ryzykiem, które miało niebagatelny wpływ na decyzję o wznowieniu publikacji.

Duże zainteresowanie problematyką zarządzania ryzykiem najprawdopodobniej związane jest także z wdrażaniem w Polsce regulacji dotyczących ochrony danych osobowych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady UE oraz dyrektywą Parlamentu Europejskiego i Rady UE z 27.04.2016 roku². Wymienione przepisy wprowadzają m.in. podejście oparte na ryzyku (ang. *risk based approach*), zgodnie z którym administrator danych osobowych będzie zobowiązany do prowadzenia oceny ryzyka oraz dobierania odpowiednich środków technicznych i nietechnicznych sprowadzających to ryzyko do poziomu akceptowalnego³. W tym miejscu warto wspomnieć o bardzo dotkliwych karach finansowych, sięgających nawet 20 mln euro, za nieprawidłowe przechowywanie oraz przetwarzanie ww. danych⁴.

W ciągu przeszło dwóch lat od momentu ukazania się pierwszego wydania *Zarządzania ryzykiem* obserwowaliśmy wzmożone zainteresowanie czytelników i wzrost oglądalności całej serii o zarządzaniu⁵ na platformie Google Books

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 04.05.2016, s. 1); dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WsiSW (Dz. Urz. UE L 119 z 04.05.2016, s. 89).

³ *Czy jesteś gotowy na RODO?*, Broszura informacyjna, Generalny Inspektor Ochrony Danych Osobowych, s. 5, 6, 14, 15, 17, 20, 21, 25, 31 [dok. elektr.] <http://www.giodo.gov.pl/pl/file/12866> [dostęp: luty 2018].

⁴ Tamże, s. 3 [dostęp: luty 2018].

⁵ D. Wróblewski (red.), *Zarządzanie ryzykiem. Przegląd wybranych metodyk*, CNBOP-PIB, Józefów 2015; D. Wróblewski (red.), *Wybrane zagadnienia z zakresu planowania cywilnego w systemie zarządzania kryzysowego RP*, CNBOP-PIB, Józefów 2014; D. Wróblewski (red.), *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, CNBOP-PIB, Józefów 2015; D. Wróblewski (red.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014; D. Wróblewski (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego. Analiza wybranych przepisów*, CNBOP-PIB, Józefów 2014; G. Abgarowicz (red.), *Pamięć przyszłości. Analiza ryzyka dla zarządzania kryzysowego*, CNBOP-PIB, Józefów 2015; D. Wróblewski (red.), *Rekomendacje formalno-prawne z zakresu zarządzania kryzysowego*, CNBOP-PIB, Józefów 2015; D. Wróblewski (red.), *Koncepcja Funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, CNBOP, Józefów 2008; D. Wróblewski (red.), *Planowanie cywilne w systemie zarządzania kryzysowego*, Józefów 2013; D. Wróblewski, T. Sowa, *Zarządzanie ryzykiem. Zagadnienia ogólne. Materiały dydaktyczne ze szkolenia dla auditorów działających w strukturze Polskiego Centrum Akredytacji*, CNBOP-PIB, Józefów 2009.

w stosunku do pozostałych pozycji wydawniczych CNBOP-PIB. Od 2015 roku Instytut umieścił tam 55 publikacji (nie wliczając w to kwartalnika naukowego „BiTP. Bezpieczeństwo i Technika Pożarnicza”) w tzw. otwartym dostępie. Wśród nich seria wydawnicza dotycząca zarządzania ryzykiem i zarządzania kryzysowego była wyświetlana 36 223 razy, co stanowi 26% całkowitej liczby wyświetleń wydawnictw CNBOP-PIB. Warto zaznaczyć, że przywołane dane liczbowe nie uwzględniają odtwarzania publikacji przez aplikację Google Play, ponieważ firma Google nie udostępnia dla tej aplikacji statystyk.

Ponadto analiza powszechności słowa „ryzyko” w systemie prawnym obowiązującym w Polsce i UE potwierdziła, że decyzja o wznowieniu wydania jest jak najbardziej uzasadniona. Na podstawie danych z Systemu Informacji Prawnej LEX stwierdzono, że pojęcie „ryzyko” występuje w 4828 aktach prawnych⁶, co daje prawie dwukrotny wzrost w ciągu ośmiu lat względem 2009 roku, w którym pojawiało się ono w 2686 dokumentach prawodawczych. Biorąc pod uwagę wyłącznie okres od pierwszego wydania niniejszej monografii do chwili obecnej, liczba aktów prawnych uwzględniających to pojęcie zwiększyła się o 621, co daje prawie 30-procentowy wzrost w ciągu niecałych trzech lat.

W związku z powyższym uzasadnione wydało się przygotowanie kolejnego wydania monografii *Zarządzanie ryzykiem. Przegląd wybranych metodyk* – rozszerzonego o komplementarne tematycznie treści zaczerpnięte z trzech publikacji:

1. *Rekomendacje formalno-prawne z zakresu zarządzania kryzysowego* – wykorzystano angielsko-polski i polsko-angielski słownik pojęć oraz słownik rekomendowanych pojęć.
2. *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem* – wykorzystano Część III *Zarządzanie ryzykiem* oraz Część IV *Wybrane pojęcia z zakresu zarządzania kryzysowego i zarządzania ryzykiem*.
3. *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego* – wykorzystano Część III *Zarządzanie ryzykiem w Unii Europejskiej*.

Z uwagi na czas, jaki upłynął od pierwszego wydania trzech powyższych publikacji, autorzy dokonali aktualizacji pierwotnych treści oraz uzupełnili je o istotne dla tego obszaru tematycznego wątki, czego efektem jest niniejsza monografia. Powstała ona z myślą zarówno o osobach zainteresowanych zawodowo przedmiotową problematyką, jak i studentach kierunków związanych z zarządzaniem – szczególnie jeżeli chodzi o przyjęty przez autorów i rekomendowany słownik terminów związanych z zarządzaniem.

Wyżej wymienione wydawnictwa zawierają wyniki badań zespołu Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowego Instytutu Badawczego uzyskane podczas realizowanego w latach

⁶ Stan na dzień 12.11.2017 r.

2012–2015 projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”. Projekt ten finansowany był przez Narodowe Centrum Badań i Rozwoju. Wykonawcą było konsorcjum naukowo-przemysłowe w składzie:

- 1) Centrum Naukowo-Badawcze Ochrony Przeciwpowodowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy,
- 2) Akademia Obrony Narodowej – Wydział Bezpieczeństwa Narodowego⁷,
- 3) Szkoła Główna Służby Pożarniczej,
- 4) Związek Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej,
- 5) Asseco Poland SA.

Zespół autorski dokonał identyfikacji i analizy zasad obowiązujących w zarządzaniu ryzykiem, standardów i norm charakterystycznych dla tego typu zarządzania, metod zarządzania ryzykiem w procesie planowania cywilnego, metodyk oceny ryzyka i zagrożeń w przepisach prawa międzynarodowego i krajowego – z uwzględnieniem prawa miejscowego oraz metodyk ujętych w normach i projektach norm z zakresu zarządzania ryzykiem. Dokonano również przeglądu wybranych pozycji literatury przedmiotu. Głównym celem analizy tych zagadnień było dostarczenie specjalistom i organizacjom wdrażającym procesy zarządzania ryzykiem uniwersalnych modeli oraz wskazanie dobrych praktyk, szczególnie w zakresie planowania cywilnego w obszarze zarządzania ryzykiem.

Autorzy wyodrębnili najważniejsze dokumenty prawne i normatywne oraz terminologię z zakresu zarządzania ryzykiem – przy zastosowaniu kryterium użyteczności dla projektu. Sprawne porozumiewanie się, czy to w sferze naukowej, czy praktycznej, zależy od stosowania jednolitej i zrozumiałej dla wszystkich terminologii. Jest to o tyle trudne, że odmienne doświadczenia różnych państw, organizacji, sektorów działalności i branż, a także niedoskonałości w przekładzie z języków obcych i wymienne stosowanie terminów do nazywania tego samego zjawiska wpływają na różnicowanie znaczeń poszczególnych pojęć i definicji w ramach danego języka i między różnymi językami. Aby możliwie skutecznie zapobiec niejednoznaczności odbiorowi treści, autorzy jasno określili aparat terminologiczny, którym posługiwali się w publikacji i który – w formie słownika oraz indeksu pojęć – został umieszczony w monografii. Większość pojęć zaczerpnięto z uznanej normy ISO Guide 73:2009 *Risk Management – Vocabulary* i zgodnie z nią ujednolicono terminologię. Jeżeli norma nie wyczerpywała danej definicji, korzystano z innych uznanych źródeł, np. słowników.

Niniejsze opracowanie składa się z sześciu zasadniczych części:

- Część I *Przegląd wybranych przepisów krajowych, zagranicznych oraz norm i standardów dotyczących zarządzania ryzykiem,*

⁷ Od 1 października 2016 r. Akademia Sztuki Wojennej – Wydział Bezpieczeństwa Narodowego.

- Część II *Zagadnienia ogólne z zakresu zarządzania ryzykiem*,
- Część III *Zarządzanie ryzykiem na szczeblu UE*,
- Część IV *Zarządzanie ryzykiem w wybranych państwach*,
- Część V *Zarządzanie ryzykiem w RP*,
- Część VI *Słownik wybranych pojęć z zakresu zarządzania ryzykiem*.

W części I *Przegląd wybranych przepisów krajowych, zagranicznych oraz norm i standardów dotyczących zarządzania ryzykiem* autorzy dokonali przeglądu i krótkiej charakterystyki krajowych przepisów prawa (sześciu ustaw, trzech rozporządzeń, jedenastu przepisów resortowych oraz czterech przepisów prawa miejscowego), a także dziewięciu norm, standardów i projektów norm międzynarodowych.

W części II *Zagadnienia ogólne z zakresu zarządzania ryzykiem* autorzy przybliżają zarządzanie ryzykiem według normy ISO 31000, a także opisują wybrane metody, które mogą zostać wykorzystane w procesie oceny ryzyka, również w ramach planowania cywilnego.

W części III *Zarządzanie ryzykiem na szczeblu UE* znalazły się wyniki analizy metodyk oceny ryzyka dla poszczególnych rodzajów zagrożeń, odnoszących się do wybranych aktywności Unii Europejskiej. Przenalizowano pięć obszarów oraz trzy przykładowe projekty badawcze z zakresu oceny ryzyka.

W części IV *Zarządzanie ryzykiem w wybranych państwach* przedstawiono analizę metodyk oceny ryzyka stosowanych w Australii, Irlandii, Niemczech, Szwecji i Wielkiej Brytanii, a także sposoby identyfikacji zagrożeń i oceny ryzyka na szczeblu krajowym.

Część V *Zarządzanie ryzykiem w RP* zawiera opis metodyk i rozwiązań wykorzystujących elementy zarządzania ryzykiem w procesie planowania cywilnego, związanych m.in. z ryzykiem powodziowym i pożarowym, a także występujących w kontroli zarządczej. Opisana została również metodyka diagnozowania systemów reagowania PomRisc, a ponadto oprogramowanie RISKO jako przykład zastosowania praktycznego narzędzia teleinformatycznego do wspomagania procesu oceny ryzyka.

W Części VI *Słownik wybranych pojęć z zakresu zarządzania ryzykiem* autorzy prezentują słownik angielsko-polski i polsko-angielski obejmujący 51 podstawowych pojęć z zakresu zarządzania ryzykiem, a także słownik terminologiczny obejmujący 127 wybranych pojęć z tego zakresu.

Wszystkie osoby zainteresowane pogłębieniem wiedzy w tym zakresie zachęcam również do sięgnięcia do innych naszych publikacji w otwartym dostępie do nieodpłatnego pobrania w aplikacji Sklep Google Play na smartfony i tablety oraz w Repozytorium Centrum Otwartej Nauki (CEON).

Życząc zajmującej lektury, zapraszam również do odwiedzania naszych stron internetowych:

- <http://www.cnbop.pl>,
- <http://bitp.cnbop.pl>,
- <http://www.cnbop.pl/pl/wydawnictwa/ksiazki>,
- <http://www.cnbop.pl/pl/wydawnictwa/standardy>.

Znajdą tam Państwo inne interesujące materiały źródłowe z dziedziny zarządzania kryzysowego, ratownictwa, ochrony przeciwpożarowej, zarządzania ryzykiem i planowania.

bryg. dr hab. inż. Dariusz Wróblewski
Redaktor wydania, Dyrektor CNBOP-PIB

WYKORZYSTANE SPRAWOZDANIA Z BADAŃ

Na potrzeby niniejszej monografii wykorzystano 30 sprawozdań z badań:

- Abgarowicz G., *Czynniki ryzyka*.
- Abgarowicz G., *Normy ISO w procesie planowania cywilnego*.
- Abgarowicz G., *Wykorzystanie metod zarządzania ryzykiem w procesie planowania cywilnego*.
- Abgarowicz I., Smoła J., *Analiza metodyk oceny ryzyka i zagrożeń ujętych w przepisach krajowego prawa powszechnie obowiązującego z elementami zarządzania ryzykiem i związanego z zarządzaniem ryzykiem – diagnoza stanu*.
- Abgarowicz I., Smoła J., *Identyfikacja przepisów krajowego prawa powszechnie obowiązującego z elementami zarządzania ryzykiem i związanego z zarządzaniem ryzykiem*.
- Abgarowicz I., *Analiza przepisów krajowego prawa powszechnie obowiązującego z elementami zarządzania ryzykiem*.
- Abgarowicz I., *Sporządzenie wykazu pojęć z zakresu zarządzania ryzykiem z województwa zachodniopomorskiego*.
- Banulska A., *Analiza norm wykorzystujących elementy z zarządzania ryzykiem*.
- Banulska A., Sowa T., *Analiza metodyk oceny ryzyka i zagrożeń ujętych w normach z zakresu zarządzania ryzykiem – diagnoza stanu*.
- Gołębiewski J., *Analiza metodyk oceny ryzyka i zagrożeń ujętych i w przepisach międzynarodowych z wyłączeniem UE związanych z zarządzaniem ryzykiem – diagnoza stanu*.
- Gołębiewski J., *Analiza pojęć w zakresie zarządzania ryzykiem*.
- Gołębiewski J., *Analiza przepisów międzynarodowych z wyłączeniem UE związanych z zarządzaniem ryzykiem*.
- Gołębiewski J., *Określenie pojęć w zakresie zarządzania ryzykiem*.
- Kędzierska M., *Opracowanie wspólnej terminologii pojęć*.
- Napiórkowski M., *Analiza metodyk oceny ryzyka i zagrożeń w przepisach krajowego prawa resortowego związanego z zarządzaniem ryzykiem – diagnoza stanu*.
- Połeć B., *Analiza metodyk oceny ryzyka i zagrożeń w przepisach krajowego prawa miejscowego z zakresu zarządzania ryzykiem – diagnoza stanu*.
- Połeć B., *Analiza przepisów krajowego prawa miejscowego związanego z zarządzaniem ryzykiem*.
- Połeć B., *Identyfikacja przepisów krajowego prawa miejscowego z zakresu zarządzania ryzykiem*.
- Połeć B., Napiórkowski M., *Analiza przepisów krajowego prawa resortowego związanego z zarządzaniem ryzykiem*.
- Połeć B., *Sporządzenie wykazu pojęć z zakresu zarządzania ryzykiem z województwa mazowieckiego*.

- Skomra W., *Opracowanie metod oceny ryzyka na potrzeby planowania cywilnego.*
- Smoła J., *Analiza przepisów krajowego prawa powszechnie obowiązującego związanego z zarządzaniem ryzykiem.*
- Smoła J., *Sporządzenie wykazu pojęć z zakresu zarządzania ryzykiem z województwa łódzkiego.*
- Sobór E., Stępień P., *Analiza metodyk oceny ryzyka i zagrożeń ujętych w projektach norm z zakresu zarządzania ryzykiem – diagnoza stanu.*
- Sobór E., Stępień P., *Analiza projektów norm związanych z zarządzaniem ryzykiem.*
- Sobór E., Stępień P., *Identyfikacja projektów norm z zakresu zarządzania ryzykiem.*
- Trzcńska M., *Analiza metodyk oceny ryzyka i zagrożeń ujętych w przepisach UE związanych z zarządzaniem ryzykiem – diagnoza stanu.*
- Trzcńska M., *Analiza przepisów unijnych związanych z zarządzaniem ryzykiem.*
- Wróblewski D., Sowa T., *Analiza norm związanych z zarządzaniem ryzykiem.*
- Wróblewski D., Sowa T., *Identyfikacja norm z zakresu zarządzania ryzykiem.*

SPIS OZNACZEŃ

- ALARP (ang. *As Low As Reasonably Practicable*) – tak niskie, jak to praktycznie możliwe;
- BCP (ang. *Business Continuity Planning*) – planowanie ciągłości działania;
- BSI (ang. *British Standards Institution*) – Brytyjski Krajowy Komitet Normalizacyjny;
- CEN (fr. *Comité Européen de Normalisation*) – Europejski Komitet Normalizacyjny;
- CFD (ang. *Computational Fluid Dynamics*) – obliczeniowa mechanika płynów;
- CIRAM (ang. *Common Integrated Risk Analysis Model*) – wspólny zintegrowany model analizy ryzyka;
- COSO (ang. *Committee of Sponsoring Organizations of the Treadway Commission*) – Komitet Organizacji Sponsorujących Komisję Treadwaya;
- CSA (ang. *Canadian Standards Association*) – Kanadyjskie Stowarzyszenie Normalizacyjne;
- CWFS (ang. *Centre of World Fire Statistics*) – Światowe Centrum Statystyki Pożarów;
- DG (ang. *Directorate-General*) – Dyrekcja Generalna;
- DG ECHO (ang. *Directorate-General for Humanitarian Aid and Civil Protection*) – Dyrekcja Generalna ds. Pomocy Humanitarnej i Ochrony Ludności;
- DG SANCO (fr. *Direction Générale de la Santé et des Consommateurs*) – Dyrekcja Generalna ds. Zdrowia i Konsumentów;
- ECDC (ang. *European Centre for Disease Prevention and Control*) – Europejskie Centrum ds. Zapobiegania i Kontroli Chorób;
- EFSA (ang. *European Food Safety Authority*) – Europejski Urząd ds. Bezpieczeństwa Żywności;
- ENSREG (ang. *European Nuclear Safety Regulators Group*) – Europejska Grupa Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego;
- EUROPOL (ang. *European Police Office*) – Europejski Urząd Policji;
- FERMA (ang. *Federation of European Risk Management Associations*) – Federacja Europejskich Stowarzyszeń Zarządzania Ryzykiem;
- FRONTEX (od fr. *Frontières extérieures*) – Europejska Agencja Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych;
- IK – infrastruktura krytyczna;
- IRM (ang. *Integrated Risk Management*) – zintegrowane zarządzanie ryzykiem;
- ISO (ang. *International Organization for Standardization*) – Międzynarodowa Organizacja Normalizacyjna;

KE (ang. *European Commission*, EC) – Komisja Europejska;
KRS – Krajowy Rejestr Sądowy;
KZGW – Krajowy Zarząd Gospodarki Wodnej;
MAiC – Ministerstwo Administracji i Cyfryzacji;
MSB (ang. *Swedish Civil Contingencies Agency*) – Szwedzka Agencja ds. Cywilnych Sytuacji Kryzysowych;
MSWiA – Ministerstwo Spraw Wewnętrznych i Administracji;
MSZ – Ministerstwo Spraw Zagranicznych;
NCBR – Narodowe Centrum Badań i Rozwoju;
OECD (ang. *Organization for Economic Co-operation and Development*) – Organizacja Współpracy Gospodarczej i Rozwoju;
ONZ (ang. *United Nations*, UN) – Organizacja Narodów Zjednoczonych;
PE (ang. *European Parliament*, EP) – Parlament Europejski;
PKB – Produkt Krajowy Brutto;
PKN – Polski Komitet Normalizacyjny;
PSA (ang. *probabilistic security assessment*) – probabilistyczna ocena bezpieczeństwa;
PZK – plan zarządzania kryzysowego;
PZRP – plany zarządzania ryzykiem powodziowym;
RCB – Rządowe Centrum Bezpieczeństwa;
RoZBN – Raport o zagrożeniach bezpieczeństwa narodowego;
RPO WP – Regionalny Program Operacyjny Województwa Pomorskiego;
RZSR WP – Regionalny Zintegrowany System Ratownictwa Województwa Pomorskiego;
SME (ang. *small & medium enterprises*) – małe i średnie przedsiębiorstwa;
UE (ang. *European Union*, EU) – Unia Europejska;
WHO (ang. *World Health Organisation*) – Światowa Organizacja Zdrowia;
WORP – wstępna ocena ryzyka powodziowego;
WUG – Wyższy Urząd Górniczy;
ZK – zarządzanie kryzysowe.

CZEŚĆ I

PRZEGLĄD WYBRANYCH
PRZEPISÓW KRAJOWYCH,
ZAGRANICZNYCH ORAZ NORM
I STANDARDÓW DOTYCZĄCYCH
ZARZĄDZANIA RYZYKIEM

WPROWADZENIE

Część pierwsza *Przegląd wybranych przepisów krajowych, zagranicznych oraz norm i standardów dotyczących zarządzania ryzykiem* zawiera charakterystykę wybranych dokumentów normatywnych wraz ze wstępną oceną ich użyteczności w kontekście rozwiązań oraz dobrych praktyk związanych z zarządzaniem ryzykiem. Celem badań prowadzonych przez zespół autorski było zidentyfikowanie i przeanalizowanie wybranych dokumentów podejmujących tematykę zarządzania ryzykiem bądź jego podprocesów i innych elementów oraz uzyskanie odpowiedzi na pytania: co dla organizacji jest istotne w kontekście zarządzania ryzykiem oraz jakie są efektywne metody oceny ryzyka.

Materiał do niniejszej części został zebrany i zaktualizowany w oparciu o wyniki badań opublikowanych w monografii pt. *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzaniem ryzykiem wraz z leksykonem* pod redakcją D. Wróblewskiego, wydanej przez CNBOP-PIB w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”, sfinansowanego przez Narodowe Centrum Badań i Rozwoju – umowa Nr DOBR/0016/R/ID2/2012/03. Treści aktów prawnych podlegały weryfikacji poprzez serwis prawniczy „Lex”, w celu potwierdzenia ich aktualnie obowiązującego statusu oraz wprowadzonych zmian w zakresie regulacji prawnych. W ramach rozszerzenia obszaru badań zagadnień związanych z zarządzaniem ryzykiem autorzy uznali za stosowne, aby procesowi przeglądu poddać akty prawa o statusie „obowiązujące”, jak również ministerstw przekształcanych oraz nowo utworzonych, a także akty obowiązujące na rok 2017 oraz wchodzące w życie z dniem 1.01.2018.

Dokumenty do analizy wybierano spośród dwóch zasadniczych grup: przepisów prawa krajowego (prawo krajowe powszechnie obowiązujące, resortowe, miejscowe) oraz międzynarodowych norm i standardów. Niniejsza część obejmuje sześć rozdziałów. Cztery pierwsze rozdziały dotyczą przeglądu: ustaw, rozporządzeń, przepisów resortowych i przepisów prawa miejscowego. Ostatnie dwa rozdziały dotyczą przeglądu ustanowionych norm i standardów oraz projektów norm i standardów.

W rozdziale pierwszym autorzy dokonali analizy sześciu ustaw: o zarządzaniu kryzysowym, prawo wodne, o ochronie żeglugi i portów morskich, prawo ochrony środowiska, o państwowej inspekcji sanitarnej, o finansach publicznych. W rozdziale drugim scharakteryzowano cztery rozporządzenia nawiązujące do kwestii zarządzania ryzykiem w zarządzaniu kryzysowym, które dotyczą: planów ochrony

infrastruktury krytycznej, Narodowego Programu Ochrony Infrastruktury Krytycznej, raportu o zagrożeniach bezpieczeństwa narodowego, opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego. W rozdziale trzecim badania objęły przepisy krajowego prawa resortowego związanego z zarządzaniem ryzykiem. Rozdział zawiera analizę wybranych dokumentów wykorzystujących elementy zarządzania ryzykiem, które mogą zostać wykorzystane przy opracowywaniu metodyk oceny ryzyka oraz w procesie zarządzania ryzykiem. W rozdziale czwartym przedstawiono przepisy prawa miejscowego, w których odnaleźć można charakterystykę procesu zarządzania ryzykiem, metodyki zarządzania ryzykiem oraz terminologię. Do analizy wytypowano zarządzenia: Wojewody Mazowieckiego w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim, Prezydenta Miasta Stołecznego Warszawy w sprawie systemu zarządzania ryzykiem w m.st. Warszawie, Burmistrza Karczewa w sprawie wprowadzenia polityki zarządzania ryzykiem oraz zarządzenia w sprawie wprowadzenia instrukcji dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej. Rozdział piąty zawiera charakterystykę czterech norm opublikowanych przez Polski Komitet Normalizacyjny, Międzynarodową Organizację Normalizacyjną, Kanadyjskie Stowarzyszenie Normalizacyjne, a także trzech standardów opublikowanych przez Międzynarodową Organizację Normalizacyjną, Brytyjską Instytucję Normalizacyjną oraz Organizację Współpracy Gospodarczej i Rozwoju. W rozdziale szóstym przedstawione zostały dwa projekty norm N 96 ISO 18482 *Security Management System – Guidance for use-Security risk assessment* oraz ISO/CD 16125 *Security management system*, procedowane przez Międzynarodową Organizację Normalizacyjną. Zarówno wybrane normy, jak również projekty norm zawierają elementy zarządzania ryzykiem, które mogą zostać wykorzystane podczas opracowywania metodyk analizy i oceny ryzyka.

W wyborze dokumentów do poszczególnych rozdziałów autorzy kierowali się ich użytecznością w zakresie terminologii, elementów struktur systemu zarządzania, opisu ról, zadań oraz procesów występujących w zarządzaniu ryzykiem.

1. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – USTAWY

W ramach prowadzonych badań zespół autorski dokonał przeglądu oraz analizy ustaw poruszających zagadnienia obejmujące tematykę zarządzania ryzykiem, w szczególności w różnych aspektach zarządzania bezpieczeństwem. Kolejnym kryterium doboru dokumentów była identyfikacja terminologii związanej z zarządzaniem ryzykiem w przeanalizowanych przepisach prawa krajowego. Biorąc pod uwagę powyższe, do grupy wybranych aktów prawnych, poddanych szerszej charakterystyce w kontekście zarządzania ryzykiem zaliczono:

- ustawę o zarządzaniu kryzysowym,
- ustawę – Prawo wodne, akt obowiązujący do 31.12.2017 r.,
- ustawę – Prawo wodne, obowiązujący od 1.01.2018 r.,
- ustawę o ochronie żeglugi i portów morskich,
- ustawę – Prawo ochrony środowiska,
- ustawę o państwowej inspekcji sanitarnej,
- ustawę o finansach publicznych.

1.1. Ustawa o zarządzaniu kryzysowym

W ustawie o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.¹ zostały przedstawione elementy składowe planów zarządzania kryzysowego, takie jak:

- plan główny zawierający charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia,
- także (zagrożeń) dotyczących infrastruktury krytycznej;
- mapy ryzyka i mapy zagrożeń,
- zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa,
- zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych,

¹ Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 stycznia 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zarządzaniu kryzysowym (Dz. U. z 2017 r., poz. 209).

- zadania określone planami działań krótkoterminowych, o których mowa w art. 92 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (Dz. U. z 2008 r. Nr 25, poz. 150, z późn. zm.)².

Spośród wskazanych elementów wchodzących w skład planu zarządzania kryzysowego, należy podkreślić ocenę ryzyka oraz przygotowanie map ryzyka, które zdecydowanie wpisują się w przykłady wykorzystania procesów zarządzania ryzykiem w zarządzaniu kryzysowym.

W ramach terminologii związanej z zarządzaniem ryzykiem jedynym pojęciem, które zaklasyfikowano do zakresu związanego z zarządzaniem ryzykiem jest mapa ryzyka. Termin ten określa mapę lub opis przedstawiający potencjalne pozytywne lub negatywne skutki oddziaływania zagrożenia na ludzi, mienie, bądź środowisko naturalne oraz infrastrukturę krytyczną³.

Ustawa o zarządzaniu kryzysowym wskazuje również na istotny obszar – ochronę infrastruktury krytycznej, która powinna prowadzić do zachowania jej ciągłości działania i integralności w celu zapobiegania zagrożeniom, ryzykom oraz szybkiemu odtworzeniu infrastruktury na wypadek awarii⁴. Akt prawny wprowadza także obowiązek przygotowywania przez ministrów kierujących działaniami administracji rządowej, kierowników urzędów centralnych oraz wojewodów *Raportu o zagrożeniach bezpieczeństwa narodowego* dla Dyrektora Rządowego Centrum Bezpieczeństwa. W dokumencie tym mają za zadanie m.in. wskazać najważniejsze zagrożenia przez stworzenie map ryzyka⁵.

1.2. Ustawa – Prawo wodne (akt obowiązujący do 31.12.2017)

Od 1 stycznia 2002 r. podstawowym aktem prawnym regulującym zagadnienia związane z gospodarką wodną i ochroną wód jest ustawa z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. z 2001 r. Nr 115, poz. 1229, z późn. zm.), która utraci moc prawną z dniem 31 grudnia 2017 r. Jednocześnie z dniem 1 stycznia 2018 r. wchodzi w życie ustawa z dnia 20 lipca 2017 r. – Prawo wodne⁶.

Przepisami prawa wodnego ww. ustawy objęte są śródlądowe wody powierzchniowe, wody podziemne oraz morskie wody wewnętrzne, natomiast w zakresie ochrony przed zanieczyszczeniem ze źródeł lądowych oraz ochrony przed powodzią, także wody morza terytorialnego wraz z wodami Zatoki Gdańskiej.

Dokument stanowi podstawę do wstępnej oceny ryzyka powodziowego. Zgodnie z art. 88c ust. 1 ustawy z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. z 2005 r.

² Art. 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.).

³ Tamże, art. 3.

⁴ Tamże.

⁵ Art. 5a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.).

⁶ Ustawa z dnia 20 lipca 2017 r. Prawo wodne (Dz. U. z 2017 r., poz. 1566).

Nr. 239, poz. 2019, z późn. zm.) za przygotowanie wstępnej oceny ryzyka powodziowego odpowiedzialny jest Prezes Krajowego Zarządu Gospodarki Wodnej.

Plany zarządzania ryzykiem powodziowym zawierają mapę obszaru dorzecza, na której zaznaczone są obszary narażone na niebezpieczeństwo powodzi, mapy zagrożenia powodziowego oraz mapy ryzyka powodziowego wraz z opisem wniosków z analizy tych map, opis celów zarządzania ryzykiem powodziowym, a także katalog działań służących osiągnięciu celów zarządzania ryzykiem powodziowym, z uwzględnieniem ich priorytetu⁷. Działania, które mogą służyć zminimalizowaniu ryzyka powinny zawierać informacje o:

- zasięgu powodzi,
- trasie przejścia wezbrania powodziowego,
- obszarze o potencjalnej retencji wód powodziowych,
- żegludze morskiej i śródlądowej,
- portach morskich i portach lub przystaniach zlokalizowanych na wodach śródlądowych uznanych za żeglowne, wraz ze związaną z nimi infrastrukturą,
- prognozowanej powodzi,
- systemach wczesnego ostrzegania przed zagrożeniami,
- sposobach ochrony infrastruktury krytycznej⁸.

Wspomniana ustawa definiuje cele zarządzania ryzykiem powodziowym, jako ograniczenie potencjalnych negatywnych skutków powodzi dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej⁹. Wymienione skutki powodzi zależą od ilości opadów, zagospodarowania terenów oraz możliwości lokalnych służb do przeciwdziałania zagrożeniu i likwidacji skutków katastrofy.

Ustawa reguluje założenia związane z zarządzaniem ryzykiem powodziowym. Według aktu, plany zarządzania ryzykiem powodziowym wykonuje się dla dorzeczy i dla regionów wodnych, z uwzględnieniem obszarów narażonych na niebezpieczeństwo powodzi wyznaczonych we wstępnej ocenie ryzyka powodziowego, bazując na przygotowanych dla tych obszarów mapach zagrożenia i ryzyka powodziowego. Podczas planowania należy uwzględniać analizę kosztów i korzyści planowanych działań. Plany zarządzania ryzykiem powinny obejmować wszystkie aspekty zarządzania kryzysowego takie jak etap prewencji, ochrony, przygotowania, reagowania i odbudowy¹⁰.

⁷ Art. 88g ustawy z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. z 2001 r. Nr 115, poz. 1229, z późn. zm.).

⁸ Tamże.

⁹ Art. 9, pkt 1b ustawy z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. z 2001 r. Nr 115, poz. 1229, z późn. zm.).

¹⁰ KZGW, *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, Etap I, Kraków 2012, s. 9–10.

Opisywana w ustawie metodyka ma na celu przygotowanie jednolitego w skali kraju podejścia do opracowania planów zarządzania ryzykiem powodziowym, a w szczególności przyjęcie dla wszystkich poziomów planowania jednolitych celów i preferowanych sposobów ich osiągnięcia¹¹.

Ustawa wprowadza pojęcie ryzyka powodziowego, które określono jako kombinację prawdopodobieństwa wystąpienia powodzi i potencjalnych negatywnych skutków powodzi dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej¹².

Ustawa – Prawo wodne przedstawia zadania organów administracji rządowej i samorządowej z zakresu ochrony przed powodzią. Według dokumentu, wskazane podmioty nadzorują zbiorniki wodne, współpracują z organami administracji rządowej i samorządowej podczas realizacji zadań z zakresu zarządzania kryzysowego. Ochrona przed powodzią prowadzona jest za pomocą map powodziowych oraz planów zarządzania ryzykiem powodziowym¹³.

1.2.1. Ustawa – Prawo wodne (akt obowiązujący od 1.01.2018)

W ramach przedmiotowych badań, analizie poddano również znowelizowaną ustawę z dnia 20 lipca 2017 r. Prawo wodne wchodzącą w życie z dniem 1 stycznia 2018 r. Analizie poddana została wersja z dnia 23 sierpnia 2017 roku. Ustawa systemowo reguluje gospodarowanie wodami zgodnie z zasadą zrównoważonego rozwoju, a w szczególności kształtowania i ochrony zasobów wodnych, korzystania z wód oraz zarządzania zasobami wodnymi, w tym sprawy własności wód oraz gruntów pokrytych wodami¹⁴.

Nowelizacja ustawy z dnia 20 lipca 2017 r. – Prawo wodne wprowadza instrumenty zapewniające osiągnięcie celu ramowej dyrektywy wodnej w zakresie pełnej realizacji zlewniowej polityki gospodarowania wodami, spełniającej warunki funkcjonalności i bezpieczeństwa, efektywności ekonomicznej, trwałości ekosystemów przy akceptacji społecznej, zgodnie z zasadą zrównoważonego gospodarowania wodami, w tym także z gospodarczym korzystaniem z zasobów wodnych¹⁵.

Zgodnie z ustawą gospodarowanie wodami ma uwzględniać zasadę wspólnych interesów publicznych, przede wszystkim w celu uniknięcia pogorszenia ekologicznych funkcji wód oraz pogorszenia stanu ekosystemów lądowych i terenów podmokłych¹⁶. Zarządzanie zasobami wodnymi będzie realizowane z uwzględnieniem podziału państwa na obszary dorzeczy, regiony wodne i zlewnie¹⁷.

¹¹ Tamże, s. 12.

¹² Art. 9, pkt 13c ustawy z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. z 2001 r. Nr 115, poz. 1229, z późn. zm.).

¹³ Tamże, art. 88a.

¹⁴ Art. 1, 2 i 3 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. poz. 1566).

¹⁵ <https://legislacja.rcl.gov.pl/docs//2/12284651/12349263/12349264/dokument218331.pdf> [dostęp: sierpień 2017].

¹⁶ Art. 9 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. poz. 1566).

¹⁷ Tamże, art. 12.

W ramach reorganizacji systemu gospodarowania wodami w ustawie proponuje się m.in. likwidację istniejącego obecnie organu centralnej administracji rządowej w postaci prezesa Krajowego Zarządu Gospodarki Wodnej i zastąpienie go Państwowym Gospodarstwem Wodnym Wody Polskie. W związku ze zmianą struktur aparatu administracji rządowej nastąpi transfer wielu istotnych zadań i kompetencji. Powołanie Państwowego Gospodarstwa Wodnego Wody Polskie, oznacza stworzenie nowego systemu gospodarowania i zarządzania wodami na terenie Polski, który zgodnie z aktem prawnym będzie główną instytucją odpowiedzialną za gospodarowanie wodami w naszym kraju¹⁸.

Naczelnym organem i władzą wodną z punktu widzenia użytkowników wód będzie minister właściwy do spraw gospodarki wodnej, natomiast Państwowe Gospodarstwo Wodne Wody Polskie będzie miało przede wszystkim charakter funkcjonalny, instytucji realizującej cele Rządu RP¹⁹.

W konsekwencji dojdzie do uszczuplenia katalogu zadań jednostek samorządu terytorialnego oraz skupienia ich w rękach właściwych organów Wód Polskich. Instytucja ta będzie miała także decydujące zadanie w zakresie planowania w gospodarowaniu wodami, ochrony zasobów wodnych oraz wprowadzenia systemu zgód wodnoprawnych, kierunków prowadzenia inwestycji na wodach i utrzymania urządzeń wodnych, a także zapewnienie osiągnięcia dobrego stanu wód i minimalizacji ryzyka powodziowego na wszystkich szczeblach zlewniowego zarządzania zasobami wodnymi w tym obwałowań oraz obszaru międzywala²⁰.

Ustawa wskazuje organy właściwe w sprawach gospodarowania wodami oraz zawiera katalog zadań ustawowych Wód Polskich, wśród których znajdują się zadania dotyczące zarządzania ryzykiem powodziowym i przeciwdziałanie skutkom suszy:

- realizacja zadań obronnych oraz zadań z zakresu zarządzania kryzysowego przekazanych przez ministra właściwego do spraw gospodarki wodnej,
- uzgadnianie projektów dokumentów, aktów oraz decyzji,
- gromadzenie, przetwarzanie, udostępnianie i przekazywanie informacji dla potrzeb planowania przestrzennego i centrów zarządzania kryzysowego,
- przygotowywanie projektów:
 - planów gospodarowania wodami na obszarach dorzeczy i ich aktualizacji,
 - planów zarządzania ryzykiem powodziowym i ich aktualizacji,
 - planów przeciwdziałania skutkom suszy i ich aktualizacji,
 - wstępnej oceny ryzyka powodziowego i jej aktualizacji,
 - map zagrożenia powodziowego i ich aktualizacji,
 - map ryzyka powodziowego i ich aktualizacji,

¹⁸ Tamże, art. 14.

¹⁹ Tamże.

²⁰ Tamże, art. 163.

- zestawu celów środowiskowych dla wód morskich i jego aktualizacji,
- programu ochrony wód morskich i jego aktualizacji;
- finansowanie działalności służb państwowych;
- współdziałanie z wojewodą w zakresie opracowywania wojewódzkiego planu zarządzania kryzysowego²¹.

Wytyczne dotyczące zarządzania ryzykiem powodziowym i przeciwdziałaniu skutkom suszy zawarte zostały w Dziale IV Zarządzanie ryzykiem powodziowym i przeciwdziałanie skutkom suszy (art. 163–182) i stanowią podstawę do zarządzania ryzykiem powodziowym.

W dziale tym szczegółowo omówiono zadania dotyczące zarządzania ryzykiem powodziowym i przeciwdziałaniu skutkom suszy, a wskazana w nim metodyka ma na celu przygotowanie jednolitego podejścia w skali kraju do opracowania planów zarządzania ryzykiem powodziowym i przeciwdziałanie skutkom suszy. Celem działań jest ograniczanie potencjalnych negatywnych skutków powodzi dla zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej, a także zarządzanie tym ryzykiem²².

Akt prawny szczegółowo reguluje tryb postępowania w zakresie wymiany informacji, współpracy i podejmowania działań niezbędnych do opracowania wstępnej oceny ryzyka, map zagrożenia powodziowego, map ryzyka powodziowego, sposób zgłaszania i zakres uwag do projektów planów zarządzania ryzykiem powodziowym od strony morza, w tym morskich wód wewnętrznych oraz dla obszaru dorzecza, którego część znajduje się na terytorium innych państw członkowskich Unii Europejskiej i państw leżących poza granicami Unii Europejskiej²³.

Dokument zawiera definicje kluczowych pojęć z zakresu zarządzania ryzykiem powodziowym: celów zarządzania ryzykiem powodziowym, obszarów narażonych na niebezpieczeństwo powodzi, obszarów szczególnego zagrożenia powodzią, ryzyka powodziowego²⁴.

W działaniach przed powodzią należy opracować wstępną ocenę ryzyka powodziowego, mapy zagrożenia powodziowego i ryzyka powodziowego oraz plany zarządzania ryzykiem powodziowym, uwzględniając wszystkie elementy zarządzania ryzykiem powodziowym, a w szczególności zapobieganie, ochronę, stan należytego przygotowania i reagowanie w przypadku wystąpienia powodzi, usuwanie skutków powodzi, odbudowę i wyciąganie wniosków²⁵.

Projekt wstępnej oceny ryzyka powodziowego przygotowują „Wody Polskie” dla obszarów dorzeczy. Powinien on zawierać mapę oraz topografię terenu i jego zagospodarowanie, opis powodzi historycznych i ich prawdopodobieństwo wystąpienia,

²¹ Tamże, art. 14.

²² Tamże, art. 16.

²³ Tamże, art. 168, 169 i 171.

²⁴ Tamże, art. 16 ust. 34–48.

²⁵ Tamże, art. 163–164.

ocenę potencjalnych negatywnych skutków mających wpływ dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej²⁶.

Z kolei projekt wstępnej oceny ryzyka od strony morza, w tym morskich wód wewnętrznych, przygotowuje minister właściwy do spraw gospodarki morskiej i przekazuje „Wodom Polskim”. Ustawa wskazuje tryb postępowania z projektem wstępnej oceny ryzyka w zakresie opiniowania, przeglądów, aktualizacji, zatwierdzenia, upubliczniania w BIP, przekazania do Rządowego Centrum Bezpieczeństwa²⁷.

W zakresie współpracy międzynarodowej, zgodnie z aktem prawnym minister właściwy do spraw gospodarki wodnej udostępnia Komisji Europejskiej przeglądy oraz aktualizacje wstępnej oceny ryzyka powodziowego²⁸.

Mapy zagrożenia powodziowego i mapy ryzyka powodziowego sporządza się dla obszarów narażonych na niebezpieczeństwo powodzi, wskazanych we wstępnej ocenie ryzyka powodziowego. Na mapach zagrożenia powodziowego przedstawia się w szczególności:

- obszary, na których prawdopodobieństwo wystąpienia powodzi jest niskie i wynosi 0,2% lub na których istnieje prawdopodobieństwo wystąpienia zdarzenia ekstremalnego,
- obszary szczególnego zagrożenia powodzią,
- obszary obejmujące tereny narażone na zalanie w przypadku uszkodzenia lub zniszczenia wału przecipowodziowego, wału przeciwsztormowego, budowli piętrzącej.

Mapy te zawierać powinny także dane dotyczące zasięgu powodzi, głębokości lub poziomu zwierciadła wody, a w uzasadnionych przypadkach prędkości lub natężenia przepływu wody²⁹.

„Uzupełnieniem map zagrożenia powodziowego są mapy ryzyka powodziowego, określające potencjalne szkody związane z powodzią. Muszą one uwzględniać informacje na temat szacunkowej liczby mieszkańców potencjalnie dotkniętych powodzią, rodzaju działalności gospodarczej i ważnych instalacjach na danym obszarze, jak też inne istotne dla konkretnego obszaru informacje dodatkowe”³⁰ np.: występowanie stref ochronnych ujęć wody lub obszarów ochronnych zbiorników wód śródlądowych, kąpielisk, obszarów Natura 2000, parków narodowych oraz rezerwatów przyrody, obszary którym towarzyszy transport dużej ilości osadów, rumowiska, potencjalne ogniska zanieczyszczeń wody³¹.

²⁶ Tamże, art. 167 ust. 2.

²⁷ Tamże, art. 168 ust. 2–12.

²⁸ Tamże, art. 168 ust. 13.

²⁹ Tamże, art. 169.

³⁰ <http://www.kzgw.gov.pl/index.php/pl/dyrektywa-powodziowa> [dostęp: sierpień 2017].

³¹ Art. 170 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. poz. 1566).

Ustawodawca zadanie przygotowania projektów obu rodzajów map zagrożenia powodziowego oraz map ryzyka powodziowego powierzył Wodom Polskim, które sporządzają je w uzgodnieniu z właściwymi wojewodami. Integralnym elementem projektów map zagrożenia i map ryzyka powodziowego są projekty map zagrożenia powodziowego oraz map ryzyka powodziowego od strony morza i morskich wód wewnętrznych, które przygotowują dyrektorzy urzędów morskich³².

Akt określa także tryb przeglądów i aktualizacji map zagrożenia oraz map ryzyka powodziowego, zatwierdzania i upubliczniania, a także wskazuje ich adresatów. Minister właściwy do spraw gospodarki wodnej zatwierdza mapy zagrożenia powodziowego i mapy ryzyka powodziowego i przekazuje w postaci elektronicznej:

- Głównemu Geodecie Kraju,
- właściwemu organowi Inspekcji Ochrony Środowiska,
- dyrektorowi Rządowego Centrum Bezpieczeństwa,
- Wodom Polskim,
- Komendantowi Głównemu Państwowej Straży Pożarnej,
- właściwym wojewodom,
- właściwym marszałkom województw,
- właściwym starostom,
- właściwym wójtom, burmistrzom lub prezydentom miast,
- właściwym komendantom wojewódzkim i powiatowym (miejskim) Państwowej Straży Pożarnej,
- właściwym dyrektorom urzędów żeglugi śródlądowej oraz właściwym dyrektorom urzędów morskich,
- właściwym zarządcom infrastruktury kolejowej oraz właściwym zarządcom dróg publicznych³³.

Minister właściwy do spraw gospodarki wodnej zobowiązany jest także udostępnić Komisji Europejskiej przeglądy i aktualizacje map zagrożenia oraz map ryzyka powodziowego w terminie 3 miesięcy od dnia ich wykonania³⁴.

Na podstawie map zagrożenia powodziowego oraz map ryzyka powodziowego przygotowywane są plany zarządzania ryzykiem powodziowym, z uwzględnieniem podziału kraju na obszary dorzeczy i regiony wodne oraz działań służących zapobieganiu powodzi i ochronie przed powodzią³⁵. Plany te muszą obejmować wszystkie aspekty zarządzania ryzykiem powodziowym z uwzględnieniem specyfiki poszczególnych obszarów dorzecza, a działania powinny być ukierunkowane na

³² Tamże, art. 171.

³³ Tamże, art. 170 ust. 4.

³⁴ Tamże, art. 171.

³⁵ Tamże, art. 172.

zapobieganie, ochronę i właściwe przygotowanie, w tym prognozowanie powodzi i systemy wczesnego ostrzeżenia³⁶.

Zgodnie z dyrektywą powodziową³⁷ dla obszarów, gdzie występuje lub może wystąpić istotne ryzyko powodzi, ustalone zostaną odpowiednie cele zarządzania ryzykiem powodziowym, kładąc nacisk na ograniczenie potencjalnych negatywnych konsekwencji powodzi przy wykorzystaniu w możliwych przypadkach nietechnicznych środków ochrony przeciwpowodziowej³⁸.

Plany zarządzania ryzykiem powodziowym obejmują wszystkie elementy zarządzania ryzykiem powodziowym i zawierają:

- mapę obszaru dorzecza, na której są zaznaczone obszary narażone na niebezpieczeństwo powodzi,
- mapy zagrożenia powodziowego oraz mapy ryzyka powodziowego wraz z opisem wniosków z analizy tych map,
- opis celów zarządzania ryzykiem powodziowym uwzględniający konieczność ograniczania potencjalnych negatywnych skutków powodzi dla zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej,
- katalog działań służących osiągnięciu celów zarządzania ryzykiem powodziowym,
- opis sposobu określania priorytetów działań służących osiągnięciu celów zarządzania ryzykiem powodziowym i nadzorowania postępów w realizacji planu,
- podsumowanie działań służących informowaniu społeczeństwa i prowadzeniu konsultacji społecznych,
- wykaz organów właściwych w sprawach zarządzania ryzykiem powodziowym,
- opis współpracy w zakresie opracowania i aktualizacji planów zarządzania ryzykiem powodziowym, opisu metodyki analizy kosztów i korzyści służącej ocenie działań wywołujących skutki międzynarodowe (jeżeli taka metodyka została określona),
- opis koordynacji czynności z uwzględnieniem postanowień planów przy sporządzaniu innych aktów planistycznych³⁹.

Przy ustalaniu działań służących osiągnięciu celów zarządzania ryzykiem powodziowym uwzględnia się w szczególności:

³⁶ Tamże, art. 165.

³⁷ 2000/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2000 r. ustanawiającej ramy wspólnotowego działania w dziedzinie polityki wodnej, zwanej dalej „Ramową Dyrektywą Wodną”, oraz dyrektywą 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim, zwanej dalej „Dyrektywą Powodziową”, Uzasadnienie projektu ustawy – Prawo wodne, s. 4.

³⁸ <http://www.kzgw.gov.pl/index.php/pl/dyrektywa-powodziowa> [dostęp: sierpień 2017].

³⁹ Art. 172 ust. 2 i 3 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. poz. 1566).

- analizę kosztów i korzyści,
- zasięg powodzi i trasy przejścia fali powodziowej,
- cele środowiskowe,
- obszary o potencjalnych możliwościach retencyjnych,
- zasady gospodarowania wodami i gruntami,
- elementy planowania przestrzennego i zagospodarowania terenu,
- ochronę przyrody oraz żeglugę i infrastrukturę portową,
- prognozowanie powodzi i systemy wczesnego ostrzegania przed zagrożeniami,
- infrastrukturę krytyczną,
- cechy obszaru dorzecza lub zlewni,
- ochronę ludności i zwierząt⁴⁰.

Projekty planów zarządzania ryzykiem powodziowym przygotowują Wody Polskie w uzgodnieniu z ministrem właściwym ds. transportu w zakresie infrastruktury transportowej, a także z wojewodami i marszałkami województw, a od strony morza i morskich wód wewnętrznych z ministrem właściwym ds. gospodarki morskiej i przekazują ministrowi właściwemu do spraw gospodarki wodnej⁴¹. Ustawodawca określił również tryb przeglądu, aktualizacji oraz opiniowania planów zarządzania ryzykiem powodziowym⁴².

Wymagania dotyczące opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego, ze szczególnym uwzględnieniem standardów i zakresu danych zawartych w państwowym zasobie geodezyjnym i kartograficznym oraz potrzebą zapewnienia ciągłego i nieprzerwanego dostępu do wizualizacji tych map określi minister właściwy do spraw gospodarki wodnej w porozumieniu z ministrem właściwym do spraw informatyzacji oraz ministrem właściwym do spraw gospodarki morskiej w drodze rozporządzenia⁴³.

Uregulowane zostały również zagadnienia dotyczące właściwych warunków przepływu wód powodziowych szczelności i stabilności wałów przeciwpowodziowych⁴⁴.

Ustawa nakłada również obowiązek na ministra właściwego do spraw gospodarki wodnej, zapewnienie aktywnego udziału wszystkich zainteresowanych w osiągnięciu celów zarządzania ryzykiem powodziowym oraz podania do publicznej wiadomości projektu planów zarządzania ryzykiem powodziowym, a po zatwierdzeniu także planów zarządzania ryzykiem powodziowym wraz z wizualizacją map zagrożenia powodziowego oraz map ryzyka powodziowego i ich aktualizacji⁴⁵.

⁴⁰ Tamże, art. 172 ust. 5.

⁴¹ Tamże, art. 173 ust. 2–5.

⁴² Przepisy art. 173 ust. 1–19 stosuje się odpowiednio do aktualizacji planów zarządzania ryzykiem powodziowym.

⁴³ Art. 174 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. poz. 1566).

⁴⁴ Tamże, art. 175–176.

⁴⁵ Tamże, art. 173.

Ustawa zobowiązuje również organy administracji rządowej i samorządowej, państwową służbę hydrologiczno-meteorologiczną i państwową służbę hydrogeologiczną oraz instytuty badawcze do nieodpłatnego przekazywania posiadanych danych organom przygotowującym i sporządzającym lub dokonującym aktualizacji i przeglądów wstępnej oceny ryzyka powodziowego, map zagrożenia i map ryzyka powodziowego oraz planów zarządzania ryzykiem powodziowym⁴⁶.

Dla obszarów międzynarodowych dorzeczy i obszaru dorzecza znajdującego się na terytorium RP przygotowuje się jeden międzynarodowy plan zarządzania ryzykiem powodziowym lub zestaw planów zarządzania ryzykiem powodziowym. W celu przygotowania i uzupełnienia planu zarządzania ryzykiem powodziowym działania podejmuje minister właściwy do spraw gospodarki wodnej we współpracy z właściwymi organami tych państw oraz wykorzystuje istniejące struktury wynikające z umów międzynarodowych⁴⁷. Minister właściwy do spraw gospodarki wodnej będzie również realizował przypisane ustawą obowiązki informacyjne i sprawozdawcze wobec Komisji Europejskiej wynikające z postanowień dyrektywy ustanawiającej ramy działań wspólnoty w dziedzinie polityki środowiska morskiego, w tym udostępni Komisji Europejskiej planów zarządzania ryzykiem powodziowym wraz z ich przeglądem i aktualizacją, z możliwością wskazania propozycji rozwiązania problemów mających wpływ na zarządzanie ryzykiem powodziowym, które nie mogą być rozwiązane na podstawie przepisów ustawy. Działania służące osiągnięciu celów zarządzania ryzykiem zawarte w planach zarządzania ryzykiem powodziowym nie mogą wpływać na zwiększenie ryzyka powodziowego na terytorium innych państw⁴⁸.

Rozdział 2 działu IV ustawy zawiera również wytyczne do opracowania planu przeciwdziałania skutkom suszy. Zadania w ramach przeciwdziałania skutkom suszy prowadzi się zgodnie z planem przeciwdziałania skutkom suszy, który sporządza się analogicznie jak plany zarządzania ryzykiem powodziowym. Niemniej jednak, Plan Przeciwdziałania Suszy powinien zawierać analizę możliwości powiększenia dyspozycyjnych zasobów wodnych, propozycje budowy lub przebudowy urządzeń wodnych, propozycje niezbędnych zmian w zakresie korzystania z zasobów wodnych oraz zmian naturalnej i sztucznej retencji, katalog działań służących przeciwdziałaniu skutkom suszy⁴⁹. Tryb przygotowywania, uzgadniania, przeglądów i aktualizacji, zatwierdzania i udostępniania jest analogiczny jak w rozdziale 1 działu IV omawianej ustawy. Projekt planu przeciwdziałania skutkom suszy uzgadniany jest z ministrem właściwym do spraw rolnictwa, ministrem właściwym do spraw rozwoju wsi, ministrem właściwym do spraw rybołówstwa, ministrem właściwym do spraw żeglugi śródlądowej oraz wojewodami, uwzględniając podział kraju na

⁴⁶ Tamże, art. 173 ust. 24.

⁴⁷ Tamże, art. 173 ust. 11–15.

⁴⁸ Tamże, art. 173 ust. 18–25.

⁴⁹ Tamże, art. 184.

obszary dorzeczy. Minister właściwy do spraw gospodarki wodnej, zapewniając aktywny udział wszystkich zainteresowanych w przygotowywaniu oraz aktualizacji planu przeciwdziałania skutkom suszy, podaje do publicznej wiadomości:

- harmonogram i program prac związanych z przygotowaniem projektu planu przeciwdziałania skutkom suszy,
- projekt planu przeciwdziałania skutkom suszy co najmniej na rok przed rozpoczęciem okresu, którego dotyczy ten plan.

Organy administracji rządowej i samorządowej i instytuty badawcze są zobowiązane do nieodpłatnego przekazywania posiadanych danych niezbędnych do przygotowania planu przeciwdziałania skutkom suszy podmiotom przygotowującym i sporządzającym ten dokument⁵⁰. Do realizacji zadania wyznaczone zostały organy administracji rządowej, samorządowej i Wód Polskich⁵¹.

1.3. Ustawa o ochronie żeglugi i portów morskich⁵²

Ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich określa zasady ochrony żeglugi morskiej i portów morskich, w tym ochrony życia i zdrowia osób znajdujących się na terenie portów morskich, obiektów portowych lub na statkach⁵³. Akt prawny dokonuje w zakresie swojej regulacji transpozycji dyrektywy 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów oraz ochrony statków i obiektów portowych w zakresie nieobjętym przepisami rozporządzenia (WE) nr 725/2004. Ocena stanu ochrony portów ma na celu zidentyfikowanie kluczowej infrastruktury na obszarze portu oraz ocenę ryzyka i zagrożeń w odniesieniu do tej infrastruktury. W tej kwestii ustawa ustanawia 3 poziomy ochrony żeglugi i portów, które przedstawiają się następująco:

- poziom ochrony 1 – poziom, dla którego w każdym czasie będą utrzymywane minimalne środki ochrony wynikające z planu ochrony,
- poziom ochrony 2 – poziom, dla którego w wyniku zwiększonego ryzyka zajścia zdarzenia naruszającego ochronę przez określony czas będą utrzymywane odpowiednie, dodatkowe środki ochrony wynikające z planu ochrony,
- poziom ochrony 3 – poziom, dla którego przez ograniczony czas będą utrzymywane dodatkowe środki ochrony wynikające z planu ochrony, związane z prawdopodobieństwem lub bezpośrednią groźbą zajścia zdarzenia

⁵⁰ Tamże, art. 185 ust. 3–7.

⁵¹ Tamże, art. 183.

⁵² Ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2008 r. Nr 171, poz. 1055 z późn. zm.).

⁵³ Tamże, art. 1.

naruszającego ochronę, przy czym identyfikacja konkretnego celu ataku może nie być możliwa⁵⁴.

W celu zapewnienia ciągłości zadań i odpowiedzialności za podejmowanie decyzji w sytuacji, gdy zostanie wprowadzony trzeci poziom ochrony oraz dojdzie do naruszenia ochrony, przepisy ustawy zostały powiązane z ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 z późn. zm.).

Na podstawie zawartych w ustawie o ochronie żeglugi i portów morskich tworzona jest ocena stanu ochrony portu, uwzględniająca system planowanego zabezpieczenia operacji portowych, podejmowanych działań na terenie portu oraz uruchamiania odpowiednich procedur w zakresie reagowania na dane zagrożenie. Skutki mogą dotyczyć wystąpienia krytycznych słabych punktów. Należy zwrócić uwagę na potrzebę kontroli dostępu lub ograniczenia dostępu do całego portu w celu wyeliminowania ryzyka⁵⁵. W trakcie eliminowania ryzyka ważna jest zdolność do oceny prawdopodobnych zdarzeń i ryzyka w zakresie ochrony, które mogą się pojawić w czasie eksploatacji statków i obiektów portowych⁵⁶. Wspomniana ocena ryzyka powinna zawierać ocenę i identyfikację ważnych składników majątku, których ochrona ma ważne znaczenie oraz identyfikację możliwych zagrożeń dla majątku i infrastruktury, w tym określenie prawdopodobieństwa ich zajścia w celu ustalenia środków ochrony. Przedstawiają ocenę ryzyka terenów nie znajdujących się w granicach portów i obiektów portowych. Tereny te mogą jednak stanowić zagrożenie dla ochrony portu lub wchodzić w skład infrastruktury kluczowej ze względu na bezpieczeństwo ekonomiczne państwa lub obronność⁵⁷.

Według ustawy konieczne jest także opracowanie oceny stanu ochrony portów oraz planów ochrony portów jako dokumentów integrujących wcześniej powstałe oceny stanu ochrony oraz plany ochrony obiektów portowych. Przy sporządzaniu dokumentacji, jaką jest ocena stanu ochrony portu uwzględnia się m.in.: specyfikę operacji portowych, obsługiwanych ładunków lub usług świadczonych na rzecz obsługiwanego statku konwencyjnego oraz obszarów sąsiadujących mogących wpływać na bezpieczeństwo danego rejonu. Zarządzający portem, jak i obiektem portowym, zobowiązany jest do działań w zakresie wdrażania planu ochrony portu, realizacji powyższych zadań wynikających z tego planu, współpracy i współdziałania z organami ochrony portu i oficerem ochrony portu a także z organami administracji państwowej, tj. Policją, Strażą Graniczną, Strażą Pożarną⁵⁸.

Statki znajdujące się na terenie portów i wód terytorialnych RP, obiekty portowe i porty podlegają próbie efektywności oraz weryfikacji. Próba efektywności ma na celu sprawdzenie środków ochrony żeglugi i portów w sposób symulowanych

⁵⁴ Tamże, art. 23.

⁵⁵ Tamże, załącznik nr 1.

⁵⁶ Tamże, załącznik nr 4.

⁵⁷ Tamże, załącznik nr 1.

⁵⁸ Tamże, art. 4.

ćwiczeń, których zadaniem jest sprawdzenie procedur oraz skuteczności ochrony portu i statku. Z kolei weryfikacja ma na celu zbadanie systemów, procedur i struktur ochrony oraz zbadania ich zgodności z ustawą, konwencją SOLAS, kodeksem ISPS, a także z rozporządzeniem (WE) 725/2004. Zgodnie z ustawą, próby skuteczności procedur reagowania na zagrożenie przeprowadza się co pięć lat w odniesieniu do portów i corocznie w odniesieniu do obiektów portowych⁵⁹.

1.4. Ustawa – Prawo ochrony środowiska⁶⁰

Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska definiuje zasady ochrony środowiska oraz warunki korzystania z jego zasobów, z uwzględnieniem wymagań zrównoważonego rozwoju, a w szczególności:

- zasady ustalania warunków ochrony zasobów środowiska, warunków wprowadzania substancji lub energii do środowiska, kosztów korzystania ze środowiska,
- obowiązki organów administracji,
- odpowiedzialność i sankcje⁶¹.

Dokument definiuje pojęcie ryzyka, które przedstawia się, jako prawdopodobieństwo wystąpienia konkretnego zdarzenia w określonym czasie i danej sytuacji⁶². Najważniejsze akty wykonawcze do ustawy z punktu widzenia oceny oddziaływania na środowisko regulują dopuszczalne poziomy substancji w powietrzu, dopuszczalne poziomy hałasu oraz standardy jakości gleby, ochronę wód z uwzględnieniem przepisów prawa Unii Europejskiej.

Zasadami odnoszącymi się do ryzyka w ustawie jest coroczne dokonywanie oceny poziomów substancji w powietrzu. W terminie 15 miesięcy od dnia otrzymania informacji o ryzyku wystąpienia w danej strefie przekroczenia stanu alarmowego, dopuszczalnego lub docelowego substancji w powietrzu od wojewódzkiego inspektora ochrony środowiska, zarząd województwa opracowuje i przedstawia do zaopiniowania właściwym wójtom, burmistrzom lub rezydentom miast i starostom projekt uchwały w sprawie planu działań krótkoterminowych⁶³. W planie tym ustala się działania mające na celu zmniejszenie ryzyka wystąpienia takich przekroczeń oraz ograniczenie skutków i czasu ich trwania⁶⁴.

W przypadku ryzyka wystąpienia zagrożenia w danej strefie wojewódzki zespół zarządzania kryzysowego, o którym mowa w art. 14 ust. 7 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 z późn. zm.),

⁵⁹ Tamże, art. 21.

⁶⁰ Ustawa z dnia 27 kwietnia 2001 r. - Prawo ochrony środowiska (tekst jedn.: Dz. U. z 2017 r. poz. 519 z późn. zm.).

⁶¹ Tamże, art. 1.

⁶² Tamże, art. 3 ust. 32c.

⁶³ Tamże, art. 91.

⁶⁴ Tamże, art. 92.

informuje właściwe organy o konieczności podjęcia działań określonych planem działań krótkoterminowych⁶⁵ oraz niezwłocznie powiadamia społeczeństwo oraz podmioty w sposób zwyczajowo przyjęty na danym terenie, o ryzyku wystąpienia przekroczenia poziomu alarmowego, dopuszczalnego lub docelowego substancji w powietrzu oraz o wystąpieniu przekroczenia poziomu alarmowego, dopuszczalnego lub docelowego substancji⁶⁶. W przypadku wystąpienia na terytorium RP, UE i innego państwa nie będącego w UE ryzyka przekroczeń poziomów dopuszczalnych, docelowych lub dopuszczalnych, lub poziomów alarmowych i celów długoterminowych lub przenoszenia zanieczyszczeń, minister właściwy do spraw środowiska, w porozumieniu i zasięgnięciu opinii Głównego Inspektora Ochrony Środowiska, za pośrednictwem zarządu województwa, prowadzi konsultacje, podejmuje współpracę w celu analizy możliwości wyeliminowania lub ograniczenia ryzyka, koordynacji wspólnych programów lub planów działań krótkoterminowych, w tym wymiany informacji o ewentualnych źródłach przekroczeń poziomów substancji w powietrzu oraz przykładowych działaniach mających na celu ograniczenie tych przekroczeń⁶⁷.

Następną kwestią omawianą w akcie prawnym jest ochrona wód polegająca na zapewnieniu ich jak najlepszej jakości, w tym utrzymywanie ilości wody na poziomie zapewniającym ochronę równowagi biologicznej oraz ich ochrony polegającej w szczególności na zmniejszaniu ryzyka zanieczyszczenia tych wód poprzez ograniczenie oddziaływania na obszary ich zasilania oraz utrzymywaniu równowagi zasobów tych wód⁶⁸. Zadania w zakresie planowania i realizacji ochrony poziomu jakości wód uwzględniające obszary zlewni hydrograficznych realizują organy administracji państwowej⁶⁹. Wody podziemne i obszary ich zasilania podlegają ochronie na zasadach określonych ustawą - Prawo wodne, obszary ochronne zbiorników wód śródlądowych⁷⁰.

Dział IV omawianej ustawy reguluje ochronę powierzchni ziemi, polegającej między innymi na racjonalnym gospodarowaniu, zachowaniu funkcji środowiskowych, gospodarczych, społecznych i kulturowych, zapobieganiu zanieczyszczeniu substancjami powodującymi ryzyko oraz na remediacji⁷¹, zachowaniu jak

⁶⁵ Tamże, art. 92 ust. 1d.

⁶⁶ Tamże, art. 93 ust. 1.

⁶⁷ Tamże, art. 92a ust. 1–8.

⁶⁸ Tamże, art. 97–98.

⁶⁹ Tamże, art. 99.

⁷⁰ Tamże, art. 98.

⁷¹ Remediacja – to poddanie gleby, ziemi i wód gruntowych działaniom mającym na celu usunięcie lub zmniejszenie ilości substancji powodujących ryzyko, ich kontrolowanie oraz ograniczenie rozprzestrzeniania się, tak aby teren zanieczyszczony przestał stwarzać zagrożenie dla zdrowia ludzi lub stanu środowiska, z uwzględnieniem obecnego i, o ile jest to możliwe, planowanego w przyszłości sposobu użytkowania terenu; remediacja może polegać na samoczyszczaniu, jeżeli przynosi największe korzyści dla środowiska, źródło: art. 3 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (tekst jedn.: Dz. U. z 2017 r. poz. 519 z późn. zm.).

najlepszego stanu gleby, minimalizacji skutków zasklepienia gleby, zapobieganiu ruchom masowym ziemi i ich skutkom, przeciwdziałaniu niekorzystnym zmianom naturalnego ukształtowania powierzchni ziemi. Zanieczyszczenie powierzchni ziemi ocenia się na podstawie przekroczenia dopuszczalnych zawartości substancji powodujących ryzyko w glebie lub w ziemi. Minister właściwy do spraw środowiska w drodze rozporządzenia sposób prowadzenia oceny zanieczyszczenia powierzchni ziemi. W rozporządzeniu określił zasady i badania zanieczyszczenia gleby i ziemi, w tym szczegółowe wymagania dotyczące substancji powodujących ryzyko, dopuszczalne zawartości w ziemi substancji powodującej ryzyko z uwzględnieniem analizy jej wpływu na zdrowie ludzi i stan środowiska, sposób ustalenia listy substancji powodujących ryzyko, źródła informacji istotnych dla oceny zagrożenia metodyki oceny oraz badań zanieczyszczenia gleby. W ramach państwowego monitoringu środowiska dokonuje się oceny oraz badań i obserwacji stanu gleby i ziemi, a uzyskane wyniki zamieszczane są w rejestrze. Generalny Dyrektor Ochrony Środowiska prowadzi rejestr, który zawiera między innymi wpisy potencjalnych historycznych zanieczyszczeniach powierzchni ziemi, w tym ich charakterystykę, miejsce i czas wystąpienia oraz aktualny status terenu, przeprowadzone remediacje oraz osiągnięty w ich wyniku efekt ekologiczny. Bezpośredni dostęp do wszystkich danych zawartych w rejestrze posiadają za pośrednictwem systemu teleinformatycznego organy ochrony środowiska oraz organy Inspekcji Ochrony Środowiska⁷². Minister właściwy do spraw środowiska w porozumieniu z ministrem właściwym do spraw zdrowia, kierując się potrzebą ujednoczenia sposobu wykonywania oceny występowania zagrożenia dla zdrowia ludzi lub stanu środowiska, może określić, w drodze rozporządzenia, sposób wykonywania oceny występowania znaczącego zagrożenia dla zdrowia ludzi lub stanu środowiska oraz referencyjne metodyki modelowania rozprzestrzeniania substancji w glebie, ziemi i wodach gruntowych⁷³.

W zakresie terenów zagrożonych ruchami masowymi ziemi oraz terenów, na których występują te ruchy, a także rejestr zawierający informacje o tych terenach zadanie wykonuje starosta, natomiast minister właściwy do spraw środowiska w porozumieniu z ministrem właściwym do spraw rolnictwa oraz ministrem właściwym do spraw budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa określi, w drodze rozporządzenia metody, zakres i częstotliwość prowadzenia obserwacji terenów i sposób ustalania tych terenów, kierując się potrzebą ograniczenia występowania szkód powodowanych przez ruchy masowe ziemi⁷⁴.

⁷² Art. 101 pkt. a–c ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (tekst jedn.: Dz. U. z 2017 r. poz. 519 z późn. zm.).

⁷³ Tamże, art. 101 ust. 1.

⁷⁴ Tamże, art. 110a.

Kolejną kwestią poruszoną w ustawie są instrumenty prawne służące przeciwdziałaniu poważnej awarii przemysłowej. Dotyczy to zakładów stwarzających zagrożenie wystąpienia poważnej awarii przemysłowej o zwiększonym lub dużym ryzyku wystąpienia awarii⁷⁵. Osoby, które zamierzają utworzyć bądź prowadzą zakłady o zwiększonym ryzyku lub o dużym ryzyku, są zobowiązani do zapewnienia, aby zakład został zaprojektowany w sposób, który uchroni środowisko przed skutkami awarii. Prowadzący zakład jest zobowiązany do zgłoszenia zakładu właściwemu organowi Państwowej Straży Pożarnej, co najmniej 30 dni przed uruchomieniem lub 3 miesiące od dnia zaliczenia istniejącego zakładu do zakładu o zwiększonym ryzyku lub dużym ryzyku. Każdą istotną zmianę ilości lub rodzaju substancji niebezpiecznej albo jej charakterystyki fizykochemicznej, pożarowej i toksycznej, zmianę technologii lub profilu produkcji oraz zmianę, która mogłaby mieć poważne skutki związane z ryzykiem awarii, w stosunku do danych zawartych w zgłoszeniu, zgłasza się właściwemu organowi Państwowej Straży Pożarnej w terminie co najmniej 30 dni przed dniem jej wprowadzenia⁷⁶. Prowadzący zakład o zwiększonym ryzyku lub zakład o dużym ryzyku sporządza program zapobiegania poważnym awariom przemysłowym, zwany dalej „programem zapobiegania awariom”⁷⁷, a także jest zobowiązany do opracowania i wdrożenia systemu zarządzania bezpieczeństwem, gwarantującego odpowiedni do zagrożeń poziom ochrony ludzi i środowiska. System zarządzania bezpieczeństwem uwzględnia zagrożenia awariami przemysłowymi i złożoność organizacji w zakładzie oraz jest oparty na ocenie ryzyka⁷⁸.

Prowadzący zakład o dużym ryzyku jest obowiązany do opracowania raportu o bezpieczeństwie i przedłożenia komendantowi wojewódzkiemu Państwowej Straży Pożarnej i wojewódzkiemu inspektorowi ochrony środowiska przestrzennego⁷⁹. Natomiast w celu zapobiegania, zwalczania i ograniczania skutków awarii przemysłowej opracowuje się wewnętrzny i zewnętrzny plan operacyjno-ratowniczy. Minister właściwy do spraw wewnętrznych w porozumieniu z ministrem właściwym do spraw gospodarki, ministrem właściwym do spraw środowiska, ministrem właściwym do spraw administracji publicznej oraz Ministrem Obrony Narodowej zobowiązani zostali do określenia w drodze rozporządzenia wymagań, jakim powinny odpowiadać wewnętrzne i zewnętrzne plany operacyjno-ratownicze, kierując się potrzebą zapewnienia jednolitych zasad planowania ratowniczego⁸⁰.

⁷⁵ Tamże, art. 249.

⁷⁶ Tamże, art. 250.

⁷⁷ Tamże, art. 251.

⁷⁸ Tamże, art. 252.

⁷⁹ Tamże, art. 254.

⁸⁰ Tamże, art. 260.

1.5. Ustawa o Państwowej Inspekcji Sanitarnej⁸¹

W ustawie o Państwowej Inspekcji Sanitarnej przedstawiono proces działania organu w obszarze zapobiegania i zwalczania chorób, który uwzględnia się w planowaniu cywilnym. Państwowa Inspekcja Sanitarna wykonuje zadania w zakresie zapobiegania i zwalczania chorób zakaźnych i innych chorób powodowanych warunkami środowiska, a także na prowadzeniu działalności oświatowo-zdrowotnej⁸². Dokument wprowadza obowiązek planowania pracy Państwowej Inspekcji Sanitarnej w oparciu o wyniki kontroli własnych i prowadzonych przez organy zewnętrzne. Do ważniejszych zadań należy zaliczyć:

- dokonywanie analizy i ocen epidemiologicznych,
- opracowywanie programów i planów działalności zapobiegawczej i przeciwepidemicznej,
- ustalanie zakresu i terminów szczepień ochronnych oraz sprawowanie nadzoru w tym zakresie,
- planowanie i organizowanie sanitarnych zabezpieczeń granic państwa,
- prowadzenie nadzoru nad ruchem pasażerskim i towarowym w morskich i lotniczych portach,
- udzielanie porad w zakresie spraw sanitarno-epidemiologicznych⁸³.

W akcie prawnym przedstawiono również dodatkowe działania Państwowej Inspekcji Sanitarnej w zakresie zapobiegania i zwalczania chorób, do których należą:

- wydawanie zarządzeń i decyzji lub występowanie do innych organów o ich wydanie,
- kierowanie akcją sanitarną przy masowych przemieszczeniach ludności, zjazdach i zgromadzeniach⁸⁴.

Do zadań Państwowej Inspekcji Sanitarnej należy również wydawanie opinii, co do zgodności z warunkami sanitarnymi określonymi przepisami Unii Europejskiej przedsięwzięć i zrealizowanych inwestycji, których realizacja jest wspomagana przez Agencję Restrukturyzacji i Modernizacji Rolnictwa ze środków pochodzących z funduszy Unii Europejskiej⁸⁵.

⁸¹ Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (tekst jedn.: Dz. U. z 2017 r. poz. 1261).

⁸² Art. 1 i 2 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (tekst jedn.: Dz. U. z 2017 r. poz. 1261).

⁸³ Tamże, art. 5.

⁸⁴ Tamże, art. 1, 2 i 5.

⁸⁵ Tamże, art. 6a.

1.6. Ustawa o finansach publicznych⁸⁶

Ustawa o finansach publicznych z dnia 27 sierpnia 2009 r. przedstawia przyjęte rozwiązania w celu wzmocnienia kontroli nad wydatkami publicznymi w jednostkach sektora finansów publicznych poprzez m.in. wprowadzenie kontroli zarządczej i audytu wewnętrznego⁸⁷.

Rozdział 6 działu I ustawy poświęcono właśnie kontroli zarządczej oraz jej koordynacji w jednostkach sektora finansów publicznych. W myśl zapisów ustawy kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy⁸⁸.

Celem kontroli zarządczej jest zarządzanie ryzykiem, w szczególności zapewnienie zgodności prowadzonej działalności z przepisami prawa oraz procedurami wewnętrznymi, skuteczności i efektywności działania, wiarygodności sprawozdań, ochrony zasobów, przestrzegania i promowania zasad etycznego postępowania, efektywności i skuteczności przepływu informacji, a także zarządzania ryzykiem⁸⁹.

Zapisy ustawy zobowiązują Ministra Finansów do określenia i ogłoszenia w formie komunikatu (publikowanego w Dzienniku Urzędowym Ministra Finansów) standardów kontroli zarządczej dla sektora finansów publicznych, zgodnych ze standardami międzynarodowymi. Kontrolę zarządczą w sektorze finansów publicznych stanowi szereg działań służących zapewnieniu realizacji celów i zadań w sposób jaki określił minister finansów. Określone zostały wytyczne w zakresie kontroli zarządczej dla sektora publicznego zgodnie z międzynarodowymi standardami. Należy również podkreślić, że zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej należy w przypadku jednostek samorządu terytorialnego do obowiązków: wójta, burmistrza, prezydenta miasta, przewodniczącego zarządu jednostki samorządu terytorialnego⁹⁰.

⁸⁶ Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych. (tekst jedn.: Dz. U. z 2016 r. poz. 1870 z późn. zm.). Akt obowiązujący wersja od: 28 czerwca 2017 r.

⁸⁷ Art. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870 z późn. zm).

⁸⁸ Tamże, art. 68.

⁸⁹ Tamże.

⁹⁰ Art. 69 ust. 1 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870 z późn. zm).

2. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – ROZPORZĄDZENIA

Zarządzanie ryzykiem jest elementem procesu planowania cywilnego. Elementy tego procesu zostały zaimplementowane do polskiego prawa w 2009 r. w drodze nowelizacji ustawy o zarządzaniu kryzysowym. Nowela ustawy odnosiła się do dwu generalnych problemów. Pierwszy to uporządkowanie sfery ochrony infrastruktury krytycznej, natomiast drugi to uzupełnienie procesu planowania cywilnego o nowy dokument – Raport o zagrożeniach bezpieczeństwa narodowego, podkreślający strategiczny aspekt planowania. Przygotowując rozwiązania w tym zakresie, Rada Ministrów zwróciła uwagę właśnie na zarządzanie ryzykiem. Mimo tego nie wdrożono całego procesu, a odniesiono się przede wszystkim do kwestii oceny ryzyka. Oczywiście przed 2009 r. obowiązywały akty prawne odwołujące się do pojęcia ryzyka. Jednak tylko jeden z nich nawiązywał do problematyki zarządzania kryzysowego.

W ramach niniejszego rozdziału dokonano analizy wybranych przepisów powszechnie obowiązującego prawa krajowego, które nawiązują do kwestii zarządzania ryzykiem w zarządzaniu kryzysowym. Dlatego też do katalogu tych aktów prawnych zaliczono: rozporządzenie w sprawie planów ochrony infrastruktury krytycznej, rozporządzenie w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, rozporządzenie w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego, a także rozporządzenie w sprawie opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego.

2.1. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej¹

Rozporządzenie określa sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej (opracowywanych przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej). Dokument precyzuje warunki i tryb, w jakich uznawane jest

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

spełnienie obowiązku posiadania planu odpowiadającego wymogom określonym w Rozporządzeniu.

Dokument wskazuje, że plan powinien zawierać charakterystykę zagrożeń dla infrastruktury krytycznej oraz oceny ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń.

2.2. Rozporządzenie Rady Ministrów w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej²

W rozporządzeniu określono sposób współdziałania organów administracji publicznej i służb odpowiedzialnych za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, oraz innymi organami i służbami publicznymi³ w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej.

Zapisy rozporządzenia w zakresie tematyki badań wskazują, że ministrowie i kierownicy urzędów centralnych po otrzymaniu kryteriów (służących do wytypowania obiektów IK), przygotowują w zakresie swojej właściwości, i przedkładają dyrektorowi RCB informacje zawierające ogólną ocenę ryzyka dla funkcjonowania opisywanego obszaru zadaniowego, uwzględniając zagrożenia, podatności na zagrożenie oraz konsekwencje zakłócenia funkcjonowania infrastruktury krytycznej.

2.3. Rozporządzenie Rady Ministrów w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego⁴

Rozporządzenie określa sposób, tryb i terminy opracowania Raportu o zagrożeniach bezpieczeństwa narodowego oraz raportów częściowych ministrów, kierowników urzędów centralnych oraz wojewodów. Jego zapisy wskazują, że częścią raportów jest charakterystyka zagrożeń oraz skutków ich wystąpienia zobrażowana na mapie ryzyka. Szerzej na temat samej metodyki opracowania Raportu o zagrożeniach bezpieczeństwa narodowego oraz raportów częściowych w części V niniejszej publikacji.

² Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. z 2010 r. Nr 83, poz. 541).

³ Tamże, § 1.

⁴ Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. z 2010 r. Nr 83, poz. 540).

2.4. Rozporządzenie Ministra Środowiska, Ministra Transportu, Budownictwa i Gospodarki Morskiej, Ministra Administracji i Cyfryzacji oraz Ministra Spraw Wewnętrznych w sprawie opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego⁵

Pomimo zachodzących zmian systemowych i przekształceń ministerstw⁶, rozporządzenie z dnia 21 grudnia 2012 r. w sprawie opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego jest aktem obowiązującym.

Mapy zagrożenia powodziowego i mapy ryzyka powodziowego jako dokumenty planistyczne stanowią w praktyce nietechniczny środek ochrony przeciwpowodziowej mający na celu ograniczenie potencjalnych negatywnych konsekwencji powodzi. Głównym celem opracowania map zagrożenia powodziowego i map ryzyka powodziowego jest stworzenie podstaw do opracowania planów zarządzania ryzykiem powodziowym – ostatniego etapu wdrażania dyrektywy powodziowej⁷.

Upublicznienie tych map i informacji o obszarach zagrożonych powodzią i poziomie tego zagrożenia, stwarza skuteczne narzędzie pozyskiwania danych, ustanawiania priorytetów i podejmowania decyzji – o charakterze technicznym, finansowym i politycznym, dotyczących zarządzania ryzykiem powodziowym

⁵ 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 r., poz. 104).

⁶ Na mocy rozporządzeń Rady Ministrów z 20 listopada 2015 r., 3 grudnia 2015 r. i 7 grudnia 2015 r. dokonano następujących przekształceń:

1. na mocy przepisów obowiązujących od 16 listopada 2015 r.:
 - w miejsce Ministerstwa Administracji i Cyfryzacji (część jego komórek włączono do nowo utworzonego Ministerstwa Spraw Wewnętrznych i Administracji) utworzono Ministerstwo Cyfryzacji,
 - po wydzieleniu części komórek ze zlikwidowanego Ministerstwa Infrastruktury i Rozwoju oraz z Ministerstwa Rolnictwa i Rozwoju Wsi utworzono Ministerstwo Gospodarki Morskiej i Żeglugi Śródlądowej,
 - po wydzieleniu części komórek ze zlikwidowanego Ministerstwa Infrastruktury i Rozwoju utworzono Ministerstwo Infrastruktury i Budownictwa,
 - w miejsce Ministerstwa Gospodarki oraz Ministerstwa Infrastruktury i Rozwoju (część jego komórek włączono do nowo utworzonego Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej oraz do nowo utworzonego Ministerstwa Infrastruktury i Budownictwa) utworzono Ministerstwo Rozwoju,
 - w miejsce Ministerstwa Spraw Wewnętrznych, a także po wydzieleniu części komórek ze zlikwidowanego Ministerstwa Administracji i Cyfryzacji utworzono Ministerstwo Spraw Wewnętrznych i Administracji,
2. na mocy przepisów obowiązujących od 27 listopada 2015 r.:
 - po wydzieleniu części komórek z Ministerstwa Rozwoju utworzono Ministerstwo Energii,
 - z Ministerstwa Infrastruktury i Budownictwa wydzielono część komórek, które następnie włączono do Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej,
 - z Ministerstwa Cyfryzacji oraz z Ministerstwa Spraw Wewnętrznych i Administracji wydzielono część komórek, które następnie włączono do Ministerstwa Infrastruktury i Budownictwa.

⁷ Raport z wykonania map zagrożenia powodziowego i map ryzyka powodziowego, KZGW s. 115: <http://mapy.isok.gov.pl> [dostęp: sierpień 2017].

oraz stanowi podstawę do właściwego zarządzania ryzykiem jakie może stwarzać powódź dla życia i zdrowia ludzi, środowiska oraz gospodarki⁸.

Mapy zagrożenia powodziowego i mapy ryzyka powodziowego sporządzane są w oparciu o następujące akty prawne:

- Dyrektywę 2007/60/WE Parlamentu Europejskiego i Rady w sprawie oceny ryzyka powodziowego i zarządzania nim (dyrektywa powodziowa).
- Ustawę – Prawo wodne.
- Rozporządzenie Ministra Środowiska, Ministra Transportu, Budownictwa i Gospodarki Morskiej, Ministra administracji i Cyfryzacji oraz Ministra Spraw Wewnętrznych w sprawie opracowania map zagrożenia powodziowego oraz map ryzyka powodziowego.

Mapy zagrożenia powodziowego i mapy ryzyka powodziowego zostały opracowane w ramach projektu „Informatyczny System Osłony Kraju przed nadzwyczajnymi zagrożeniami” (ISOK) przez Instytut Meteorologii i Gospodarki Wodnej PIB – Centra Modelowania Powodzi i Suszy w Gdyni, Poznaniu, Krakowie i we Wrocławiu⁹. Szczegółowa metodyka opracowania dokumentów oraz harmonogram dotychczasowych prac przedstawiony został w części V niniejszej publikacji.

⁸ Tamże.

⁹ KZGW, Raport z wykonania map zagrożenia powodziowego i map ryzyka powodziowego, http://www.isok.gov.pl/dane/web_articles_files/2783/raport-z-wykonania-map-zagrozenia-powodziowego-i-map-ryzyka-powodziowego-v-1.01.pdf [dostęp: sierpień 2017].

3. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – PRZEPISY RESORTOWE

Zarządzanie ryzykiem polega na wprowadzeniu przez kierownictwo takiej kombinacji procesów oraz struktur, która umożliwi właściwy przepływ informacji, zarządzanie, kierowanie oraz monitorowanie działań w organizacji¹. Celem zarządzania ryzykiem w resorcie i urzędzie centralnym jest dopasowanie mechanizmów identyfikacji ryzyka określenie jego oddziaływania oraz dostosowanie do niego środków zapobiegawczych, tak aby zminimalizować zagrożenia stojące na przeszkodzie osiągnięciu zaplanowanego celu.

Analiza przepisów krajowego prawa resortowego związanego z zarządzaniem ryzykiem została przeprowadzona przede wszystkim na podstawie zarządzeń ustanowionych przez resorty z wyłączeniem Ministerstwa Obrony Narodowej. Przepis nakazujący realizowanie zadań dotyczących zarządzania ryzykiem wprowadzony został w ustawie o finansach publicznych z dnia 27 sierpnia 2009 roku². Jednak przepisy te nie precyzują, w jaki sposób analiza ryzyka powinna być prowadzona oraz jaki powinien być jej zakres. Dlatego też resorty wprowadziły tę praktykę na własnych zasadach.

W serwisie prawniczym „LexPolonica” zawierającym bazę aktów wszystkich resortów wyszukano akty prawne, które w swojej treści zawierały hasło „zarządzanie ryzykiem”. Wyniki wyszukiwania tych aktów objęły zarządzenia uchwalone przez:

- Ministra Spraw Zagranicznych,
- Ministra Administracji i Cyfryzacji³,
- Ministra Spraw Wewnętrznych i Administracji⁴,

¹ *Zarządzanie ryzykiem w sektorze publicznym – Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce*, wyd. Bentley Dennison, Warszawa 2007, s. 4.

² Rozdział 6 ustawy o finansach publicznych z dnia 27 sierpnia 2009 r. (Dz. U. z 2009 r. Nr 157, poz. 1240 z późn. zm.).

³ Na mocy przepisów obowiązujących od 16 listopada 2015 r. w miejsce Ministerstwa Administracji i Cyfryzacji (część jego komórek włączono do nowo utworzonego Ministerstwa Spraw Wewnętrznych i Administracji) utworzono Ministerstwo Cyfryzacji.

⁴ Na mocy przepisów obowiązujących od 16 listopada 2015 r. w miejsce Ministerstwa Spraw Wewnętrznych, a także po wydzieleniu części komórek ze zlikwidowanego Ministerstwa Administracji i Cyfryzacji utworzono Ministerstwo Spraw Wewnętrznych i Administracji.

- Ministra Cyfryzacji,
- Ministra Infrastruktury i Budownictwa,
- Ministra Rozwoju i Finansów,
- Wyższy Urząd Górniczy.

3.1. Zarządzenie Ministra Spraw Zagranicznych w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych⁵

Celem ustanowienia zasad zarządzania ryzykiem jest zapewnienie mechanizmów identyfikowania ryzyk, określania ich oddziaływania, prawdopodobieństwa i istotności⁶ oraz podejmowanie adekwatnych działań zapobiegawczych w celu minimalizacji ryzyka. Przestrzeganie tych zasad powinno przyczynić się do poprawy efektywności i skuteczności realizacji celów i zadań ministra. W Ministerstwie Spraw Zagranicznych zostały zdefiniowane cztery cele zarządzania:

- zwiększenie prawdopodobieństwa realizacji założonych celów i zadań,
- poprawa efektywności wykorzystania istniejących zasobów,
- podniesienie świadomości podejmowanych decyzji i związanego z tym ryzyka,
- podniesienie jakości realizowanych zadań.

Utworzony został komitet do spraw zarządzania ryzykiem, którego zadaniem jest dokonywanie analizy i akceptacji wykazu ryzyk, planowanych działań zapobiegawczych oraz przygotowywanie informacji na temat procesu zarządzania ryzykiem w ministerstwie. Analiza i akceptacja ryzyka polega na określeniu poziomu ryzyka i na tej podstawie jego akceptowalności, a następnie przyjęciu sposobu działań zapobiegawczych w przypadku ryzyka nieakceptowanego. Ryzyko może zostać określone jako:

- ryzyko małe – akceptowalne,
- ryzyko średnie – nieakceptowalne, może wywierać istotny wpływ na działalność ministerstwa,
- ryzyko wysokie – ryzyko nieakceptowalne, stanowi zagrożenie dla działalności ministerstwa⁷.

⁵ Zarządzenie Nr 27 Ministra Spraw Zagranicznych z dnia 26 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych (Dz. Urz. MSZ 34).

⁶ Istotność ryzyka – należy przez to rozumieć wynik oceny prawdopodobieństwa wystąpienia i oddziaływania ryzyka. Źródło: § 2 zarządzenia Nr 27 Ministra Spraw Zagranicznych z dnia 26 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych (Dz. Urz. MSZ poz. 34).

⁷ § 5 zarządzenia Nr 27 Ministra Spraw Zagranicznych z dnia 26 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych (Dz. Urz. MSZ poz. 34).

Drugim ważnym elementem w zarządzaniu ryzykiem jest monitoring realizowany w ramach kontroli zarządczej na każdym szczeblu zarządzania w ministerstwie i w placówkach zagranicznych. Proces ten jest ciągły i obejmuje:

- wykonanie przeglądu ryzyk w celu określenia, czy ryzyko uległo zmianie,
- sprawdzenie, czy punktowa ocena wagi ryzyka jest wciąż odpowiednia,
- zapewnienie skuteczności dotychczasowych mechanizmów kontrolnych,
- monitorowanie rozwoju uzgodnionych działań w zakresie zarządzania ryzykiem⁸.

3.2. Zarządzenie Ministra Administracji i Cyfryzacji w sprawie powołania Zespołu do spraw zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji⁹

W drodze przekształcenia Ministerstwa Administracji i Cyfryzacji utworzono Ministerstwo Spraw Wewnętrznych i Administracji (powołane Rozporządzeniem Rady Ministrów z dnia 20 listopada 2015 r.) oraz Ministerstwo Cyfryzacji.

Ministerstwo Spraw Wewnętrznych i Administracji utworzono w drodze przekształcenia dotychczasowego Ministerstwa Spraw Wewnętrznych. Przekształcenie, o którym mowa, polegało na włączeniu do dotychczasowego Ministerstwa Spraw Wewnętrznych, obsługującego dział sprawy wewnętrzne, komórek organizacyjnych dotychczasowego Ministerstwa Administracji i Cyfryzacji zajmujących się sprawami działów administracja publiczna i wyznania religijne oraz mniejszości narodowe i etniczne.

Ministerstwo Cyfryzacji powstało na mocy rozporządzenia Rady Ministrów z dnia 7 grudnia 2015 roku (w drodze przekształcenia dotychczasowego Ministerstwa Administracji i Cyfryzacji). Zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 9 grudnia 2015 r. Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja.

Pomimo tych zmian, Zarządzenie nr 4 Ministra Administracji i Cyfryzacji z dnia 25 stycznia 2013 r. w sprawie powołania Zespołu do spraw zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji ma status aktu obowiązującego.

W przypadku Ministerstwa Cyfryzacji utworzony został Zespół do spraw zarządzania ryzykiem. Paragraf drugi zarządzenia zawiera skład zespołu do zarządzania ryzykiem, a paragraf trzeci zadania, jakie należą do jego obowiązków:

- opracowanie polityki zarządzania ryzykiem w Ministerstwie, w szczególności poprzez opracowanie schematu odpowiedzialności i przypisanie

⁸ Tamże, § 12, § 13 i § 16.

⁹ Zarządzenie Nr 4 Ministra Administracji i Cyfryzacji z dnia 25 stycznia 2013 r. w sprawie powołania Zespołu do spraw zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji (Dz. Urz. MAiC poz. 4).

odpowiedzialności za realizację wyodrębnionych procesów poszczególnym komórkom organizacyjnym lub osobom,

- opracowanie metodyki zarządzania ryzykiem w Ministerstwie:
 - wskazanie źródeł i wysokości środków koniecznych do zmniejszenia ryzyka,
 - dokonanie oceny skuteczności wdrożenia i optymalizacji strategii,
 - identyfikacja, aktualizacja lub opracowanie wewnętrznych procedur dotyczących zarządzania ryzykiem,
 - informowanie Ministra Administracji i Cyfryzacji¹⁰.

3.3. Zarządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie systemu kontroli zarządczej w działach administracji rządowej – administracja publiczna, sprawy wewnętrzne, wyznania religijne oraz mniejszości narodowe i etniczne¹¹

Zarządzenie Nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r.¹² w sprawie systemu kontroli zarządczej w działach administracji rządowej – administracja publiczna, sprawy wewnętrzne, wyznania religijne oraz mniejszości narodowe i etniczne ustanawia obowiązek wykonywania kontroli zarządczej w tych działach.

Zarządzenie wskazuje zakres zadań dla członków kierownictwa ministerstwa, które sprawuje nadzór nad funkcjonowaniem adekwatnej, skutecznej i efektywnej kontroli zarządczej w komórkach organizacyjnych oraz w jednostkach. Natomiast kierownicy komórek organizacyjnych ministerstwa oraz kierownicy jednostek zapewniają funkcjonowanie adekwatnej, skutecznej i efektywnej kontroli zarządczej w jednostkach, którymi kierują, w oparciu o standardy kontroli zarządczej dla sektora finansów publicznych oraz niniejszego zarządzenia¹³.

Zarządzenie opisuje proces zarządzania ryzykiem jako proces ciągły, wykonywany stale w odniesieniu do wszystkich celów i zadań i obejmujący swym zakresem identyfikację i ocenę ryzyka, postępowanie z ryzykiem oraz jego monitorowanie i raportowanie.

Dokumentowanie procesu zarządzania ryzykiem dla realizowanych celów i zadań wynika z planu działalności ministra i odbywa się na podstawie wytycznych

¹⁰ Tamże.

¹¹ Zarządzenie Nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w działach administracji rządowej - administracja publiczna, sprawy wewnętrzne, wyznania religijne oraz mniejszości narodowe i etniczne (Dz. Urz. MSWiA poz. 16).

¹² Minister Spraw Wewnętrznych i Administracji jest naczelnym organem administracji publicznej, któremu obsługę zapewnia Ministerstwo Spraw Wewnętrznych i Administracji będące jednostką budżetową. Ministerstwo Spraw Wewnętrznych i Administracji zostało powołane rozporządzeniem Rady Ministrów z dnia 20 listopada 2015 r. w sprawie utworzenia Ministerstwa Spraw Wewnętrznych i Administracji.

¹³ § 4 zarządzenia Nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w działach administracji rządowej - administracja publiczna, sprawy wewnętrzne, wyznania religijne oraz mniejszości narodowe i etniczne (Dz. Urz. MSWiA z 2016 r. poz. 16).

zawartych w powyżej omawianym zarządzeniu, dołączonych w postaci załączników wraz z metodologią¹⁴.

Proces zarządzania ryzykiem jest dokumentowany w formie:

- arkusza analizy ryzyka,
- planu postępowania z ryzykiem,
- rejestru ryzyk.

Właściwie skonstruowany, kompleksowy rejestr ryzyka służy jako podstawowe narzędzie oceny ryzyka i może dostarczyć kompleksowej informacji potrzebnej do zarządzania ryzykiem. Dostęp do kompleksowej informacji o ryzyku zwiększa skuteczność zarządzania nim i wpływa na efektywność kontroli zarządczej.

Warunkiem koniecznym jest, aby z działaniami związanymi z zarządzaniem ryzykiem w jednostce ustanowiono mechanizmy umożliwiające monitorowanie wdrożonych rozwiązań i dokonywanie oceny ich efektywności. Ponadto, aby zarządzanie ryzykiem funkcjonowało efektywnie i wspierało podejmowane działania, należy systematycznie raportować ocenę ryzyka i poziom realizacji planu postępowania z nim. Należy również z wykorzystaniem określonych mierników i wskaźników weryfikować, w jakim stopniu system zarządzania ryzykiem spełnia założone cele, a także okresowo przeglądać zasady zarządzania ryzykiem pod względem aktualności, adekwatności i efektywności w stosunku do zmian w organizacji i jej otoczeniu.

Metodologia zarządzania ryzykiem w ministerstwie została szczegółowo przedstawiona w części V niniejszej publikacji.

3.4. Zarządzenie Ministra Cyfryzacji w sprawie systemu kontroli zarządczej w dziale administracji rządowej – informatyzacja¹⁵

Zarządzenie określa zasady wykonywania kontroli zarządczej w dziale administracji rządowej – informatyzacja. Chociaż akt prawny nie zawiera bezpośrednio odniesień do zarządzania ryzykiem, to w informacji o poziomie realizacji celów, zadań i mierników uwzględniono informacje o zagrożeniach i działaniach zapobiegawczych. Realizowane zadania polegają między innymi na identyfikowaniu i szacowaniu potencjalnego ryzyka w ramach działalności ministerstwa poprzez prowadzenie analiz ryzyka oraz czynności doradcze¹⁶.

W ramach kontroli zarządczej w dziale administracji rządowej – informatyzacja, podejmowane są działania polegające na wprowadzaniu rozwiązań zarządczych, ocenianiu funkcjonowania rozwiązań zarządczych, usystematyzowaniu i udoskonaleniu bądź zintegrowaniu stosowanych metod, mechanizmów lub procedur w celu

¹⁴ Tamże, § 11.

¹⁵ Zarządzenie Nr 45 Ministra Cyfryzacji z dnia 29 listopada 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej - informatyzacja (Dz. Urz. MC poz. 52).

¹⁶ Zarządzenie Nr 9 Ministra Cyfryzacji z dnia 5 kwietnia 2016 r. w sprawie Karty Audytu Wewnętrzno w Ministerstwie Cyfryzacji (Dz. Urz. MC poz. 9).

zapewnienia ich przyszłej skuteczności organizacyjnej i ekonomicznej, monitorowania i sprawozdawczości¹⁷. W ministerstwie działa Zespół Audytu Wewnętrznego, a także utworzone zostało stanowisko koordynatora do spraw kontroli zarządczej. Koordynator do spraw kontroli zarządczej realizuje zadania w zakresie przygotowania projektu planu działalności, oceny adekwatności mierników, zadań i celów określonych w planie działalności, a także sporządza projekty oświadczenia o stanie kontroli zarządczej oraz projekt sprawozdania z wykonania planu działalności¹⁸. Natomiast Zespół Audytu Wewnętrznego¹⁹ przeprowadza systematyczną ocenę w szczególności adekwatności, skuteczności i efektywności kontroli zarządczej w ramach prowadzonych w ministerstwie zadań audytowych oraz czynności doradczych²⁰. Zarządzeniem Nr 9 Ministra Cyfryzacji z dnia 5 kwietnia 2016 r. w sprawie Karty Audytu Wewnętrznego w Ministerstwie Cyfryzacji (Dz. Urz. MC poz. 9) minister określił cele i zasady audytu wewnętrznego, rozumianego jako systematyczną ocenę kontroli zarządczej oraz czynności doradczych. Realizowane zadania między innymi polegają na identyfikowaniu i szacowaniu potencjalnego ryzyka mogącego się pojawiać w ramach działalności ministerstwa przez przeprowadzanie analizy ryzyka i czynności doradczych²¹.

3.5. Zarządzenie Ministra Infrastruktury i Budownictwa w sprawie ustalenia opisu systemu kontroli zarządczej w Ministerstwie Infrastruktury i Budownictwa²²

Zarządzenie zawiera szczegółowe wytyczne w zakresie kontroli zarządczej dla Ministerstwa Infrastruktury i Budownictwa²³ oraz działów administracji rządowej

¹⁷ § 3 Zarządzenia Nr 45 Ministra Cyfryzacji z dnia 29 listopada 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej - informatyzacja (Dz. Urz. MC poz. 52).

¹⁸ Tamże, § 6.

¹⁹ Zarządzenie Nr 1 Ministra Cyfryzacji z dnia 12 stycznia 2016 r. w sprawie powołania Komitetu Audytu. (Dz. Urz. MC. poz. 1).

²⁰ § 7 zarządzenia Nr 45 Ministra Cyfryzacji z dnia 29 listopada 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej - informatyzacja (Dz. Urz. MC poz. 52).

²¹ Zarządzenie Nr 9 Ministra Cyfryzacji z dnia 5 kwietnia 2016 r. w sprawie Karty Audytu Wewnętrznego w Ministerstwie Cyfryzacji (Dz. Urz. MC poz. 9). Źródło: <http://e-dziennik.mc.gov.pl/#/legalact/2016/1>

²² Zarządzenie Nr 19 Ministra Infrastruktury i Budownictwa z dnia 16 czerwca 2016 r. w sprawie ustalenia opisu systemu kontroli zarządczej w Ministerstwie Infrastruktury i Budownictwa (Dz. Urz. MliB poz. 46).

²³ Ministerstwo Infrastruktury i Budownictwa – polski urząd administracji rządowej obsługujący ministra właściwego do spraw trzech działów administracji rządowej: budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, łączność i transport. Ministerstwo zostało utworzone 8 grudnia 2015 r. (z mocą obowiązującą od dnia 16 listopada 2015 r.) poprzez wydzielenie z dotychczasowego Ministerstwa Infrastruktury i Rozwoju komórek organizacyjnych i pracowników obsługujących sprawy dwóch działów: budownictwo, lokalne planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo (od 27 listopada 2015 r. budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo) i transport (Dz. U. z 2015 r. poz. 2080). Zgodnie z przepisami

– budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, łączność i transport. Kontrola zarządcza w ministerstwie obejmuje ogół działań podejmowanych przez członków kierownictwa ministerstwa oraz komórki organizacyjne we wszystkich rodzajach ich aktywności, które są konieczne dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Akt prawny zawiera podstawowe definicje odnoszące się do ryzyka, a za proces zarządzania ryzykiem i koordynację zadań odpowiedzialny jest koordynator kontroli zarządczej²⁴.

Rozdział 5 aktu prawnego szczegółowo określa rolę i zadania, które należy podjąć w procesie identyfikacji i analizy ryzyka w oparciu o projekt planu działalności ministra. W ministerstwie wyodrębniono następujące ryzyka:

- związane ze zmianami zachodzącymi w ministerstwie i jego otoczeniu,
- związane z systemami informatycznymi,
- o charakterze finansowym, w tym ryzyka nadużyć finansowych oraz korupcji,
- zagrażające wizerunkowi ministerstwa jako urzędu administracji publicznej sprawnego i przyjaznego obywatelom,
- związane z procesem decyzyjnym w Unii Europejskiej.

Opisana metodyka przybliży metody identyfikacji ryzyka, określa jego wpływ na realizację celów i zadań, prawdopodobieństwo jego wystąpienia oraz wskazuje podjęcie działań zapobiegawczych.

Do szacowania prawdopodobieństwa wystąpienia ryzyka oraz szacowania jego wpływu na realizację celów ministerstwa stosuje się 5 stopniową skalę oceny. Zidentyfikowane ryzyko o istotności od 1 do 9 punktów jest ryzykiem akceptowalnym, co oznacza brak obowiązku podejmowania działań ograniczających jego istotność. Natomiast ryzyko o istotności od 10 do 25 punktów jest ryzykiem kluczowym, wymagającym zaplanowania i podjęcia dodatkowych działań. Rezultatem jest sporządzony rejestr ryzyk, który jest brany pod uwagę podczas aktualizacji czy też tworzenia nowych planów²⁵.

obowiązującymi od 27 listopada 2015 r. do ministerstwa włączono również komórki organizacyjne i pracowników Ministerstwa Cyfryzacji obsługujących dział łączność oraz komórki organizacyjne i pracowników Ministerstwa Spraw Wewnętrznych i Administracji obsługujących sprawy z zakresu geodezji i kartografii (przekazane 27 listopada 2015 r. z działu administracja publiczna do działu budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo (Dz. U. z 2015 r. poz. 1960).

²⁴ § 1–4 zarządzenia Nr 19 Ministra Infrastruktury i Budownictwa z dnia 16 czerwca 2016 r. w sprawie ustalenia opisu systemu kontroli zarządczej w Ministerstwie Infrastruktury i Budownictwa (Dz. Urz. MliB z 2016 r. poz. 46).

²⁵ Tamże, § 7–12.

3.6. Komunikat w sprawie szczegółowych wytycznych w zakresie kontroli zarządczej dla Ministerstwa Infrastruktury i Budownictwa oraz działów administracji rządowej – budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, łączność, transport²⁶

Uzupełnieniem Zarządzenia Nr 19 Ministra Infrastruktury i Budownictwa z dnia 16 czerwca 2016 r. w sprawie ustalenia opisu systemu kontroli zarządczej w Ministerstwie Infrastruktury i Budownictwa jest Komunikat z dnia 16 czerwca 2016 r. w sprawie szczegółowych wytycznych w zakresie kontroli zarządczej dla Ministerstwa Infrastruktury i Budownictwa oraz działów administracji rządowej – budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, łączność, transport.

Komunikat ustanawia standardy kontroli zarządczej w jednostce, które wyznacza zbiór procedur i wytycznych odnoszących się do definiowania celów i zadań oraz monitorowania ich realizacji. Standardy odpowiadają poszczególnym elementom kontroli zarządczej w zakresie²⁷:

- środowisko wewnętrzne,
- cele i zarządzanie ryzykiem,
- mechanizmy kontroli,
- informacja i komunikacja,
- monitorowanie i ocena.

W ramach wdrożonego standardu: cele i zarządzanie ryzykiem zaleca się, aby w jednostce została wdrożona procedura zarządzania ryzykiem, która poprawi zarządzanie we wszystkich obszarach jej działalności oraz ograniczy ewentualne negatywne skutki zdarzeń do akceptowalnego poziomu, w szczególności w zakresie skutecznego i efektywnego zarządzania zasobami, zapewnienia ochrony majątku i efektywności finansowej oraz ochrony wizerunku jednostki. System celów i zarządzania ryzykiem zdefiniowano jako:

- określenie misji jednostki,
- określenie celów i zadań oraz monitorowanie i ocenę ich realizacji,
- identyfikację ryzyka,
- analizę ryzyka,
- określenie reakcji na ryzyko.

Każde istotne *ryzyko* należy ocenić pod kątem prawdopodobieństwa jego wystąpienia oraz jego możliwych skutków. Należy także określić rodzaj reakcji na *ryzyko*

²⁶ Komunikat Ministra Infrastruktury i Budownictwa z dnia 16 czerwca 2016 r. w sprawie szczegółowych wytycznych w zakresie kontroli zarządczej dla Ministerstwa Infrastruktury i Budownictwa oraz działów administracji rządowej - budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, łączność, transport (Dz. Urz. MliB poz. 45).

²⁷ Tamże, § 6.

oraz zaplanować działania, które powinny zostać podjęte w celu zmniejszenia danego *ryzyka* do akceptowalnego poziomu. W obszarze standardu mechanizmy kontroli oraz system kontroli powinny być adekwatne do potrzeb danej jednostki i efektywne, tj. powinny skutecznie ograniczać dane *ryzyko* przy minimalizowaniu kosztów²⁸. Zaleca się również przeprowadzanie samooceny systemu kontroli zarządczej przez osoby kierujące komórkami organizacyjnymi jednostki i wyznaczonych pracowników, która umożliwi identyfikację *ryzyk* w funkcjonowaniu istniejącego systemu²⁹.

3.7. Zarządzenie Ministra Rozwoju i Finansów³⁰ w sprawie kontroli zarządczej w Ministerstwie Rozwoju³¹

Zarządzenie określa sposób wykonywania kontroli zarządczej w Ministerstwie Rozwoju³², w tym: zakres odpowiedzialności, misję i cele strategiczne *ministerstwa*, plan działalności ministra, zarządzanie ryzykiem, monitorowanie stopnia realizacji celów i zadań, monitorowanie i samoocenę *kontroli zarządczej oraz sprawozdawczość*. Aby wypełnić kryteria kontroli zarządczej ustalone zostały procedury i wytyczne odnoszące się do wyznaczania celów oraz zadań – w tym monitorowania ich realizacji w zakresie środowiska wewnętrznego, celów i zarządzania ryzykiem, mechanizmów kontroli, informacji i komunikacji, monitorowania i oceny³³.

Kontrola zarządcza w ministerstwie jest dokumentowana w postaci wewnętrznych aktów normatywnych, procedur wewnętrznych, regulaminów, instrukcji, wytycznych, dokumentów określających zakres obowiązków, uprawnień i odpowiedzialności pracowników. Za zapewnienie adekwatnej, skutecznej i efektywnej kontroli

²⁸ Tamże, § 8.

²⁹ Tamże, § 11.

³⁰ Rozporządzenie Prezesa Rady Ministrów z dnia 30 września 2016 r. w sprawie szczegółowego zakresu działania Ministra Rozwoju i Finansów (Dz. U. poz. 1595). Zarządzenie Ministra Rozwoju i Finansów z dnia 3 marca 2017 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Finansów (Dz. Urz. MRiF poz. 46, z późn. zm.). Ministerstwo Finansów zapewnia obsługę Ministra Rozwoju i Finansów, zwanego dalej „Ministrem”, w zakresie zadań określonych w przepisach odrębnych i innych dokumentach dla ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych oraz ogólnie dla ministra i Ministra, jako organu administracji rządowej. Zarządzenie Ministra Rozwoju i Finansów z dnia 3 marca 2017 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Finansów (Dz. Urz. MRiF poz. 46, z późn. zm.).

³¹ Zarządzenie Ministra Rozwoju i Finansów z dnia 21 grudnia 2016 r. w sprawie kontroli zarządczej w Ministerstwie Rozwoju (Dz. Urz. MRiF poz. 33).

³² Ministerstwo Rozwoju jest urzędem administracji rządowej zapewniającym obsługę Ministra Rozwoju i Finansów w zakresie działów administracji rządowej: gospodarka oraz rozwój regionalny. Ministerstwo powstało na mocy rozporządzenia Rady Ministrów z dnia 7 grudnia 2015 r. w sprawie utworzenia Ministerstwa Rozwoju oraz zniesienia Ministerstwa Gospodarki. Aktem prawnym, który określa zakres kompetencji Ministra Rozwoju i Finansów jest Rozporządzenie Prezesa Rady Ministrów z dnia 30 września 2016 r. w sprawie szczegółowego zakresu działania Ministra Rozwoju i Finansów; Źródło: <http://mr.bip.gov.pl/informacje-o-ministerstwie.html> [dostęp: sierpień 2017].

³³ § 4 zarządzenia Ministra Rozwoju i Finansów z dnia 21 grudnia 2016 r. w sprawie kontroli zarządczej w Ministerstwie Rozwoju (Dz. Urz. MRiF poz. 33).

zarządczej w ministerstwie oraz w nadzorowanych w nim działach odpowiedzialny jest minister, a członkowie kierownictwa ministerstwa nadzorują funkcjonowanie kontroli zarządczej w komórkach organizacyjnych ministerstwa i jednostkach podległych, wobec których wykonują czynności nadzorcze. Za koordynację procesu zarządzania ryzykiem w ministerstwie odpowiedzialne jest Biuro Kontroli. Ponadto w ministerstwie powołany jest Zespół do spraw Zarządzania Ryzykiem i Samooceny. Zarządzenie zawiera podstawowe definicje określające między innymi:

- istotność ryzyka, rozumianą jako punktową ocenę ryzyka wyliczaną jako iloczyn prawdopodobieństwa wystąpienia danego ryzyka i jego wpływu na realizację celów i zadań określonych w planie działalności ministra lub celów i zadań komórki organizacyjnej ministerstwa;
- ryzyko, czyli możliwość wystąpienia zdarzenia, które będzie miało negatywny wpływ na realizację celów i zadań określonych w planie działalności ministra lub celów i zadań komórki organizacyjnej ministerstwa;
- ryzyko kluczowe, mogące spowodować niezrealizowanie celów i zadań określonych w planie działalności ministra lub celów i zadań komórki organizacyjnej ministerstwa, którego istotność przyjmuje wartość od 16 do 25 punktów;
- właściciela ryzyka, wskazaną przez kierującego komórką organizacyjną ministerstwa komórkę wewnętrzną bezpośrednio zarządzającą ryzykiem, w tym odpowiedzialną za podjęcie działań, jeżeli poziom istotności ryzyka przekracza poziom akceptowalny³⁴.

W procesie identyfikacji i analizy ryzyk wykorzystuje się wszelkie dostępne źródła informacji, w szczególności ustalenia wewnętrznych i zewnętrznych audytów i kontroli oraz wyniki samooceny dokonywanej przez komórki organizacyjne ministerstwa. W procesie identyfikacji ryzyk w ministerstwie wyróżniono ryzyka:

- związane ze zmianami zachodzącymi w ministerstwie lub jego otoczeniu,
- związane z systemami teleinformatycznymi,
- o charakterze finansowym, w tym ryzyka nadużyć finansowych oraz korupcji,
- zagrażające wizerunkowi ministerstwa,
- związane z procesem decyzyjnym w Unii Europejskiej,
- dotyczące środowiska prawnego, w tym zmian legislacyjnych.

Metodyka zarządzania ryzykiem w ministerstwie określa także zakres podejmowanych działań w przypadku zidentyfikowanego ryzyka, jego wpływ na realizację celów i zadań oraz prawdopodobieństwo jego wystąpienia, a także wskazuje jak zaplanować działania zaradcze. Efektem tych działań jest Rejestr ryzyk kluczowych w Ministerstwie Rozwoju³⁵.

³⁴ Tamże, § 2.

³⁵ Tamże, § 6–13.

Integralną część zarządzenia stanowią wzory dokumentów w formie załączników:

- schemat organizacji kontroli zarządczej w Ministerstwie Rozwoju,
- sposób szacowania prawdopodobieństwa wystąpienia ryzyka oraz wpływu zidentyfikowanego ryzyka na realizację celów i zadań określonych w planie działalności Ministra Rozwoju i Finansów,
- rejestr ryzyk kluczowych,
- ocena stanu kontroli zarządczej.

3.8. Zarządzenie Ministra Rozwoju i Finansów³⁶ w sprawie systemu kontroli zarządczej w Ministerstwie Finansów³⁷

Zarządzenie określa zasady i tryb funkcjonowania systemu kontroli zarządczej, który obejmuje wyznaczanie celów w odniesieniu do planu działalności Ministerstwa Finansów.

Nadzór nad funkcjonowaniem systemu kontroli zarządczej w ministerstwie sprawuje Dyrektor Generalny przy pomocy komórek organizacyjnych. Odbyna się on w porozumieniu z Szefem Krajowej Administracji Skarbowej i dotyczy komórek organizacyjnych będących jednostkami organizacyjnymi Krajowej Administracji Skarbowej³⁸. Akt prawny odnosi się do systemu kontroli zarządczej, a także określa planowanie działalności i zarządzanie ryzykiem.

System kontroli zarządczej w ministerstwie obejmuje w szczególności:

- wyznaczanie celów do planu działalności ministerstwa, mierników określających stopień realizacji celów i zadań służących ich osiągnięciu,
- zarządzanie ryzykiem w ministerstwie,
- monitorowanie funkcjonowania systemu kontroli zarządczej, w szczególności sporządzanie sprawozdań z wykonania planu działalności ministerstwa,
- kontrolę i audyt,
- zarządzanie portfelem programów i projektów,
- zarządzanie bezpieczeństwem informacji,
- politykę antykorupcyjną,
- zarządzanie ciągłością działania,
- zarządzanie finansami,

³⁶ Minister Rozwoju i Finansów kieruje działami administracji rządowej – budżet, finanse publiczne oraz instytucje finansowe, na podstawie § 1 ust. 2 pkt 1, 2 i 4 rozporządzenia Prezesa Rady Ministrów z dnia 30 września 2016 r. w sprawie szczegółowego zakresu działania Ministra Rozwoju i Finansów (Dz. U. poz. 1595).

³⁷ Zarządzenie Ministra Rozwoju i Finansów z dnia 8 czerwca 2017 r. w sprawie systemu kontroli zarządczej w Ministerstwie Finansów (Dz. Urz. MRiF poz. 116).

³⁸ Tamże, § 4.

- zarządzanie zasobami ludzkimi,
- dokonywanie oceny systemu kontroli zarządczej, w tym sporządzanie oświadczenia o stanie kontroli zarządczej w ministerstwie,
- zapewnianie członkom kierownictwa informacji o stanie kontroli zarządczej w ministerstwie³⁹.

Na podstawie propozycji celów wyznaczonych do realizacji na dany rok dyrektorzy komórek organizacyjnych, w porozumieniu z nadzorującymi członkami kierownictwa, przygotowują i przekazują do BZK⁴⁰ do uzgodnienia w zakresie swojej właściwości projekty informacji o realizacji zadań i projektów oraz najważniejszych ryzykach mających wpływ na osiągnięcie celów⁴¹. Planowanie działalności i zarządzanie ryzykiem na poziomie ministerstwa obejmuje:

- cele komórek organizacyjnych na dany rok,
- mierniki stopnia realizacji celów,
- wartość bazową oraz planowane wartości mierników w kolejnych okresach sprawozdawczych,
- zadania i projekty służące realizacji każdego z celów⁴².

Komórki organizacyjne zarządzają ryzykiem w odniesieniu do celów, zadań i projektów określonych w planie działalności ministerstwa⁴³.

3.9. Rozporządzenie Ministra Rozwoju i Finansów⁴⁴ w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach⁴⁵

Rozporządzenie określa szczegółowy sposób funkcjonowania w bankach systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, tryb zgłaszania naruszeń prawa, procedur i standardów etycznych, zakres polityki wynagrodzeń i sposób jej ustalania,

³⁹ Tamże, § 3.

⁴⁰ Biuro Zarządzania Programami i Kontroli Wewnętrznej Ministerstwa Finansów.

⁴¹ § 8 zarządzenia Ministra Rozwoju i Finansów z dnia 8 czerwca 2017 r. w sprawie systemu kontroli zarządczej w Ministerstwie Finansów (Dz. Urz. MRiF poz. 116).

⁴² Tamże, § 6.

⁴³ Tamże, § 10.

⁴⁴ Ministerstwo powstało na mocy Rozporządzenia Rady Ministrów z dnia 7 grudnia 2015 r. w sprawie utworzenia Ministerstwa Rozwoju oraz zniesienia Ministerstwa Gospodarki. Ministerstwo Rozwoju jest urzędem administracji rządowej zapewniającym obsługę Ministra Rozwoju i Finansów w zakresie działów administracji rządowej: gospodarka oraz rozwój regionalny. Aktem prawnym, który określa zakres kompetencji Ministra Rozwoju i Finansów jest Rozporządzenie Prezesa Rady Ministrów z dnia 30 września 2016 r. w sprawie szczegółowego zakresu działania Ministra Rozwoju i Finansów wraz z załącznikiem do rozporządzenia (poz. 1595) zawierającym wykaz organów podległych ministrowi rozwoju i finansów lub przez niego nadzorowanych.

⁴⁵ Rozporządzenie Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz. U. 2017 poz. 637).

sposób szacowania kapitału wewnętrznego oraz dokonywania przeglądów strategii i procedur szacowania stałego utrzymywania kapitału wewnętrznego w banku.

Do najważniejszych czynności zarządzania można zaliczyć:

- podział obowiązków, stosownie do struktury organizacyjnej banku,
- zasady współpracy jednostek i komórek organizacyjnych banku,
- zasady wyboru, wynagradzania i monitorowania pracowników sprawujących funkcje istotne dla banku oraz działania, których celem jest zapewnienie ciągłości realizacji funkcji istotnych dla banku.

System realizowany jest na podstawie strategii zarządzania bankiem, strategii zarządzania ryzykiem, polityk, procedur i planów⁴⁶. Zarządzanie ryzykiem w banku realizowane jest przez zarząd w ramach przypisanych mu obowiązków na podstawie polityk i procedur dotyczących identyfikacji, pomiaru, monitorowania i kontroli ryzyka oraz raportowaniu o ryzyku.

W ramach kontroli ryzyka bank zabezpiecza się przed ryzykiem lub je ogranicza, wprowadzając odpowiednie do skali i złożoności działalności banku mechanizmy kontroli ryzyka, w szczególności w postaci limitów dostosowanych do wielkości i profilu *ryzyka* występującego w *banku*⁴⁷.

System zarządzania ryzykiem i system kontroli wewnętrznej są zorganizowane w banku na trzech niezależnych poziomach:

- pierwszy poziom składa się z zarządzania ryzykiem w działalności operacyjnej banku,
- drugi poziom składa się co najmniej z:
- zarządzania ryzykiem przez pracowników na specjalnie powoływanych do tego stanowiskach lub w komórkach organizacyjnych, niezależnie od zarządzania ryzykiem,
- działalność komórki do spraw zgodności,
- trzeci poziom składa się z działalności komórki audytu wewnętrznego.

Na wszystkich trzech poziomach, w ramach systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, pracownicy banku w związku z wykonywaniem obowiązków służbowych stosują odpowiednie mechanizmy kontrolne, a w przypadku banków będących uczestnikami systemu ochrony – mechanizmy kontrolne na trzecim poziomie. Niezależne monitorowanie ich przestrzegania stosuje bank zrzeszający zarządzający tym systemem albo inna jednostka zarządzająca⁴⁸.

Zdefiniowane zakresy zarządzania ryzykiem dotyczą: ryzyka kredytowego i kontrahenta, *ryzyka* rezydualnego, ryzyka koncentracji (zarówno na poziomie jednostkowym, jak i skonsolidowanym), *ryzyka* sekurytyzacji, ryzyka rynkowego, ryzyka

⁴⁶ Tamże, § 1 i § 2.

⁴⁷ Tamże, § 12.

⁴⁸ Tamże, § 14.

stopy procentowej, ryzyka operacyjnego, ryzyka płynności i finansowania, ryzyka nadmiernej dźwigni finansowej i innych rodzajów *ryzyka*, które zostały zidentyfikowane jako istotne w prowadzonej działalności bankowej⁴⁹.

3.10. Rozporządzenie Ministra Rozwoju i Finansów w sprawie kapitału wewnętrznego, systemu zarządzania ryzykiem, programu oceny nadzorczej oraz badania i oceny nadzorczej, a także polityki wynagrodzeń w domu maklerskim⁵⁰

Rozporządzenie określa w sposób szczegółowy:

- warunki szacowania przez dom maklerski kapitału wewnętrznego,
- warunki dokonywania przeglądów procesu szacowania i utrzymywania tego kapitału,
- warunki funkcjonowania systemu zarządzania ryzykiem, w tym zadań, składu i sposobu funkcjonowania Komitetu do spraw ryzyka,
- kryteria techniczne oceny nadzorczej i monitoringu,
- politykę wynagrodzeń i sposób jej ustalania⁵¹.

W ramach systemu zarządzania ryzykiem dom maklerski opracowuje i wdraża wewnętrzne polityki, strategie i procedury w zakresie identyfikacji, pomiaru lub szacowania, monitorowania i kontroli oraz ograniczania ryzyka. W procesie tym bierze pod uwagę skutki podejmowania ryzyka oraz sposoby zarządzania ryzykiem włącznie z ryzykiem, jakie niesie otoczenie zewnętrzne.

Rozporządzenie wyodrębnia w swojej strukturze organizacyjnej jednostkę realizującą funkcję zarządzania ryzykiem, niezależną od jednostek realizujących zadania operacyjne, posiadającą uprawnienia i zasoby oraz możliwość bezpośredniego przekazywania informacji do zarządu i rady nadzorczej⁵². W celu wymiany informacji pomiędzy powołaną jednostką a zarządem, radą nadzorczą oraz komitetem do spraw ryzyka (jeżeli komitet taki został powołany) opracowano jednolity dokument określający zasady przekazywania informacji w zakresie kwestii istotnych dotyczących zarządzania ryzykiem, w szczególności w zakresie istotnych rodzajów ryzyka, ich poziomu i wpływu na stabilną sytuację finansową domu maklerskiego oraz realizacji polityk, strategii i procedur związanych z zarządzaniem ryzykiem oraz ich zmian z uwzględnieniem ustaleń rady nadzorczej i komitetu do spraw ryzyka⁵³.

⁴⁹ Tamże, § 18 i § 20.

⁵⁰ Rozporządzenie Ministra Rozwoju i Finansów z dnia 25 kwietnia 2017 r. w sprawie kapitału wewnętrznego, systemu zarządzania ryzykiem, programu oceny nadzorczej oraz badania i oceny nadzorczej, a także polityki wynagrodzeń w domu maklerskim (Dz. U. poz. 856).

⁵¹ Tamże, § 1 i § 2.

⁵² Tamże, § 8.

⁵³ Tamże, § 10.

W ramach polityk, strategii i procedur zdefiniowane zostały zakresy zarządzania ryzykiem, do których należą w szczególności:

- ryzyka operacyjne obejmujące procedury *zarządzania ryzykiem* operacyjnym,
- ryzyka kredytowe i kontrahenta, rezydualnego, sekurytyzacji, koncentracji, rynkowego,
- ryzyka stopy procentowej w portfelu niehandlowym, utraty płynności, nadmiernej dźwigni finansowej, rynkowego⁵⁴.

W ramach systemu zarządzania ryzykiem dom maklerski stosuje metody identyfikacji i pomiaru ryzyka związanego z jego działalnością, które są dostosowane do profilu, skali i poziomu ryzyka. Przeprowadza także testy warunków skrajnych, co najmniej dla wszystkich rodzajów ryzyka, które zostały zidentyfikowane jako istotne w prowadzonej działalności. Ponadto wprowadza system limitów wewnętrznych ograniczających poziom ryzyka⁵⁵.

W ramach ustanowionego programu oceny nadzorczej podstawowym instrumentem przeprowadzania badania i oceny nadzorczej jest nadzór analityczny. Obejmują on analizę danych w zakresie modelu biznesowego, sytuacji finansowej i kapitałowej, wdrożonych systemów zarządzania ryzykiem, w szczególności informacje o poszczególnych istotnych rodzajach ryzyka związanego z działalnością danego domu maklerskiego, procesie szacowania kapitału wewnętrznego, procesie zarządzania domem maklerskim, ładu korporacyjnego, a także kompetencji członków zarządu i rady nadzorczej do wykonywania obowiązków⁵⁶.

Dom maklerski bada i ocenia, w ramach audytu wewnętrznego, adekwatność i skuteczność wdrożonego systemu zarządzania ryzykiem oraz poziom jego wykorzystywania, a następnie przekazuje radzie nadzorczej pisemne sprawozdania, raporty i istotne informacje dotyczące funkcjonowania systemu zarządzania ryzykiem⁵⁷. Rada nadzorcza zatwierdza akceptowalny ogólny poziom ryzyka domu maklerskiego (określany jako apetyt na ryzyko) w formie jednolitego dokumentu określającego w sposób jakościowo-ilościowy skłonność do podejmowania ryzyka.

3.11. Zarządzenie Prezesa Wyższego Urzędu Górniczego w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych⁵⁸

Zarządzenie określa zasady planowania działalności oraz zarządzania ryzykiem w Wyższym Urzędzie Górniczym (WUG), Okręgowych Urzędach Górniczych (OUG) oraz Specjalistycznym Urzędzie Górniczym (SUG), będące istotnym

⁵⁴ Tamże, § 12.

⁵⁵ Tamże, § 14.

⁵⁶ Tamże, § 24.

⁵⁷ Tamże, § 5.

⁵⁸ Zarządzenie Nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (Dz. Urz. WUG poz. 65).

elementem efektywnego zarządzania zasobami oraz kontroli zarządczej. Zarządzanie ryzykiem jest ściśle powiązane z planowaniem działalności, a celem jest działanie na rzecz realizacji priorytetów i celów strategicznych, poprawa jakości zarządzania na wszystkich poziomach kierowania WUG, komórkami, OUG oraz SUG oraz usprawnienie procesów pracy przez optymalne wykorzystanie posiadanych zasobów⁵⁹.

Planowanie działalności oraz zarządzanie ryzykiem w urzędach górniczych następuje zgodnie ze standardami i wytycznymi w zakresie kontroli zarządczej dla sektora finansów publicznych. Dokument określa, jak planować działania, w których może występować ryzyko oraz jak reagować, gdy ryzyko już wystąpi. Zasady, na jakich określa się ryzyko, identyfikuje się w odniesieniu do celów i zadań zawartych w planie strategicznym, planie operacyjnym oraz planach pracy. Każdy z planów realizuje różne cele, przez co narażony jest na inne zagrożenia. Dlatego też każdy w swoim zakresie identyfikuje, ocenia i wybiera sposób reakcji na ryzyko. Rezultatem jest sporządzony rejestr ryzyk, który jest brany pod uwagę podczas aktualizacji czy też tworzenia nowych planów⁶⁰.

⁵⁹ Tamże, § 1.

⁶⁰ Zarządzenie Nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn.: Dz. Urz. WUG poz. 65).

4. PRZEGLĄD WYBRANYCH PRZEPISÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM – PRAWO MIEJSCOWE NA PRZYKŁADZIE WOJEWÓDZTWA MAZOWIECKIEGO

Niniejszy rozdział prezentuje wybrane dokumenty normatywne, w których odnaleźć można charakterystykę procesu zarządzania ryzykiem w jednostkach samorządu terytorialnego, metodyki zarządzania ryzykiem oraz niezbędną terminologię. W Polsce zarządzanie ryzykiem to zagadnienie, które sukcesywnie wdrażane jest w kolejne sfery działalności administracji publicznej. W województwie mazowieckim (wytypowanym w projekcie „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”), w którym prowadzone były badania, zarówno na szczeblu administracyjnym województwa, jak i powiatu zidentyfikowano przepisy prawne wdrażające do niektórych sfer działalności procedury zarządzania ryzykiem bądź jego elementy.

Obowiązujące w tym zakresie akty prawne zidentyfikowano także w gminach, np. w gminie Karczew. Poszczególne akty prawa miejscowego zawierają zarówno terminologię związaną z zarządzaniem ryzykiem, jak i role oraz zadania organów uczestniczących w jego procesie. Celem analiz wybranych dokumentów źródłowych z zakresu zarządzania ryzykiem było wyselekcjonowanie użytecznej wiedzy w tym obszarze oraz przeprowadzenie diagnozy obecnego stanu, obejmującej uregulowania związane z zarządzaniem ryzykiem w samorządzie terytorialnym.

Analizie poddano wybrane cztery dokumenty:

- zarządzenie Nr 587 Wojewody Mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie,
- zarządzenie Nr 828/2015 Prezydenta Miasta Stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie,
- zarządzenie Nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku w sprawie wprowadzenia polityki zarządzania ryzykiem,

- zarządzenie Nr 156/2014 Burmistrza Karczewa z dnia 22 grudnia 2014 roku w sprawie wprowadzenia instrukcji dokonywania samooceny oraz sporządzenia oświadczenia o stanie kontroli zarządczej.

4.1. Zarządzenie Wojewody Mazowieckiego w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie¹

Od 14 grudnia 2016 r. zasady wykonywania kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim funkcjonują w oparciu o zarządzenie Nr 587 Wojewody Mazowieckiego z dnia 14 grudnia 2016 r. wraz z załącznikami. Dokument ten reguluje zarówno politykę kontroli zarządczej, jak i działania w zakresie zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim.

Zarządzenie określa podstawowe zadania i zasady wykonywania kontroli zarządczej, w tym m.in. planowanie, organizację i koordynację systemu kontroli zarządczej oraz podejmowanie działań w zakresie zarządzania ryzykiem.

Wprowadzone zarządzenie nr 587 spowodowało, że wcześniej obowiązujące zarządzenia utraciły moc prawną:

- zarządzenie Nr 311 Wojewody Mazowieckiego z dnia 26 lipca 2010 r. w sprawie ustalenia procedur kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie zmienione zarządzeniem Nr 572 z dnia 5 grudnia 2011 r., zarządzeniem Nr 381 z dnia 7 sierpnia 2013 r. oraz zarządzeniem Nr 22 z dnia 19 stycznia 2016 r.,
- zarządzenie Nr 80 Wojewody Mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia Polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie zmienione zarządzeniem Nr 571 z dnia 22 listopada 2013 r.,
- zarządzenie Nr 80 Wojewody Mazowieckiego z dnia 28 lutego 2013 r. w sprawie powołania Zespołu do spraw kontroli zarządczej i zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie, zmienione zarządzeniem Nr 572 z dnia 22 listopada 2013 r. oraz zarządzeniem Nr 1140 z dnia 20 listopada 2015 r.

Cel kontroli zarządczej stosowanej w Mazowieckim Urzędzie Wojewódzkim jest tożsamy z jego definicją ustawową, zgodnie z art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870 z późn. zm).

Członkowie kierownictwa, dyrektorzy oraz pracownicy Urzędu wykonują zadania związane z kontrolą zarządczą z zachowaniem ustanowionych standardów². Ich działania polegają między innymi na:

¹ Zarządzenie Nr 587 Wojewody Mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

² Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Min. Fin. poz. 84).

- wprowadzaniu rozwiązań zarządczych,
- ocenianiu funkcjonowania rozwiązań zarządczych z punktu widzenia ich zgodności z regulacjami dotyczącymi kontroli zarządczej,
- usystematyzowaniu i udoskonaleniu, bądź zintegrowaniu stosowanych metod, mechanizmów lub procedur postępowania z punktu widzenia przyjętych do realizacji celów,
- proponowaniu rozwiązań, regulowaniu oraz korygowaniu podejmowanych czynności dla zapewnienia ich przyszłej skuteczności organizacyjnej i ekonomicznej,
- zgodnym z prawem, skutecznym i efektywnym osiągnięciu rezultatów³.

W urządzie powołany jest Zespół do spraw kontroli zarządczej i zarządzania ryzykiem, który podejmuje działania w zakresie zarządzania ryzykiem oraz monitorowania systemu zarządzania ryzykiem⁴. Koordynację systemu kontroli zarządczej realizują komórka organizacyjna urzędu (Biuro Kadr i Organizacji Urzędu) oraz powołany przez wojewodę Zespół do spraw kontroli zarządczej i zarządzania ryzykiem. Biuro Kadr i Organizacji Urzędu koordynuje zadania związane z analizą ryzyka i jego oceną, dokonuje hierarchizacji działań podejmowanych w celu zmniejszenia ryzyka, sporządza arkusz identyfikacji i oceny ryzyka⁵. Natomiast Zespół do spraw kontroli zarządczej i zarządzania ryzykiem, powołany przez wojewodę corocznie na podstawie monitoringu i oceny realizacji celów i zadań, wyników samooceny, przeprowadzonych audytów i kontroli oraz oświadczeń o stanie kontroli zarządczej złożonych przez dyrektorów wydziałów, przedstawia wojewodzie oświadczenie o stanie kontroli zarządczej w urzędzie⁶.

Zarządzenie określa wszystkie jednostki organizacyjne biorące udział w procesie zarządzania ryzykiem, wprowadza do stosowania z przedmiotowego obszaru badań podstawową terminologię wraz z definicjami: **planu działalności, ryzyka, czynnika ryzyka, istotności ryzyka, akceptowanym poziomie ryzyka, zarządzania ryzykiem**.

Zarządzenie określa również zasady przeprowadzania samooceny kontroli zarządczej, treść i tryb składania oświadczenia przez wojewodów, wicewojewodów i dyrektorów generalnych urzędu o stanie kontroli zarządczej w podległych komórkach organizacyjnych⁷.

Rozdział 5 zarządzenia wraz z załącznikami zawiera wytyczne do zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim. Analiza ryzyka wykonywana

³ § 3 ust. 3 zarządzenia Nr 587 Wojewody Mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

⁴ Zarządzenie Nr 1140 z dnia 20 listopada 2015 r. w sprawie powołania Zespołu do spraw kontroli zarządczej i zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

⁵ § 5 zarządzenia Nr 587 Wojewody Mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

⁶ Tamże, § 12.

⁷ Tamże.

jest na podstawie planu działalności urzędu i sposobu jego realizacji. Metodyka została szczegółowo przedstawiona w części V niniejszej publikacji.

Za całość systemu odpowiada wojewoda, jednakże może tę odpowiedzialność cedować na podwładnych: Dyrektora Generalnego bądź dyrektorów wydziałów. Wspomniany już wcześniej Zespół (BKO) do spraw kontroli zarządczej i zarządzania ryzykiem ma za zadanie monitorować system i wydawać opinie odnośnie stanu jego funkcjonowania, opracowując analizy, a także raporty wykorzystywane również przez Zespół Audytu Wewnętrznego. Arkusze identyfikacji i oceny ryzyka, ewentualnie raporty z zarządzania ryzykiem – jeśli będą opracowywane – Zespół Audytu Wewnętrznego wykorzystuje do przygotowania rocznego planu audytu⁸.

4.2. Zarządzenie Prezydenta Miasta Stołecznego Warszawy w sprawie systemu zarządzania ryzykiem w m.st. Warszawie⁹

Od 1 stycznia 2013 roku do 9 czerwca 2015 roku system zarządzania ryzykiem w m.st. Warszawie funkcjonował w oparciu o Zarządzenie Prezydenta m.st. Warszawy 3666/2012 z dnia 18 grudnia 2012 r. (z późn. zm.) w sprawie systemu zarządzania ryzykiem w m.st. Warszawie, które wskazywało uczestników systemu oraz regulowało:

- strukturę organizacyjną,
- poziomy zarządzania ryzykiem,
- rolę w systemie, zakres podmiotowy i przedmiotowy,
- uprawnienia i obowiązki,
- zakres odpowiedzialności, częstotliwość, terminy i zakres raportowania.

Aktem uchylającym zarządzenie Prezydenta Miasta Stołecznego Warszawy nr 3666/2012 z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie, zmienione zarządzeniem Prezydenta m.st. Warszawy nr 3943/2013 z dnia 26 lutego 2013 r. oraz zarządzeniem nr 3944/2013 z dnia 26 lutego 2013 r. w sprawie wprowadzenia polityki zarządzania ryzykiem w m.st. Warszawie oraz powołania Pełnomocnika Prezydenta m.st. Warszawy ds. ryzyka jest Zarządzenie nr 828/2015 Prezydenta Miasta Stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.

W ramach doskonalenia system zarządzania ryzykiem podlega procesowi przeglądu i wdrażania zmian w celu dostosowania do zmieniającej się sytuacji zewnętrznej i wewnętrznej organizacji. Wytyczne zawarte w akcie wykonawczym charakteryzują politykę zarządzania ryzykiem w m.st. Warszawie. Wskazują przede wszystkim rolę, zakres zadań i obowiązków uczestników systemu oraz zasady:

⁸ Tamże, § 11.

⁹ Zarządzenie Nr 828/2015 Prezydenta Miasta Stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.

- dokonywania oceny ryzyka (identyfikacji, analizy i ewaluacji),
- określania reakcji na ryzyko,
- identyfikowania i raportowania incydentów,
- zakres i sposób monitorowania oraz raportowania ryzyka¹⁰.

Zarządzenie wprowadza do stosowania terminologię w ramach systemu zarządzania ryzykiem w oparciu o normę PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne: analiza ryzyka, ewaluacja ryzyka, identyfikacja ryzyka, kryteriów oceny ryzyka, mechanizmów kontrolnych, monitorowania ryzyka*¹¹. Zgodnie z normą PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne* organizacje powinny opracować, wdrożyć i ciągle doskonalić zarządzanie ryzykiem.

Funkcjonowanie systemu dostosowane jest do specyfiki m.st. Warszawy, złożoności struktury organizacyjnej, zakresu delegowanych uprawnień i pełnomocnictw oraz realizowanych celów i zadań na poszczególnych poziomach zarządzania. Proces zarządzania ryzykiem stanowiący element systemu kontroli zarządczej, polegający na systematycznym stosowaniu polityk, instrukcji i procedur opisujących ciąg zaplanowanych, wykonywanych i monitorowanych działań udokumentowanych został szczegółowo opisany w rozdziale zarządzenia „Polityka zarządzania ryzykiem w m.st. Warszawie”¹².

Akt określa zakres zadań, obowiązków i kompetencji należących do wszystkich uczestników systemu zarządzania ryzykiem, a w szczególności Prezydenta m.st. Warszawy w zakresie zarządzania ryzykiem. Uczestnikami procesu zarządzania ryzykiem jest Prezydent, Zastępcy Prezydenta, Skarbnik Sekretarz m.st. Warszawy, dyrektorzy biur, burmistrzowie, kierownicy jednostek oraz pozostali pracownicy jednostek samorządu terytorialnego według posiadanych uprawnień i zakresu wykonywanych obowiązków¹³.

Funkcjonowanie systemu zarządzania ryzykiem oparte jest na trzech podstawowych poziomach:

- zarządzania strategicznego – zadania realizuje Prezydent m.st. Warszawy przy współudziale Zastępców Prezydenta m.st. Warszawy, Sekretarza m.st. Warszawy, Skarbnika m.st. Warszawy i współpracy Pełnomocnika ds. ryzyka,
- zarządzania operacyjnego – zadania realizują dyrektorzy biur, burmistrzowie i kierownicy jednostek,
- koordynowania systemu zarządzania ryzykiem – zadania realizuje Pełnomocnik ds. ryzyka oraz właściciele procesów przekrojowych.

Pełnomocnik ds. ryzyka wykonuje swoje zadania przy pomocy Wydziału Ryzyka Gabinetu Prezydenta Urzędu m.st. Warszawy¹⁴.

¹⁰ Tamże, § 1 pkt. 1.

¹¹ Tamże, § 2.

¹² Tamże.

¹³ Tamże, § 2 i § 3.

¹⁴ Tamże, § 4.

Zadania podstawowe związane z obowiązującą metodyką zarządzania ryzykiem wykonują właściciele ryzyk, a są to: identyfikowanie i ocena ryzyk związanych z realizacją przypisanych celów i procesów, określanie reakcji w odniesieniu do poszczególnych ryzyk, wdrażanie działań zaradczych w stosunku do zidentyfikowanych ryzyk, wypełnianie określonych w zarządzeniu obowiązków w zakresie raportowania, bieżącej współpracy z Pełnomocnikiem ds. ryzyka. Szczegółowo metodyka zarządzania ryzykiem w m.st. Warszawie przedstawiona została w części V niniejszej publikacji.

Zarządzenie określa również tryb raportowania ryzyka w oparciu o procesy, obszary i funkcje określone „Systemem Zarządzania Jakością Urzędu”, wprowadzonym odrębnym zarządzeniem Prezydenta m.st. Warszawy. Z kolei schemat przepływu informacji w systemie zarządzania ryzykiem w m.st. Warszawie określa załącznik nr 9 do zarządzenia, który wskazuje, że wszystkie informacje i raporty w ramach systemu zarządzania ryzykiem w tym rejestr ryzyka i jego półroczna aktualizacja przekazywane są do Pełnomocnika ds. ryzyka, jednak z pewnym ograniczeniem¹⁵.

Rozdział VII omawianego zarządzenia dotyczy kluczowych wskaźników ryzyka. Liczone i monitorowane cyklicznie wskaźniki stanowią system ostrzegania, pozwalają na wczesne wykrycie zagrożeń i wypracowanie optymalnych rozwiązań¹⁶. Właściciele procesów przekrojowych opracowują katalog kluczowych wskaźników ryzyka dla nadzorowanego obszaru działalności w oparciu o dostępne źródła informacji. Monitorują także trendy i wskazują potrzeby podejmowania decyzji zaradczych w sytuacji, gdy trendy mogą negatywnie wpływać na realizację celów przez Urząd i/lub m.st. Warszawę¹⁷.

Zakres regulacji w ramach systemu zarządzania ryzykiem w jednostkach dostosowuje się do struktury organizacyjnej i systemu zarządzania jednostką. Działania podejmowane w ramach systemu zarządzania ryzykiem są uwzględniane w wewnętrznych regulaminach organizacyjnych biur, urzędów dzielnic i regulaminach organizacyjnych lub statutach jednostek. Regulaminy te powinny wskazywać co najmniej:

- koordynatora ds. ryzyka,
- zadań z zakresu zarządzania ryzykiem wraz z ich przypisaniem do wewnętrznych komórek organizacyjnych i osób pełniących określone funkcje oraz zakresu odpowiedzialności za bieżące zarządzanie ryzykiem,
- procedury dotyczącej przepływu informacji do koordynatora ds. ryzyka, zarządu dzielnicy i do właściciela ryzyka (wewnętrzny system raportowania),
- obowiązek rejestrowania ryzyka, jego oceny, dokumentowania, raportowania i monitorowania.

¹⁵ Tamże, § 20–27.

¹⁶ Tamże, § 28.

¹⁷ Tamże, § 29.

Ponieważ rolą wyższego kierownictwa jest wdrożenie skutecznych procesów zarządzania ryzykiem, personel kierowniczy powinien przeanalizować i aktualizować treść polityki dotyczącej zarządzania ryzykiem przynajmniej raz w roku, a także sporządzać raport zawierający wyniki tej oceny.

4.3. Zarządzenie Burmistrza Karczewa w sprawie wprowadzenia instrukcji dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej¹⁸

Zarządzeniem Nr 156/2014 Burmistrza Karczewa z dnia 22 grudnia 2014 roku wprowadzona została instrukcja dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej. Zarządzenie wprowadza do stosowania terminologię w ramach polityki zarządzania ryzykiem: analiza ryzyka, cel, czynnik ryzyka, hierarchizacja ryzyka, incydent, miernik, monitorowanie ryzyka, ocena ryzyka, raport ryzyka, rejestr ryzyka, ryzyko, ryzyko strategiczne, system zarządzania ryzykiem, właściciel celu, właściciel ryzyka, zarządzanie ryzykiem.

Instrukcja stanowiąca załącznik do zarządzenia Nr 156/2014 bezpośrednio odnosi się do identyfikowania i oceny ryzyka niepowodzenia (nieprawidłowości i błędów) związanego z konkretnym obszarem działań, ustalenia zasad postępowania z planami, systemów i innych środków w celu zminimalizowania, ograniczenia lub usunięcia ryzyka związanego ze zidentyfikowanym zagrożeniem. Dokument wprowadza także praktyczne narzędzia i procedury nadzorowania i kontrolowania oraz samoceny, w taki sposób, aby osiągnąć cele kontroli zarządczej. Instrukcja wraz z załącznikami stanowi podstawę do weryfikacji funkcjonującego systemu kontroli zarządczej w Urzędzie Miejskim w Karczewie i jednostkach organizacyjnych Gminy Karczew, a także wprowadza załączniki dotyczące samooceny oraz określa tryb sporządzania oświadczenia o stanie kontroli zarządczej¹⁹.

Podstawą udokumentowania samooceny jest kwestionariusz, w którym dokonuje się oceny wypełniania kryteriów kontroli zarządczej, w tym oceny istotnych ryzyk i zagrożeń w odniesieniu do założeń przyjętych w planie działalności jednostki i szczegółowego zakresu odpowiedzialności. Samoocenę przeprowadza się przy zachowaniu zasady rzetelności i bezstronności dokonywanych ocen, z wykorzystaniem informacji zebranych między innymi w wyniku sprawowanego nadzoru merytorycznego, wykonywanych przeglądów bieżących (monitoring) działalności, analizy i oceny ryzyka, procedur wewnętrznych oraz wszelkich informacji na temat nieprawidłowości i ryzyk funkcjonowania systemu kontroli zarządczej w urzędzie. Wynikiem przeprowadzonej samooceny powinna być propozycja działań mających charakter prewencyjny, odnoszących się do możliwości usprawnienia

¹⁸ Zarządzenie Nr 156/2014 Burmistrza Karczewa z dnia 22 grudnia 2014 roku w sprawie wprowadzenia instrukcji dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej.

¹⁹ Tamże, § 1.

funkcjonowania systemu kontroli zarządczej w jednostce, a także zapobieganiu nieprawidłowościom, stratom lub złemu zarządzaniu. Integralną częścią instrukcji dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej są załączniki: kwestionariusz samooceny kontroli zarządczej dla dyrektora jednostki, pracowników administracji, pracowników obsługi Urzędu, wzór oświadczenia o stanie kontroli zarządczej kierownika jednostki organizacyjnej oraz oświadczenie cząstkowe o stanie kontroli zarządczej²⁰.

4.4. Zarządzenie Burmistrza Karczewa w sprawie wprowadzenia polityki zarządzania ryzykiem²¹

Drugim aktem prawa miejscowego w gminie powiązany z opisywaną tematyką jest zarządzenie Nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku. Zarządzenie określa zakres, zasady i sposób funkcjonowania systemu zarządzania ryzykiem, w szczególności dotyczy zakresu zadań i obowiązków uczestników systemu, zasad identyfikowania ryzyka, dokonywania oceny ryzyka, reakcji na ryzyko oraz zakresu i sposobu monitorowania²².

System zarządzania ryzykiem w gminie Karczew realizowany jest na trzech poziomach:

- zarządzania strategicznego – Burmistrz Karczewa,
- zarządzania operacyjnego – kierownicy jednostek, osoby zatrudnione na stanowiskach kierowniczych, właściciele ryzyka,
- koordynowania systemu zarządzania ryzykiem – koordynator ds. kontroli zarządczej oraz właściciele ryzyka²³.

Zadania dotyczące zarządzania strategicznego, analizy informacji o ryzykach otrzymywanych w ramach systemu raportowania oraz oceny skuteczności systemu zarządzania ryzykiem przypisane zostały Burmistrzowi Gminy Karczew. Natomiast kierownicy jednostek i osoby zatrudnione na stanowiskach kierowniczych sprawują nadzór w zakresie zarządzania ryzykiem w nadzorowanych jednostkach. Bezpośredni nadzór nad ryzykiem zidentyfikowanym sprawują właściciele ryzyk, którzy każde zidentyfikowane ryzyko dotyczące realizowanych celów ujmują w rejestrze ryzyka. Właściciel ryzyka przeprowadza ocenę ryzyka równoległe z procesem identyfikacji ryzyka. Integralną częścią aktu prawnego są załączniki w formie tabelarycznej dotyczące polityki zarządzania ryzykiem w gminie Karczew. W cyklu rocznym kierownicy jednostek, osoby zatrudnione na stanowiskach kierowniczych, właściciele procesów przekazują raport z przeglądu ryzyk koordynatorowi ds. kontroli

²⁰ Instrukcja dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej, załącznik do zarządzenia Nr 156/2014 Burmistrza Karczewa z dnia 22 grudnia 2014 r.

²¹ Zarządzenie Nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku w sprawie wprowadzenia polityki zarządzania ryzykiem.

²² Tamże, § 1.

²³ Tamże, § 3.

zarządczej, który jest następnie zobowiązany do przedstawiania Burmistrzowi zbiorczego rejestru ryzyka gminy Karczew za bieżący rok oraz zbiorczego raportu z przeglądu ryzyk za poprzedni rok budżetowy²⁴.

Działalność Urzędu w gminie Karczew wiąże się ze spełnianiem oczekiwań wielu stron. Strony te i ich oczekiwania stanowią kontekst działalności urzędu, a oczekiwania względem przepływu i bezpieczeństwa informacji są kryteriami ryzyka, które podlega bieżącej analizie i ocenie. Z analizowanych dokumentów wynika, że elementy stanowiące zewnętrzne i wewnętrzne zależności organizacyjne zostały zidentyfikowane i opisane.

Klasyfikacja zasobów i aktywów związanych z istniejącymi lub potencjalnymi zagrożeniami, naruszeniem ciągłości działania stanowią punkt wyjściowy do identyfikacji ryzyk i wynikających z nich zagrożeń, a także podstawę do ustalenia kryterium dla analizy, szacowania i oceny ryzyka. Powyższe działania dokumentowane są w postaci metodyki zarządzania ryzykiem, zawierającej definicje kryteriów klasyfikacji informacji, definicję kryteriów ryzyk akceptowalnych i nieakceptowalnych, raportu z analizy ryzyka, planu postępowania z ryzykiem. Szczegółowo metodyka zarządzania ryzykiem w gminie Karczew przedstawiona została w części V niniejszej publikacji.

²⁴ Zarządzenie Nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku w sprawie wprowadzenia polityki zarządzania ryzykiem.

5. PRZEGLĄD WYBRANYCH NORM I STANDARDÓW Z ZAKRESU ZARZĄDZANIA RYZYKIEM

Przy wyborze odpowiedniej metodyki zarządzania ryzykiem konieczne jest określenie stanu bieżącego. W oparciu o uzyskane informacje należy wtedy podjąć decyzję, jaka metodyka będzie w sposób optymalny spełniała oczekiwania i będzie mogła zostać skutecznie zaimplementowana w warunkach rzeczywistych. Obserwacja aktualnych trendów na świecie w zakresie zarządzania kryzysowego i zarządzania ryzykiem (np. wprowadzanie systemów zarządzania ryzykiem przez banki i organizacje finansowe) pokazuje, że kluczowym aktem prawnym powinna być norma PN-ISO 31000 uzupełniona o zapisy z pozostałych aktów normatywnych.

Zarządzanie ryzykiem stało się w ostatnim czasie popularną dziedziną w działalności większości przedsiębiorstw. Potwierdzają to np. przyjmowane przez firmy procedury zarządzania ryzykiem finansowym i procedury zarządzania ryzykiem inwestycyjnym. Poszczególni członkowie najwyższego kierownictwa dokonują analiz ryzyka, szacowania ryzyka, wykonują matryce zagrożeń, obliczają ryzyko akceptowalne.

Dokonując analizy, zespół postanowił skoncentrować się na normach opublikowanych przez Polski Komitet Normalizacyjny i Międzynarodową Organizację Normalizacyjną. Dodatkowo rozdział uzupełniono o normę kanadyjską, która może wnieść wartościowe informacje w zakresie zarządzania ryzykiem w szczególności w odniesieniu do osób, które z racji zajmowanych wysokich stanowisk muszą podejmować decyzje np. wojewodowie, starostowie, wójtowie.

Na potrzeby niniejszego rozdziału wybrano następujące normy i standardy z zakresu analizy i oceny zagrożeń i ryzyka:

- ISO 31000:2009 *Risk management – Principles and guidelines*,
- ISO GUIDE 73:2009 *Risk management – Vocabulary*,
- ISO/IEC 31010:2009 *Risk management – Risk assessment techniques*,
- BSI-Standard 100-4 *Business Continuity Management*,
- OECD *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*,

- PKN-CEN/CWA 15537 *Network Enabled Abilities – Service-Oriented Architecture for civilian and military crisis management*,
- CAN/CSA-Q850-97:2009 *Risk Management: Guideline for Decision-Makers*.

5.1. ISO/IEC 31010:2009 Risk management – Risk assessment techniques

Norma stanowi uzupełnienie dla normy ISO 31000 i zawiera poradnik z zakresu systematycznych technik oceny ryzyka. Oczywiście opisane są w niej tylko wybrane techniki, te najbardziej popularne z zastrzeżeniem, że brak jakiegś techniki nie dyskwalifikuje jej pod względem użyteczności. Norma stanowi doskonałe narzędzie dla osób zajmujących się zarządzaniem ryzykiem i z powodzeniem może być wykorzystany w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

Norma zawiera krótkie charakterystyki dla 31 technik oceny ryzyka oraz ich wzajemne porównanie w kontekście przydatności do identyfikacji ryzyka, analizy ryzyka pod względem konsekwencji, prawdopodobieństwa i poziomu ryzyka oraz oceny ryzyka (możliwość uzyskania wyników ilościowych, a nie tylko jakościowych).

Syntetyczną analizę *technik zawartych w normie ISO/IEC 31010:2009 Risk management – Risk assessment techniques* wraz z przykładami zastosowania przedstawiono w części II niniejszej publikacji.

5.2. ISO GUIDE 73:2009 Risk management – Vocabulary

Przewodnik zawiera podstawową terminologię z zakresu zarządzania ryzykiem, mającą na celu ułatwienie wzajemnego zrozumienia i komunikacji uczestników procesu zarządzania ryzykiem w organizacjach. Przewodnik zawiera terminologię podzieloną na kilka grup w zależności, jaki aspekt procesu zarządzania ryzykiem jest omawiany. Znajdują się w nim definicje związane z: istotą ryzyka, zarządzaniem ryzykiem, procesem zarządzania ryzykiem, komunikacją i konsultacjami, kontekstem, oceną ryzyka, identyfikacją ryzyka, analizą, szacowaniem, postępowaniem z ryzykiem, monitorowaniem.

Standard definiuje następujące terminy: ryzyko, źródło ryzyka, konsekwencje, zarządzanie ryzykiem, zarządzanie kryzysowe, struktura ramowa zarządzania ryzykiem, nastawienie do ryzyka, plan zarządzania ryzykiem, właściciel ryzyka, ocena ryzyka, identyfikacja ryzyka, prawdopodobieństwo, profil ryzyka, analiza ryzyka, kryteria ryzyka, poziom ryzyka, ewaluacja ryzyka, postępowanie z ryzykiem, ryzyko rezydualne, akceptacja ryzyka, unikanie ryzyka, dzielenie się ryzykiem, rejestr ryzyk. Zespół autorski dokonał selekcji definicji przywołanej normy – najbardziej użyteczne zostały przywołane w części VI niniejszej publikacji, stanowiącej słownik wybranych pojęć z zakresu zarządzania ryzykiem.

5.3. ISO 31000:2009 *Risk management – Principles and guidelines*

Różnego rodzaju organizacje (zarówno te małe, jaki i duże) stawiają czoła wewnętrznym i zewnętrznym czynnikom i wpływom, które składają się na niepewność tego, czy i kiedy organizacje osiągną swoje cele. Wpływ, jaki wywiera ta niepewność na cele organizacji, nazywa się „ryzykiem”. Implementacja normy ma na celu: zwiększenie prawdopodobieństwa osiągnięcia celów, wsparcie proaktywne zarządzania oraz zwiększenie świadomości o potrzebie identyfikacji i postępowania z ryzykiem w całej organizacji. Ważnymi jej aspektami są również: doskonalenie identyfikacji szans i zagrożeń, spełnianie wymagań prawnych i regulacyjnych, doskonalenie obowiązkowego i dobrowolnego raportowania, doskonalenie ładu organizacyjnego, ustalenie wiarygodnej podstawy dla podejmowania decyzji i planowania. Nie można zapominać o doskonaleniu skuteczności i efektywności operacyjnej, poprawianiu wyników w obszarze bezpieczeństwa, doskonaleniu w zapobieganiu stratom i zarządzaniu incydentami, minimalizowaniu straty oraz doskonaleniu nauki o organizacji i jej odporności. Poszczególne sektory lub zastosowania zarządzania ryzykiem charakteryzują się własnymi, indywidualnymi potrzebami, odbiorcami, postrzeganiem i kryteriami¹.

Norma podaje:

- jakie zasady należy stosować w celu zapewnienia skuteczności zarządzania ryzykiem,
- jak stworzyć odpowiednią strukturę ramową zarządzania,
- jakie elementy powinien zawierać proces zarządzania ryzykiem i dokładny opis poszczególnych działań, takich jak: komunikacja i konsultacje, ustalanie kontekstu, ocena ryzyka (identyfikacja ryzyka, analiza ryzyka, ewaluacja ryzyka), postępowanie z ryzykiem, monitorowanie i przegląd.

Systemowe podejście do zarządzania ryzykiem oparte na normie ISO 31000 szerzej scharakteryzowano w części II niniejszej publikacji.

Należy pamiętać, że w procesie zarządzania ryzykiem zapisy stanowią podstawę doskonalenia metod i narzędzi, podobnie jak i całego procesu. Należy je dokumentować na każdym etapie procesu. Norma zawiera definicje następujących terminów: ryzyko, zarządzanie ryzykiem, struktura ramowa zarządzania ryzykiem, plan zarządzania ryzykiem, właściciel ryzyka, proces zarządzania ryzykiem, kontekst zewnętrzny, kontekst wewnętrzny, ocena ryzyka, analiza ryzyka. Terminy podane 73:2009.

5.4. BSI-Standard 100-4 *Business Continuity Management*

Autorzy powyższego standardu przedstawili metodologię tworzenia i utrzymywania systemu zarządzania ciągłością biznesową w przedsiębiorstwie. Dokument opisuje wymagania zarządzania kryzysowego oraz oceny ryzyka w biznesie.

¹ ISO 31000:2009 Risk management – Principles and guidelines.

Standard BSI 100-4 jest skierowany do zatrudnionych w organizacji/przedsiębiorstwie menedżerów i członków zespołów kryzysowych, osób odpowiedzialnych za bezpieczeństwo, oficerów bezpieczeństwa, ekspertów ds. bezpieczeństwa i konsultantów bezpieczeństwa, którzy są zaznajomieni z zarządzaniem w sytuacjach nadzwyczajnych i kryzysowych.

Standard zawiera również definicje² m.in. pojęć takich jak: szkoda, awaria, kryzys, katastrofa. Standard przedstawia klasyczne podejście do analizy ryzyka jako identyfikację zagrożeń związanych z organizacją w odniesieniu do procesu lub do zasobów oraz następnie dokonanie oceny ryzyka. Ryzyko cechują w tym przypadku skutki/szkody poniesione wskutek wystąpienia zagrożenia oraz prawdopodobieństwo wystąpienia tego zagrożenia. Autorzy zauważają, że podczas przeprowadzania analizy ryzyka należy zawsze brać pod uwagę:

- niemożliwość zidentyfikowania wszystkich zagrożeń tzn. zawsze jest co najmniej jedno ryzyko, które nie zostało wzięte pod uwagę, dlatego uzasadniona jest zasada, że podczas analizy ryzyka należy podjąć próbę identyfikacji wszystkich zagrożeń, które mogłyby mieć miejsce;
- prawdopodobieństwo wystąpienia można jedynie subiektywnie oszacować; nie zawsze istnieje możliwość oparcia się na wnioskach z przeszłości, ponieważ panujące warunki otoczenia są zazwyczaj bardzo dynamiczne³.

W dalszej części standardu wymienia się etapy analizy ryzyka tj.⁴:

- identyfikację zagrożeń (dotyczy wszystkich możliwych zagrożeń dla krytycznych procesów biznesowych; zagrożenia są rozumiane jako niebezpieczeństwa, które mogą mieć szczególnie negatywny wpływ na procesy lub zasoby dla różnych klas zagrożeń m.in.: siła wyższa, niedociągnięcia organizacyjne, błąd ludzki, awaria techniczna, celowe działania);
- ocenę ryzyka (aby dokonać oceny ryzyka, należy oszacować prawdopodobieństwa występowania zagrożeń oraz szkody, jakie mogą wywołać; metoda ta ma dobrze znane utrudnienia wynikające z nieklarownych danych statystycznych. Z tego powodu w celu oszacowania prawdopodobieństwa wystąpienia danego zagrożenia należy zastosować podejście jakościowe; obydwa elementy – prawdopodobieństwo i skutki należy zestawić w stosunku do siebie; zagrożenia mogą być rejestrowane i przedstawiane za pomocą różnych formatów; zastosowanie narzędzia informatycznego może być pomocne w graficznym przedstawieniu ryzyka; macierze ryzyka często używane są do przeglądów ryzyka; macierz ryzyka może być szczególnie przydatna przy wyborze konkretnej strategii zarządzania ryzykiem);

² BSI-Standard 100-4 Business Continuity Management, wersja 1, listopad 2008.

³ Tamże.

⁴ Tamże.

- tworzenie grup i scenariuszy (po dokonanej ocenie ryzyk w organizacji tworzy się grupy robocze, które nadzorują lub opracowują scenariusze (kryzysowe); w odniesieniu do zidentyfikowanych zagrożeń tworzy się scenariusze postępowania na wypadek ich wystąpienia; scenariusze zawierają działania, jakie należy podjąć oraz wskazują osoby/stanowiska odpowiedzialne),
- określenie wariantów strategii ryzyka (ryzyko może być zaakceptowane, przenoszone, unikane lub ograniczane; opcje strategiczne są podstawowymi decyzjami dotyczącymi postępowania z ryzykiem; dla każdego krytycznego procesu biznesowego i każdego zidentyfikowanego ryzyka określa się odpowiednie opcje strategiczne, które są udokumentowane; podczas wybierania strategii ryzyka pod uwagę bierze się nie tylko poziom ryzyka, ale również aspekty ekonomiczne, operacyjne i techniczne; identyfikuje się następujące możliwe strategie ryzyka: przejęcie ryzyka, przeniesienie ryzyka, unikanie ryzyka, zmniejszenie ryzyka),
- raport z analizy ryzyka (na zakończenie procesu analizy ryzyka sporządza się raport; raport może zawierać: przegląd zarządzania, wykorzystaną metodę analizy ryzyka, listę zagrożeń, wyniki oceny ryzyka, opcje strategii ryzyka dla krytycznych procesów, wybór strategii ryzyk).

5.5. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Przyjęte w 2002 r. wytyczne Organizacji Współpracy Gospodarczej i Rozwoju *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informatycznych: W kierunku kultury bezpieczeństwa)* odnoszą się do szeroko pojętego zarządzania bezpieczeństwem informacyjnym. Ustanawiają ramy zasad bezpieczeństwa, które mają zastosowanie do wszystkich uczestników w celu zwiększenia bezpieczeństwa systemów informacyjnych i sieci. Wytyczne miały przyczynić się do pobudzenia dobrobytu gospodarczego i rozwoju społecznego.

Autorzy wytycznych OECD stawiają nacisk na wspieranie rozwoju kultury bezpieczeństwa – bezpieczeństwo w rozwoju sieci i systemów informatycznych oraz rozpowszechnianiu nowych sposobów myślenia i zachowania podczas korzystania i interakcji w ramach różnych systemów informacyjnych i sieci.

Autorzy prezentują zasady bezpieczeństwa, które należy traktować jako całość. Dotyczą one uczestników na wszystkich szczeblach, w tym na poziomie polityki bezpieczeństwa i poziomie operacyjnym⁵. Obejmują one:

- świadomość – uczestnicy powinni być świadomi potrzeby zabezpieczenia systemów informatycznych i sieci jak również czynności, które zwiększają bezpieczeństwo. Świadomość istniejących zagrożeń i dostępnych zabezpieczeń to

⁵ OECD Guidelines for the security Information Systems and Networks.

podstawowa linia obrony systemów i sieci informatycznych. Systemy informacyjne i sieci mogą być kształtowane przez ryzyka wewnętrzne i zewnętrzne. Użytkownicy powinni być świadomi zagrożeń i powinni rozumieć, że błędy w systemie bezpieczeństwa mogą zaszkodzić systemom i sieciom;

- odpowiedzialność – wszyscy użytkownicy powinni być świadomi swojej odpowiedzialności za bezpieczeństwo systemów i sieci informatycznych. Stosowane polityki, praktyki, środki i procedury powinny być poddawane przeglądom pod względem ich dostosowania do środowiska;
- reagowanie – użytkownicy powinni działać w sposób zorganizowany w zakresie zapobiegania, wykrywania i reagowania na incydenty bezpieczeństwa. Uznając wzajemne połączenia sieci i systemów informatycznych oraz możliwość szybkiego rozprzestrzeniania się w nich zagrożeń i rozległych szkód, użytkownicy powinni działać skutecznie i w odpowiednim czasie reagować na incydenty bezpieczeństwa;
- etykę – użytkownicy powinni szanować interesy innych. Biorąc pod uwagę wszechobecność sieci i systemów informatycznych w społeczeństwach, uczestnicy muszą uznać, że ich działanie lub brak działania może krzywdzić innych. Etyczne postępowanie jest więc kluczowe i uczestnicy powinni dążyć do opracowania i przyjęcia dobrych praktyk oraz promowania zachowań, które uwzględniają potrzeby innych;
- demokrację – bezpieczeństwo systemów informatycznych i sieci powinno być zgodne z podstawowymi wartościami demokratycznego społeczeństwa. Bezpieczeństwo powinno być realizowane w sposób zgodny z wartościami uznanymi ogólnie za demokratyczne, w tym wolności do wymiany myśli i idei, swobodnego przepływu informacji, poufności informacji i komunikacji;
- ocenę ryzyka – użytkownicy powinni przeprowadzić ocenę ryzyka. Ocena ryzyka powinna identyfikować zagrożenia i słabe punkty w wystarczająco szerokim obszarze, aby objąć kluczowe czynniki wewnętrzne i zewnętrzne (...). Ocena ryzyka pozwoli na określenie dopuszczalnego poziomu ryzyka i pomoże wybrać odpowiednie kroki w celu ograniczenia ryzyka potencjalnego zagrożenia;
- projektowanie i wdrażanie zabezpieczeń – systemy, sieci i polityki muszą być odpowiednio zaprojektowane, wdrożone i koordynowane w celu optymalizacji bezpieczeństwa. Jednym z kluczowych wysiłków jest projektowanie i przyjęcie odpowiednich zabezpieczeń i rozwiązań służących uniknięciu lub ograniczeniu potencjalnych szkód. Oba rodzaje zabezpieczeń – techniczne i nietechniczne – powinny być proporcjonalne do wartości, którą mają chronić;

- zarządzanie bezpieczeństwem – powinno przyjąć się kompleksowe podejście do zarządzania bezpieczeństwem. Wskazane, aby było oparte na ocenie ryzyka, było dynamiczne oraz obejmowało wszystkie poziomy działalności użytkowników. Powinno ono pozwalać na znalezienie odpowiedzi na pojawiające się zagrożenia oraz wskazywać na metody zapobiegania zagrożeniom, wykrywania i reagowania na incydenty, planowania konserwacji, przeglądów i auditów (...);
- ponowną ocenę – powinno się dokonywać ponownych przeglądów i ocen bezpieczeństwa systemów informacyjnych i sieci, a także wprowadzić odpowiednie zmiany do polityki bezpieczeństwa, praktyk, środków i procedur.

W 2012 r. OECD rozpoczęła przegląd tych wytycznych⁶, a wyniki ogłosiła w raporcie z listopada 2012 r. pt. *Rola wytycznych w sprawie bezpieczeństwa z 2002 roku: W kierunku cyberprzestrzeni dla otwartej i wzajemnie połączonej gospodarki*. Przez ostatnie trzy dekady XX w. OECD odegrała ważną rolę w promowaniu polityk i instrumentów na rzecz innowacyjności i zaufania do gospodarki cyfrowej. Efektem prac grupy roboczej OECD ds. bezpieczeństwa i prywatności w gospodarce cyfrowej (SPDE) powołanej w celu przeglądu zalecenia Rady z 2002 r. w sprawie wytycznych dotyczących bezpieczeństwa systemów i sieci informacyjnych: *w kierunku kultury bezpieczeństwa jest przyjęcie dokumentu określającego zalecenia Rady OECD w dniu 17 września 2015 r.*

*Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informacyjnych: w kierunku kultury bezpieczeństwa z dniem 1 października 2015 r. zostały zastąpione zaleceniem Rady w sprawie zarządzania ryzykiem w zakresie bezpieczeństwa cyfrowego na rzecz dobrobytu gospodarczego i społecznego*⁷.

Cyberzagrożenia na dużą skalę związane z bezpieczeństwem i mające potencjalne konsekwencje ekonomiczne wzrosły w częstotliwości i wyrafinowaniu, w kontekście, w którym cyberprzestrzeń stała się kluczowa dla funkcjonowania gospodarki i czynnikiem wzrostu, dobrobytu i integracji. Powoduje to powstawanie nowych wyzwań w zakresie bezpieczeństwa. Dlatego też wytyczne te dotyczą wszystkich uczestników nowego społeczeństwa informatycznego, w których zasugerowano potrzebę większej świadomości i zrozumienia kwestii związanych z bezpieczeństwem oraz rozwoju „kultury bezpieczeństwa”.

Aby czerpać korzyści związane z cyberprzestrzenią, zainteresowane strony muszą odstąpić od podejmowania ryzyka związanego z cyberbezpieczeństwem wyłącznie z technicznego punktu widzenia w oderwaniu od szerszych względów gospodarczych i społecznych. Zgodnie z nowym zaleceniem OECD dla państw członkowskich cyfrowe zagrożenie dla bezpieczeństwa powinno być traktowane raczej jako sprawa gospodarcza, a nie techniczna. Powinna stanowić część ogólnej organizacji zarządzania ryzykiem i podejmowania decyzji. Istnieje pilna potrzeba

⁶ <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf> [dostęp: sierpień 2017].

⁷ Tamże.

zintegrowania cyfrowego zarządzania ryzykiem w procesie podejmowania decyzji ekonomicznych i społecznych⁸.

5.6. PKN-CEN/CWA 15537 *Network Enabled Abilities – Service-Oriented Architecture for civilian and military crisis management*

Powyższa norma opisuje oprogramowanie (platformę multimedialną) Service-Oriented Architecture oraz działania, które należy uwzględnić podczas opracowywania i wdrażania projektu systemu. Service-Oriented Architecture umożliwia wykorzystanie zasobów w dowolnym miejscu w sieci. Celem nakreślonym w dokumencie jest stworzenie systemu, który efektywnie wykorzysta zasoby krajowe w dowodzeniu i kontroli operacji europejskich tj. operacji wojskowych i cywilnych, takich jak akcje poszukiwawcze i ratunkowe oraz działań w zakresie ochrony środowiska.

Norma zawiera wykaz dokumentów odniesienia i standardów technicznych zastosowanych w projektowanym systemie. Powyższe dokumenty dotyczą głównie zasad projektowania systemów informatycznych. Autorzy dokumentu wśród norm i standardów pomocnych w projektowaniu przedmiotowego systemu wymieniają między innymi:

- ISO 11179 *Metadata Registries*,
- ISO 15489 *Records Management*,
- ISO 19119 *Geographic Information – Services*,
- ISO/IEC TR 18044 *Information technology – Security techniques – Information security incident management*,
- ISO 7894-4 *Management Framework*,
- ISO 20000-1 – *Information technology – Service management – Specification*,
- ISO 20000-2 – *Information technology – Service management – Code of practice*,
- *Web Services Policy Framework (WS-Policy) v 1.1* September 2004,
- *Web Services Policy Assertions Language (WS-Policy Assertions) Version 1.0* December 18, 2002 Figure 8 – *Services specific for certain communities of interest*,
- *Web Services Policy Attachment (WS-Policy Attachment)* September 2004,
- LT1K P04-0278 *Framework Service Description*,
- *OMG UML Profile for Modelling Quality for Services and Fault Tolerance Characteristics & Mechanisms (ptc/04-09-01)*,
- IETF RFC 2460 *Internet Protocol, Version 6 (IPv6)*,
- IETF RFC 3164 *BSD Syslog Protocol*,
- IETF RFC 3195 *Reliable Delivery for syslog*.

⁸ Komunikat prasowy 1/10/2015 – Prezesi i rządy powinny traktować bezpieczeństwo cyfrowe jako zagrożenie ekonomiczne – mówi OECD.

Wszystkie wymienione w PKN-CEN/CWA 15537 normy i standardy obejmują ogólne zasady i ramy projektowanego systemu, informacje o architekturze, uniwersalne funkcje, koncepcje, konwencje i terminologię.

Service-Oriented Architecture (SOA) jest postrzegany jako możliwość integracji istniejących i rozproszonych dzisiaj systemów. Zaletą tworzonego systemu jest zwiększona elastyczność tzn. możliwość włączenia w nowe struktury istniejących już systemów i aplikacji⁹. Wśród różnych funkcjonalności, jakie można zdefiniować czy dodać do oprogramowania już działającego, są różne metodyki analizy ryzyka. Dzięki swojej elastyczności oprogramowanie może udostępniać aplikacje dodane przez inne podmioty, co służy powszechnej wymianie doświadczeń i informacji.

Service-Oriented Architecture odzwierciedla łatwą do zrozumienia organizację pracy, która przy swojej prostocie ma możliwości zapewnienia zaawansowanych rozwiązań (analizy ryzyka, prawdopodobieństwa, szacowania skutków itd.) dla złożonych problemów na wszystkich szczeblach organizacyjnych. Efektywna funkcja, która jest bądź była realizowana w jednej dziedzinie, może być używana przez wiele aplikacji w całej sieci. Nowe rozwiązania mogą mieć natychmiastowy wpływ na całą sieć, a tym samym mogą przyczyniać się do rozwoju dziedziny zarządzania ryzykiem i sytuacjami kryzysowymi.

Analizowana norma koncentruje się głównie na przedstawieniu możliwości oprogramowania, które służyć ma zarządzaniu m.in. ryzykiem. Autorzy zaprezentowali podstawowe usługi, funkcjonalności systemu. Jednocześnie zwrócili uwagę na główne aspekty, które należy wziąć pod uwagę przy opracowywaniu i wdrażaniu systemu SOA oraz wszystkich usług związanych z systemem.

5.7. CAN/CSA-Q850-97:2009 Risk Management: Guideline for Decision-Makers

Norma CAN/CSA-Q850-97:2009 *Risk Management: Guideline for Decision-Makers* wydana została przez kanadyjską organizację normalizacyjną i ma status normy wycofanej. Z uwagi na fakt, że odnosi się ona do kluczowych zagadnień dotyczących zarządzania ryzykiem, w kontekście procesu podejmowania decyzji przez decydentów, autorzy niniejszej publikacji postanowili przywołać dokument jako przykład stosowania dobrych praktyk w procesie zarządzania ryzykiem, a także zarządzania wiedzą.

Norma CAN/CSA-Q850-97:2009 *Risk Management: Guideline for Decision-Makers* została opisana w publikacji autorstwa D. Wróblewskiego i T. Sowy pt. *Zarządzanie ryzykiem. Zagadnienia ogólne*¹⁰ oraz wykorzystana w 2009 roku w szkoleniu dla audytorów wiodących Polskiego Centrum Akredytacji pt. *Ocena i zarządzanie ryzykiem*.

Według normy w procesie podejmowania decyzji przez decydentów szczególnie nacisk położono na percepcję ryzyka i komunikację ryzyka, które to elementy

⁹ PKN-CEN/CWA 15537 Network Enabled Abilities.

¹⁰ D. Wróblewski, T. Sowa, *Zarządzanie ryzykiem. Zagadnienia ogólne*, CNBOP, Józefów 2009, s. 68–69.

powinny być uwzględnione w każdym z pozostałych elementów procesu zarządzania ryzykiem takim jak: identyfikacja, analiza, ocena, i kontrola.

Zarządzanie ryzykiem to kwestia kluczowa dla wszystkich organizacji, zarówno w sektorze publicznym, jak i prywatnym. Ważnym podmiotem procesu zarządzania ryzykiem, na który zwrócono w opisywanej normie szczególną uwagę jest interesariusz (udziałowiec) procesu zarządzania ryzykiem. Należy również dodać, że opisano kwestię finansowania procesu zarządzania ryzykiem pod kątem optymalizacji kosztów, jednak uczyniono to w bardzo ograniczonym zakresie.

Norma zawiera informacje na temat procesu podejmowania decyzji podczas zarządzania ryzykiem, opis inicjacji całego procesu, wykonywania analiz wstępnych, szacowania ryzyka, oceny ryzyka, sposobów kontroli ryzyka i jego finansowania, podejmowania działań naprawczych.

Norma prezentuje szczegółowe informacje z zakresu podejmowania decyzji z uwzględnieniem procesu zarządzania ryzykiem. Należy mieć świadomość, że podejmowanie decyzji przez kierownictwo jest bardzo ważnym elementem procesu zarządzania ryzykiem. Bez tego elementu cały proces traci uzasadnienie istnienia. Jednocześnie powszechnie wiadomym jest, jak trudno jest podejmować właściwe decyzje, szczególnie pod presją czasu i w obliczu zagrożenia, które wyrze niekorzystne skutki na organizację. Norma jest przydatnym dokumentem dla osób zarządzających różnego typu organizacjami. Uwzględniono w niej również kontekst udziałowców (kwestia istotna przede wszystkim dla spółek akcyjnych), którzy zawsze są zainteresowani kondycją firm/spółek, których udziały posiadają.

Zarządzanie ryzykiem zostało dość szczegółowo omówione w przedmiotowej normie. Może ona posłużyć jako uzupełnienie normy ISO 31000. W CAN/CSA-Q850-97:2009 znalazły się definicje następujących terminów: decydent, dialog, niebezpieczeństwo, identyfikacja niebezpieczeństwa, strata, organizacja, strategia kontroli ryzyka, biblioteka informacji o ryzyku, percepcja ryzyka, scenariusz ryzyka, interesariusz.

6. PRZEGLĄD WYBRANYCH PROJEKTÓW NORM Z ZAKRESU ZARZĄDZANIA RYZYKIEM

W niniejszym rozdziale przedstawiono wybrane projekty norm związanych z zarządzaniem ryzykiem. Podczas wyboru projektów norm autorzy kierowali się użytecznością projektów w zakresie: terminologii, elementów struktur systemu zarządzania, ról i zadań organów zarządzania kryzysowego, procesów występujących w zarządzaniu kryzysowym.

W związku z powyższym w rozdziale szczegółowo omówiono dwa projekty:

- N 96 ISO 18482 *Security Management System – Guidance for use – Security risk assessment*,
- ISO/CD 16125 *Security management system*.

Analiza projektów norm wykorzystujących elementy zarządzania ryzykiem powinna stanowić wsparcie dla wdrażania modelowych metod analizy ryzyka.

6.1. N 96 ISO 18482 *Security Management System – Guidance for use – Security risk assessment*

Projekt normy N 96 ISO 18482 *Security Management System – Guidance for use – Security risk assessment* opisuje zadania, jakie powinny podejmować organy zarządzania kryzysowego w celu ustanowienia, wdrożenia, utrzymywania i ciągłego poprawiania bezpieczeństwa zarządzania ryzykiem. Aby osiągnąć powyższe cele, organy zarządzania kryzysowego powinny odpowiednio oceniać ryzyko i nim zarządzać. W związku z tym niezbędna jest realizacja minimum 4 etapów czynności, które pozwolą na skuteczne działanie w przypadku wystąpienia sytuacji kryzysowej. Minimalne czynności, jakie należy wykonać to: planowanie, realizacja, sprawdzenie i naprawa (w razie konieczności).

Ponadto projekt normy N 96 ISO 18482 wymaga od organizacji ustanowienia, wdrożenia i utrzymywania sformalizowanych procesów komunikacji i konsultacji z wewnętrznymi i zewnętrznymi stronami zainteresowanymi w celu potwierdzenia, że:

- chroni ona integralność oraz poufność informacji poufnych i zastrzeżonych (w stosownych przypadkach);

- aktywa, ryzyka i obowiązki zostały odpowiednio zidentyfikowane;
- interesy stron zainteresowanych, jak również zależności i powiązania z zewnętrznymi zasobami są przez obie strony zrozumiałe i zabezpieczone;
- została wykonana ocena zagrożeń bezpieczeństwa w powiązaniu z innymi dziedzinami gospodarki;
- uwzględniono różne stanowiska i poglądy odpowiednio w kontekście ocenianych kryteriów zagrożenia dla bezpieczeństwa;
- ocena ryzyka prowadzona jest w odpowiednim kontekście wewnętrznym i zewnętrznym oraz przy uwzględnieniu parametrów istotnych dla organizacji i zainteresowanych stron;
- istnieje odpowiednia komunikacja pomiędzy osobami pracującymi dla organizacji lub w jej imieniu, oraz że osobom tym przypisano konkretne obowiązki;
- organizacja otrzymuje, dokumentuje i reaguje na komunikaty pochodzące od wewnętrznych i zewnętrznych stron zainteresowanych;
- określono i zapewniono dostępność środków komunikacji w nietypowych sytuacjach;
- wykonywane są regularne kontrole systemu zapewnienia bezpieczeństwa łączności dla warunków normalnych i szczególnych.

6.2. ISO/CD 16125 *Security management system*

W projekcie powyższej normy opisane zostały wytyczne, które dotyczą sposobu postępowania i przygotowania organizacji na wypadek powstania sytuacji o podwyższonym ryzyku.

Kluczowe znaczenie w zarządzaniu ryzykiem ma kadra kierownicza, ponieważ to właśnie ona określa kierunki działań oraz ponosi odpowiedzialność za funkcjonowanie całej organizacji. Wytyczne te są na tyle uniwersalne, że mogą być dostosowane do różnych sytuacji związanych z ryzykiem. Ponadto projekt normy opisuje etapy zarządzania ryzykiem. Praca skupia się na przeglądzie zarządzania na etapach planowania, działania i wyciągania wniosków z działań.

Ostatni etap powinien kończyć się wnioskami i opisem działań korygujących, mającymi na celu zmniejszenie lub zniwelowanie sytuacji, które mogłyby wystąpić w przyszłości.

Projekt normy ISO/CD 16125 *Security management system*:

- określa i stawia zadania dla kierownictwa najwyższego szczebla, odpowiedzialnego za funkcjonowanie organizacji;
- dostarcza wskazówek dla kierownictwa najwyższego szczebla w celu doskonalenia zdolności do reagowania podczas wystąpienia nieakceptowalnego ryzyka;

- używa wskaźników i narzędzi do oceny zdolności organizacji do zarządzania ryzykiem na etapach przygotowania, reagowania i/lub odbudowy;
- charakteryzuje role, jakie powinny panować w organizacji;
- opisuje najważniejsze etapy w zarządzaniu ryzykiem i przedstawia wytyczne na etapach planowania, działania i omówienia wniosków z działań;
- ustanawia cztery główne typy zagrożeń oraz opisuje, jakie mogą być ich konsekwencje.

W projekcie normy szczegółowo omówiono analizę ryzyka. Objąsniiono, jak przed przystąpieniem do oceny ryzyka organizacja powinna określać zewnętrzne i wewnętrzne problemy, które są istotne dla osiągnięcia planowanych celów, a także oszacować wpływ zdolności oceny do osiągnięcia zamierzonych wyników systemu zarządzania ryzykiem. Kwestie te powinny być brane pod uwagę w trakcie tworzenia, wdrażania, utrzymania i poprawy organizacji systemu zarządzania ryzykiem.

Przy tworzeniu systemu zarządzania ryzykiem organizacja powinna określić:

- charakter strony,
- wymagania (tj. potrzeby i oczekiwania).

Organizacja powinna określić także zakres wdrażanego systemu zarządzania ryzykiem oraz granice jego stosowania, które będą mogły być wyraźnie przekazane do odpowiednich stron organizacji – zarówno wewnętrznych, jak i zewnętrznych. Organizacja powinna również określić i zachować udokumentowane informacje na temat zakresu systemu zarządzania ryzykiem, w tym szczegółowe dane o wszelkich odstępstwach od założonego zakresu działalności.

Potrzeby i wymagania

Ustanawiając system zarządzania ryzykiem, organizacja musi określić zainteresowane strony, w tym kontrahentów, pracowników i partnerów z łańcucha dostaw, a także ich potrzeby i wymagania, w tym obowiązujące wymogi prawne.

Określenie kryteriów ryzyka

Organizacja powinna określić i udokumentować kryteria do oceny ryzyka. Kryteria te odzwierciedlają wartości organizacji, cele i zasoby. Przy określaniu kryteriów ryzyka organizacja uwzględni:

- wymogi prawne i regulacyjne oraz inne wymagania, do których spełnienia jest zobligowana,
- ogólną politykę zarządzania ryzykiem,
- charakter i rodzaje zagrożeń oraz ich skutki, które mogą wystąpić w trakcie jej działalności,
- prawdopodobieństwo, konsekwencje i poziom ryzyka,
- opinie zainteresowanych stron,

- poziom tolerancji ryzyka.

Ponadto w normie wyodrębniono metody analizy zagrożeń z wykorzystaniem:

- scenariusza ryzyka,
- drzewa zdarzeń,
- analizy danych zdarzeń historycznych (wykorzystanie wniosków z innych podobnych zdarzeń).

Scenariusz ryzyka

Metody scenariuszowe są narzędziem zarządzania strategicznego, wspomagającym planowanie strategii organizacji w dłuższym okresie. Metody te pozwalają organizacji przewidzieć różnego rodzaju zjawiska, które mogą wystąpić w zmieniającym się otoczeniu i przygotować się na nie. Scenariusz zawierający ryzyka może być prosty lub bardzo skomplikowany. Występujące zagrożenie w rzeczywistości nie od razu powoduje straty, ma jednak potencjał do zainicjowania takiego zdarzenia.

Drzewo zdarzeń

Drzewo zdarzeń jest graficznym modelem zależności przyczynowo-skutkowych występujących w rozpatrywanym problemie. Przy budowie drzewa zdarzeń zakłada się, że określony skutek jest wynikiem ciągu zdarzeń. Drzewo zdarzeń rozpoczyna się zatem pewnym zdarzeniem inicjującym i przedstawia wszystkie możliwe ciągi zdarzeń będące następstwami zdarzenia inicjującego. W różnych miejscach drzewa zdarzeń znajdują się węzły rozgałęzień ilustrujące fakt, że po pewnych zdarzeniach istnieje możliwość wystąpienia innych zdarzeń.

Analiza danych historycznych

Niektóre branże używają dobrze rozwiniętej metody identyfikacji zagrożeń w oparciu o wieloletnie doświadczenie. HAZOP jest wykorzystywany przez przemysł procesów chemicznych od ponad 25 lat. Podczas tworzenia HAZOP, każdy etap procesu jest kolejno analizowany, a następnie modyfikowany w celu ustalenia, co może się zdarzyć w wyniku modyfikacji procesu.

W projekcie normy ISO/CD 16125 *Security management system* zawarto również metodyki oceny ryzyka, które są procesem identyfikacji i analizy ryzyka. Proces identyfikacji ryzyka może składać się z następujących działań:

- identyfikacji ryzyka,
- analizy ryzyka,
- postępowania z ryzykiem,
- wyboru opcji postępowania z ryzykiem,
- opracowania i wdrożenia planów postępowania z ryzykiem,
- monitorowania i przeglądu.

Identyfikacja ryzyka

Organizacja zajmująca się oceną ryzyka powinna zidentyfikować źródła ryzyka, obszary jego oddziaływania, przyczyny powstania oraz potencjalne konsekwencje zdarzenia. Celem tego etapu jest tworzenie obszernej listy zagrożeń, która mogłaby poprawić i przyspieszyć realizację zamierzonych zadań. Kompleksowa identyfikacja ryzyka jest kluczowa podczas oceny, ponieważ ryzyko, które nie zostało zidentyfikowane w początkowej fazie analizy nie będzie brane pod uwagę w dalszej części analizy.

Analiza ryzyka

Analiza ryzyka jest systematycznym korzystaniem z informacji w celu identyfikacji zagrożeń. Wymaga rozważenia przyczyn, źródeł i konsekwencji ryzyka z oszacowaniem prawdopodobieństwa wystąpienia niepożądanych skutków. Czynniki, które wpływają na skutki i prawdopodobieństwo, powinny być zidentyfikowane.

Ocena ryzyka

Celem oceny ryzyka jest pomoc w podejmowaniu decyzji. W oparciu o wyniki analizy ryzyka, zidentyfikowane ryzyko może wymagać modyfikacji i przetworzenia tj. poprawy stanu zaistnienia sytuacji związanej z ryzykiem, która powinna zakończyć się podjęciem decyzji. Decyzje powinny uwzględniać szerszy zakres ryzyka i uwzględniać tolerancję ryzyka ponoszoną przez podmioty inne niż organizacja. Decyzje powinny być podejmowane i wykonane zgodnie z wymogami prawa.

Postępowanie z ryzykiem

Działanie to polega na wyborze jednej lub kilku opcji i ich realizacji. Postępowanie z ryzykiem polega na cyklicznym procesie:

- oceny podejścia do ryzyka,
- podejmowania decyzji, czy założone poziomy ryzyka są dopuszczalne, jeśli nie to podjęcie działań korygujących,
- oceny skuteczności tej analizy.

Wybór opcji postępowania z ryzykiem

Wybór najbardziej odpowiedniej opcji postępowania z ryzykiem wymaga zrównoważenia kosztów w odniesieniu do uzyskanych korzyści, wymogów prawnych i regulacyjnych oraz innych wymagań, takich jak odpowiedzialność społeczna i ochrona środowiska naturalnego. Decyzje powinny również uwzględniać ryzyko, które nie jest uzasadnione ze względów ekonomicznych.

Opracowanie i wdrożenie planów postępowania z ryzykiem

Celem planów postępowania z ryzykiem jest udokumentowanie, w jaki sposób wybrane działania naprawcze będą realizowane. Plany naprawcze powinny zawierać:

- powody wyboru działań naprawczych, w tym spodziewanych korzyści, jakie można osiągnąć,
- proponowane działania,
- wymagania dotyczące zasobów,
- środki sprawozdawczości i monitoringu,
- wydajność i ograniczenia.

Monitorowanie i przegląd

Zarówno monitorowanie, jak i przegląd wymagają regularnej kontroli lub nadzoru i powinny być planowane jako część procesu zarządzania ryzykiem. Odpowiedzialność za monitorowanie i przeglądy powinna być jasno określona, a procesy przeglądu powinny obejmować wszystkie aspekty zarządzania ryzykiem. Ponieważ większość zdarzeń jest dość skomplikowana, możliwe jest, że nie wszystkie scenariusze ryzyka zidentyfikują możliwe zagrożenia.

PODSUMOWANIE I WNIOSKI

Celem badań prowadzonych przez zespół autorski było zidentyfikowanie i przeanalizowanie wybranych dokumentów związanych z zarządzaniem ryzykiem. Od momentu wprowadzenia elementów zarządzania ryzykiem do procesu planowania cywilnego w Polsce w 2009 r. jego znaczenie stale wzrasta i uważa się je za dobrą praktykę kierowniczą. Ważne, aby pracownicy wyższego szczebla jednostek administracji państwowej, ministerstw, agencji lub władz samorządowych w pełni rozumieli koncepcję zarządzania ryzykiem. Właściwe zarządzanie ryzykiem może przynieść wartość dodaną organizacjom, które świadomie wpisują ryzyko w ramy swojej działalności i potrafią wykorzystać proces zarządzania ryzykiem w celu poprawy uzyskiwanych wyników.

Stąd też rekomendowane jest wykorzystanie wytycznych w zakresie zarządzania ryzykiem zawartych w analizowanych dokumentach przepisów prawa krajowego (krajowe powszechnie obowiązujące, resortowe, miejscowe) oraz międzynarodowych normach i standardach, które formalizują wymagania w postaci określonych rozwiązań prawnych i ujednolicają proces zarządzania ryzykiem.

Dokumenty do analizy wybierano spośród ustaw, rozporządzeń, przepisów resortowych i przepisów prawa miejscowego, ustanowionych norm i standardów oraz ich projektów. Treści aktów prawnych podlegały weryfikacji poprzez serwis prawniczy „Lex”. Weryfikacja miała na celu potwierdzenie ich statusu oraz wprowadzonych zmian w zakresie regulacji prawnych. Autorzy uznali za stosowne, aby w przeglądzie uwzględnić akty prawa ministerstw przekształcanych oraz nowo utworzonych, a także akty obowiązujące na rok 2017 oraz wchodzące w życie z dniem 1.01.2018.

W ramach rozdziału pierwszego dokonano przeglądu i analizy ustaw dotyczących zarządzania ryzykiem. Na ich podstawie sformułowano następujące wnioski:

- 1) Ustawa o zarządzaniu kryzysowym wprowadza obowiązek przeprowadzenia oceny ryzyka w planach zarządzania kryzysowego oraz tworzenia map ryzyka. Ustawa przedstawia definicję mapy ryzyka oraz zobowiązuje odpowiednie organy do przedstawienia zagrożeń do zobrazowania na mapach ryzyka w raporcie o zagrożeniach bezpieczeństwa narodowego;
- 2) Ustawa – Prawo wodne omawia kwestie ochrony zasobów wodnych, gospodarowania wodami powierzchniowymi i podziemnymi z uwzględnieniem ich ilości i jakości, a także zarządzanie zasobami wodnymi. W celu zapewnienia wspomnianej ochrony ważne jest wykonanie dla znacznych obszarów Polski

tw. wstępnej oceny ryzyka powodziowego, map zagrożenia powodziowego i map ryzyka powodziowego oraz planów zarządzania ryzykiem powodziowym. W dokumencie zawarto ponadto metodykę planowania działań związanych z ochroną przeciwpowodziową oraz podstawowe pojęcia w tym zakresie, także te powiązane z zarządzaniem ryzykiem;

- 3) Znowelizowana ustawa – Prawo wodne wchodząca w życie z dniem 1 stycznia 2018 r. zawiera zakres zmian dotyczących rozwiązań prawnych, organizacyjnych, finansowych i technicznych w gospodarowaniu wodami, kompetencji organów właściwych w sprawach gospodarowania wodami, a także katalog zadań ustawowych Wód Polskich, wśród których znajdują się zadania dotyczące zarządzania ryzykiem powodziowym i przeciwdziałanie skutkom suszy;
- 4) Opisywana w znowelizowanej ustawie – Prawo wodne (Dział IV) metodyka reguluje kwestie opracowywania wstępnej oceny ryzyka powodziowego, map zagrożenia i ryzyka powodziowego oraz planu zarządzania ryzykiem powodziowym. Wskazuje na jednolite podejście w skali kraju do opracowania wstępnej oceny ryzyka powodziowego, map zagrożenia powodziowego i map ryzyka powodziowego oraz planów zarządzania ryzykiem powodziowym;
- 5) Ustawa – Prawo wodne reguluje zagadnienia związane z opracowywaniem jednego międzynarodowego planu zarządzania ryzykiem powodziowym lub zestawu planów zarządzania ryzykiem powodziowym dla obszarów międzynarodowych dorzeczy i obszaru dorzecza znajdującego się na terytorium RP oraz obowiązki w zakresie przepływu informacji i raportowania wobec Komisji Europejskiej;
- 6) Ustalony jest tryb i zakres współpracy z organami administracji rządowej i samorządowej oraz przepływ informacji, jednak brak jest rozporządzeń wykonawczych do ustawy; w ustawie nie określono również, w jaki sposób będzie wskazywany użytkownik infrastruktury przeciwpowodziowej;
- 7) Ustawa o ochronie żeglugi i portów morskich wprowadza obowiązek stosowania na rzecz bezpieczeństwa i ochrony infrastruktury portowej elementów procesu zarządzania ryzykiem, takich jak: identyfikacja i ocena ryzyka oraz zagrożeń;
- 8) Ustawa – Prawo ochrony środowiska wprowadza pojęcie ryzyka w ramach regulowanego przez ten dokument obszaru działalności administracji publicznej. W ustawie zawarto opis sposobu raportowania ryzyk w zakresie ochrony ziemi, roślin, zwierząt, powietrza oraz walorów przyrodniczych środowiska. Wskazano ponadto, jak na dalszym etapie wygląda postępowanie ze zidentyfikowanym ryzykiem;
- 9) Ustawa o Państwowej Inspekcji Sanitarnej określa zadania z zakresu ochrony zdrowia, w tym działania wpisujące się w obszar planowania cywilnego, związane z zapobieganiem i zwalczaniem chorób;

- 10) Ustawa o finansach publicznych stanowi przydatne narzędzie dla osób zajmujących się organizacją zarządzania ryzykiem. Dokument wskazuje także na kontrolę zarządczą, która ma zastosowanie także w innych obszarach działalności niż sprawy związane z finansami.

W rozdziale drugim dokonano charakterystyki przepisów uwzględniających problematykę ryzyka w zakresie szeroko rozumianego bezpieczeństwa powszechnego oraz obowiązków sporządzania oceny ryzyka w procesie planowania cywilnego. Kwestie obejmujące elementy procesu oceny ryzyka zostały wprowadzone do polskiego porządku prawnego poprzez ustawę o zarządzaniu kryzysowym, której nowelizacja z 2009 r. wprowadziła obowiązek sporządzania oceny ryzyka w procesie planowania cywilnego, natomiast drugą jest ustawa – Prawo wodne.

Należy wskazać, że dyskurs nad tym rozporządzeniem z punktu widzenia planowania cywilnego, a więc i tworzenia planów zarządzania kryzysowego, był niezwykle istotny, ponieważ:

- analiza dokumentów stanowiących podstawę dla planów, jakimi są raporty cząstkowe i raport o zagrożeniach bezpieczeństwa narodowego pozwala zauważyć, że powódź jest zagrożeniem występującym w każdym z tych dokumentów; jest ona wskazywana przez twórców ww. dokumentów jako jedno z najistotniejszych zagrożeń bezpieczeństwa powszechnego. Należy przyjąć, że większość planów zarządzania kryzysowego przygotowywanych na wszystkich poziomach administracji powinno zawierać procedury przeciwpowodziowe;
- biorąc pod uwagę warunek, że zagrożenia wskazywane w PZK powinny zostać poprzedzone analizą ryzyka¹, a dokumenty wykonujące tę dyrektywę prezentują katalog zagrożeń², można wnioskować, że ryzyko dla zagrożeń powodziowych jest najbliższe jego rzeczywistej wartości;
- analizy odnoszące się do zmian klimatycznych wskazują, że wraz ze zmieniającym się klimatem zagrożenie powodziowe będzie wzrastać³, ryzyko powodziowe staje się tym samym coraz bardziej istotne;
- analizowane rozporządzenie w sprawie opracowywania map zagrożenia powodziowego oraz map ryzyka powodziowego zawiera załącznik, w którym opisany jest sposób obliczania wartości potencjalnych strat powodziowych dla poszczególnych klas użytkowania terenu na potrzeby opracowania map

¹ Jest to warunek wpływający na przykład z rozporządzenia w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego.

² W konsekwencji metoda stosowana dla spełnienia warunku oceny jest generalna dla każdego ryzyka, a więc nieuwzględniająca wszystkich możliwych aspektów zagrożeń.

³ Mówi o tym m.in. Ramowa Konwencja Narodów Zjednoczonych w sprawie Zmian Klimatu (ang. *United Nations Framework Convention on Climate Change*, UNFCCC) podpisana 9 maja 1992 r. w Rio de Janeiro oraz raporty Międzyrządowego Zespołu do spraw Zmian Klimatu (IPCC), które ukazały się 1990, 1995, 2001 i 2007 roku.

ryzyka powodziowego. Przedstawia on także metodykę określenia sumarycznej wartości potencjalnych strat powodziowych dla poszczególnych klas użytkowania terenu;

- mapy zagrożenia powodziowego i mapy ryzyka powodziowego jako dokumenty planistyczne stanowią w praktyce nietechniczny środek ochrony przeciwpowodziowej mający na celu ograniczenie potencjalnych negatywnych konsekwencji powodzi⁴.

Rozdział trzeci poświęcony został analizie aktów prawa resortowego związanego z zarządzaniem ryzykiem, którego elementy mogą zostać wykorzystane przy opracowywaniu metodyk analizy bądź oceny ryzyka oraz w procesie zarządzania ryzykiem. Celem ustanowienia zasad zarządzania ryzykiem w urzędach centralnych i działach administracji rządowej jest zapewnienie mechanizmów identyfikowania, określania oddziaływania, prawdopodobieństwa i istotności ryzyk oraz podejmowania adekwatnych działań zapobiegawczych w celu minimalizacji ryzyka oraz poprawy efektywności i skuteczności realizacji celów i zadań właściwego ministra.

Badania wybranych zarządzeń i rozporządzeń pozwalają stwierdzić, że dotychczas nie powstała ujednoczona, wspólna dla wszystkich resortów i urzędów centralnych ścieżka procesu zarządzania ryzykiem. Przedsięwzięcia zmierzające do jej opracowania są realizowane od kilku lat i nadal nie można ich uznać za zakończone. Na podstawie analizowanych aktów prawnych można sformułować następujące tezy:

- 1) Kluczowym elementem w zarządzaniu ryzykiem jest jego właściwa identyfikacja;
- 2) Przy dobrze zidentyfikowanych zagrożeniach kontrola ryzyka wymaga mniejszych nakładów finansowych oraz czasowych;
- 3) Istotne jest również dobieranie takich mechanizmów kontroli ryzyka, aby zagrożenie cały czas było monitorowane, a w razie konieczności reakcja była szybka i skuteczna;
- 4) Właściwie skonstruowany, kompleksowy rejestr ryzyka będący podstawowym narzędziem oceny ryzyka może być źródłem kompleksowej informacji do zarządzania ryzykiem. Dostęp do kompleksowej informacji o ryzyku zwiększa skuteczność zarządzania nim i wpływa na efektywność kontroli zarządczej;
- 5) Najważniejszą zmianą powinno być doprecyzowanie przepisu zarządzania ryzykiem w każdym z resortów. Rozdziały poświęcone kontroli zarządczej powinny w większym stopniu opisywać wymagania dotyczące zarządzania ryzykiem, odnoszące się do: sposobów i środków reagowania, organizacji monitoringu czy przygotowania planów naprawczych;

⁴ Raport z wykonania map zagrożenia powodziowego i map ryzyka powodziowego, KZGW s. 115, (<http://mapy.isok.gov.pl>) [dostęp: sierpień 2017].

- 6) Należy uznać, że zaproponowane w analizowanych zarządzeniach rozwiązania do zarządzania ryzykiem, będą stanowiły podstawę właściwego ładu organizacyjnego jednostki, czyli kombinacji procesów i struktur wprowadzonych w jednostce w celu uzyskania kompleksowego przepływu informacji, zarządzania, kierowania oraz monitorowania działań nakierowanych na realizację misji, celów i zadań;
- 7) Porównując analizowane przez autorów zarządzenia, można zauważyć, że wszystkie metodyki zarządzania ryzykiem są do siebie zbliżone, a jedyną istotną różnicą między nimi są cele, do jakich się odnoszą. Jest to bardzo istotna kwestia ponieważ, świadczy o tym, że we wszystkich resortach może zostać wprowadzona wspólna metodyka zarządzania ryzykiem. Każdy z resortów będzie miał za zadanie odpowiednie jej dopasowanie do własnych celów oraz staranne dobranie mechanizmów kontroli;
- 8) Sprawna realizacja procesu zarządzania ryzykiem obejmuje co najmniej identyfikację ryzyka, jego analizę, sposoby reakcji na ryzyko i działania zaradcze. Na każdym etapie proces zarządzania ryzykiem należy odpowiednio udokumentować, a dokumentacja całego procesu powinna tworzyć spójną całość.

Rozdział czwarty prezentuje wybrane dokumenty normatywne, w których odnaleźć można charakterystykę procesu zarządzania ryzykiem w jednostkach samorządu terytorialnego, w tym metodyki zarządzania ryzykiem oraz wykorzystywaną terminologię.

Analiza przepisów prawa miejscowego wykazała, że w województwie mazowieckim i w wybranych jednostkach administracyjnych niższego szczebla na obszarze tego województwa stosowane są dobre praktyki z zakresu zarządzania ryzykiem, zalecane przez krajowe oraz zagraniczne podmioty i instytucje związane z tym obszarem aktywności, tj.: Międzynarodową Organizację Normalizacyjną (ISO), Federację Europejskich Stowarzyszeń Zarządzania Ryzykiem (FERMA) czy Komisję Nadzoru Finansowego.

Poszczególne akty prawa miejscowego zawierają zarówno terminologię związaną z zarządzaniem ryzykiem, jak i role oraz zadania organów uczestniczących w procesie zarządzania ryzykiem.

Na podstawie przeprowadzonej analizy należy wskazać, że:

- 1) Na przykładzie Mazowieckiego Urzędu Wojewódzkiego kontrola zarządcza oraz działania w zakresie zarządzania ryzykiem zostały uregulowane odpowiednim zarządzeniem. Dokument ten określa podstawowe zadania i zasady wykonywania kontroli zarządczej, jednostki organizacyjne biorące udział w procesie zarządzania ryzykiem, jak również podstawową terminologię;
- 2) Zarządzenie Nr 828/2015 Prezydenta m.st. Warszawy w sprawie systemu zarządzania ryzykiem w Warszawie powołuje komórki właściwe w sprawach zarządzania ryzykiem; funkcjonowanie systemu dostosowane jest do specyfiki

złożoności struktury organizacyjnej urzędu oraz samego miasta, zakresu delegowanych uprawnień i pełnomocnictw oraz realizowanych celów i zadań na poszczególnych poziomach zarządzania;

- 3) Ww. zarządzenie zawiera szczegółowe wytyczne dotyczące zasad, procedur, zadań i obowiązków organów odpowiedzialnych za zarządzanie ryzykiem, określa zakres zadań, obowiązków i kompetencji należących do wszystkich uczestników systemu zarządzania ryzykiem, w tym Prezydenta m.st. Warszawy, nie pomijając przy tym relacji, w jakich się znajdują z innymi podmiotami;
- 4) Terminologia stosowana w ramach systemu zarządzania ryzykiem m.st. Warszawy została oparta o normę PN-ISO 31000:2012 Zarządzanie ryzykiem - Zasady i wytyczne;
- 5) Zarządzenie Nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku w sprawie wprowadzenia polityki zarządzania ryzykiem oraz Zarządzenie Nr 156/2014 Burmistrza Karczewa z dnia 22 grudnia 2014 roku w sprawie wprowadzenia instrukcji dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej wprowadzają do stosowania terminologię w ramach polityki zarządzania ryzykiem. Określają również role i zadania organów uczestniczących w procesie zarządzania ryzykiem i kontroli zarządczej w celu zapewnienia osiągnięcia wyznaczonych celów, a także poprawy jakości oraz efektywności zarządzania na poziomie jednostki samorządu terytorialnego, jaką jest gmina;
- 6) W poddanych analizie dokumentach prawa miejscowego zwraca się uwagę na potrzebę skutecznej identyfikacji ryzyk i zarządzania nimi; załączone do nich przykładowe dokumenty stanowią wsparcie merytoryczne dla osób wykonujących zadania związane z procesem oceny ryzyka. Zarządzanie ryzykiem to kwestia kluczowa dla jednostek administracji samorządowej szczebla gminnego, powiatowego oraz wojewódzkiego, a omawiane zarządzenia są dokumentami szeroko sankcjonującymi omawiane zagadnienie;
- 7) Organizacje, które w realizacji swoich zadań świadomie uwzględniają proces zarządzania ryzykiem, będą także w stanie wykorzystać ten proces na rzecz aktywności w zakresie szeroko pojętego bezpieczeństwa;
- 8) Ważnymi obszarami, których nie dotyczą wdrożone systemy zarządzania ryzykiem – a zdaniem zespołu autorskiego powinny – są przede wszystkim zarządzanie kryzysowe, obrona cywilna i ochrona ludności, jak również zarządzanie informacją w omówionych jednostkach organizacyjnych.

W wyniku przeprowadzonej analizy wybranych norm i standardów z zakresu zarządzania ryzykiem przedstawionych w rozdziale piątym, sformułowano następujące wnioski:

- 1) Norma ISO 31000 powinna stanowić dla organizacji podstawę tworzenia systemu zarządzania ryzykiem ze względu na swoją uniwersalność, a jednocześnie uwzględnienie w przedstawionej przez nią metodyce kluczowych elementów zarządzania ryzykiem;
- 2) Norma ISO/IEC 31010:2009 *Risk management – Risk assessment techniques* stanowi doskonałe narzędzie dla osób zajmujących się zarządzaniem ryzykiem, ponieważ zawiera opisy ponad 30 różnych metod analizy ryzyka. Każda z metod (jakościowe, jak i ilościowe) posiada swoje cechy charakterystyczne; osoby odpowiedzialne za proces oceny ryzyka mogą dokonać wyboru optymalnej metody w zależności od sytuacji i aktualnych potrzeb;
- 3) Norma CAN/CSA-Q850-97:2009 *Risk Management: Guideline for Decision-Makers* zawiera wiele przydatnych informacji z zakresu zarządzania ryzykiem w kontekście procesu podejmowania decyzji. Informacje zawarte w normie mogą być wykorzystane zarówno przez kadrę kierowniczą/zarządzającą w jednostkach administracji rządowej i samorządowej, jak i w podmiotach prywatnych. Dokument ten stanowi uzupełnienie normy ISO 31000;
- 4) BSI-Standard 100-4 w sposób bezpośredni odnosi się do analizy ryzyka w kontekście przedsiębiorstwa. Przedmiotem standardu nie jest postępowanie w przypadku sytuacji kryzysowych, w których stosuje się szeroko pojęte ratownictwo, tj. klęsk żywiołowych w obszarze działania służb ratowniczych czy władz terytorialnych. Opisuje on zasady zarządzania kryzysowego, analizy ryzyka i postępowania w sytuacjach niekorzystnych w organizacjach, firmach i przedsiębiorstwach. Z badawczego punktu widzenia opisana metoda/metody analizy ryzyka nie wnoszą istotnych rozwiązań. Opisana metodyka jest zbieżna z współcześnie stosowanymi działaniami, które ponadto opisane są również w innych dokumentach normatywnych i wytycznych;
- 5) Wytyczne OECD *Guidelines for the Security of Information Systems and Networks* odnoszą się do bezpieczeństwa systemów informatycznych i sieci. Przedstawiają w skrócie potrzebę dokonywania analizy ryzyk, nie przedstawiają żadnej metody, metodyki czy zasad przeprowadzania takiej analizy;
- 6) Poddane analizie dokumenty BSI-Standard 100-4 *Business Continuity Management* oraz OECD *Guidelines for the Security of Information Systems and Networks* zawierają elementy analizy ryzyka, jednakże żaden z nich nie odnosi się do analizy ryzyka w rozumieniu zarządzania kryzysowego w sytuacjach kryzysowych, czy działalności służb ratowniczych. Bliższy przedmiotowej tematyce jest dokument BSI Standard 100-4, ponieważ dokładniej opisuje wybraną metodę analizy ryzyka, aczkolwiek nie może on stanowić jedynej podstawy kryterialnej do stworzenia możliwej do zastosowania metodyki analizy ryzyka;

- 7) Norma PKN-CEN/CWA 15537 odnosi się bezpośrednio do tworzonego nowego systemu, który ma zwiększyć efektywne wykorzystanie zasobów krajowych w celu sprawnego zarządzania operacjami krajowymi i europejskimi. Norma nie opisuje konkretnej metodyki analizy ryzyka. Opisuje podstawowe wytyczne do wdrożenia systemu SOA oraz elementy krytyczne, na które należy zwrócić szczególną uwagę przy wdrażaniu systemu.

Ciągłe doskonalenie systemu zarządzania ryzykiem może w przyszłości w znaczący sposób poprawić bezpieczeństwo. Dobra i sprawdzona praktyka umożliwi organizacjom uchronienie się od wystąpienia zagrożenia. Przeanalizowane w rozdziale szóstym projekty norm ISO/CD 16125 *Security management system* oraz N 96 ISO 18482 *Security Management System – Guidance for use – Security risk assessment* przedstawiają ogólne wytyczne do obniżania ryzyka, ponieważ zarządzanie bezpieczeństwem, jak i powstające problemy stwarzają trudności do stworzenia jednego schematu pasującego do wszystkich sytuacji i zdarzeń.

Projekt normy ISO/CD 16125 *Security management system* przyjmuje za stosowne opracowanie kilku scenariuszy, które muszą zostać określone na wypadek wystąpienia zdarzenia niepożądanego. Zastosowanie tej normy przewidziane jest np. dla zakładów chemicznych, militarnych. Metoda „burzy mózgów” wspomagana przez drzewo zdarzeń jest pomocna w identyfikacji możliwych do wystąpienia zdarzeń oraz ich skutków. Jeśli możliwe skutki zagrożenia są określone w scenariuszu ryzyka, zespół powinien dokonać porównań polegających na przypisaniu każdemu zdarzeniu początkowej częstotliwość oraz określić skutki jego wystąpienia.

W projekcie normy N 96 ISO 18482 *Security Management System – Guidance for use – Security risk assessment* opisane zostały wytyczne dla organizacji, dotyczące sposobu postępowania i przygotowywania się do sytuacji kryzysowej. Wytyczne te są na tyle uniwersalne, że mogą być wykorzystywane przez różne podmioty np. organy zarządzania kryzysowego. Projekt normy opisuje również sytuację, w której poziom ryzyka został już oszacowany i przeanalizowany.

Organy zarządzania ryzykiem powinny mieć świadomość swoich możliwości i z tego względu konieczna jest regularna ocena i ewaluacja ich przygotowania. Różnicowane funkcje i role w zarządzaniu ryzykiem są dzielone pomiędzy organizacje i agencje (rządowe), sektor prywatny i publiczny na różnych poziomach/szczeblach, co często powoduje dysonans w ocenie zdolności do reagowania.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

- Wróblewski D., Sowa T., *Zarządzanie ryzykiem. Zagadnienia ogólne*, CNBOP, Józefów 2009, s. 68–69.
- Zarządzanie ryzykiem w sektorze publicznym – Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce*, wyd. Bentley Dennison, Warszawa 2007.

Akty prawne

- Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (Dz. U. z 2017 r. poz. 1261).
- Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (tekst jedn. Dz. U. z 2017 r. poz. 519 z późn. zm.).
- Ustawa z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. z 2001 r. Nr 115, poz. 1229 z późn. zm.).
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.).
- Ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2017 r. poz. 519 z późn. zm.).
- Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870 z późn. zm.).
- Ustawa z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. poz. 1566).
- Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 16 grudnia 2015 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie żeglugi i portów morskich (Dz. U. z 2016 r. poz. 49).
- Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 14 października 2016 r. w sprawie ogłoszenia jednolitego tekstu ustawy o finansach publicznych (Dz. U. z 2016 r. poz. 1870 z późn. zm.).
- Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 stycznia 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zarządzaniu kryzysowym (Dz. U. z 2017 r., poz. 209).
- Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 8 czerwca 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy o Państwowej Inspekcji Sanitarnej (Dz. U. z 2017 r. poz. 1261).
- Dyrektywa 2000/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2000 r. ustanawiająca ramy wspólnotowego działania w dziedzinie polityki wodnej (Dz. Urz. UE L 327 z 22.12.2000, s. 1–73).
- Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz. Urz. UE L 288, z 06.11.2007, s. 27–34).

- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. z 2010 r. Nr 83, poz. 541).
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. z 2010 r. Nr 83, poz. 540).
- Rozporządzenia Rady Ministrów z dnia 7 grudnia 2015 r. w sprawie utworzenia Ministerstwa Rozwoju oraz zniesienia Ministerstwa Gospodarki.
- Rozporządzenie Prezesa Rady Ministrów z dnia 30 września 2016 r. w sprawie szczegółowego zakresu działania Ministra Rozwoju i Finansów (Dz. U. poz. 1595).
- 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 r., poz. 104).
- Rozporządzenia Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz. U. MRiF poz. 637).
- Rozporządzenie Ministra Rozwoju i Finansów z dnia 25 kwietnia 2017 r. w sprawie kapitału wewnętrznego, systemu zarządzania ryzykiem, programu oceny nadzorczej oraz badania i oceny nadzorczej, a także polityki wynagrodzeń w domu maklerskim (Dz. U. poz. 856).
- Zarządzenie Nr 4 Ministra Administracji i Cyfryzacji z dnia 25 stycznia 2013 r. w sprawie powołania Zespołu do spraw zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji (Dz. Urz. MAiC poz. 4).
- Zarządzenie nr 1 Ministra Cyfryzacji z dnia 12 stycznia 2016 r. w sprawie powołania Komitetu Audytu (Dz. Urz. MC. poz. 1).
- Zarządzenie Nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w działach administracji rządowej - administracja publiczna, sprawy wewnętrzne, wyznania religijne oraz mniejszości narodowe i etniczne (Dz. Urz. MSWiA poz. 16).
- Zarządzenie Nr 9 Ministra Cyfryzacji z dnia 5 kwietnia 2016 r. w sprawie Karty Audytu Wewnętrznego w Ministerstwie Cyfryzacji (Dz. Urz. MC poz. 9).
- Zarządzenie Nr 19 Ministra Infrastruktury i Budownictwa z dnia 16 czerwca 2016 r. w sprawie ustalenia opisu systemu kontroli zarządczej w Ministerstwie Infrastruktury i Budownictwa (Dz. Urz. MiiB poz. 46).
- Zarządzenie Nr 27 Ministra Spraw Zagranicznych z dnia 26 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych (Dz. Urz. MSZ poz. 34).
- Zarządzenie Nr 45 Ministra Cyfryzacji z dnia 29 listopada 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – informatyzacja (Dz. Urz. MC poz. 52).
- Zarządzenie Ministra Rozwoju i Finansów z dnia 21 grudnia 2016 r. w sprawie kontroli zarządczej w Ministerstwie Rozwoju (Dz. Urz. MRiF poz. 33).
- Zarządzenie Ministra Rozwoju i Finansów z dnia 3 marca 2017 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Finansów (Dz. Urz. MRiF poz. 46, z późn. zm.).

- Zarządzenie Ministra Rozwoju i Finansów z dnia 8 czerwca 2017 r. w sprawie systemu kontroli zarządczej w Ministerstwie Finansów (Dz. Urz. MRiF poz. 116).
- Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Min. Fin. poz. 84).
- Komunikat Ministra Infrastruktury i Budownictwa z dnia 16 czerwca 2016 r. w sprawie szczegółowych wytycznych w zakresie kontroli zarządczej dla Ministerstwa Infrastruktury i Budownictwa oraz działów administracji rządowej - budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, łączność, transport. (Dz. Urz. MliB poz. 45).
- Zarządzenie Wojewody Mazowieckiego Nr 1140 z dnia 20 listopada 2015 r. w sprawie powołania Zespołu do spraw kontroli zarządczej i zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.
- Zarządzenie Nr 587 Wojewody Mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.
- Zarządzenie Nr 828/2015 Prezydenta Miasta Stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.
- Zarządzenie Nr 156/2014 Burmistrza Karczewa z dnia 22 grudnia 2014 roku w sprawie wprowadzenia instrukcji dokonywania samooceny oraz sporządzania oświadczenia o stanie kontroli zarządczej.
- Zarządzenie Nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku w sprawie wprowadzenia polityki zarządzania ryzykiem.
- Zarządzenie Nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (Dz. Urz. WUG z 2015 r. poz. 65).

Normy i standardy

- BSI-Standard 100-4 Business Continuity Management.
- CAN/CSA-Q850-97:2009 Risk Management: Guideline for Decision-Makers.
- ISO 31000:2009 Risk management – Principles and guidelines.
- ISO Guide 73:2009 Risk management — Vocabulary.
- ISO/CD 16125 Security management system.
- ISO/IEC 31010:2009 Risk management – Risk assessment techniques.
- N 96 ISO 18482 Security Management System – Guidance for use-Security risk assessment.
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
- PKN-CEN/CWA 15537 Network Enabled Abilities – Service-Oriented Architecture for civilian and military crisis management.

Dokumenty elektroniczne, strony internetowe i inne

- <http://mapy.isok.gov.pl>.
- <http://mr.bip.gov.pl/informacje-o-ministerstwie.html>.
- <http://www.isok.gov.pl>.

<https://legislacja.rcl.gov.pl>.

<https://sip.lex.pl>.

Komunikat prasowy 1/10/2015 – Prezesi i rządy powinny traktować bezpieczeństwo cyfrowe jako zagrożenie ekonomiczne – mówi OECD.

KZGW, Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych, Etap I, Kraków 2012.

KZGW, Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych, Kraków 2013.

OECD, Digital Security Risk Management for Economic and Social Prosperity, 2015, [dok. elektr.] <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>.

CZEŚĆ II

ZAGADNIENIA OGÓLNE Z ZAKRESU ZARZĄDZANIA RYZYKIEM

WPROWADZENIE

W licznych opracowaniach poświęconych ostatniemu kryzysowi finansowemu stawia się diagnozę, że został on spowodowany niedoskonałością zarządzania ryzykiem¹. Analitycy sugerują również, że zbyt ulgowo podchodzono do obszaru tzw. ryzyka relikтового². Niezależnie od źródeł tego kryzysu, w zakresie zarządzania ryzykiem wdrożonych zostało wiele działań naprawczych. W 2009 r. wprowadzono zasady zarządzania ryzykiem i opracowano przewodnik po nowych standardach.

Punktem wyjścia było stwierdzenie, że niepodejmowanie ryzyka nie prowadzi do sukcesów ani nie jest drogą wiodącą do postępu, ale z drugiej strony nadmierne ryzyko może zadziałać z podobnym skutkiem. Przede wszystkim uznano więc, że skuteczność zarządzania ryzykiem zależy od jego właściwej oceny. Ryzyko nie może być ani przeszacowane, ani niedoszacowane. Nowe normy dotyczące zarządzania ryzykiem to rezultat prac zespołu ekspertów z 28 krajów ze wszystkich kontynentów. Odbłyło się wiele spotkań, służących wymianie myśli i doświadczeń. Organizowane one były w różnych krajach, gromadziły od 40 do 60 delegatów. W spotkaniach tych uczestniczyła zawsze grupa stała, czuwająca nad koordynacją i kontynuacją prac. Prace tego zespołu były wspierane przez narodowe zespoły zarządzania ryzykiem, w Polsce np. przez POLRISK.

Wynikiem prac ekspertów w takiej formule był pełen kompromis w postaci nowej normy, zalecanej do zaadaptowania w każdym uwarunkowaniu. Norma ISO 31000:2009³ jest zestawem zasad, ram i procesów do zastosowania w każdej organizacji w zakresie zarządzania ryzykiem i szerzej – zarządzania kryzysowego. Nie daje gotowych rozwiązań, ale komponenty zarządzania ryzykiem do zaadaptowania w systemach, służące poprawie ich skuteczności. Wdrożenie tych komponentów nie komplikuje działań organizacji, ale zwiększa szanse osiągnięcia

¹ *Wnioski wypływające z kryzysu finansowego z perspektywy nadzorczej*, prezentacja ze spotkania szefów banków działających w Polsce z kierownictwem UKNF, Warszawa, 25 lutego 2011 [dok. elektr.], http://www.knf.gov.pl/Images/Wnioski_wplywajace_z_kryzysu_tcm75-25681.pdf [dostęp: czerwiec 2013].

² Ryzyko reliktowe (rezydualne, szczątkowe) [ang. *residual risk*] – pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 3.8.1.6. Patrz szerzej: D. Wróblewski (red.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 174.

³ Wersja polska normy: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.

jej celu. Należy podkreślić, że warunkiem jest zastosowanie wspólnej, zrozumiałej terminologii, przejrzystych procesów oraz dysponowanie wystarczającym zasobem informacji.

W rozdziale pierwszym przedstawione zostały potrzeby i korzyści związane z systemowym podejściem do problemu zarządzania ryzykiem. Za przykład w kontekście prowadzonych badań wskazano normę ISO 31000:2009, rekomendując ten dokument jako podstawę do uniwersalnego i kompleksowego zastosowania w organizacjach, które na co dzień stykają się z szeroko rozumianym ryzykiem. Przedstawione zostały także przykłady dokumentowania procesu zarządzania ryzykiem. W rozdziale drugim znalazł się opis wybranych metod oceny ryzyka, możliwych do zastosowania także w ramach planowania cywilnego.

1. ZARZĄDZANIE RYZYKIEM WEDŁUG NORMY ISO 31000

Zarządzanie ryzykiem¹ stało się wyznacznikiem i integralnym elementem kultury organizacyjnej², co oznacza przełożenie na cele strategiczne³, taktyczne i operacyjne⁴ oraz ściśle sprecyzowanie odpowiedzialności⁵ ludzi w ujęciu jednostkowym, funkcyjnym i terytorialnym.

Niezwykle istotną kwestią w tym obszarze jest przyjęcie wspólnych standardów, co jednak wcale nie jest proste, dlatego wiele państw do 2009 r. bazowało na normach wypracowanych przez krajowe instytucje normalizacyjne. Obecnie sięga się po międzynarodowe normy ISO, co zapewnia ujednoczenie pojęć w danym obszarze na szczeblu międzynarodowym.

Nad doskonaleniem międzynarodowych norm pracują zespoły interdyscyplinarne – złożone z inżynierów, ludzi biznesu, naukowców, członków władz i różnych ekspertów, którzy badają funkcjonowanie systemów. Ich praca – dyskusje, wymiana myśli i poglądów – skupia się na poszukiwaniu uniwersalnych rozwiązań, wywodzących się wprost ze zbioru doświadczeń, które zdobyli ze swojego obszaru działalności. Procedury opracowania norm przewidują obowiązkowy etap ankietowania,

¹ Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka. Źródło: ISO Guide 73:2009, definicja 2.1.

² Kultura organizacyjna – normy społeczne i systemy wartości stymulujące pracowników, właściwy klimat organizacyjny, sposób zarządzania, podzielane znaczenia i symbole, schematy poznawcze, wymogi zachowania. Źródło: B. Nogalski, *Kultura organizacyjna. Duch organizacji*, Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz 1998, s. 105. To także: system wzorów myślenia i działania, które są utrwalone w środowisku społecznym organizacji i mają znaczenie dla realizacji jej formalnych celów. Źródło: C. Sikorski, *Kultura organizacyjna*, C.H. Beck, Warszawa 2002, s. 4.

³ Cel strategiczny – określony podmiotowo i przedmiotowo przyszły, pożądany przez organizację stan rzeczy, będący rezultatem interakcji aprobowanych przez większość jej członków co do interesów uznawanych za mające istotne znaczenie w odniesieniu do warunków występujących w otoczeniu, przewidywany do osiągnięcia w dłuższej perspektywie czasowej. Źródło: *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2008, s. 25.

⁴ Cele taktyczne i operacyjne – cele taktyczne dotyczą części organizacji lub przedsiębiorstwa znajdującej się powyżej jednostki, np. działów, wydziałów itp., cele operacyjne dotyczą zawsze pojedynczych osób. Cele taktyczne i operacyjne są uzgadniane lub ustalane w sposób wiążący na okres jednego roku i formułowane zgodnie z kryteriami jakości. Źródło: P. Maas, *Wiedza praktyczna: Zarządzanie poprzez cele*, wyd. Verlag Dashofer, Warszawa 2004, s. 4–5 [dok. elektr.], <http://www.dashofer.pl/przyklady/ED-ZPC.pdf> [dostęp: marzec 2015].

⁵ A Risk Management Standard, IRM 2002, s. 2.

tj. poddawania normy publicznej dyskusji – po to, by wyeliminować możliwe niedoskonałości i zdobyć dla niej poparcie wśród specjalistów. Normy międzynarodowe, ale również europejskie i krajowe, można podzielić na normy zawierające wymagania ogólne, pewne zasady oraz normy zawierające wymagania szczegółowe. Cechą charakterystyczną tzw. norm ogólnych jest ich elastyczność, tj. możliwość przełożenia wymagań w nich zawartych na organizacje czy systemy o różnorodnej specyfice. Innymi słowy, niezależnie od rodzaju prowadzonej działalności czy świadczonych usług organizacje mają możliwość zastosowania wymagań tej samej normy. Normy zawierające wymagania szczegółowe odnoszą się zazwyczaj do konkretnych grup wyrobów, procesów czy systemów. Oba rodzaje norm są stosowane w różnych państwach, w zależności od wyznaczonego celu, warunków technicznych, klimatycznych, geograficznych, infrastruktury i potrzeb bezpieczeństwa.

W rozdziale pierwszym przedstawiono potrzeby i korzyści związane z systemowym podejściem do problemu zarządzania ryzykiem. Analizie poddano normę ISO 31000:2009, oceniając ten dokument pod kątem wykorzystania jego wytycznych w organizacjach, podkreślając elementy użyteczne w planowaniu cywilnym. Uzupełnienie rozdziału stanowi charakterystyka dokumentowania procesów zarządzania ryzykiem, ze szczególnym uwzględnieniem jego znaczenia oraz zalet.

1.1. Norma ISO 31000:2009 – zakres i przeznaczenie

Normy dotyczące zarządzania ryzykiem dają organizacjom (także systemom bezpieczeństwa) podstawowe zasady, w ramach których powinny one się poruszać. Wspierają je także w⁶:

1. Działaniach organizacyjnych polegających na:
 - zwiększeniu prawdopodobieństwa osiągnięcia celu,
 - uświadomieniu potrzeby identyfikacji ryzyka⁷,
 - stosowaniu właściwych, wymaganych regulacji prawnych i norm międzynarodowych,
 - zwiększaniu zaufania i pewności wśród zainteresowanych podmiotów,
 - ustanowieniu dogodnej bazy dla planowania i podejmowania decyzji,
 - efektywnej alokacji i wykorzystaniu zasobów w zakresie postępowania z ryzykiem⁸,
 - zapewnieniu ustalonych norm zdrowia i bezpieczeństwa oraz ochrony środowiska,

⁶ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 14–16.

⁷ Identyfikacja ryzyka – proces wyszukiwania, rozpoznawania i opisywania ryzyka. Źródło: ISO Guide 73:2009, definicja 3.5.1.

⁸ Postępowanie z ryzykiem – proces modyfikacji ryzyka m.in. poprzez unikanie ryzyka, podjęcie lub zwiększenie ryzyka, usunięcie źródła ryzyka, zmianę następstw, dzielenie ryzyka, retencję ryzyka. Źródło: ISO Guide 73:2009, definicja 3.8.1.

- minimalizowaniu strat.
2. Działaniach doskonalących w zakresie:
- identyfikacji szans i zagrożeń,
 - sprawozdawczości finansowej,
 - organizacji procesów,
 - procesu kontroli,
 - operacyjnej skuteczności i efektywności systemu,
 - zapobiegania stratom i kierowania w miejscach zdarzeń (incydentów),
 - wykorzystania doświadczeń w organizacji,
 - elastyczności organizacyjnej.

Międzynarodowa norma zarządzania ryzykiem wprowadziła cztery zasadnicze ustalenia⁹:

- zmieniła definicję ryzyka¹⁰ na „wpływ niepewności na cele”,
- wdrożyła jedenaście zasad zarządzania ryzykiem,
- podała pięć atrybutów określających ramy zarządzania ryzykiem,
- włączyła rekomendacje w zakresie podejścia do rozwoju ram zarządzania ryzykiem w skali całej organizacji.

Wprowadzona w 2009 r. norma ISO 31000 jest przede wszystkim zbiorem ram, procesów i zasad, których należy przestrzegać przy wdrażaniu procesu oceny ryzyka w każdej organizacji. Norma ta wskazuje, że każda ocena ryzyka¹¹, nieważne, czy dotycząca bezpieczeństwa informacji, ryzyka finansowego czy innego obszaru, powinna kierować się zaleceniami nowej normy – przy założeniu, że głównym celem ISO 31000 nie jest zamiana wymagań innych standardów, lecz ujednoczenie w nich procesów zarządzania ryzykiem¹². W związku z tym, że ISO 31000 nie wyspecyfikowano dla wybranego sektora czy dla konkretnego przedsiębiorstwa, potencjalnych użytkowników dokumentu określono terminem „organizacja”. Dlatego też zawarte w tej normie zalecenia mogą być wykorzystane przez przedsiębiorstwa o dowolnej formie własności, stowarzyszenia i grupy, a nawet osoby fizyczne¹³.

⁹ AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, Australian Government, August 2010, Fact Sheet, s. 1 [dok. elektr.], http://www.finance.gov.au/sites/default/files/COV_216905_Risk_Management_Fact_Sheet_FA3_23082010_0.pdf [dostęp: czerwiec 2013].

¹⁰ Ryzyko – wpływ niepewności na cele. Źródło: ISO Guide 73:2009, definicja 1.1. Patrz szerzej: D. Wróblewski, (red.), *Przegląd...*, dz. cyt., s. 173.

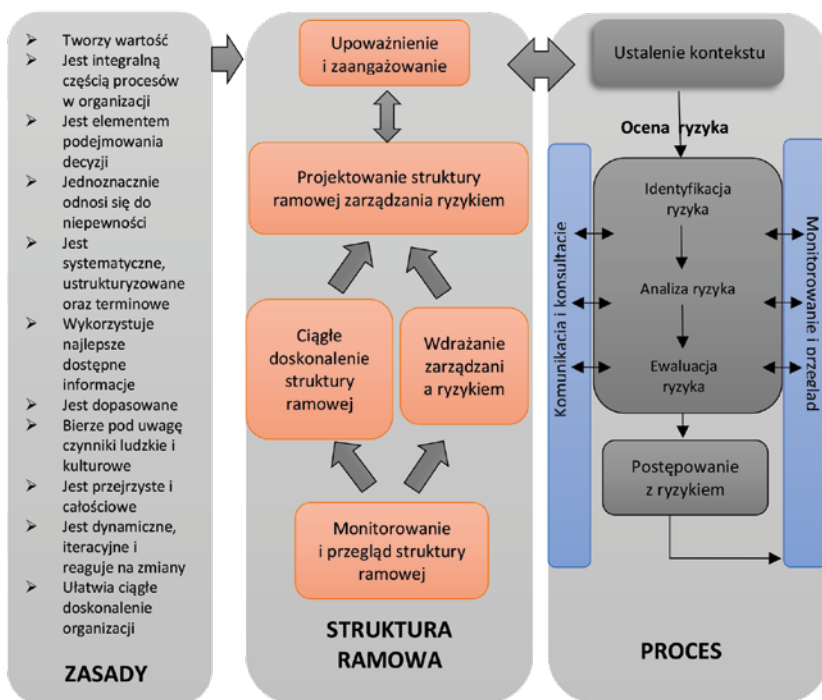
¹¹ Ocena ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz ewaluacji ryzyka. Źródło: ISO Guide 73:2009, definicja 3.4.1. Patrz szerzej: D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 161.

¹² <http://www.pbsg.pl/wiadomosci/analiza-ryzyka/iso-31000-pbsg.html>, [dostęp: czerwiec 2013].

¹³ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, D. Majchrzak (red.), AON, Warszawa 2014, s. 198–199.

Zasady gwarantujące skuteczność procesu, strukturę ramową, która zapewnia obieg informacji na jego potrzeby oraz procesy cząstkowe zarządzania ryzykiem, w tym zależności pomiędzy wymienionymi zagadnieniami, pokazuje rys. 1.

Wskazane na rycinie fundamentalne filary, na których oparto zarządzanie ryzykiem w normie ISO 31000, nie stanowią wyodrębnionych i niezależnych elementów. Zgodnie z logiką norm powyższe zalecenia należy postrzegać jako komplementarne i powiązane ze sobą obszary, których niewypełnienie skutkuje niewystarczającym przygotowaniem organizacji do minimalizacji ryzyka¹⁴ lub wystąpienia jego potencjalnych konsekwencji¹⁵. Wszystkie trzy filary zostały scharakteryzowane poniżej.



Rys. 1. Relacje między zasadami, strukturą ramową i procesem zarządzania ryzykiem

Źródło: Opracowanie własne na podstawie PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.

1.2. Zasady zarządzania ryzykiem

W pierwszym filarze wyodrębnionych zostało jedenaście zasad, których kompleksowe wdrożenie w całej organizacji i poszczególnych obszarach jej działalności

¹⁴ Patrz: ograniczanie ryzyka, s. 238.

¹⁵ Konsekwencje – rezultat zdarzenia mający wpływ na cele. Źródło: ISO Guide 73:2009, definicja 3.6.1.3.

wpływa na efektywność zarządzania ryzykiem. Po pierwsze – zarządzanie ryzykiem powinno tworzyć oraz chronić wartość, która przekłada się na wyższą skuteczność osiągnięcia celów. Pozwala to również stale doskonalić prowadzoną działalność na każdym kierunku¹⁶. Po drugie – zarządzanie ryzykiem stanowi element wszystkich działań podejmowanych w organizacji – od najwyższego kierownictwa aż po najniższy szczebel wykonawczy. Stąd też nie może być ono wydzielane jako proces niezależny, niezwiązany z całością funkcjonowania organizacji. Po trzecie – to także proces, który stanowi bardzo ważny element wspierający podejmowanie decyzji, ponieważ ujawnia cały przekrój dostępnych danych i informacji na potrzeby bieżących oraz przyszłych działań. Po czwarte – ważną zasadą jest jednoznaczne odnoszenie się w zarządzaniu ryzykiem do niepewności: jej charakteru i sposobu uwzględnienia w podejmowaniu konkretnych działań, co pozwala ją ograniczać¹⁷. Po piąte – w kontekście osiągniętych celów i uzyskiwanych wyników, a także samej efektywności zarządzania istotne jest, by zarządzanie ryzykiem było systematyczne, ustrukturyzowane oraz terminowe. Po szóste – niebagatelne znaczenie ma dostęp do najlepszych, potwierdzonych informacji i ich efektywne wykorzystanie. Zlekceważenie tego elementu na którymkolwiek etapie procesu zarządzania ryzykiem może skutkować podjęciem niekorzystnych dla organizacji decyzji, czy to w wyniku błędnego ustalenia kontekstu¹⁸, czy niewłaściwie przeprowadzonej identyfikacji bądź analizy ryzyka¹⁹ i dalej – wątpliwie oszacowanej niepewności²⁰. Po siódme – dopasowanie zarządzania ryzykiem wynika z jego elastyczności. Organizacja musi być świadoma, że przeniesienie jego koncepcji wprost z normy do własnych uwarunkowań może nie zapewnić osiągnięcia zakładanego celu. Poszczególne elementy i wytyczne należy właściwie wkomponować w strukturę organizacji i funkcjonujące w niej procesy. Po ósme – norma ISO 31000 nakazuje pamiętać o czynniku ludzkim i kulturowym. Nieuwzględnienie specyficznych zachowań ludzkich czy lokalnych zwyczajów może stanowić poważne ograniczenie dla procesu zarządzania ryzykiem. Po dziewiąte – bardzo ważnym elementem zarządzania ryzykiem jest umożliwienie jego identyfikacji w dowolnym momencie przez każdego z pracowników – wskazanego jako właściciel ryzyka²¹, ponieważ poszczególni decydenci mogą nie być świadomi niektórych ryzyk występujących w organizacji. Zwiększa to skuteczność podejmowanych działań, a tym samym jakość funkcjonowania

¹⁶ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem...*, dz. cyt., s. 200–201.

¹⁷ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 27–29.

¹⁸ 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. Źródło: ISO Guide 73:2009, definicja 3.3.1.

¹⁹ Analiza ryzyka – proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka. Źródło: ISO Guide 73:2009, definicja 3.6.1.

²⁰ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem...*, dz. cyt., s. 201.

²¹ Właściciel ryzyka – osoba lub jednostka rozliczana z zarządzania ryzykiem i uprawniona do tego zarządzania. Źródło: ISO Guide 73:2009, definicja 3.5.1.5. Patrz szerzej: D. Wróblewski, (red.), *Przegląd...*, dz. cyt., s. 181–182.

całej organizacji²². Po dziesiąte – zarządzanie ryzykiem powinno być przejrzyste i całościowe. Po jedenaste – w normie podkreśla się znaczenie wdrażania strategii doskonalenia dojrzałości zarządzania ryzykiem, przy czym istotnym elementem jest zespolenie tego procesu z pozostałymi aspektami zarządzania organizacją.

1.3. Struktura ramowa zarządzania ryzykiem²³

Ramy zarządzania ryzykiem określone zostały poprzez pięć atrybutów²⁴:

1. Pełną akceptację odpowiedzialności za własne ryzyko oraz doskonalenie wszechstronnej kontroli i strategii postępowania z ryzykiem.
2. Zwiększenie nacisku na doskonalenie zarządzania ryzykiem – konieczne jest opracowanie zestawu celów i przedsięwzięć, a następnie analizowanie i doskonalenie procesów odpowiednio do potrzeb (oznacza to zobowiązanie do prowadzenia przeglądów i modyfikowania systemu, zasobów i zdolności zapewniających permanentne doskonalenie).
3. Identyfikację każdej osoby w zakresie odpowiedzialności za zarządzanie ryzykiem – wszystkie powinny być odpowiednio przygotowane, dysponować odpowiednimi zasobami, a także prowadzić i doskonalić kontrolę oraz monitorowanie ryzyka i zdolności skutecznej komunikacji z odpowiednimi służbami.
4. Podejmowanie decyzji – na każdym szczeblu w tym procesie musi być uwzględniane ryzyko, z zastosowaniem odpowiednich procesów zarządzania ryzykiem.
5. Okresowe raporty dla komórek, zespołów bądź referatów odpowiedzialnych za nadzór oraz kontrolę zarządzania ryzykiem – powinny zawierać opisy stosowanych procesów, być kompletne i sporządzane terminowo.

Norma akcentuje potrzebę doskonalenia ram²⁵, które pomogą zintegrować zarządzanie ryzykiem z zarządzaniem organizacją. Dlatego zachęca się do zapewnienia bliższych powiązań ram zarządzania ryzykiem z celami organizacji. Ramy zarządzania ryzykiem powinny być osadzone na strategii²⁶ ogólnej oraz

²² D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem...*, dz. cyt., s. 201.

²³ 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. Źródło: ISO Guide 73:2009 Risk Management. Vocabulary, definicja 2.1.1.

²⁴ AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, Australian Government, August 2010, Fact Sheet, s. 2 [dok. elektr.], http://www.finance.gov.au/sites/default/files/COV_216905_Risk_Management_Fact_Sheet_FA3_23082010_0.pdf [dostęp: czerwiec 2013].

²⁵ Tamże.

²⁶ Strategia – oznacza logicznie skonstruowany plan lub metodę osiągnięcia celów, szczególnie w długim okresie. Źródło: PN-ISO 9004:2009 Zarządzanie ukierunkowane na trwały sukces organizacji. Podejście wykorzystujące zarządzanie jakością, s. 17.

polityce²⁷ prowadzonych działań i praktyce. Powinny uwzględniać związki zewnętrzne i wewnętrzne, zakresy odpowiedzialności, zasoby, procesy i prowadzone działania.

Struktura ramowa, którą określa ISO, umożliwia skuteczne zarządzanie ryzykiem poprzez zaangażowanie w ten proces całej organizacji oraz właściwe zaplanowanie sposobu zarządzania przez nią informacją. Norma nie narzuca własnej struktury, koncentruje się raczej na dostosowaniu struktury ramowej do struktury organizacji – modyfikuje ją i dostosowuje do potrzeb procesu poprzez wskazanie jej nowej funkcji. Relacje pomiędzy jej elementami ukazuje rys. 2.



Rys. 2. Relacje pomiędzy elementami struktury ramowej

Źródło: opracowanie własne na podstawie PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.

Przed rozpoczęciem projektowania struktury ramowej dla organizacji należy zagwarantować włączenie się w proces zarządzania ryzykiem jej kierownictwa. Jak wskazuje rys. 2, jest to etap konieczny i mający wpływ na działania podejmowane

²⁷ Polityka – ogół zamierzeń i ukierunkowanie organizacji odnoszące się do całokształtu lub określonego aspektu działalności organizacji. Na podstawie: PN-ISO 9000:2006 System zarządzania jakością. Podstawy i terminologia, s. 27; Polityka zarządzania ryzykiem – deklaracja dotycząca ogółu zamierzeń i ukierunkowania organizacji odnoszących się do zarządzania ryzykiem. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 2.1.2.

w dalszym ciągu procesu. Pod pojęciem upoważnienia i zaangażowania rozumie się mechanizm zapewniający silny i trwały udział kierownictwa w procesie zarządzania ryzykiem²⁸. Funkcja ta powinna być realizowana przede wszystkim na poziomie strategicznego planowania polityki organizacji i zawierać się między innymi w procesach:

- definiowania i zatwierdzania polityki zarządzania ryzykiem,
- zapewnienia spójności kultury organizacyjnej i polityki zarządzania ryzykiem,
- określania wskaźników wyników zarządzania ryzykiem, które są spójne ze wskaźnikami rozwoju organizacji²⁹,
- dostosowania celów zarządzania ryzykiem do celów i strategii organizacji,
- zapewnienia zgodności zarządzania ryzykiem z przepisami prawa i wymaganiami regulacyjnymi,
- zagwarantowania zasobów niezbędnych do zarządzania ryzykiem,
- ciągłej weryfikacji, czy struktura ramowa zarządzania ryzykiem pozostaje właściwa³⁰.

Włączenie się kierownictwa organizacji w proces projektowania struktury jest warunkiem koniecznym przystąpienia do programowania struktury ramowej – ale nie jedynym. Kolejny warunek, który powinien zostać spełniony, to opis środowiska organizacji (analiza kontekstu zewnętrznego) oraz jej wnętrza (kontekst wewnętrzny) – w normie określany jako zrozumienie organizacji i jej kontekstu³¹. Dokonując analizy środowiska zewnętrznego organizacji, należy wziąć pod uwagę między innymi otoczenie społeczne i kulturowe, polityczne i prawne, a także czynniki determinujące jej cele. Podczas analizy uwarunkowań wewnętrznych organizacji należy posiłkować się wiedzą z zakresu: ładu organizacyjnego³² i struktury organizacyjnej, celów i strategii ich osiągnięcia, sił i środków dostępnych w organizacji, systemów informacyjnych, sposobów zarządzania informacją i podejmowania decyzji, a także norm, standardów, wytycznych i pragmatyk działania organizacji³³.

²⁸ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 31.

²⁹ Jako główne wskaźniki rozwoju organizacji przyjmuje się najczęściej:

- wzrost ilościowy, mierzony wielkością zatrudnienia,
- udział produktów firmy w rynku lokalnym, regionalnym czy globalnym,
- wzrost obrotu kapitałem, zysków, rentowności,
- zaawansowanie technologiczne i nowoczesność wyrobów,
- zróżnicowanie produkcji,
- złożoność struktury organizacyjnej,
- złożoność problemów rozwiązywanych w organizacji.

Źródło: A. Peszko, *Podstawy zarządzania organizacjami*, Skrypty uczelniane AGH nr 1485, Wydawnictwa AGH, Kraków 1997, s. 96.

³⁰ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 33.

³¹ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 33.

³² Ład organizacyjny – system, według którego organizacja podejmuje i wdraża decyzje służące realizacji jej celów. Źródło: PN-ISO 26000:2012 Wytyczne dotyczące społecznej odpowiedzialności.

³³ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 33.

Elementem ustalania zasad dotyczących struktury zarządzania ryzykiem jest ustanowienie polityki zarządzania ryzykiem. Polityka ta jest swego rodzaju deklaracją, która powinna uzasadniać, dlaczego organizacja podejmuje się kontrolowania swojego ryzyka i zarządzania nim oraz wskazywać zależności pomiędzy misją organizacji i jej celami a samym procesem. Ponadto norma wskazuje, że należy zapewnić dostępność zasobów niezbędnych do ograniczania skutków ryzyka, a także określić zasady przygotowywania okresowych przeglądów polityki (włącznie z propozycjami jej doskonalenia) oraz raportowania³⁴.

Powyższe zasady powinny zostać uzupełnione poprzez wprowadzenie w organizacji odpowiedzialności za poszczególne ryzyka poprzez przypisanie jej konkretnym członkom instytucji³⁵, uwzględnienie przyjętych norm we wszystkich procesach i procedurach organizacji oraz ustalenie właściwych sposobów komunikacji wewnątrz organizacji i komunikowania się jej ze środowiskiem zewnętrznym.

Aby można było zrealizować zaprezentowane powyżej procesy, organizacja musi zapewnić zasoby adekwatne do ich potrzeb. Przygotowując niezbędne środki, powinno się zwrócić uwagę na personel i jego doświadczenie, metody i narzędzia zarządzania już obowiązujące w organizacji oraz systemy szkolenia i zarządzania wiedzą. Należy pamiętać, że zasoby powinny być zagwarantowane dla każdego etapu procesu zarządzania ryzykiem³⁶.

Kolejnym krokiem po zaprojektowaniu struktury jest jej wdrożenie oraz ciągle monitorowanie³⁷ i przegląd³⁸. Podczas wdrażania struktury ramowej ISO zaleca się między innymi:

- określenie harmonogramu i strategii wdrażania struktury ramowej,
- respektowanie wymagań formalnych (w tym prawnych),
- organizowanie szkoleń i kampanii informacyjnych,
- stworzenie mechanizmów gwarantujących skuteczne informowanie otoczenia o adekwatności struktury ramowej.

Monitorowanie opiera się na weryfikacji wyników zarządzania ryzykiem poprzez odniesienie do określonych w tym celu wskaźników, analizie sposobu realizacji planu zarządzaniem ryzykiem oraz adekwatności struktury ramowej, planu i polityki

³⁴ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 35.

³⁵ Osoby odpowiedzialne zarówno za wdrożenie i utrzymanie struktury ramowej, jak i proces zarządzania ryzykiem.

³⁶ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 37.

³⁷ Monitorowanie – ciągle sprawdzanie, nadzorowanie, krytyczne obserwowanie lub określanie stanu prowadzone w celu zidentyfikowania zmian w zakresie wymaganego lub oczekiwanego poziomu skuteczności. Źródło: ISO Guide 73:2009, definicja 3.8.2.1.

³⁸ Przegląd – działanie podejmowane w celu określenia przydatności, adekwatności oraz skuteczności przedmiotu rozważań do osiągnięcia ustalonych celów. Źródło: ISO Guide 73:2009, definicja 3.8.2.2.

do wewnętrznego i zewnętrznego kontekstu organizacji. To właśnie monitorowanie umożliwia ciągle doskonalenie kultury zarządzania ryzykiem³⁹.

1.4. Proces zarządzania ryzykiem

Zgodnie z międzynarodowymi normami proces zarządzania ryzykiem sprowadza się do: oceny ryzyka – w tym jego identyfikacji, analizy i ewaluacji⁴⁰, podejmowania decyzji, postępowania z ryzykiem, monitoringu i przeglądu. Proces ten dotyczy każdego ryzyka i musi być integralną częścią działań organizacji w praktyce, musi mieć wykonawcę, który potrafi zapewnić właściwe metody i narzędzia jego wdrożenia. Zarządzanie ryzykiem nie polega tylko na zestawieniu listy zagrożeń i podejmowanych działań. Wymaga poważnego podejścia do oceny ryzyka, które jest zbiorem wielu czynności, między innymi identyfikacji, analizy i ewaluacji ryzyka. To systemowe ujęcie całego przedsięwzięcia, wymagające odpowiednio zaplanowanej strategii.

Strategie zarządzania ryzykiem zapewniają równowagę celów i całego zakresu aktywności zabezpieczających ich osiągnięcie. Równowaga ta jest możliwa do osiągnięcia tylko wtedy, jeżeli:

- właściwie precyzuje się cel (bądź cele),
- dysponuje się zrozumiałym i przejrzystym procesem planowania,
- stworzy się adekwatną do wymogów strukturę organizacyjną,
- zapewni się przejrzyste rozpisanie ról (przygotowanych) członków organizacji.

Strategia zarządzania ryzykiem wymaga z jednej strony uczciwości, terminowości, wiarygodności i wystarczalności informacji, a z drugiej: wiedzy, doświadczenia, znajomości otoczenia, kompetencji formalnych, zakresu odpowiedzialności, dokładnie sprecyzowanego miejsca w procesie decyzyjnym. Punktem wyjścia dla zarządzania ryzykiem jest sprecyzowanie celu i to cel określa metodykę⁴¹ zarządzania ryzykiem, a nie odwrotnie.

Zarządzanie ryzykiem to proces leżący w kompetencji dyrekcji, zarządu, menedżerów i personelu, desygnowanych do identyfikacji ryzyka i zajmujących się

³⁹ Kultura zarządzania ryzykiem – normy i tradycje zachowań jednostek i grup w ramach organizacji, które mają wpływ na to, jak ryzyka są identyfikowane, analizowane oraz jakie działania są podejmowane przez organizację w zetknięciu z ryzykiem. Źródło: opracowanie własne na podstawie IIF Report Reform In the Financial Services Industry: Strengthening Practices for a More Stable System, Institute of International Finance, 2009.

⁴⁰ Ewaluacja ryzyka – proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane. Źródło: ISO Guide 73:2009, definicja 3.7.1.

⁴¹ Referencyjne metodyki zarządzania ryzykiem występują także w standardach (COSO, FERMA, COBIT, IIA) i przewodnikach do zarządzania projektami (PMBOK, PRINCE II). Są to jednak jedynie kompendia wiedzy, a nie jak w przypadku norm – przyjęty na zasadzie konsensu i zatwierdzony przez upoważnioną jednostkę organizacyjną dokument ustalający zasady, wytyczne lub charakterystyki do powszechnego i wielokrotnego stosowania, odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzające do uzyskania optymalnego stopnia uporządkowania w określonej dziedzinie. Patrz: D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 159.

zestawieniem strategii działań organizacji, które mogą wpłynąć pozytywnie lub negatywnie na procesy funkcjonowania organizacji oraz – mając na względzie osiągnięcie celu – zabezpieczenie organizacji przed ryzykiem wyższym niż akceptowalne⁴². Zarządzanie ryzykiem to również ograniczanie niepewności i możliwość sprostania jej.

Percepcja ryzyka⁴³ w społeczeństwie informacyjnym jest szczególna i może się znacząco różnić w zależności od grupy bądź nawet jednostki, która nierzadko ocenia dane ryzyko wyłącznie z własnej perspektywy – oczekiwanych celów, specyficznych potrzeb. Z technicznego punktu widzenia liczy się to, czy ryzyko jest: przypadkowe, rozpoznane, nowe, z poważnymi konsekwencjami, nieuchronne, natychmiastowe, skumulowane, możliwe do wyeliminowania, ograniczenia lub zapobieżenia. Z drugiej strony istotna jest wrażliwość ekspozycji⁴⁴ na dane ryzyko, liczebność grup wystawionych na ryzyko, skala i trwałość jego skutków oraz poziom ryzyka⁴⁵ w odniesieniu do konkretnego środowiska. Niebagatelne znaczenie mają również możliwe zmiany ryzyka lub odporności⁴⁶ ekspozycji, dostępność alternatywnych rozwiązań, skala profesjonalizmu personelu (w tym: efekty nadużyć, zaniedbań, zaniechań i ignorancji), a także odwracalność skutków oraz możliwość i potrzeba zbalansowania ryzyka. Te cechy determinują metodykę zarządzania ryzykiem.

Szacowanie ryzyka⁴⁷ reliketowego artykułowane jest po to, by uwzględnić je podczas zarządzania ryzykiem, ustalania wartości kryteriów ryzyka⁴⁸ i zarysowania

⁴² Ryzyko akceptowalne – wielkość ryzyka, którą organizacja może zaakceptować bez żadnych dodatkowych działań zaradczych bądź zmian w funkcjonowaniu. Patrz: D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 174.

⁴³ Percepcja ryzyka (ang. *risk perception*) – znaczenie przypisywane ryzyku przez poszczególnych interesariuszy. Percepcja ta jest pochodną potrzeb, zagadnień i spraw poszczególnych interesariuszy. Źródło: CAN/CSA-Q850-97 (2009) Risk Management: Guidelines for Decision-makers.

⁴⁴ Wrażliwość ekspozycji – słaba odporność na czynniki oddziaływania zewnętrznego lub wewnętrznego będące wynikiem incydentu lub katastrofy. To podatność na skutki zdarzenia niekorzystnego. Patrz: D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 182, cyt. za: J. Gołębiwski, *Vademecum zarządzania kryzysowego*, część III, Warszawa 2009, s. 84.

⁴⁵ Poziom ryzyka – wartość ryzyka lub suma ryzyk. Źródło: opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”. Poziom ryzyka – wielkość ryzyka lub kombinacji ryzyk, wyrażona w postaci kombinacji konsekwencji oraz ich prawdopodobieństwa. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 3.6.1.8.

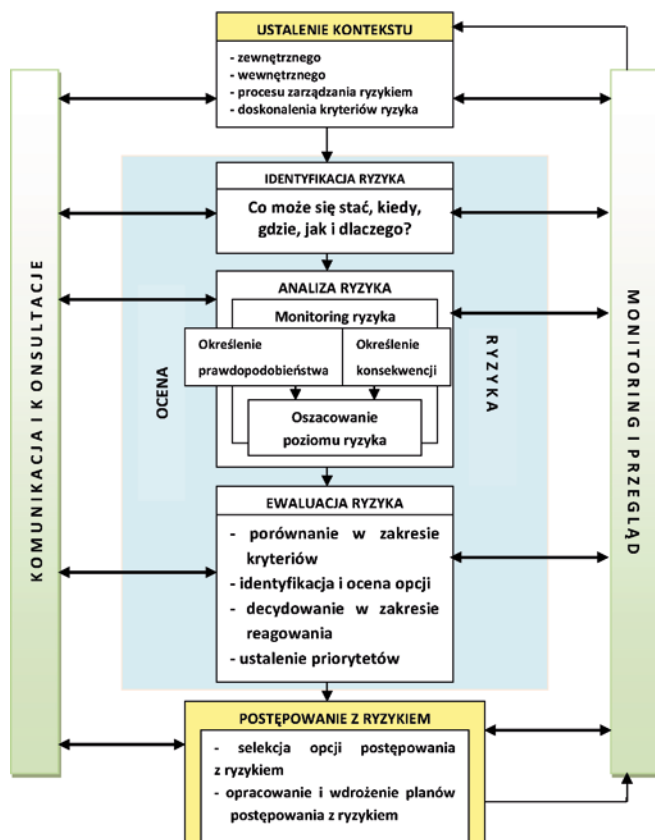
⁴⁶ Odporność – zdolność radzenia sobie z ryzykiem. Źródło: J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 30.

⁴⁷ Szacowanie ryzyka – procedura oparta na analizie ryzyka, łącznie z uwzględnieniem skutków socjologicznych, ekonomicznych, środowiskowych, a także wartościowania elementów istotnych przy dokonywaniu wyborów, w procesie podejmowania decyzji związanych ze zmniejszaniem ryzyka do akceptowanego społecznie poziomu. Szacowanie ryzyka może być jakościowe lub ilościowe. Ilościowe szacowanie ryzyka polega na określeniu wartości iloczynu prawdopodobieństwa wystąpienia zdarzenia i jego skutków. Źródło: J. Wolanin, *Zarys...*, dz. cyt., s. 183.

⁴⁸ Kryteria ryzyka – poziomy odniesienia, względem których określa się ważność ryzyka. Kryteria oparte są na celach organizacyjnych oraz na zewnętrznym i wewnętrznym kontekście danej organizacji. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 3.3.1.3.

całego procesu. Bardzo ważne są parametry organizacji, które muszą spełniać kryteria ryzyka. Norma z serii ISO 31000 jest bez wątpienia dokumentem wartym zastosowania, pozwala bowiem wdrożyć w organizacji skuteczny proces zarządzania ryzykiem. Oczywiście w opracowaniach krajowych, w przypadku adaptacji do warunków lokalnych, należy odnieść wymagania normy do specyfiki organizacji, ale główne założenia pozostają niezmienione (rys. 3).

Proces ten obejmuje pięć przedstawionych poniżej głównych zadań: komunikację i konsultacje⁴⁹, ustalenie kontekstu, ocenę ryzyka, postępowanie z ryzykiem oraz monitorowanie i przegląd.



Rys. 3. Proces zarządzania ryzykiem

Źródło: K.W. Knight, The New Standard For Risk Management, materiał przygotowany na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.

⁴⁹ Komunikacja i konsultacje – ciągle i prowadzone w sposób iteracyjny procesy, które są przez organizację prowadzone w celu zapewnienia, przekazywania lub uzyskania informacji, jak również w celu porozumiewania się z interesariuszami, odnoszące się do zarządzaniem ryzykiem. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 3.3.1.2.

1.4.1. Komunikacja i konsultacje

Zasady komunikacji i konsultacji należy ustalić przed przystąpieniem do realizacji kolejnych elementów procesu. Działania te powinny uwzględniać nie tylko kwestię samego ryzyka (wraz z jego przyczynami i konsekwencjami), ale także etap postępowania z nim. Jest to istotne, ponieważ element ten jest podstawą właściwego komunikowania się ze wszystkimi zaangażowanymi osobami i podmiotami zarówno w samej organizacji, jak i z jej interesariuszami⁵⁰. Komunikowanie się i konsultacje nie są przy tym celem same w sobie – to ich właściwe wykorzystanie pozwala na zrozumienie podejmowanych decyzji, ich przyczyn oraz oczekiwanych konsekwencji.

1.4.2. Ustalenie kontekstu

Żadna organizacja nie funkcjonuje w próżni, dlatego ważne jest zbadanie więzi zewnętrznych i wewnętrznych i ich wpływu na samo ryzyko, jak i proces zarządzania ryzykiem. O ile więzi zewnętrzne nie zawsze zależą od organizacji, to więzi wewnętrzne mogą, powinny i muszą być podporządkowane racjonalnemu podejściu do zarządzania ryzykiem. Dlatego też, tak jak w przypadku projektowania struktury ramowej, również w tym działaniu należy dążyć do ustalenia kontekstu⁵¹. W obu przypadkach pozwala ono na zdefiniowanie celów organizacji wobec jej zewnętrznych i wewnętrznych warunków. Ponadto jest informacją wyjściową dla pozostałych, kolejnych procesów. W odróżnieniu od działań odnoszących się do struktury ramowej, podczas tego etapu należy zdefiniować je bardziej szczegółowo, odnosząc do konkretnych sposobów postępowania. Dlatego też ustalając kontekst procesu zarządzania ryzykiem, należy zwrócić uwagę, by odnosił się on między innymi do zdefiniowanych celów, odpowiedzialności, zakresu oraz skali podejmowanych działań. Niezbędne jest również uwzględnienie przyjętej metody oceny ryzyka, sposobów szacowania jego wyników oraz kryteriów. Uzgadnianie kryteriów ryzyka stanowi ważny element procesu. Pozwala przede wszystkim określić jego istotność poprzez odwołanie się do wartości organizacji oraz jej celów i misji⁵². Norma wskazuje, że definiując kryteria, należy brać pod uwagę⁵³:

- charakter i rodzaje przyczyn i następstw, które mogą wystąpić, a także sposób ich mierzenia,
- sposób definiowania prawdopodobieństwa⁵⁴ wystąpienia,
- ramy czasowe wystąpienia prawdopodobieństwa i/lub następstw,

⁵⁰ Interesariusz (ang. *stakeholder*) – osoba, grupa osób lub organizacja wpływająca, na którą mogą wpływać lub która jest przekonana że mogą na nią wpłynąć podejmowane decyzje i zdarzenia. Źródło: CAN/CSA-Q850-97 (2009) Risk Management: Guidelines for Decision-makers.

⁵¹ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 43–47.

⁵² D. Wróblewski, B. Poleć, *Teoria i praktyka zarządzania ryzykiem...*, dz. cyt. s. 205–206.

⁵³ Opracowanie własne na podstawie: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 47.

⁵⁴ Prawdopodobieństwo – możliwość, szansa wystąpienia zdarzenia. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 3.6.1.1.

- sposób ustalania poziomu ryzyka⁵⁵,
- poziom ryzyka akceptowalnego⁵⁶ lub tolerowanego⁵⁷.

Należy także odpowiedzieć sobie na pytanie, czy organizacja będzie rozpatrywała każde ryzyko oddzielnie, czy też kombinacje ryzyk (przy ustaleniu, które zależności tych kombinacji należy rozważyć).

Równie ważną kwestią jest zabezpieczenie całego procesu pod względem: informacyjnym, personalnym, finansowym, logistycznym oraz technicznym. Proces zarządzania ryzykiem powinien być dopasowany do funkcjonującej struktury organizacyjnej, zrozumiały dla otoczenia i prowadzony zgodnie z przyjętą metodyką i prawem. Kompetencje⁵⁸ i odpowiedzialność personelu powinny być precyzyjnie rozdzielone, kryteria ryzyka zdefiniowane i zgodne z celami organizacji. Wszystkie te działania powinny być prowadzone pod kątem szeroko rozumianego planowania oraz być użyteczne w planowaniu.

1.4.3. Ocena ryzyka

Kolejnym istotnym działaniem jest ocena ryzyka. Wymaga ona wytypowania wyczerpującej listy zagrożeń⁵⁹. Zgodnie z normą ISO Guide 73:2009 przez zagrożenia rozumiemy źródła potencjalnej szkody, natomiast ryzyko wyrażane jest w odniesieniu do możliwych konsekwencji i prawdopodobieństwa ich wystąpienia. Celem oceny ryzyka jest stworzenie możliwie szerokiej listy ryzyk, które będą wpływały na zdefiniowane cele – bez względu na to, czy ich źródła znajdują się pod kontrolą organizacji, czy też nie ma ona wpływu na ich zaistnienie⁶⁰. Dokonując identyfikacji, należy pamiętać o efekcie kaskadowym (domina)⁶¹, który wpływa

⁵⁵ Patrz: definicja na s. 115.

⁵⁶ Patrz: definicja na s. 115.

⁵⁷ Akceptowany poziom ryzyka – jest wartością umowną. Stanowi rezultat oceny ryzyka, która obejmuje porównanie poziomu ryzyka zidentyfikowanego w procesie analizy z przyjętymi kryteriami. Ocenia się, czy oczekiwane ryzyko mieści się w granicach akceptacji lub tolerancji, czy też jest poza tymi granicami. Każde ryzyko, którego wartość wykracza poza poziom akceptowany, ale znajduje się jeszcze w granicach tolerancji, powinno wzmocnić czujność i uruchomić działania mające na celu jego monitorowanie, kontrolę i mechanizmy jego redukcji. Zanim jednak podejmie się jakiegokolwiek działania, należy ocenić skuteczność monitoringu, wiarygodność informacji, poprawność analizy, możliwe straty lub korzyści wystąpienia ryzyka, przewidywane nakłady jego redukcji i ekonomiczność całego przedsięwzięcia. Źródło: J. Gołębiowski, *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, Kraków 2011, s. 120 i 121.

⁵⁸ Kompetencje – wykazana zdolność stosowania wiedzy i umiejętności. Źródło: PN-EN ISO 9000:2006 Systemy zarządzania jakością. Podstawy i terminologia. Kompetencje – zdolność do stosowania wiedzy i umiejętności do osiągania zamierzonych wyników. Źródło: PN-EN ISO/IEC 17021:2011 Ocena zgodności. Wymagania dla jednostek prowadzących audyty i certyfikację systemów zarządzania.

⁵⁹ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem...*, dz. cyt., s. 206.

⁶⁰ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 47–49.

⁶¹ Efekt domina – teoria zakładająca, że jedno zdarzenie wywołuje ciąg kolejnych wydarzeń. Źródło: *Wielki słownik języka polskiego*, Instytut Języka Polskiego PAN, http://www.wsjp.pl/do_druku.php?id_hasla=38755&id_znaczenia=4842695 [dostęp: marzec 2015].

na pojawienie się kolejnych ryzyk⁶². Celem identyfikacji ryzyka jest zestawienie kompletnej listy ryzyk, wynikających z możliwych zdarzeń, które w zależności od okoliczności mogą kreować, zapobiegać, ograniczać, przyspieszać, opóźniać lub uniemożliwiać osiągnięcie celu. Identyfikacja ryzyka jest działalnością ciągłą, ponieważ niewykryte na czas ryzyko lub jego czynniki mogą nie tylko uniemożliwić osiągnięcie celu, ale także stanowić zagrożenie dla organizacji.

Podstawą identyfikacji jest informacja, która musi spełniać określone kryteria. Powinna być wiarygodna, terminowa, pełna i – o ile to możliwe – zweryfikowana. Stawia to określone wymogi dla źródeł informacji i zajmujących się tym zadaniem ludzi. Źródła muszą być wiarygodne i pewne, ludzie profesjonalnie przygotowani. Komponenty ryzyka są następujące:

- źródła ryzyka⁶³ lub zagrożenia,
- zdarzenia lub incydenty będące źródłami ryzyka,
- konsekwencje dla organizacji i otoczenia,
- przyczyny obecnych zagrożeń lub występujących zdarzeń,
- skuteczność monitoringu i systemów detekcyjnych,
- miejsce i czas wystąpienia ryzyka.

Komponenty te rozpatrujemy oddzielnie w odniesieniu do każdego zdarzenia mogącego stworzyć zagrożenie (huragany, mecze piłkarskie, powodzie, koncerty gwiazd, powódź, społeczne inicjatywy legislacyjne i inne).

1. **Możliwe metody identyfikacji:** pomiary, dyskusje, symulacje, doświadczenia, oceny ekspertów, badania laboratoryjne, systemy detekcyjne, modelowanie, scenariusze, kwestionariusze, prognozy, analizy zagrożeń, struktur, rozwiązań (słabych i mocnych stron, możliwości i potrzeb).
2. **Możliwe źródła ryzyka:** zagrożenia naturalne i techniczne, niedoskonałość (brak) prawa, niewłaściwe nawyki, mentalność ludzi, słabość organizacji, brak wykształcenia, niska świadomość zagrożeń, brak gotowości, nieprzygotowany personel, brak systemu, nieprzystające do rzeczywistości standardy bezpieczeństwa, zapóźnienia techniczne i technologiczne, nieprzestrzeganie norm technologicznych, błędy w działaniu, zaniechania i zaniedbania, ignorancja, niekompetencja, korupcja (systemowa).
3. **Możliwe obszary ryzyka⁶⁴:** państwo, dział administracji rządowej, środowisko naturalne, społeczeństwo, społeczności, wspólnoty, działalność

⁶² Element ten jest istotny, ponieważ niektóre ryzyka (zagrożenia) mogą występować jedynie jako następstwa innych ryzyk.

⁶³ Źródła ryzyka – obiekty i okoliczności stwarzające zagrożenie. Źródło: opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

⁶⁴ Obszar ryzyka – obszar, w którym występują istotne z punktu widzenia danego podmiotu czynniki ryzyka. Źródło: załącznik do zarządzenia nr 80 Wojewody Mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

gospodarcza, organizacja, procesy rozwojowe, otoczenie bezpieczeństwa, informowanie i inne nieustalone.

W dalszej kolejności właściwie zagregowane ryzyka⁶⁵ należy poddać analizie. Analiza ryzyka służy jego szczegółowemu zrozumieniu. Wiedza zdobyta na tym etapie pozwala na podjęcie decyzji o sposobie postępowania z ryzykiem (wybór strategii⁶⁶ i dobór metod⁶⁷). Analiza powinna skoncentrować się na ustaleniu następstwa ryzyk i ich prawdopodobieństwa (wynikiem mogą być dane: jakościowe, ilościowe, ilościowe lub ich kombinacja, w zależności od potrzeb organizacji i wyboru metody). Powinna również zostać przeprowadzona w taki sposób, aby mogła dostarczyć danych wejściowych do ewaluacji ryzyka. Szeroko stosowaną metodą skutecznego wartościowania ryzyka jest maczyca skutek/prawdopodobieństwo – szerzej opisana w rozdziale 2 „Metody wykorzystywane w ocenie ryzyka”.

Ewaluacja ryzyka ma istotny wpływ na proces podejmowania decyzji. Wyniki analizy ryzyka stanowią podstawę do podjęcia decyzji, które ryzyka i w jakim stopniu wymagają wdrożenia przez organizację właściwego algorytmu postępowania z nimi oraz ustalenia priorytetu ich uruchamiania. Następnie ustalone poziomy ryzyka powinny zostać porównane z ich kryteriami, z uwzględnieniem ustanowionego na wejściu kontekstu. Ewaluacja umożliwi w tym wypadku określenie, w jaki sposób postąpić z danymi ryzykiem⁶⁸.

Ewaluacja ryzyka, jako ostatni krok oceny ryzyka, obejmuje porównanie poziomu ryzyka zidentyfikowanego w procesie analizy z przyjętymi kryteriami. To porównanie wymaga dużej dokładności i rzetelności. Ocenia się, czy oczekiwane ryzyko mieści się w granicach akceptacji lub tolerancji, ewentualnie czy jest poza tymi granicami. Ryzyko akceptowane nie wymaga szczególnej uwagi (działania codzienne), a ryzyko w granicach tolerancji powinno już wzmocnić czujność i uruchomić działania mające na celu jego monitorowanie, kontrolę i mechanizmy jego redukcji. Tolerancja w sprawach ryzyka nie jest akceptacją zaistniałego stanu rzeczy i wymaga reakcji. Zanim jednak podejmie się jakiegokolwiek działania, ocenia się skuteczność monitoringu, wiarygodność informacji, kompetencje personelu, poprawność analizy, możliwe straty lub korzyści wynikające z wystąpienia ryzyka, przewidywane nakłady na jego redukcję i ekonomiczność całego przedsięwzięcia.

⁶⁵ Agregacja ryzyka – opis zestawu ryzyk. Źródło: opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

⁶⁶ Strategia postępowania z ryzykiem – teoria i praktyka działania, ukierunkowana na osiągnięcie założonych celów długofalowych w ramach procesu modyfikacji ryzyka. Źródło: opracowanie własne na podstawie *Słownik terminów z zakresu bezpieczeństwa narodowego*, „Myśl Wojskowa” 2002, nr 6 oraz ISO Guide 73:2009, definicja 3.8.1.

⁶⁷ Metoda postępowania z ryzykiem – sposób modyfikacji ryzyka, do którego można zaliczyć m.in.: unikanie ryzyka, podjęcie lub zwiększenie ryzyka, usunięcie źródła ryzyka, zmianę następstw, dzielenie ryzyka, retencję ryzyka. Źródło: opracowanie własne na podstawie ISO Guide 73:2009, definicja 3.8.1.

⁶⁸ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem...*, dz. cyt., s. 206.

Im wyższy poziom ryzyka, tym więcej wymaga ono uwagi – przygotowania możliwych do wdrożenia specjalnych programów je eliminujących lub redukujących, wdrożenia procesu i zakresu działań sprowadzających ryzyko do poziomu tolerancji lub akceptacji, w zależności od konieczności zrównoważenia kosztów skutków i nakładów w zakresie przyjętych kryteriów. Kryteria powinny wynikać z gotowości organizacji, przy czym zdolność organizacji do sprostania ryzyku zależy od jej personelu i parametrów: rozmiaru, struktury, wyposażenia, możliwości finansowych, profesjonalnego podejścia oraz wrażliwości i odporności na przewidywane ryzyko.

Fundamentalnym wymogiem jest skupienie się na sprowadzeniu ryzyka do poziomu akceptowanego. Nie zawsze będzie to możliwe – w pewnych okolicznościach mogą wystąpić czynniki usprawiedliwiające tolerancję ryzyka powyżej poziomu akceptacji. Należą do nich następujące przypadki:

1. Możliwości organizacji przewyższają potrzeby w zakresie sprostania ryzyku akceptowalnemu i można okresowo pozwolić sobie na zwiększenie ryzyka – by wykorzystać okoliczności stanowiące szansę dla organizacji.
2. Poziom ryzyka poza granicami akceptacji jest na tyle niski, że nie wymaga specjalnego traktowania ani specjalnych programów mieszczących się w granicach dostępnych zasobów.
3. Ryzyko jest niesprecyzowane i nie mieści się w zakresie monitoringu organizacji.
4. Koszty zajęcia się ryzykiem i jego redukcją, włącznie z kosztami ubezpieczeń i zabezpieczeń, są niewspółmierne do możliwych korzyści; jedyną opcją w działaniu może być tolerancja ryzyka nieznacznie przekraczającego granice akceptacji.

Podczas oceny ryzyka każde ryzyko musi zostać sklasyfikowane i porównane z jego wartością tolerowaną i akceptowaną. Trzeba jednak wcześniej przyjąć kryteria, które pomogą jednoznacznie zidentyfikować ryzyko znaczące, wymagające zdecydowanych działań. Jest to krok w kierunku zdefiniowania ryzyka szczególnej uwagi. Rejestr ryzyk⁶⁹, który zostanie sporządzony w wyniku oceny, pomoże zracjonalizować zarządzanie ryzykiem, a w konsekwencji – zarządzanie kryzysowe.

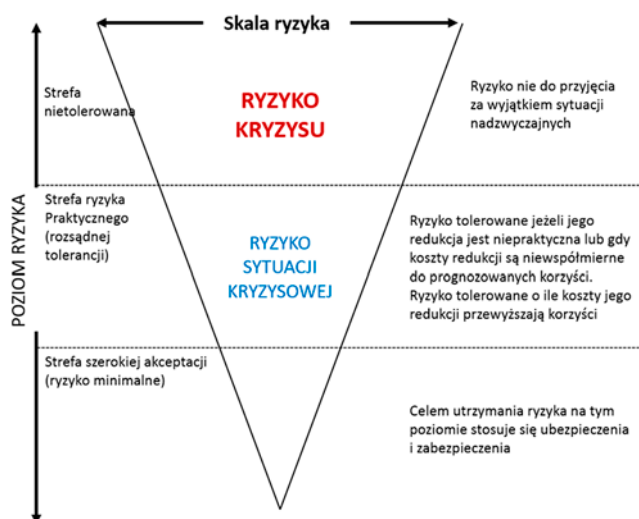
1.4.4. Postępowanie z ryzykiem

Punktem wyjścia w zakresie postępowania z ryzykiem są dwa jego poziomy: pierwszy – niewymagający innego postępowania niż monitoring, zawsze do zaakceptowania i drugi – nietolerowany, wymagający podjęcia natychmiastowych środków zaradczych, mających sprowadzić je do strefy tolerancji. Ryzyko sytuujące się między tymi poziomami ocenia się w kategoriach ekonomicznych (kosztów i korzyści),

⁶⁹ Rejestr ryzyk (ang. *risk register*) – wykaz informacji o zidentyfikowanych ryzykach. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 3.8.2.4. Patrz szerzej: D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 172.

np. w zarządzaniu ryzykiem powodziowym. Ryzyko nie jest jednak czymś stałym i może eskalować w stronę granicy nietolerancji. Takie ryzyko wymaga większej uwagi i musi być monitorowane. Sytuacja upoważnia do zakwalifikowania ryzyka jako „ryzyka sytuacji kryzysowej”. Działania należy podejmować natychmiast, gdy szacunek wielkości koszt/efekt < 1 . Ryzyko z tego zakresu przyjmuje się jako rozsądnie praktyczne, ale musi być monitorowane i trzeba poczynić przygotowania do reagowania w sytuacjach, gdy wyniknie taka potrzeba. Przygotowania te obejmują:

1. Ustalenie skali bezwzględności oczekiwanego ryzyka.
2. Doskonalenie wiedzy, sposobów i ustaleń związanych z ograniczaniem lub modyfikacją ryzyka oraz jego konsekwencji.
3. Zapewnienie odpowiedniego poziomu gotowości do sprostania sytuacji, gdy w następstwie eskalacji ryzyka wystąpi jakieś zdarzenie niepożądane.
4. Przygotowanie się na poniesienie kosztów związanych z pokryciem strat, jeżeli zawiodły działania mające doprowadzić do wyeliminowania lub ograniczenia ryzyka oraz zapobieżenia zdarzeniu⁷⁰, które może je spowodować, a także zapobieżenia zagrożeniu będącemu skutkiem ryzyka.



Rys. 4. Koncepcja reagowania na ryzyko

Źródło: K.W. Knight, The New Standard for Risk Management, materiał przygotowany na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.

⁷⁰ Zdarzenie – wystąpienie lub zmiana określonego stanu rzeczy, który może wystąpić jeden raz bądź wielokrotnie i może mieć wiele przyczyn. Źródło: opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

Ocena ryzyka warunkuje sposób postępowania z ryzykiem. Sposoby te zdefiniowane w normie to⁷¹:

- unikanie ryzyka poprzez decyzję o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko,
- podjęcie lub zwiększenie ryzyka w celu wykorzystania szansy,
- usunięcie źródła ryzyka,
- zmiana prawdopodobieństwa (wystąpienia ryzyka),
- zmiana konsekwencji,
- dzielenie ryzyka z inną stroną lub stronami (łącznie z umowami i finansowaniem ryzyka),
- utrzymanie ryzyka na podstawie świadomej decyzji.

Aby dokonać wyboru odpowiedniego sposobu postępowania z ryzykiem, należy wziąć pod uwagę potencjalne koszty w kontekście uzyskiwanych użyteczności. Nie jest to jednak warunek konieczny. Norma zaleca uwzględnienie również tych ryzyk, które trudno jest uzasadnić, biorąc pod uwagę jedynie ekonomiczność wyboru. Należy rozpatrywać również tzw. ryzyka dotkliwe (o dużych, negatywnych następstwach, ale o niskim prawdopodobieństwie)⁷².

Sposób postępowania z ryzykiem powinien zostać wyartykułowany i właściwie opisany. Służą do tego plany postępowania z ryzykiem. Powinny one zawierać większość ze wskazanych uprzednio elementów, a więc⁷³:

- uzasadnienie wyboru danej opcji postępowania,
- osoby odpowiedzialne za jego wdrożenie,
- proponowane działania,
- wymagania dotyczące zasobów z uwzględnieniem zasobów na wypadek sytuacji kryzysowych,
- wymagania raportowania i monitorowania,
- ramy czasowe i harmonogram.

1.4.5. Monitorowanie i przegląd

Ostatnie dwa działania to monitorowanie i przegląd. Pierwsze z nich powinno zostać uwzględnione już na etapie sporządzania planów (okresowo), choć norma zaleca także weryfikację procesu ad hoc. Planując, należy dążyć do przypisania jednoznacznie odpowiedzialności za to działanie oraz objęcia nim każdego aspektu zarządzania ryzykiem. Monitoring rejestruje zmiany zachodzące w otoczeniu, nie zapobiega zagrożeniom, nie eliminuje ani nie ogranicza ryzyka, ale zapewnia informacje i jest podstawą do prowadzenia działań oraz kontrolowania ryzyka. Tylko stały monitoring daje gwarancję zaufania do informacji. Zmianom podlega wszystko: otoczenie, klimat, wrażliwość, organizacje, prawo, programy i procesy.

⁷¹ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 51.

⁷² D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem...*, dz. cyt., s. 207.

⁷³ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 53.

Te zmiany wpływają na cele, zasady, politykę i praktykę zarządzania ryzykiem. Zmieniają się władze, rządy, ludzie, personel i otoczenie, ale zarządzanie ryzykiem jest i musi być realizowane, ponieważ zapewnia racjonalny rozwój społeczeństwa w bezpiecznym otoczeniu. Procesy monitorowania i przeglądu powinny być także we właściwy sposób dokumentowane. Celem tego zabiegu jest nie tylko samo udokumentowanie procesu, ale również, a nawet przede wszystkim, stworzenie warunków do poprawy i udoskonalenia wybranych metod i narzędzi.

Oprócz międzynarodowej normy ISO istnieje również kilka innych zaleceń dotyczących zarządzania ryzykiem, takich jak standard opracowany w Wielkiej Brytanii, opublikowany przez Federację Europejskich Stowarzyszeń Zarządzania Ryzykiem (Federation of European Risk Management Associations, FERMA) czy amerykański Enterprise Risk Management – Integrated Framework (Zarządzanie Ryzykiem Korporacyjnym – Zintegrowana Struktura Ramowa), zwany COSO II, który został opracowany przez Committee of Sponsoring Organizations of the Treadway Commission (COSO)⁷⁴.

Wszystkie te normy i standardy, podobnie jak wskazane na wstępie tego rozdziału, opierają się na podobnych założeniach. Dąży się do określenia relacji zdefiniowanych celów organizacji ze wszystkimi elementami zarządzania ryzykiem, tj. ustaleniem kontekstu, oceną ryzyka, reakcją na wystąpienie ryzyka i postępowaniem z nim, działaniami kontrolnymi, zasadą informowania i komunikacji oraz monitorowaniem, które odbywa się poprzez ciągłą ocenę osiągniętych wyników.

1.5. Dokumentowanie zarządzania ryzykiem⁷⁵

Dokumentowanie działań związanych z zarządzaniem ryzykiem jest jednym z ostatnich elementów filaru odnoszącego się do procesów. Norma zaleca przede wszystkim wykorzystywanie dostępnych narzędzi do utrwalania wiedzy na temat zidentyfikowanych ryzyk, ale także działań i decyzji podjętych w procesie zarządzania nimi. Element ten spełnia kilka istotnych funkcji, dzięki którym organizacja realizuje swoje cele. Tym najważniejszym jest możliwość uczenia się i wewnętrznego doskonalenia stosowanych metod oraz procesów w ramach zarządzania ryzykiem. Rejestrowanie informacji przynosi także korzyści dla samego zarządzania organizacją, wspierając proces podejmowania decyzji dzięki możliwości wielokrotnego wykorzystania przechowywanych danych historycznych.

Wykorzystywane w administracji publicznej wytyczne dotyczące dokumentowania ryzyka wskazują co najmniej dwa typy stosowanych dokumentów. Pierwszy

⁷⁴ P. Urbanek (red.), *Ekonomia i zarządzanie w teorii i praktyce*, WUŁ, Łódź 2011, s. 45.

⁷⁵ Norma ISO 31000:2009 nie rekomenduje wzorcowych ani też przykładowych form dokumentowania zarządzania ryzykiem, a przedstawia jedynie ogólne zalecenia dotyczące jego identyfikowania. Ze względu na wagę tego zagadnienia zostało ono rozszerzone w niniejszym rozdziale.

stanowią arkusze identyfikacji bądź identyfikacji i oceny ryzyka. Służą one jako podstawowy materiał do analizy ryzyka.

Drugim rodzajem dokumentów są tzw. rejestry ryzyka. Zawierają one poszerzoną informację nt. zidentyfikowanych i ocenionych ryzyk wraz z określeniem działania wobec danego ryzyka. Rejestry ryzyka wykorzystywane są najczęściej jako integralne zestawienia do raportów ryzyka⁷⁶, które podlegają weryfikacji oraz analizie na etapie monitorowania i przeglądu.

Przykłady rejestrów ryzyka odnajdziemy m.in. w wypartej już przez ISO 31000 normie *Risk Management Guidelines Companion to AS/NZS 4360:2004* (tabela 1). Pierwszy dokument zawiera krótką metryczkę, podającą podstawowe dane, tj. informacje o osobie sporządzającej i sprawdzającej rejestr wraz odpowiednimi datami, jak również datę ostatniego przeglądu ryzyka. Pierwsza kolumna rejestru służy do numeracji zidentyfikowanych ryzyk. W następnej dokument określa działanie lub czynność, której dotyczy dane ryzyko. W trzeciej kolumnie zostaje ono zdefiniowane (nazwane). W następnych kolumnach zawarto w pięciu krokach bardziej szczegółowy opis ryzyka, poprzez odpowiednio postawione pytania: co się może zdarzyć, gdy dane ryzyko wystąpi? jak może się ono ziścić? jakie niesie ze sobą konsekwencje? czy istnieją obecnie jakieś środki zapobiegawcze? w jakim stopniu środki te są wdrożone i skutecznie przeciwdziałają powstaniu ryzyka? W dalszej kolejności zidentyfikowane ryzyko zostaje poddane analizie, której wynikiem jest ustalenie stopnia prawdopodobieństwa jego wystąpienia i konsekwencji, co określi poziom danego ryzyka – to kolumny: 9, 10 i 11. Przedostatnia kolumna wskazuje priorytet danego ryzyka, wyznaczający kolejność podjęcia działań względem ryzyka i stopień ich pilności. W ostatnim kroku ujmowany jest sposób postępowania z zidentyfikowanym ryzykiem.

Tabela 1. Rejestr ryzyka

Stanowisko:				Zestawił:				Data:				
Data przeglądu ryzyka:				Sprawdził:				Data:				
Nr ryzyka	Działanie/ czynność	Ryzyko	Co się może zdarzyć?	Jak może do tego dojść?	Jakie wiążą się ze zdarzeniem skutki?	Istniejące środki zapobiegawcze	Stopień wdrożenia i skuteczność istniejących środków zapobiegawczych	Analiza			Priorytet	Postępowanie z ryzykiem
								Prawdopodobieństwo	Skutki ¹	Poziom ryzyka		

Źródło: Risk Management Guidelines Companion to AS/NZS 4360:2004.

⁷⁶ Patrz: D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 172.

W drugim przykładzie (tabela 2) również wprowadzono metryczkę, w celu identyfikacji działań właścicieli ryzyk. W rejestrze występuje także lista numeracji zidentyfikowanych ryzyk, jednak w kolejnej kolumnie zestawienia zobligowano wykonawcę do wskazania priorytetu ryzyka. Trzecia kolumna służy dokonaniu analizy możliwych działań obniżających dane ryzyko. Wykonanie tego procesu powinno zaowocować wyborem ze wskazanej listy jednego, najkorzystniejszego i rekomendowanego do podjęcia działania. Piąta kolumna stanowi rezultat krótkiej analizy kosztów i zysków z podjęcia wskazanego działania. W następnych trzech krokach ujęte zostały: osoba odpowiedzialna za przeprowadzenie działań, harmonogram zaplanowanych działań oraz zasady monitorowania ich realizacji, w tym poziomie ryzyka.

Tabela 2. Rejestr ryzyka

Stanowisko:		Zestawił:		Data:			
Data przeglądu ryzyka:		Sprawdził:		Data:			
Nr ryzyka	Ryzyko wg priorytetów w rejestrze ryzyk	Możliwe działania obniżające ryzyko	Najbardziej korzystne działanie	Koszty/Zyski: A: akceptowalne B: nieakceptowalne	Osoba odpowiedzialna za przeprowadzenie działań	Harmonogram działań	Zadania monitorowania działań i ryzyka

Źródło: Risk Management Guidelines Companion to AS/NZS 4360:2004.

Oprócz wspomnianych sposobów dokumentowania zarządzania ryzykiem zarówno administracja publiczna, jak i inne podmioty oraz organizacje stosują różnego rodzaju kwestionariusze bądź ankiety skierowane do wszystkich uczestników tego procesu (przykłady odnaleźć można w części IV niniejszej publikacji – przyp. autora). Są to dodatkowe formy doskonalenia zarządzania ryzykiem w danej jednostce. Ponadto w ramach wdrażania i rozwoju systemu zarządzania ryzykiem powstają strategie, polityki, zasady oraz wytyczne, które ewoluują w ramach ciągłego procesu monitorowania i przeglądu stosowanych rozwiązań.

2. METODY WYKORZYSTYWANE W OCENIE RYZYKA¹

W ostatnim czasie pojęcie oceny ryzyka² zyskało na popularności w niemalże wszystkich dziedzinach życia, począwszy od biznesu przez medycynę po ratownictwo. Zarządzanie kryzysowe nie tylko korzysta z oceny ryzyka, niejednokrotnie jest ona głównym czynnikiem determinującym poszczególne fazy zarządzania.

Każdy decydent w sytuacji mającej znamiona kryzysu działa w przestrzeni niepewności, nadmiaru informacji lub wręcz przeciwnie – ich niedoboru. W takich sytuacjach szczególnie ważne wydaje się szacowanie ryzyka³. Warunkiem dokonania trafnej oceny ryzyka jest przemyślany wybór metody odpowiedniej do sytuacji.

W literaturze opisane są liczne metody, opierające się na doświadczeniach, statystyce czy wiedzy eksperckiej. W niniejszym rozdziale autorzy scharakteryzowali wybrane metody oceny ryzyka, opierając się na normie ISO/IEC 31010 Risk Management – Risk Assessment Techniques. Norma zawiera krótkie charakterystyki 31 metod oceny ryzyka oraz ich wzajemne porównanie w kontekście przydatności do identyfikacji ryzyka⁴, analizy ryzyka⁵ pod względem konsekwencji, prawdopodobieństwa i poziomu ryzyka oraz ewaluacji ryzyka⁶ (możliwość uzyskania wyników ilościowych, a nie tylko jakościowych)⁷.

Autorzy wybrali 14 metod na podstawie analizy możliwego zastosowania w zarządzaniu kryzysowym. Wybrane zostały metody, które zaimplementowane w procesy decyzyjne na każdym szczeblu administracji publicznej, wspomogą najskuteczniejszą ocenę ryzyka. Każda z wybranych metod została krótko scharakteryzowana pod kątem ogólnego zastosowania, cech korzystnych i niekorzystnych, jak również możliwych zastosowań.

¹ Patrz: definicja na s. 107.

² D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 161.

³ Patrz: definicja na s. 115.

⁴ Patrz: definicja na s. 106.

⁵ Patrz: definicja na s. 109.

⁶ Patrz: definicja na s. 114.

⁷ Patrz: D. Wróblewski (red.), *Przegląd...*, dz. cyt., s. 161.

2.1. Metoda, metodyka, metodologia

Wprowadzenie do tematu wymaga wyjaśnienia, co rozumiemy i co powinniśmy rozumieć pod pojęciem metodyka. W języku polskim używamy trzech określeń spokrewnionych: metoda, metodyka i metodologia, by opisać sposób, zasady lub system rozwiązywania zagadnień czy problemów.

Metoda według T. Kotarbińskiego to „sposób działania złożonego”⁸, „sposób uświadomiony i systematyczny”⁹, „system postępowania, sposób wykonywania czynu złożonego, polegający na określonym doborze i układzie jego działań składowych, a przy tym uplanowany i nadający się do wielokrotnego stosowania”¹⁰. Metodę postrzega się również jako procedurę postępowania umożliwiającą w danych warunkach posługiwanie się posiadanymi narzędziami w celu poznania prawdy, obiektywnej rzeczywistości oraz przekształcenia jej zgodnie z przyjętym celem działania. Metodę stanowi zatem świadome i konsekwentne stosowanie procedur dla osiągnięcia zamierzonego celu.

Metoda to powtarzalny sposób postępowania albo rozwiązywania pewnego zagadnienia, dochodzenie do stwierdzeń drogą dedukcji lub przez wnioskowanie indukcyjne. To zespół teoretycznie uzasadnionych zabiegów koncepcyjnych i instrumentalnych, obejmujących całość postępowania badacza, zmierzający do rozwiązania określonego problemu¹¹. Ważną cechą metody jest celowość działania.

Metoda jest to droga, sposób badania, systematycznie stosowany sposób postępowania prowadzący do założonego wyniku. Na dany sposób postępowania składają się czynności myślowe i praktyczne, odpowiednio dobrane i realizowane w ustalonej kolejności. Sposób sprawdzony, powtarzający się cyklicznie w określonych warunkach i prowadzący do osiągnięcia celu staje się metodą. Metoda to sposób wykonywania czynu złożonego, polegający na określonym doborze i układzie działań składowych, a przy tym zaplanowany i nadający się do wielokrotnego stosowania¹².

Metodyka to *zespół reguł opisujących* sposoby (metody) postępowania w danej sytuacji dla osiągnięcia określonego celu. Przedstawiana jest również jako ustandaryzowane dla wybranego obszaru podejście do rozwiązywania problemów. To *zbiór metod* wykonywania określonej pracy, osiągnięcia określonego celu lub *zbiór zasad i sposobów* dotyczących wykonywania jakiejś czynności i zmierzania do określonego celu. Metodyka poszukuje odpowiedzi na pytanie: jak to należy zrobić?

Metodologia to ogół zasad dotyczących danej dziedziny wiedzy, na których opierają się metody badań. W aspekcie pragmatycznym oznacza naukę o metodach działalności naukowej i stosowanych w nauce procedurach badawczych, w aspekcie

⁸ T. Kotarbiński, *Traktat o dobrej robocie*, Ossolineum, Wrocław 1973, s. 85.

⁹ Tamże, s. 61.

¹⁰ Tamże, s. 86–87.

¹¹ T. Pilch, T. Bauman, *Zasady badań pedagogicznych: strategie ilościowe i jakościowe*, wyd. Żak, Warszawa 2001, s. 42.

¹² T. Kotarbiński, *Traktat...*, dz. cyt., s. 85–87.

poznawczym to nauka o elementach i strukturze systemów naukowych. Obejmuje: strategię, proces i plan badań. Metodologię prezentuje się również jako dyscyplinę nauki związaną z badaniem metod w różnych dyscyplinach naukowych. Metodologia poszukuje odpowiedzi na pytanie: co należy zrobić?

Reasumując, metoda to sposób realizacji jakiegoś działania, metodyka to jego opis, a metodologia to nauka o metodach działania. Trudności wynikają z naleciałości językowych (rusycyzmy) i aktualnych tłumaczeń, najczęściej z języka angielskiego. W języku rosyjskim, z którego tłumaczono wiele materiałów w przeszłości, metoda to система (system), w związku z tym słowo metoda było używane rzadko; preferowano słowo system (edukacyjny, szkolenia, kar i wynagradzania, podatkowy, wychowania itd.). W języku rosyjskim słowo метод (metoda) zarezerwowane jest dla badań naukowych. W języku angielskim najczęściej mamy do czynienia ze słowem *methodology* np. *Risk Assessment Methodology*, gdzie *methodology* – metodyka oznacza zestaw metod lub zasad dla wykonania czegoś. Z powyższych rozważań można zatem wyciągnąć zasadniczy wniosek, że występujące i opisane w niniejszym rozdziale narzędzia do oceny ryzyka są metodami, czyli powtarzalnym sposobem działania, służącym osiągnięciu określonego celu i możliwym do wielokrotnego zastosowania.

Obszar badań literaturowych objął poszerzoną analizę międzynarodowej normy ISO/IEC 31010 *Risk Management — Risk Assessment Techniques*. Dokument ten wskazuje, którymi narzędziami w których etapach oceny ryzyka należy się posługiwać. Metody te wskazuje tabela 1.

Tabela 1. Możliwe metody do zastosowania przy ocenie ryzyka

Metody oceny ryzyka	Proces oceny ryzyka					Metody opisane w podrozdziale
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka	
		Konsekwencje	Prawdopodobieństwo	Poziom ryzyka		
Burza mózgów (ang. <i>brainstorming</i>)	++	–	–	–	–	–
Wywiady ustrukturalizowane lub ustrukturalizowane częściowo (ang. <i>structured or semi-structured interviews</i>)	++	–	–	–	–	–
Metoda delficka (ang. <i>Delphi method</i>)	++	–	–	–	–	–

Metody oceny ryzyka	Proces oceny ryzyka					Metody opisane w podrozdziale
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka	
		Konsekwencje	Prawdopodobieństwo	Poziom ryzyka		
Lista kontrolna (ang. <i>checklist</i>)	++	-	-	-	-	-
Podstawowa analiza zagrożeń (ang. <i>preliminary hazard analysis</i>)	++	-	-	-	-	-
Analiza zagrożeń i zdolności operacyjnych (ang. <i>hazard and operability study</i>)	++	++	+	+	+	-
Analiza zagrożeń i krytycznych punktów kontroli (ang. <i>hazard analysis and critical control points</i>)	++	++	-	-	++	-
Ocena ryzyka środowiskowego (ang. <i>toxicity assessment</i>)	++	++	++	++	++	-
Metoda „co, jeśli?” (ang. <i>structured „what if?” technique</i>)	++	++	++	++	++	2,12
Analiza scenariuszowa (ang. <i>scenario analysis</i>)	++	++	+	+	+	2,13
Analiza wpływu na działalność (ang. <i>business impact analysis</i>)	+	++	+	+	+	2,14
Analiza przyczyn źródłowych (ang. <i>root cause analysis</i>)	-	++	++	++	++	-

Metody oceny ryzyka	Proces oceny ryzyka					Metody opisane w podrozdziale
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka	
		Konsekwencje	Prawdopodobieństwo	Poziom ryzyka		
Analiza rodzajów i skutków możliwych błędów (ang. <i>failure mode and effects analysis</i>)	++	++	++	++	++	-
Analiza drzewa błędów (ang. <i>fault tree analysis</i>)	+	-	++	+	+	2,6
Analiza drzewa zdarzeń (ang. <i>event tree analysis</i>)	+	++	+	+	-	2,7
Analiza przyczyn i konsekwencji (ang. <i>cause and consequence analysis</i>)	+	++	++	+	+	2,2
Analiza przyczynowo-skutkowa (ang. <i>cause and effect analysis</i>)	++	++	-	-	-	2,3
Analiza warstw ochrony (ang. <i>layer protection analysis</i>)	+	++	+	+	-	2,4
Analiza drzewa decyzji (ang. <i>decision tree analysis</i>)	-	++	++	-	-	2,5
Ocena niezawodności człowieka (ang. <i>human reliability analysis</i>)	++	++	++	++	-	2,8
Analiza muchy (ang. <i>bow tie analysis</i>)	-	+	++	++	-	2,9

Metody oceny ryzyka	Proces oceny ryzyka					Metody opisane w podrozdziale
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka	
		Konsekwencje	Prawdopodobieństwo	Poziom ryzyka		
Metoda konserwacji ukierunkowana na niezawodność (ang. <i>reliability centred maintenance</i>)	++	++	++	++	++	2,10
Zapowiedź analizy – SA i zapowiedź analizy obwodu – SCA (ang. <i>sneak analysis & sneak circuit analysis</i>)	+	-	-	-	-	2,11
Analiza Markowa (ang. <i>Markov analysis</i>)	+	++	-	-	-	-
Symulacja Monte Carlo (ang. <i>Monte Carlo simulation</i>)	-	-	-	-	++	-
Statystyki i sieci Bayesa (ang. <i>Bayesian statistics and Bayes nets</i>)	-	++	-	-	-	-
Krzywe wyniku fałszywie ujemnego (ang. <i>FN curve</i>)	+	++	++	+	++	-
Wskaźniki ryzyka (ang. <i>risk index</i>)	+	++	++	+	++	-
Matryca skutek/prawdopodobieństwo (ang. <i>consequence/probability matrix</i>)	++	++	++	++	+	2,15

Metody oceny ryzyka	Proces oceny ryzyka					Metody opisane w podrozdziale
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka	
		Konsekwencje	Prawdopodobieństwo	Poziom ryzyka		
Analiza koszty/korzyści* (ang. <i>cost/benefit analysis</i>)	+	++	+	+	+	-
Analiza wielokryterialnej decyzji (ang. <i>multiple-criteria decision analysis</i>)	+	++	+	+	+	-

*Analiza koszty/korzyści – definicja wraz z krótką charakterystyką na s. 237

Legenda:

++ – zdecydowanie dotyczy

+ – dotyczy

-- nie dotyczy

Źródło: Opracowanie własne na podstawie ISO/IEC 31010:2009 Risk Management – Risk Assessment Techniques.

W trakcie tego badania wskazano, że z katalogu narzędzi wymienionych w normie można wykorzystać następujące metody:

- analizę przyczyn i konsekwencji,
- analizę przyczynowo-skutkową,
- analizę warstw ochrony,
- analizę drzewa decyzji,
- analizę drzewa błędów,
- analizę drzewa zdarzeń,
- ocenę niezawodności człowieka,
- analizę muchy,
- metodę konserwacji ukierunkowaną na niezawodność,
- zapowiedź analizy i zapowiedź analizy obwodu,
- metodę „co, jeśli?”,
- analizę scenariuszową,
- analizę wpływu na działalność,
- macrycę skutek/prawdopodobieństwo.

Powyższe metody zostały poniżej dokładnie opisane, ponieważ rekomenduje się ich zastosowanie na potrzeby realizacji działań powiązanych z zarządzaniem ryzykiem i zarządzaniem kryzysowym. Należy zauważyć, że zawierają one wiele elementów wspólnych i mogą się wzajemnie uzupełniać, dlatego dokonując wyboru metody oceny ryzyka, należy kierować się specyfiką obszaru działania. Oczywiście

istnieją również inne, mniej lub bardziej popularne metody oceny ryzyka, często opracowane przez prywatne instytucje i dopasowane do profilu ich działalności – co oczywiście nie kwestionuje ich zasadności i wiarygodności.

Wraz z rozwojem cywilizacyjnym wzrasta liczba różnorodnych zagrożeń na różnych płaszczyznach życia. Zarówno w obszarze życia społecznego, jak i biznesowego istnieje potrzeba określenia poziomu prawdopodobieństwa wystąpienia różnorodnych zdarzeń niekorzystnych.

Każda metoda oceny ryzyka zawiera pewne podstawowe elementy, takie jak identyfikacja zagrożeń, oszacowanie prawdopodobieństwa wystąpienia danego zagrożenia, jak również ewentualnych strat, które ze sobą niesie. Nie ma znaczenia, czy ocena ryzyka jest wykonywana na płaszczyźnie biznesowej, czy społecznej. Wymienione etapy czy też elementy są nierozzerwalnie związane z procesem oceny ryzyka.

W dostępnej literaturze opisane są różne metody oceny ryzyka oraz oceny zagrożeń. Zarówno metody ilościowe, jak i jakościowe mają wspomagać zarządzających danym przedsięwzięciem czy grupą osób w obszarze niwelowania ryzyka zdarzeń niekorzystnych poprzez obniżanie prawdopodobieństwa ich wystąpienia lub obniżaniu dotkliwości skutków. Niezależnie od obranej strategii należy zebrać informacje, które pomogą w wytypowaniu i opracowaniu optymalnej metodologii zarządzania ryzykiem dla danego podmiotu.

Opis niniejszego rozdziału zawiera syntetyczną analizę normy ISO/IEC 31010:2009 Risk Management – Risk Assessment Techniques, opisującej 31 metod oceny ryzyka. Każda z tych metod zawiera w sobie podproces identyfikacji zagrożeń. W normie ujęte zostało również porównanie wszystkich metod pod kątem ich użyteczności i uzyskiwanych wyników.

2.2. Analiza przyczyn i konsekwencji (*cause and consequence analysis*)¹³

Metoda ta jest połączeniem metody drzewa błędów (patrz pkt 2.6 niniejszego rozdziału) i metody drzewa zdarzeń (patrz pkt 2.7), a jednocześnie pozwala wprowadzić opóźnienia czasowe. Rozważane są przyczyny i konsekwencje zdarzenia inicjującego (zdarzenia krytycznego), czyli zdarzenia rozpoczynającego serię zdarzeń. Analizę zaczyna się od określenia zdarzenia krytycznego, a następnie analizuje się konsekwencje tego zdarzenia za pomocą bramek logicznych tak/nie, które przedstawiają sytuacje mogące wystąpić w zaprojektowanym systemie (zdarzenia mogą pogłębić lub załagodzić moment krytyczny). Przyczyny zdarzenia analizowane są za pomocą drzewa błędów.

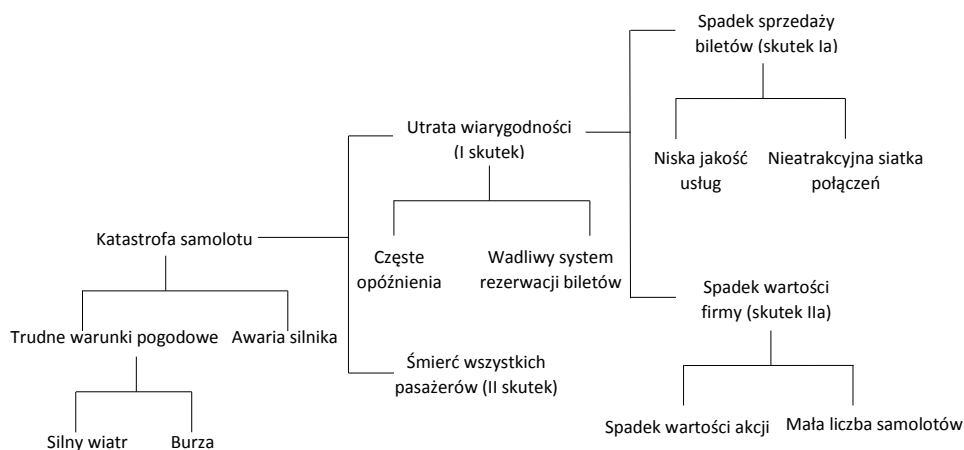
¹³ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, annex B.16.

Metoda ta została opracowana jako wiarygodne narzędzie służące do zapewnienia bezpieczeństwa systemów krytycznych (czyli takich, które mają bezpośredni wpływ na zdrowie, mienie i środowisko) i pozwalające pokazać dokładniej ich awarie¹⁴. Umożliwia ona wskazanie różnych ścieżek rozwoju w momencie wystąpienia niepożądanego zdarzenia, zależnych od zachowania poszczególnych podsystemów. Może ponadto służyć do dokładniejszej analizy przyczyn wystąpienia sytuacji kryzysowej. Postępowanie obejmuje pięć etapów:

- wybór zdarzenia lub sytuacji do analizy,
- identyfikację funkcji bezpieczeństwa dla poszczególnych elementów systemu,
- określenie ścieżek zdarzenia, począwszy od zdarzenia inicjującego (drzewo zdarzeń),
- wyznaczenie zdarzeń elementarnych dla zdarzenia inicjującego (drzewo skutków),
- wyznaczenie kryteriów działań.

Analizowane zdarzenie można wybrać na dwa sposoby: jako zdarzenie będące konsekwencją zdarzeń poprzedzających (jak w drzewie skutków) lub zdarzenie inicjujące (jak w drzewie zdarzeń)¹⁵.

Niniejszą metodę można przedstawić schematycznie, obrazując przyczyny i konsekwencje konkretnego zdarzenia. Przykład zilustrowano na rys. 1.



Rys. 1. Przykład analizy przyczyn i konsekwencji

Źródło: Opracowanie własne.

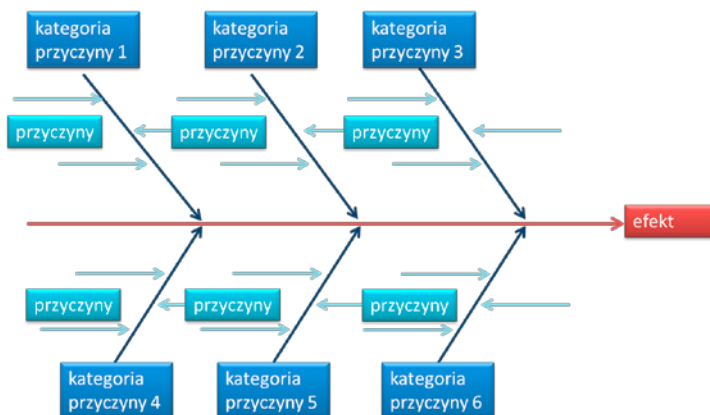
¹⁴ Awaria – przerwanie pracy urządzenia technicznego w wyniku jego uszkodzenia. Źródło: *Instytut Języka Polskiego PAN*, http://www.wsjp.pl/index.php?id_hasla=33068&ind=0&cw_szukaj=awaria [dostęp: marzec 2015].

¹⁵ B. Chrószcz, *Analiza i ocena ryzyka zawodowego osób obsługujących systemy maszynowe transportu pionowego w polskich kopalniach węgla kamiennego*, rozprawa doktorska, AGH, Kraków 2007.

Zalety metody przyczyn i konsekwencji są takie same, jak metody drzewa zdarzeń i drzewa błędów. Eliminuje ona niektóre ograniczenia metod drzew zdarzeń i błędów dzięki możliwości analizy zdarzeń, które rozwijają się w czasie. Daje kompleksowy przegląd działania systemu. Ograniczeniem jest złożoność metody w odniesieniu do budowy oraz sposobu rozpatrywania zależności pomiędzy zdarzeniami.

2.3. Analiza przyczynowo-skutkowa (*cause and effect analysis*)¹⁶

Ta metoda jest uporządkowanym sposobem pomagającym określić możliwe przyczyny zdarzenia. Sama w sobie nie wykazuje rzeczywistych przyczyn, ale przedstawia je za pomocą diagramu Ishikawy lub drzewa. Podczas uzupełniania diagramu (rysunek poniżej) wpisując przyczynę, należy sobie odpowiedzieć na pytanie: dlaczego?, a określając skutek: co się stanie?

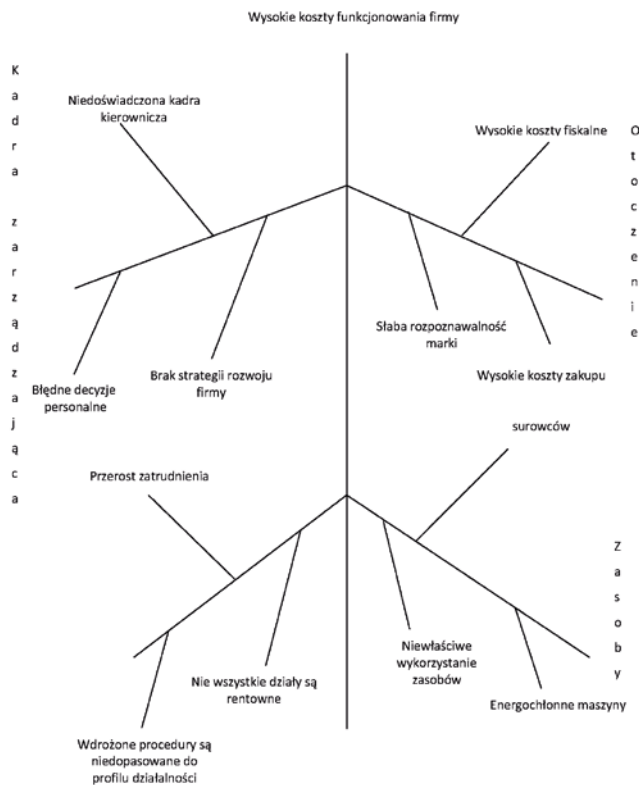


Rys. 2. Model diagramu Ishikawy

Źródło: Opracowanie własne.

Czasami zamiast diagramu Ishikawy wykorzystuje się odwrócony o 90 stopni (w prawo) diagram drzewa błędów (patrz również pkt 2.6 niniejszego rozdziału).

¹⁶ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, annex B.17.



Rys. 3. Przykład analizy przyczynowo-skutkowej

Źródło: Opracowanie własne.

Powyższa metoda może zostać wykorzystana, jeśli zachodzi potrzeba określenia podstawowych przyczyn określonego problemu, wyselekcjonowania interakcji pomiędzy czynnikami wpływającymi na dany proces, a także w celu przeanalizowania problemu i podjęcia odpowiedniej akcji. Jej zaletą jest nacisk na hierarchię danych, zlokalizowanie i wyeliminowanie przyczyn problemu.

Metoda ta używana jest do ilustrowania związków przyczynowo-skutkowych. Opiera się na opracowaniu (najczęściej przy wykorzystaniu burzy mózgów¹⁷) katalogu przyczyn i konsekwencji oraz przedstawieniu graficznym wyników. Pomaga w ten sposób oddzielić przyczyny danej sytuacji od jej konsekwencji i dostrzec złożoność problemu. W formie wykresu przedstawione są różne przyczyny dla skutków zarówno pozytywnych, jak i negatywnych. Zdarzenia mogą być wywoływane przez szereg różnych czynników (inicjatorów), przypisanych do różnych kategorii.

Po metodę tę sięga się także w celu rozważenia wszystkich możliwych scenariuszy i przyczyn zdarzenia generowanych przez zespół kryzysowy. Za pomocą burzy mózgów specjalistów ustala się najbardziej prawdopodobne przyczyny, które mogą

¹⁷ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, p. B.1.

być badane doświadczalnie lub ocenione za pomocą dostępnych danych. Analiza tego typu pozwala poszerzyć myślenie o alternatywne prawdopodobne przyczyny wystąpienia zdarzenia, a następnie ustalić hipotezy, które mogą być uznane za bardziej prawdopodobne. Analizę przyczynowo-skutkową stosuje się, gdy zachodzi potrzeba:

- identyfikacji potencjalnych przyczyn, głównych powodów określonego zdarzenia, problemu,
- uporządkowania niektórych interakcji wśród czynników wpływających na zachodzący proces,
- dokonania analizy istniejących problemów, w wyniku której mogą zostać podjęte działania naprawcze.

Korzyści z analizy przyczynowo-skutkowej to:

- koncentrowanie uwagi członków zespołu na konkretnym problemie,
- pomoc w ustaleniu przyczyny wystąpienia problemu dzięki zastosowaniu usystematyzowanego podejścia,
- zachęcenie do udziału w procesie analizy całej grupy i wykorzystanie wiedzy grupy,
- uporządkowana forma przedstawienia wyników w postaci diagramu,
- wskazanie możliwej przyczyny zmienności w procesie,
- identyfikacja obszarów, w których powinny być gromadzone dane do dalszych badań.

Metoda przyczynowo-skutkowa powinna być stosowana przez zespół ekspertów w danym obszarze.

Atuty to:

- zaangażowanie ekspertów,
- zorganizowany sposób dokonania analizy,
- rozważenie wszystkich możliwych hipotez,
- graficzna, łatwa do odczytania ilustracja wyników.

Częstym problemem związanym z wykorzystywaniem tej metody jest:

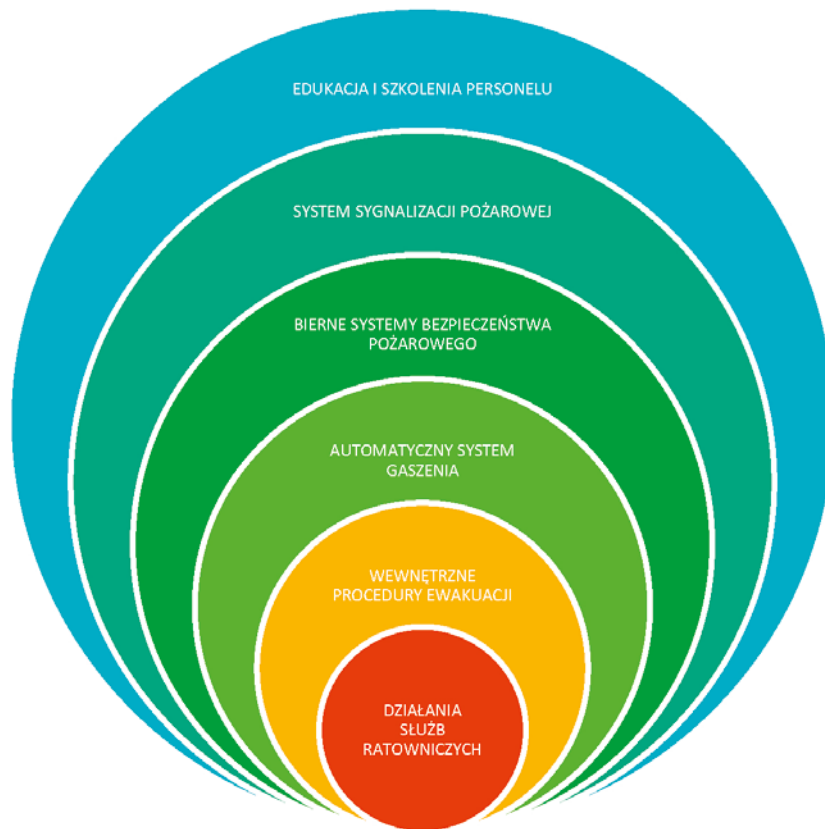
- trudność klasyfikacji poszczególnych przyczyn do właściwych grup lub podgrup,
- nieprzejrzystość złożonych problemów,
- brak niezbędnej wiedzy w zespole ekspertów,
- sam proces analizy nie jest kompletny – wymaga opracowania zaleceń.

2.4. Analiza warstw ochrony – LOPA (*layer protection analysis*)¹⁸

LOPA to ilościowa metoda oceny ryzyka związanego z niepożądanym zdarzeniem lub scenariuszem zdarzeń. W tej metodzie analizuje się, czy istnieją

¹⁸ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, annex B.18.

wystarczające środki kontroli, aby zmniejszyć ryzyko wystąpienia zdarzenia niekorzystnego¹⁹. Przyczyny i skutki są dopasowane w pary. Do każdej z par wybrany jest środek zapobiegawczy, tzn. warstwy ochrony, które eliminują przyczynę prowadzącą do niepożądanych skutków. Metodę tę stosuje się w celu określenia, czy zabezpieczenia (warstwy ochrony) są wystarczające, aby zmniejszyć ryzyko do akceptowalnego poziomu. LOPA może być stosowana jako metoda jakościowa.



Rys. 4. Przykład analizy warstw ochrony – LOPA

Źródło: Opracowanie własne.

Podstawą analizy warstw ochrony jest odwołanie do pojęcia ryzyka rozumianego jako wzajemna relacja między zagrożeniami procesowymi a zastosowanymi systemami bezpieczeństwa i ochrony²⁰.

¹⁹ Zdarzenie niekorzystne – podzbiór zbioru zdarzeń niepożądanych i nieoczekiwanych, zdarzenie powstające nagle i powodujące śmierć lub uszczerbek na zdrowiu, szkody w mieniu lub/i negatywnie oddziałujące na środowisko naturalne i przestrzeń cywilizacyjną. Źródło: J. Wolanin, *Zarys...*, dz. cyt. s. 174.

²⁰ Zapis ten precyzuje definicję ryzyka zawartą w normie PN-ISO 31000, według której ryzyko jest to wpływ niepewności na cele.

Zalety metody LOPA:

- wymaga mniej czasu i środków niż analiza drzewa błędów, ryzyka całkowitego²¹ czy analiza ilościowa²²,
- pomaga zidentyfikować zasoby i skupić je na najistotniejszych poziomach ochrony,
- identyfikuje operacje, systemy i procesy, dla których nie ma wystarczających zabezpieczeń,
- koncentruje się na najpoważniejszych konsekwencjach.

Ograniczenia metody:

- LOPA koncentruje się na jednej parze przyczyn-konsekwencji i jednym scenariuszu następstw,
- LOPA nie stosuje się do bardzo złożonych scenariuszy następstw, gdzie istnieje wiele par przyczyn-konsekwencji lub gdy istnieje wiele konsekwencji wpływających na różne zainteresowane strony.

2.5. Analiza drzewa decyzji (*decision tree analysis*)²³

Drzewo decyzyjne stanowi zbiór alternatywnych decyzji i ich skutków, które uwzględniają niepewność wyników. Jest to metoda podobna do metody drzewa zdarzeń – z tą różnicą, że proces analizy rozpoczyna się od zdarzenia inicjującego lub decyzji inicjującej i opisuje różne modele rozwiązań z uwzględnieniem różnych pośrednich zdarzeń i decyzji. Drzewo decyzyjne (drzewo decyzji) jest stosowane w procesie oceny ryzyka, aby pomóc wybrać najlepsze rozwiązania w sytuacji obarczonej niepewnością.

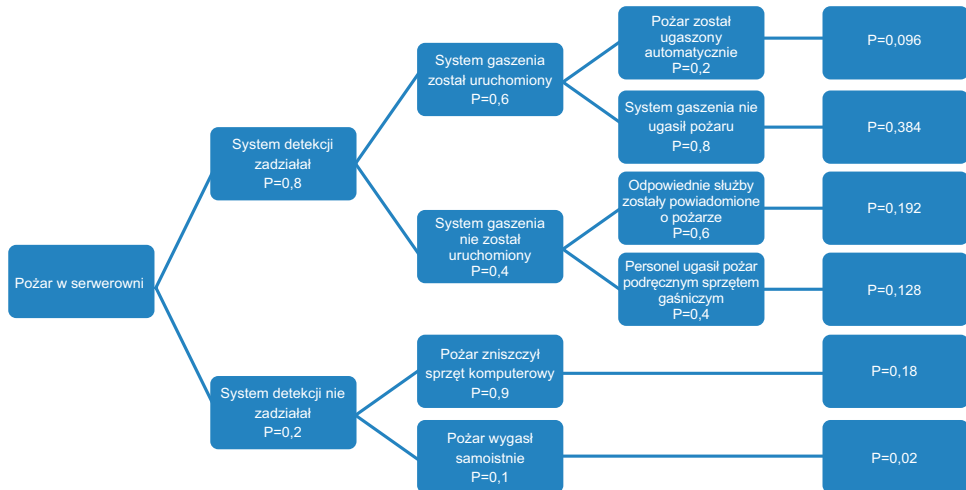
Drzewo decyzyjne rozpoczyna się od pierwszego inicjującego zdarzenia. Następnie określa się możliwe decyzje – zarówno rozwiązania korzystne, jak i niekorzystne oraz prawdopodobieństwo ich podjęcia. Kolejnym krokiem w budowie drzewa decyzji jest oszacowanie konsekwencji, jakie pociągają za sobą potencjalne

²¹ Ryzyko całkowite – dzieli się na systematyczne i specyficzne. Ryzyko systematyczne (zewnętrzne) determinowane jest przez siły zewnętrzne i niepodlegające kontroli podmiotu, który jest w jego zasięgu. Ryzyko to jest związane z siłami przyrody, a także z warunkami ekonomicznymi danego rynku oraz rynku globalnego (np. zmianą pogody, inflacją czy bezrobociem). Ten typ ryzyka nie może być wyeliminowany przez inwestora, a za zasadnicze jego źródła uznaje się zmiany stopy procentowej, inflacji, przepisów podatkowych, sytuacji polityczno-ekonomicznej. Ryzyko specyficzne (niesystematyczne, wewnętrzne) obejmuje obszar działania danego podmiotu i może być przez ten podmiot kontrolowane (przyszłe zdarzenia, które można przynajmniej częściowo kontrolować). Za najważniejsze przyczyny tego ryzyka uznaje się: zarządzanie firmą, konkurencję, dostępność surowców, płynność, bankructwo firmy. Źródło: <http://mfiles.pl/pl/index.php/Ryzyko> [dostęp: marzec 2015].

²² Zgodnie z zapisami normy ISO/IEC 31010 analiza ilościowa ma za zadanie oszacować wartości liczbowe dla konsekwencji i ich prawdopodobieństw; dane te pozwalają obliczyć poziom ryzyka w konkretnych jednostkach określonych podczas opisu kontekstu.

²³ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, annex B.19.

wcześniej wytypowane decyzje. Następnie oblicza się prawdopodobieństwa i wybiera najlepszą decyzję, biorąc pod uwagę oszacowane konsekwencje. Drzewa decyzji stosuje się w procesach zarządzania ryzykiem, w których istnieje nieakceptowana niepewność decyzyjna. Metoda ta wspomaga proces podjęcia decyzji w odniesieniu do najlepszego rozwiązania. Dużą zaletą jest możliwość zilustrowania jej w prosty sposób, który ułatwia komunikację i zrozumienie powodów danej decyzji. Przykład tej metody przedstawia rys. 5.



Rys. 5. Przykład analizy drzewa decyzji

Źródło: Opracowanie własne.

Informacjami wejściowymi niezbędnymi do zastosowania metody drzew decyzji są:

- plan danego przedsięwzięcia czy projektu, którego analiza ma dotyczyć – wraz z punktami decyzyjnymi,
- informacje na temat skutków potencjalnych decyzji.

Analizę ryzyka za pomocą tej metody należy rozpocząć od określenia pierwszych decyzji w odniesieniu do zdarzenia inicjującego. W zależności od decyzji, różne będą dalsze losy procesu. Niezależnie od pierwszego wyboru, każdy następny skutkuje decyzjami, które będą musiały być wykonane. Powyższe decyzje przedstawiane są w formie drzewa zdarzeń. Dla każdej decyzji należy oszacować prawdopodobieństwa. Najlepszą decyzję wyznacza najwyższy iloczyn poszczególnych prawdopodobieństw wzdłuż wybranej ścieżki decyzyjnej zilustrowanej na drzewie decyzji.

Informacjami wyjściowymi z zastosowanej metody są:

- logiczna analiza ryzyka, uwzględniająca różne decyzje, które mogą być brane pod uwagę,
- wynik oczekiwanej wartości dla każdej możliwej ścieżki.

Największymi atutami przedstawianej metody są:

- wyraźne, graficzne przedstawienie szczegółów problemu decyzyjnego,
- możliwość wybrania najlepszej drogi podjęcia decyzji.

Ograniczenia metody:

- duże drzewa decyzyjne mogą być skomplikowane i trudne do przesłedzenia,
- występuje niebezpieczeństwo nadmiernego upraszczania sytuacji w celu sformułowania diagramu.

2.6. Analiza drzewa błędów (*fault tree analysis*)

To jedna z metod QRA: Qualitative Risk Assessment (jakościowa metoda oceny), czyli definiujących konsekwencje, prawdopodobieństwo i poziom ryzyka poprzez określenia: duże, średnie i małe – bez wartości liczbowych²⁴. Do tego rodzaju zalicza się także metody: drzewa decyzji i drzewa zdarzeń. Wszystkie metody QRA bazują na konstruowaniu drzewa logicznego. Pokazuje ono powiązane poszczególne przyczyny określonego zdarzenia (i jego konsekwencje). Dane pokazujące liczbę zdarzeń niepożądanych mogą być wykorzystywane w drzewach w celu obliczenia prawdopodobieństwa wystąpienia danej przyczyny i konsekwencji.

Metodę uznaje się wtedy za mieszaną: ilościową i jakościową²⁵. Technika polega na pokazaniu głównego zdarzenia i rozrysowania w formie diagramu wszystkich czynników mogących doprowadzić do jego powstania (rys. 6). Po rozrysowaniu należy rozważyć metody redukcji bądź eliminacji potencjalnych zagrożeń i ich źródeł. Metoda ta jest pomocna przy identyfikowaniu potencjalnych przyczyn i rozwoju sytuacji i wyliczaniu prawdopodobieństwa wystąpienia zdarzenia.



Rys. 6. Przykład analizy drzewa błędów

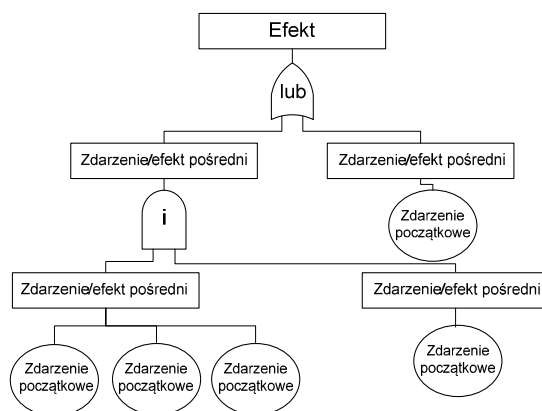
Źródło: Opracowanie własne.

²⁴ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, pkt 5.3.1.

²⁵ Patrz: AS/NZS 4360:2004 Risk Management, s. 18–19.

Metodę tę stosuje się w fazie projektowania systemu, w celu wskazania jego pozwala wówczas pokazać, jak poszczególne zdarzenia, połączone w całość, miały wpływ na powstanie/rozwój sytuacji. Dzięki zastosowaniu tej formy analizy użyjemy przedstawione w formie graficznej zdarzenie oraz prowadzące do niego ścieżki rozwoju, wraz z prawdopodobieństwem ich wystąpienia. Prostotą, ale i ograniczeniem tej metody jest to, iż rozważa tylko dwie opcje: zadziało/nie zadziało lub wydarzyło się/nie wydarzyło się.

Tworząc drzewo błędów, rozpoczyna się od pierwszego zidentyfikowanego zdarzenia, które stanowi górę diagramu, a następnie porządkuje w sposób logiczny zdarzenia mające wpływ na zaistnienie wydarzenia. Zdarzenia są powiązane za pomocą dwóch rodzajów tzw. bramek: „i” albo „lub”, w zależności od ich zależności logicznych. Bramka „lub” przedstawia sytuację, w której następane wydarzenie wystąpi, gdy zaistnieje przynajmniej jedno ze zdarzeń wychodzących. Bramka „i” przedstawia sytuację, w której następane wydarzenie wystąpi tylko i wyłącznie wtedy, gdy zaistnieją wszystkie zdarzenia „wchodzące”²⁶.



Rys. 7. Przykładowe drzewo logiczne wykorzystywane w analizie drzewa błędów²⁷

Źródło: P.T. Mitkowski, *Ocena ilościowa ryzyka: analiza drzewa błędu (konsekwencji)*, materiały dydaktyczne, Politechnika Poznańska, Poznań 2010.

2.7. Analiza drzewa zdarzeń (event tree analysis)

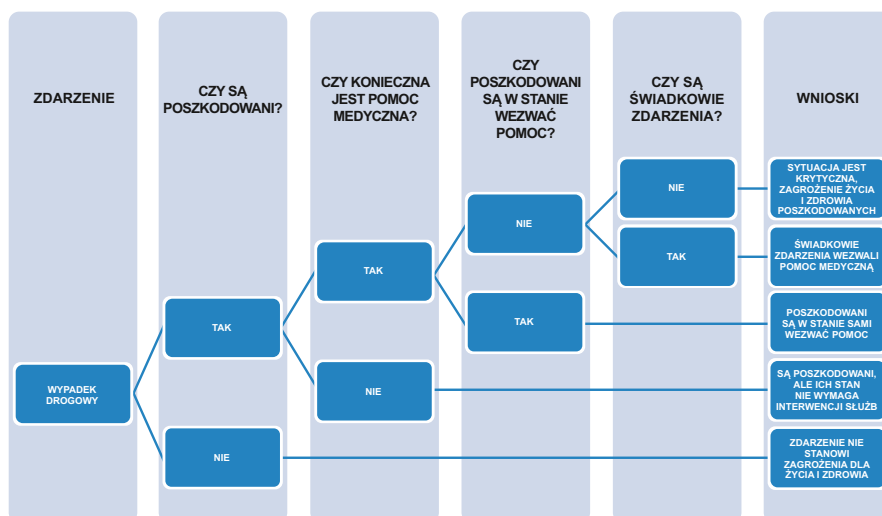
Drzewa zdarzeń są tworzone po analizie drzewa błędów. Analizują zdarzenia, które wynikają z pojedynczego zdarzenia w postaci prostych bramek logicznych.

²⁶ Na podstawie: P.T. Mitkowski, *Ocena ilościowa ryzyka: analiza drzewa błędu (konsekwencji)*, materiały dydaktyczne, Politechnika Poznańska, Poznań 2010.

²⁷ W przywołanym przykładzie definicja pojęcia „efekt” jest tożsama z przywołaną definicją pojęcia „konsekwencje”. Patrz: rozdział 1, Zarządzanie ryzykiem według normy ISO 31000, podrozdział 1.1 Norma ISO 31000:2009 – zakres i przeznaczenie, s. 106.

Drzewo zdarzeń (rys. 8) pozwala na analizę możliwego skutku konkretnego zdarzenia inicjującego²⁸.

Analiza ta przekształca prawdopodobieństwo różnych zdarzeń w możliwe wyniki. Używana jest do wyliczania, modelowania i pozycjonowania scenariuszy następstw podążających za głównym zdarzeniem. Pokazuje rozwój danej sytuacji w zależności od wybranego scenariusza. Pracę rozpoczyna się od możliwych przyczyn, celem jest określenie finalnego zagrożenia i określenie jego poziomu. Metoda ta jest użyteczna w analizie systemów zabezpieczających i procedur awaryjnych (procedur reagowania w sytuacjach niekorzystnych dla rozpatrywanego podmiotu).



Rys. 8. Przykład analizy drzewa zdarzeń

Źródło: Opracowanie własne.

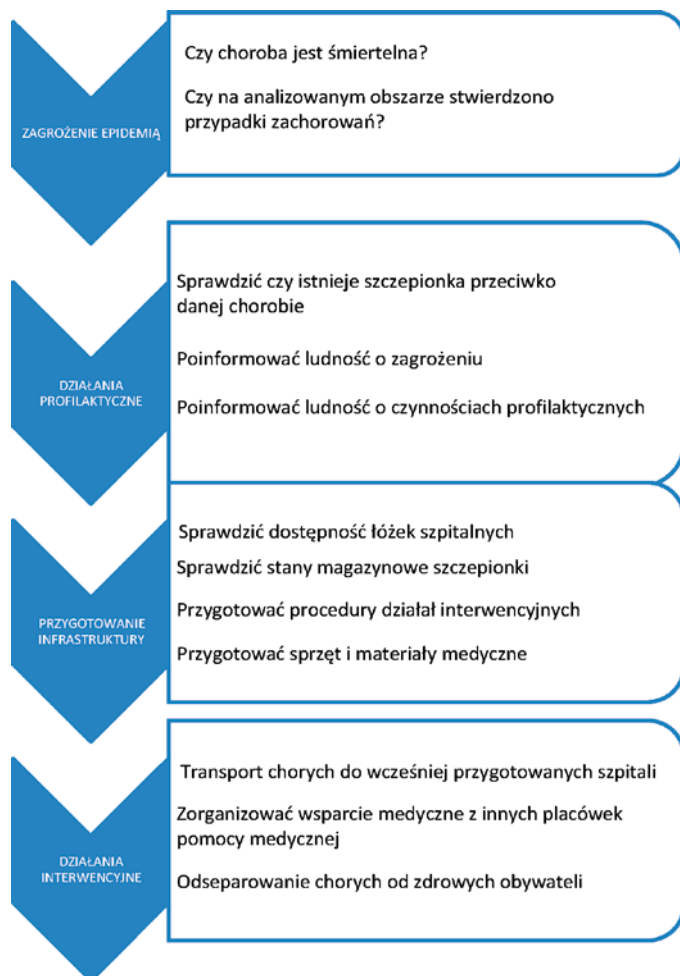
2.8. Ocena niezawodności człowieka (*human reliability analysis*)²⁹

Ocena niezawodności człowieka dotyczy analizy ryzyka pod kątem błędów popełnianych przez ludzi i wpływu tych błędów na wydajność analizowanego systemu. Możliwość popełnienia błędu przez człowieka istnieje właściwie w każdym procesie decyzyjnym, zwłaszcza gdy czas na podjęcie decyzji jest zbyt krótki. Znaczenie tzw. czynnika ludzkiego zostało zaobserwowane w różnych przypadkach, w których błędy popełniane przez człowieka prowadziły do zdarzeń o konsekwencjach dotkliwych dla rozpatrywanego podmiotu. Przypadki tego rodzaju są ostrzeżeniem dla

²⁸ Zdarzenie inicjujące – zdarzenie początkowe w całym łańcuchu zdarzeń, prowadzące do kolejnych, sekwencyjnie występujących zdarzeń niekorzystnych. Źródło: J. Wolanin, *Zarys...*, dz. cyt., s. 174.

²⁹ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, annex B.20.

osób dokonujących oceny ryzyka przed ograniczaniem się do oceny, która skupia się wyłącznie na wyposażeniu, maszynach czy oprogramowaniu, ale nie uwzględnia czynnika ludzkiego. Ocena ryzyka, która ignoruje możliwość popełnienia błędu przez ludzi, a uwzględnia jedynie zawodność wyposażenia, nie może być traktowana jako pełna. Metoda HRA jest przydatna w określaniu błędów, które mogą wpływać negatywnie na wydajność prowadzonych procesów oraz miejsc, gdzie można wprowadzić działania korygujące, które zapobiegą tym błędom.



Rys. 9. Przykład oceny niezawodności człowieka

Źródło: Opracowanie własne.

Metodę HRA można wykorzystać pod kątem jakościowym i ilościowym. Spojrzenie jakościowe polega na identyfikacji możliwości wystąpienia błędów człowieka i ich przyczyn. Dzięki temu można podjąć działania zmniejszające prawdopodobieństwo

ich wystąpienia. Wykorzystanie pod kątem ilościowym polega na dostarczaniu danych – np. statystycznych, dotyczących błędów popełnianych przez ludzi.

Danymi wejściowymi do metody analizy ryzyka metodą HRA są doświadczenia z występowania w praktyce różnych rodzajów błędów.

Proces oceny ryzyka metodą HRA obejmuje następujące etapy:

- **określenie rodzaju problemu** – co ma być badane/oceniane,
- **analiza zadań** – w jaki sposób proces jest wykonywany i w jaki sposób można wesprzeć to zadanie,
- **analiza błędów ludzkich** – jakie błędy mogą wystąpić i jak można im zapobiec,
- **przedstawienie** powiązań zadania z innymi elementami systemu (sprzęt, oprogramowanie, środowisko) i określenie ich relacji,
- **oddzielenie błędów** ważnych od tych, które nie wymagają szczegółowej analizy,
- **ocena błędów** pod kątem prawdopodobieństwa wystąpienia,
- **ocena skutków** – które błędy lub zadania są najbardziej wrażliwe, czyli które z nich mają największy wpływ na wysokość ryzyka,
- **redukcja błędów** – jak można uzyskać większą niezawodność prowadzonych działań,
- **dokumentowanie** – wszystkie działania muszą zostać udokumentowane.

Największe atuty metody HRA:

- stanowi formalny mechanizm w ocenie roli błędów człowieka,
- może pomóc w zmniejszeniu prawdopodobieństwa wystąpienia zdarzeń niekorzystnych wynikających z błędów popełnianych przez człowieka.

Ograniczenia metody HRA:

1. Złożoność i różnorodność osobowości ludzi sprawia, że trudno określić proste przyczyny wystąpienia błędów człowieka, co wiąże się z trudnością oszacowania prawdopodobieństwa wystąpienia tych błędów, które doprowadzą do zdarzenia niekorzystnego.
2. Działania ludzi nie zawsze są czarno-białe, dobre lub złe – metoda ta nie uwzględnia „małych” lub „nieistotnych” błędów.

2.9. Analiza muchy (*bow tie analysis*)³⁰

Analiza muchy jest prostym, schematycznym sposobem opisywania i analizowania ścieżek rozwoju zdarzenia od przyczyny do konsekwencji. Koncentruje się na barierach między przyczynami i zdarzeniem oraz zdarzeniem i jego konsekwencjami.

³⁰ IEC/ISO 31010 Risk Management – Risk Assessment Techniques, annex B.21.

Metoda ta służy do zobrazowania zagrożenia wraz z zakresem możliwych przyczyn i konsekwencji danego zdarzenia. Schemat muchy można skonstruować, wychodząc od możliwych błędów drzewa zdarzeń (patrz pkt 2.7 niniejszego rozdziału), jednakże najczęściej taki schemat sporządza się podczas burzy mózgów (ang. *brainstorming*)³¹. Jest on stosowany, gdy sytuacja nie gwarantuje pełnej złożoności drzewa błędów. Metoda muchy jest przydatna w przypadkach, w których istnieje wiele ścieżek/przyczyn zdarzenia niekorzystnego. Metoda ta jest uważana za prostszą do zrozumienia niż drzewa błędów czy drzewa zdarzeń (patrz pkt 2.6 i 2.7 niniejszego rozdziału), co powoduje, że stanowi użyteczne narzędzie komunikacyjne.

Wymaganą informacją wejściową w analizie ryzyka metodą muchy są informacje na temat przyczyn i konsekwencji zdarzenia, jak również czynników, które mogą zapobiec zdarzeniu lub złagodzić jego przebieg.

Tworzenie diagramu muchy (ang. *bow tie*) rozpoczyna się od zdefiniowania zdarzenia niekorzystnego, które generuje zagrożenie oraz od zdefiniowania samego zagrożenia. Diagram w swoim centralnym punkcie przedstawia niepożądane zdarzenie/zagrożenie. Po lewej stronie przedstawiona jest ścieżka pokazująca drzewo zdarzeń, które doprowadziły do jego zaistnienia, a po prawej jego konsekwencje. Zasoby wskazują, w których momentach zostały uruchomione środki zaradcze systemu. Wskazując zarówno przyczyny, jak i konsekwencje, należy pamiętać o różnych ich klasach (np. ludność, środowisko, gospodarka itp.)³².

W praktyce tworzenie diagramu trwa niekiedy wiele godzin. Praca nad nim może polegać na zadawaniu ukierunkowanego zestawu pytań zespołowi ekspertów, którzy mają codziennie styczność z zagrożeniem. Pytania powinny być zadawane przez osobę mającą doświadczenie w tworzeniu diagramów tego typu. Odpowiedzi na pytania pozwolą na zbudowanie całego diagramu. Analiza muchy opiera się na technice burzy mózgów, jednak jest to metoda sformalizowana, wymaga racjonalnego, analitycznego spojrzenia na mechanizmy rządzące danym ryzykiem.

Obecnie istnieją narzędzia informatyczne, które wspomagają i ułatwiają stworzenie diagramu. Jeżeli takie właśnie oprogramowanie jest używane, wiedza ekspercka na temat ryzyka może być ograniczona.

Efektom analizy ryzyka metodą muchy jest schemat przedstawiający główne szlaki ryzyka oraz bariery, które mają zapobiegać skutkom zagrożenia lub złagodzić je. Przykład takiego schematu przedstawia rys. 10.

Zaletą tej metody jest łatwość w zrozumieniu i przejrzysta forma pokazania zdarzenia. Wymaga ona zrozumienia przyczyn i skutków ryzyka oraz barier i kontroli,

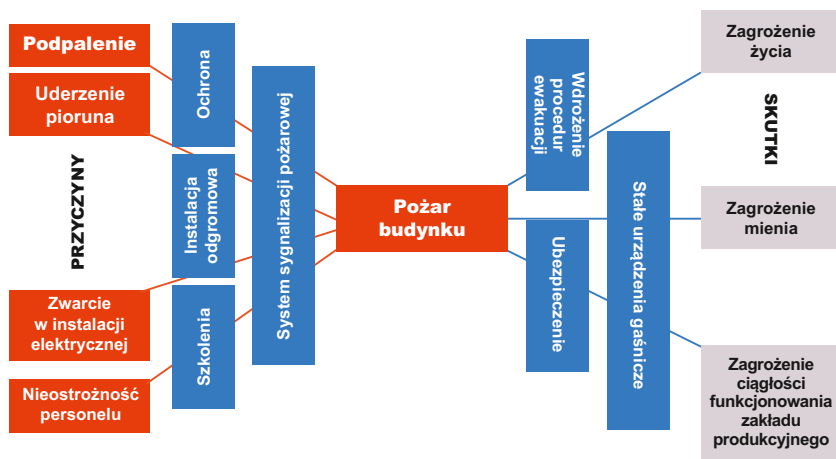
³¹ IEC/ISO 31010 Risk Management – Risk Assessment Techniques, annex B.1.

³² Patrz szerzej: L. Fabbri, M. Struckl, M. Wood, *Guidance on the Preparation of a Safety Report to Meet the Requirements of Directive 96/82/EC as Amended by Directive 2003/105/EC (Seveso II)*, European Communities, 2005, s. 17–24.

które mogą mu zapobiec, zmniejszyć je lub stymulować. W rezultacie otrzymujemy główne ścieżki rozwoju ryzyka.

Ograniczenia metody:

- nie może posłużyć do opisu zdarzenia mającego kilka przyczyn (jednocześnie),
- może nadmiernie upraszczać skomplikowane sytuacje.



Rys. 10. Przykład analizy ryzyka

Źródło: Opracowanie własne.

2.10. Metoda konserwacji ukierunkowana na niezawodność – RCM (reliability centred maintenance)³³

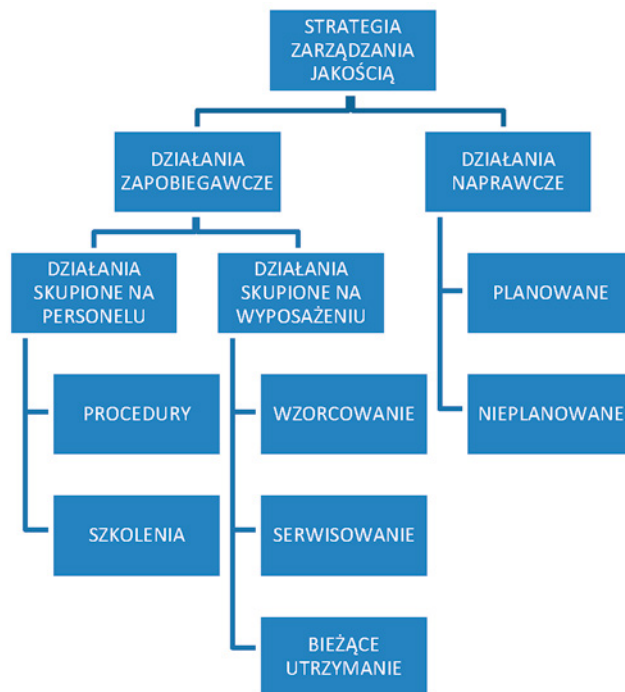
RCM to metoda określenia zasad, które powinny być przestrzegane w zarządzaniu awariami, tak aby osiągnąć wymagany stopień bezpieczeństwa, dostępności i oszczędności pracy dla wszystkich typów urządzeń w systemie.

RCM jest uznana za sprawdzoną metodę i stosowana w wielu gałęziach przemysłu. Zapewnia ona, że w procesie decyzyjnym określane są właściwe i skuteczne działania zapobiegawcze dla urządzeń. Efektem końcowym procesu oceny ryzyka metodą RCM jest decyzja o konieczności wykonywania zadań konserwacyjnych lub innych, jak również zmian operacyjnych. Szczegółowe informacje dotyczące używania i stosowania RCM zawarte są w normie IEC 60300-3-11.

Wszystkie zadania w metodzie RCM są oparte na bezpieczeństwie w odniesieniu do personelu i środowiska, a także na obawach operacyjnych lub ekonomicznych. Kryteria będą jednak zależały od charakteru produktu i jego zastosowania. W niektórych procesach, np. produkcyjnych, głównym kryterium będzie ekonomiczność produkcji, podczas gdy produkcja innych elementów powinna być

³³ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, annex B.22.

operacyjnie skuteczna, ale może mieć mniej rygorystyczne kryteria bezpieczeństwa i ekonomiczności. Największe korzyści można osiągnąć poprzez ukierunkowanie analizy na te obszary, w których miałyby miejsce poważne błędy.



Rys. 11. Przykład metody konserwacji ukierunkowanej na niezawodność – RCM

Źródło: Opracowanie własne.

Udane zastosowanie metody RCM wymaga dobrego zrozumienia urządzeń i konstrukcji, środowiska operacyjnego i związanych z nimi systemów, podsystemów i elementów wyposażenia, łącznie z występującymi błędami oraz konsekwencjami tych błędów w odniesieniu do analizowanego obszaru.

Podstawowymi etapami programu RCM są:

- inicjowanie i planowanie,
- analiza błędów funkcjonalnych,
- wybór zadań,
- wdrożenie,
- ciągle doskonalenie.

Metoda RCM zawiera definicję zadań konserwacyjnych, m.in. monitorowanie stanu, planowanie, zaplanowanie wymiany. Inne możliwe działania, które mogą wynikać z analizy RCM, obejmują zmiany procedur operacyjnych lub konserwacyjnych lub też wytyczne wskazujące na konieczność wykonania dodatkowego szkolenia.

2.11. Zapowiedź analizy – SA (*sneak analysis*) i zapowiedź analizy obwodu – SCA (*sneak circuit analysis*)³⁴

SA jest metodą rozpoznawania błędów projektowych. Identyfikuje utajone szkodliwe oprogramowanie lub stany, które mogą spowodować wystąpienie zdarzenia niepożądanego lub je hamować.

Metoda SCA została opracowana w latach 60. XX wieku na potrzeby NASA, aby sprawdzić integralność i funkcjonalność ustalonych wzorców i systemów. Służyła jako narzędzie do wykrywania przypadkowych usterek elektrycznych na obwodach i pomagała w tworzeniu rozwiązań do izolacji poszczególnych funkcji.

Narzędzia metody SA mogą integrować kilka różnych metod analizy, np. drzewa błędów, drzewa zdarzeń, analizy przyczyn i konsekwencji, pozwalając na oszacowanie niezawodności w jednej analizie, co daje oszczędność czasu i kosztów.

Metoda analizy obwodu jest wykorzystywana przede wszystkim w elektronice i elektroenergetyce. Jej celem jest zapewnienie, że układ elektryczny lub elektroniczny będzie pracował prawidłowo, zabezpieczony przed sabotażem, przypadkowym uruchomieniem i uszkodzeniem. Przykładem może być tutaj winda osobowa, mająca zabezpieczenie przed otwarciem drzwi, gdy znajduje się pomiędzy piętrami.

Analiza SA jest wyjątkowym procesem projektowania, ponieważ korzysta z różnych narzędzi (drzewa, sieci i wskazówki lub pytania wspierające analityków w zidentyfikowaniu warunków SA), aby znaleźć konkretny rodzaj problemu. Drzewa są sieciami topologicznymi rzeczywistego systemu. Każde drzewo sieci stanowi funkcję pomocniczą i pokazuje wszystkie wejścia, które mogą mieć wpływ na wydajność systemu. Z połączenia drzew sieciowych powstają lasy, które przyczyniają się do konkretnego wyniku z systemu.

Podstawowe kroki analizy stanowią:

- przygotowanie danych,
- budowa drzewa sieci,
- ocena ścieżek sieciowych,
- ostateczne rekomendacje i raport.

Atuty metody SA:

- pomocna przy identyfikacji błędów projektowych,
- działa najefektywniej w połączeniu z metodą HAZOP.

Wady:

- proces może się różnić w zależności od tego, do czego jest stosowany – np. obwodów elektrycznych, instalacji technologicznych czy urządzeń mechanicznych,
- metoda jest uzależniona od ustanowienia właściwej sieci drzew.

³⁴ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, annex B.23.

2.12. Metoda SWIFT – „co, jeśli?” (*structured „what if?” technique*)

Jest to metoda wykorzystująca zestaw słów/zdań stymulujących uczestników do identyfikacji zagrożeń. Użycie przez zespół zwrotów „co, jeśli?” pozwala zbadać, jak system czy procedura będą działały po wystąpieniu niepożądanego zjawiska, jakie będą odstępstwa od normy. Początkowo metoda była zaprojektowana do oceny ryzyka w zakładach chemicznych. Aby przystąpić do analizy metodą SWIFT, trzeba znać zagrożenia, wcześniej występujące zdarzenia, obecnie obowiązujące zabezpieczenia oraz wymagania i ograniczenia prawne. Celem zadawanych pytań typu: „co, jeśli...?”, „czy kiedykolwiek...?”, „co mogłoby się stać...?” jest zmuszenie zespołu do przeanalizowania potencjalnych scenariuszy zdarzeń mogących wystąpić w środowisku działania podmiotu (np. osoby fizycznej, organizacji itp.), ich przyczyn i konsekwencji. Dużą zaletą tej metody jest to, że może być szeroko stosowana, praktycznie w każdej sytuacji. Katalog pytań jest przygotowywany każdorazowo przed przystąpieniem do badania.

Przykładem analizy SWIFT może być np. sytuacja, w której skradziono nam kartę kredytową (pytanie brzmi: co zrobić, aby zabezpieczyć kartę kredytową przed kradzieżą?). Wynikiem analizy będzie instrukcja postępowania w takiej sytuacji, np.:

- nie nosić wszystkich pieniędzy i kart razem,
- znać numer telefonu, pod którym możemy zastrzec kartę, a przynajmniej numer infolinii swojego banku,
- nie udostępniać nikomu numeru PIN i zasłaniać klawiaturę w bankomacie,
- ubezpieczyć kartę (to oczywiście kosztuje, ale bank w razie kradzieży najczęściej zwraca całą kwotę).

Analiza „what if?” może być wykonana jako analiza jakościowa, ale również ilościowa – ze wskazaniem konkretnych wartości liczbowych oraz wartości prawdopodobieństwa. Analiza ilościowa jest trudniejsza, ponieważ wymaga od nas dokładnej specyfikacji obszaru i doświadczenia w rozwiązywaniu problemów w tej dziedzinie.

2.13. Analiza scenariuszowa (*scenario analysis*)

W metodzie tej scenariusze są przewidywane/prognozowane, bierze się pod uwagę różne rodzaje ryzyka mogące wystąpić w każdym z nich. Możemy rozważyć najlepszą, najgorszą i spodziewaną opcję. Analiza scenariuszy może być pomocna w planowaniu przyszłej polityki i strategii, a także rozważaniu bieżących aktywności. Pokazuje, jak na rozwój sytuacji wpływają szanse i zagrożenia. Analiza scenariuszowa może być przydatna podczas wykonywania planów zarządzania kryzysowego np. dla obszaru gminy (poniżej przykład takiej analizy), jednak może mieć bardzo różne formy.

Opis sytuacji: trwające 10 dni intensywne opady deszczu spowodowały podniesienie poziomu wody w regionie oraz w górnej części rzeki. Gmina posiada

zabezpieczenie przeciwpowodziowe w postaci wałów przeciwpowodziowych, jednak są one w nie najlepszym stanie i od kilku lat nie były modernizowane. Konieczne jest podjęcie decyzji, jakie kroki należy podjąć, by zminimalizować ewentualne straty, ale trzeba liczyć się z faktem, że fundusze są ograniczone. Dlatego opracowano trzy scenariusze.

Scenariusz I (najlepsza opcja)

W wyniku silnych opadów deszczu dochodzi do podniesienia się stanu wody nieznacznie powyżej stanu alarmowego, zalane zostają tylko nisko położone łąki, ale nie dochodzi do strat materialnych. Profilaktycznie sytuacja jest nadzorowana przez strażaków ochotniczej straży pożarnej, ale pozostaje stabilna i zagrożenie dla gminy szybko mija.

Scenariusz II (spodziewana opcja)

W wyniku silnych opadów deszczu dochodzi do podniesienia się stanu wody powyżej stanu alarmowego, który utrzymuje się przez kilka dni. Konieczne jest stałe nadzorowanie sytuacji na wałach przeciwpowodziowych i dokonywanie bieżących napraw w miejscach, w których wały zaczynają przeciekać. Naprawy polegają na układaniu worków z piaskiem i zabezpieczaniu wałów folią przed przeciekaniem. Do działań zaangażowano OSP, okoliczną ludność oraz lokalnych przedsiębiorców posiadających sprzęt budowlany. Po kilku dniach sytuacja się stabilizuje, choć doszło do zalania łąk i pól w pobliżu rzeki, a woda przesiąkła do kilku piwnic bliżej znajdujących się domostw. Straty są akceptowalne.

Scenariusz III (najgorsza opcja)

W wyniku silnych opadów deszczu dochodzi do podniesienia się stanu wody powyżej stanu alarmowego, który utrzymuje się przez kilka dni. Konieczne jest stałe nadzorowanie sytuacji na wałach przeciwpowodziowych i dokonywanie bieżących napraw w miejscach, w których wały zaczynają przeciekać. Naprawy polegają na układaniu worków z piaskiem i zabezpieczaniu wałów folią. Mimo zintensyfikowania działań sytuacja staje się krytyczna i konieczne jest podjęcie decyzji o wysadzeniu wałów przeciwpowodziowych po tej stronie rzeki, na której znajduje się tylko kilka zabudowań gospodarskich, by uchronić przed zalaniem budynki mieszkalne i użyteczności publicznej znajdujące się po drugiej stronie rzeki. Po kilku dniach stan wody obniża się, konieczna jest pomoc finansowa dla mieszkańców, których budynki zostały zalane.

Analiza scenariuszowa może zostać użyta do opisania każdego rodzaju ryzyka, zarówno długo-, jak i krótkoterminowego. Podstawową wadą tej metody jest problem z opisaniem realistycznego rozwoju scenariusza przez osoby odpowiedzialne za jego stworzenie.

2.14. Analiza wpływu na działalność – BIA (*business impact analysis*)³⁵

Analizę taką przeprowadza się, by pokazać, jak poszczególne zagrożenia wpływają na funkcjonowanie organizacji i jakich przedsięwzięć wymagają.

Służy ona określeniu ram czasowych i powiązanych zasobów niezbędnych do zapewnienia ciągłej realizacji zadań.

Do zalet tej metody można zaliczyć:

- umożliwienie zrozumienia procesów, które zapewniają ciągłość działania i osiągnięcie celu,
- pokazanie niezbędnych zasobów,
- zdefiniowanie procesu operacyjnego pozwalającego zwiększyć odporność podmiotu³⁶.

Wadą jest trudność w odpowiednim zrozumieniu działalności podmiotu.

Analiza BIA stanowi podstawowe narzędzie wykorzystywane w procesie zapewnienia ciągłości działania. Składa się ona z czterech elementów (etapów):

1. Działanie przygotowawcze: określenie obszaru analizy i celów, wybór metod, wyznaczenie ról i przypisanie do nich osób z organizacji, uzyskanie wsparcia ze strony kierownictwa oraz szkolenia.
2. Gromadzenie danych: wypełnienie formularzy, określenie potencjalnych strat, wymagań odtworzeniowych dla RTO³⁷ i RPO³⁸ oraz priorytetów procesów odtworzeniowych.
3. Opracowanie wyników: weryfikacja RTO i RPO, wyznaczenie procesów krytycznych oraz określenie priorytetów procesów odtworzeniowych.
4. Wdrożenie: prezentacja wyników kierownictwu i ich zatwierdzenie oraz wprowadzenie w życie przygotowanych rozwiązań.

Analiza ta koncentruje się na procesie. Umożliwia spójną ocenę procesów oraz porównanie ich krytyczności. W procesie analizy wpływu na działalność termin ten należy rozumieć jako oczekiwaną wartość (względną lub bezwzględną) determinującą rzeczywisty wpływ (obiektywny lub subiektywny) danego zdarzenia na działalność podmiotu. Istotne jest przyjęcie jednolitej metody analizy, aby możliwe było porównanie krytyczności badanych procesów.

Kluczowe działania to:

- określenie strat finansowych i niefinansowych, na jakie organizacja jest narażona w sytuacji zatrzymania procesu/procesów,

³⁵ Charakterystyka BIA przygotowana na podstawie: R. Kaszubski, D. Romańczuk (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, wyd. Związek Banków Polskich, Warszawa 2012.

³⁶ ISO/IEC 31010 Risk Management – Risk Assessment Techniques, s. 42–44.

³⁷ Recovery Time Objective – parametr określający maksymalny czas po awarii potrzebny do przywrócenia działania aplikacji, systemów i procesów biznesowych.

³⁸ Recovery Point Objective – parametr określający moment w przeszłości, w którym po raz ostatni została wykonana kopia danych i do którego momentu działalności będzie można wrócić.

- określenie RTO, czyli czasu, po którego upływie określone straty są już dla organizacji nieakceptowalne,
- określenie RPO, czyli akceptowalnego przez organizację poziomu utraty danych – na podstawie technicznych zdolności ich odtworzenia;
- określenie priorytetów odtworzeniowych z uwzględnieniem: pracowników, wyposażenia, systemów IT, niezbędnych danych oraz podmiotów współpracujących.

To właśnie ustalenie priorytetów pozwala na uporządkowanie działań podejmowanych w sytuacjach kryzysowych.

Tabela 2. Przykład analizy wpływu na działalność – BIA

Zdarzenie	Zagrożony rodzaj działalności	Potencjalne straty operacyjne	Potencjalna strata finansowa	Czas potrzebny na naprawę
Utrata wykwalifikowanego personelu	działania firmy opierające się na wykwalifikowanym personelu	zagrożenie ciągłości funkcjonowania, utrata zaufania klientów	trudna do oszacowania: zależna od podjętych działań systemowych i obrotu firmy	w zależności od charakteru działalności firmy i możliwości finansowych, jednak co najmniej 4–6 miesięcy
Awaria serwera pocztowego	kontakt i współpraca z klientem, realizacja zleceń	utrata rzetelności i wiarygodności	2000–5000 PLN dziennie	min. 3–5 godz.

Źródło: Opracowanie własne.

2.15. Matryca skutek/prawdopodobieństwo (*consequence/probability matrix*)

Matryca skutek/prawdopodobieństwo jest wykorzystywana do klasyfikacji ryzyka³⁹, hierarchizacji⁴⁰ źródeł ryzyka i postępowania z ryzykiem (tabela 3 i 4). Metoda ta stanowi wsparcie w procesie ustalania, które ryzyka wymagają dalszej

³⁹ Klasyfikacja ryzyka – jest to podział ryzyka według wcześniej ustalonych kryteriów. Źródło: opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

⁴⁰ Hierarchizacja ryzyka – w rozumieniu dosłownym oznacza ustalanie kolejności następujących po sobie rzeczy, zdarzeń, zagadnień od najważniejszych do najmniej ważnych. Źródło: opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

lub głębszej analizy, a wobec których należy podjąć działania zapobiegawcze, ponieważ przewidywalne konsekwencje przy uwzględnieniu prawdopodobieństwa ich zaistnienia powodują, że poziom ryzyka przyjmuje wartości nieakceptowalne – oczywiście w zależności od przyjętej klasyfikacji.

Tabela 3. Określenie prawdopodobieństwa wystąpienia zdarzenia

Możliwość wystąpienia	Opis	Częstotliwość
prawie pewne	oczekiwane w każdych okolicznościach	raz, dwa razy na rok
bardzo możliwe	możliwe w sprzyjających okolicznościach	raz na dwa lata
możliwe	może kiedyś wystąpić	raz na 10 lat
niemożliwe	nie oczekuje się	raz na 100 lat

Źródło: K.W. Knight, The New Standard For Risk Management, materiał konferencyjny na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.

Określenie prawdopodobieństwa jest czynnością złożoną, ale przy ocenie jakościowej nie wymaga przeprowadzania skomplikowanych kalkulacji. Metoda podana w tabeli 4 różni się od nakreślonej powyżej, ale nie są one sprzeczne, raczej stanowią uzupełnienie dla siebie. Określenie prawdopodobieństwa wystąpienia zdarzenia niekorzystnego daje informacje wyjściowe do nakreślenia poziomu ryzyka, co zależy od prawdopodobieństwa i konsekwencji, te parametry zaś zależą od dokładności informacji.

Tabela 4. Ocena poziomu ryzyka⁴¹

Konsekwencje Prawdopodobieństwo	Małe	Większe	Ekstremalne	Krytyczne
prawie pewne	średni	wysoki	poważny	bardzo poważny
bardzo możliwe	niski	średni	wysoki	poważny
możliwe	niski	średni	wysoki	wysoki
niemożliwe	niski	niski	średni	wysoki

Źródło: Opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

Poszczególne kategorie konsekwencji oraz prawdopodobieństwa⁴², jak również poziomu ryzyka mogą zostać nazwane i zdefiniowane na wiele sposobów. Także

⁴¹ Tamże.

⁴² Opis jakościowy/ilościowy dla konsekwencji i prawdopodobieństwa lub ich kombinacja.

rozpiętość macryc ryzyka bywa różna i ulega modyfikacjom w zależności od potrzeb i specyfiki danej organizacji.

Po określeniu poziomu ryzyka i dokonaniu jego klasyfikacji kolejnym krokiem będzie sprecyzowanie poziomu zaangażowania w podejściu do konkretnych ryzyk.

1. Ryzyko ocenione jako bardzo poważne i poważne wymaga natychmiastowego działania menedżerów, nawet z pomocą wyższych szczebli, o ile własne możliwości obniżenia jego poziomu są niewystarczające.
2. Ryzyko wysokie wymaga zwrócenia uwagi, monitorowania, wskazania odpowiedzialnej osoby i podejmowania działań, które obniżą jego poziom przynajmniej do średniego.
3. Ryzyko średnie wymaga wzmocnienia monitoringu lub przygotowania procedur reagowania w łańcuchu odpowiedzialności.
4. Ryzyko niskie nie wymaga żadnych dodatkowych działań, stosuje się procedury rutynowe.

W niektórych sytuacjach, gdy wymagane są działania wobec zdarzeń szczególnie wrażliwych dla realizacji celów organizacji, z mniejszą tolerancją dla ryzyka w ogóle, te oceny prowadzi się, stosując dokładniejszą skalę prawdopodobieństwa (o pięciu, a nawet siedmiu poziomach). Kolejnym krokiem jest ustalenie listy priorytetów (tabela 5).

Tabela 5. Szablon do sporządzania listy priorytetów dla każdego ryzyka

Prawdopodobieństwo	Konsekwencje		
	bardzo wysokie	średnie	bardzo niskie
bardzo wysokie	1	1	2
możliwe	1	2	3
rzadkie	2	3	3

Źródło: K.W. Knight, dz. cyt.

W obszarze bezpieczeństwa zazwyczaj ocenę ryzyka prowadzi się, szacując straty i prawdopodobieństwo jego wystąpienia. Praktyka jednak pokazuje, że szacowane są również korzyści i prawdopodobieństwo ich wystąpienia. Daje to możliwość sporządzenia macryc prognozowania konsekwencji zarówno pozytywnych (korzyści), jak i negatywnych (strat).

Tabela 6. Przykładowa matryca prognozowania konsekwencji pozytywnych i negatywnych

-S	-S	-S	-S	PRAWIE PEWNE	+W	+S	+S	+S
-S	-S	-W	-W	BARDZO PRAWDOPODOBNE	+W	+W	+S	+S
-S	-S	-W	-M	MOŻLIWE	+M	+W	+S	+S
-S	-W	-M	-N	NIEPRAWDOPODOBNE	+N	+M	+W	+S
-W	-W	-M	-N	RZADKIE	+N	+M	+W	+W
-5	-4	-3	-2	PRAWDOPODOBIEŃSTWO	+2	+3	+4	+5
ekstremalne	krytyczne	większe	mniejsze		mniejsze	większe	wyjątkowe	ekstremalne
Konsekwencje negatywne					Konsekwencje pozytywne			

Legenda

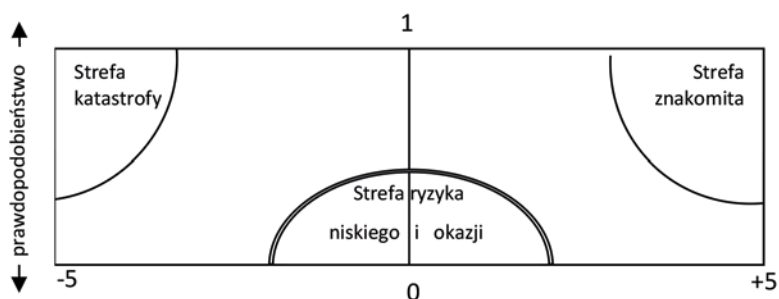
S – szczególne, wymaga szczególnego zaangażowania szczebla kierowniczego,

W – wysokie, wymaga zaangażowania właściwego menedżera,

M – małe, wymaga uwagi,

N – niskie, procedury rutynowe.

Źródło: K.W. Knight, dz. cyt.

**Rys. 12.** Diagram stref rozmieszczenia ryzyka (pozytywnego i negatywnego)⁴³

Źródło: K.W. Knight, dz. cyt.

Analiza powinna odpowiedzieć na kluczowe pytania:

1. W jakim stopniu personel zarządzania ryzykiem jest zapoznany z prawem i możliwością jego stosowania w praktyce?
2. Jaki charakter ma istniejący monitoring: detekcyjny, detekcyjno-ograniczający poziom ryzyka, zapobiegający, detekcyjny i eliminujący czynniki ryzyka?

⁴³ Tamże.

3. Jakie mogą być konsekwencje ryzyka, jeśli wystąpi ono w prognozowanej skali i jakie po zastosowaniu przedsięwzięć ograniczających ryzyko?
4. Jakie czynniki mogą zwiększyć lub zmniejszyć ryzyko i jaki mamy na to wpływ?
5. Jakie jest prawdopodobieństwo wystąpienia ryzyka?

Uzyskane odpowiedzi pozwolą ocenić ryzyko i zakwalifikować dany przypadek do odpowiedniej strefy postępowania z ryzykiem.

PODSUMOWANIE I WNIOSKI

Analizując normy rekomendowane przez ISO, jak również te przyjęte przez PKN, dostrzeżemy, że problematyka zarządzania ryzykiem pojawia się w wielu normach, dotyczących różnorodnych dziedzin. Do czasu przyjęcia normy ISO 31000:2009 Risk Management – Principles and Guidelines, ISO Guide 73:2009 Risk Assessment Techniques problematykę tę poruszały m.in. normy: ISO 14000 Ocena wpływu na środowisko, ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji, PN-EN ISO 9001:2008 Organizacja i zarządzanie przedsiębiorstwami czy normy związane z bezpieczeństwem urządzeń technicznych, tj.: EN ISO 14121-1 oraz EN ISO 12100:2010. Normy te jednak zalecały stosowanie procesu oceny ryzyka, nie wskazując szczegółowych procedur postępowania w całym tym procesie.

Należy zwrócić uwagę, że znaczenie norm odnalazło swoje miejsce nie tylko w świadomości teoretyków i praktyków, którzy je tworzą i stosują, ale zostało potwierdzone m.in. w polskich przepisach prawnych. Art. 2 ustawy o normalizacji (Dz. U. z 2002 r. nr 169, poz. 1386, z późn. zm.) reguluje status norm jako dokumentów wydawanych przez upoważnione jednostki organizacyjne, które stanowią dla danej dziedziny działalności zasady, wytyczne bądź charakterystyki oparte na wieloletniej praktyce i doświadczeniu.

Pierwszą znaczącą korzyścią z zastosowania norm z rodziny ISO 31000 jest uporządkowanie terminologii w czytelnych grupach pojęć i ich definicjach. Dokumenty pozwalają na zrozumienie oraz zastosowanie spójnego słownictwa odnoszącego się do zarządzania ryzykiem, jego elementów i procesów we wszystkich dziedzinach aktywności, w których jest obecne.

Kolejną istotną kwestią jest możliwie najbardziej uniwersalne i jednolite podejście normy ISO 31000 do procesów zarządzania ryzykiem, co umożliwia jej elastyczne zastosowanie przez każdą organizację działającą w dowolnej sferze sektora publicznego oraz prywatnego. Norma zapewnia zasady, strukturę oraz procesy możliwe do trwałej implementacji we wszystkich obszarach działalności organizacji, niezależnie od typu ryzyka, z jakim ma styczność.

Następną bardzo ważną korzyścią z wdrożenia wytycznych normy ISO 31000, oprócz wspomnianej wcześniej możliwości jej elastycznego dopasowania do bieżących potrzeb organizacji, jest otwartość na zmiany wynikające ze zmieniających się warunków i potrzeb.

Uważna analiza opisanych w normie zasad uświadamia m.in., jakie korzyści organizacja może uzyskać w wyniku wdrożenia systemu. Stanowią one w pewnym sensie odpowiedź na pytanie: po co wdrażać system lub co dzięki niemu uzyskamy? Szczegółowa analiza zapisów dotyczących struktury ramowej jednoznacznie wskazuje natomiast na odpowiedź na pytanie: w jaki sposób skutecznie i sprawnie wdrożyć system w organizacji? Charakterystyka procesów pozwala z kolei odpowiedzieć sobie na pytanie: w jaki sposób zarządzać ryzykiem w organizacji?

Istotną zaletą normy jest kompleksowe i uporządkowane ujęcie procesu zarządzania ryzykiem. Obejmuje on wszelkie procesy, które zachodzą w organizacji. Ważnym aspektem jest określenie na wstępie wszystkich warunków niezbędnych w ramach ustalenia kontekstu. Wykorzystanie tej wiedzy umożliwia właściwe dokonanie oceny ryzyka. Zastosowanie zaleceń na tym etapie pozwala organizacji na efektywne przeprowadzenie procesu postępowania z ryzykiem. W zależności od potrzeb rekomenduje się prowadzenie konsultacji i komunikowania ryzyka, a także monitorowania oraz przeglądu – jako narzędzi uzupełniających i wspomagających w ramach wszystkich etapów. Nieodłącznym elementem zarządzania ryzykiem w organizacji zalecanym przez normę ISO 31000 jest rzetelne dokumentowanie działań, może to bowiem mieć wpływ na przyszłość organizacji: wspieranie procesu podejmowania decyzji, rozwój i doskonalenie metod i procesów w organizacji.

Aktualne podejście do oceny ryzyka oparte jest przede wszystkim na wiedzy eksperckiej i doświadczeniach z dotychczasowymi zagrożeniami. Stosuje się również różnorodne metody oceny ryzyka, które znacznie usprawniają zarządzanie sytuacją kryzysową.

W niniejszej części zaprezentowano również wybrane metody oceny ryzyka, które – zaimplementowane w procesach decyzyjnych – usprawnią ocenę ryzyka.

Efektom przeprowadzenia oceny ryzyka jest zaplanowanie reakcji na ryzyko. Jest to proces opracowywania wariantów postępowania i czynności zmniejszających zagrożenia i zwiększających potencjalne korzyści dla sformułowanych celów. Plan reakcji na ryzyko to kluczowy etap procesu zarządzania ryzykiem, gdyż opracowuje się w nim metody reagowania na zdarzenia korzystne i niekorzystne. Skuteczność planowania reakcji na ryzyka zadań zagrożonych ma bezpośredni wpływ na wzrost lub spadek ryzyka powodzenia całego przedsięwzięcia⁴⁴.

Planowane reakcje muszą być proporcjonalne do konsekwencji wystąpienia niekorzystnych zjawisk, likwidować (lub niwelować) wpływy danego zagrożenia w sposób kosztowo efektywny i być realizowane terminowo. W procesie planowania reakcji na ryzyka powszechnie stosuje się kilka strategii. Do każdego z ryzyk należy tak dobrać plan postępowania, by podjęte działania były najskuteczniejsze.

W procesie analizy oceny ryzyka i zagrożeń zidentyfikowano wiele metod. W normie ISO/IEC 31010:200931 opisano ich 31. Wybrane metody przedstawione

⁴⁴ <http://wartowiedziec.org/index.php/pracownik-samorzadowy/zarzdanie/16316-jakociowa-i-ilociowa-analiza-ryzyka> [dostęp: luty 2015].

w niniejszej części pozwalają na zapoznanie się z różnym podejściem do tego zagadnienia. Obrazują one przekrój metod oceny ryzyka: od rozważań eksperckich po metody oparte na budowaniu schematów i logicznych scenariuszy zdarzeń. Zaleca się wykorzystanie następujących metod:

1. Metoda SWIFT

Pytania typu: „co, jeśli...?”, „czy kiedykolwiek...?”, „co mogłoby się stać...?” zmuszają do przeanalizowania większości potencjalnych scenariuszy, ich przyczyn i konsekwencji. Metoda ta może być szeroko stosowana.

2. Drzewo zdarzeń

Użyteczna przy wyliczaniu, modelowaniu i pozycjonowaniu różnych scenariuszy podążających, związanych ze zdarzeniem głównym. Pokazuje rozwój danej sytuacji w zależności od wybranego scenariusza. Użyteczna w analizie systemów zabezpieczających i procedur awaryjnych.

3. Analiza przyczyn i konsekwencji

Eliminuje niektóre ograniczenia metody drzewa zdarzeń i błędów dzięki możliwości analize zdarzeń, które rozwijają się w czasie. Daje kompleksowy przegląd działania systemu.

4. Analiza scenariuszowa

Pomaga w opisanie każdego rodzaju ryzyka, zarówno długo-, jak i krótkoterminowego.

5. Analiza muchy

Łatwa w zrozumieniu i przejrzysta w formie pokazania zdarzenia.

6. Matryca skutek/prawdopodobieństwo

Bardzo czytelna, z możliwością zastosowania różnych skal (4x4, 5x5, 6x6) i wag.

Praktyka wykorzystania norm z zakresu zarządzania ryzykiem pokazuje, że są one uniwersalnym źródłem wiedzy, dostarczającym sprawdzone narzędzia wspomagające zarządzanie wszystkimi procesami organizacyjnymi w warunkach niepewności. Dzięki ich wykorzystaniu organizacje mogą efektywniej realizować misję, dla której zostały stworzone, a także cele i zadania istotne ze względów biznesowych czy też publicznych.

Od momentu wprowadzenia elementów zarządzania ryzykiem w 2009 r. jego znaczenie stale rośnie. Stąd też rekomenduje się wykorzystanie uznanych wytycznych w zakresie zarządzania ryzykiem, które ujednolicają terminologię, wnoszą uniwersalne zasady, elastyczną strukturę ramową i właściwie dopasowane procesy, w tym narzędzia wspomagające ocenę ryzyka i dokumentowanie zarządzania ryzykiem.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

- Chrószcz B., *Analiza i ocena ryzyka zawodowego osób obsługujących systemy maszynowe transportu pionowego w polskich kopalniach węgla kamiennego*, rozprawa doktorska, AGH, Kraków 2007.
- Gołębiewski J., *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, Kraków 2011.
- Kaszubski R., Romańczuk D. (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, wyd. Związek Banków Polskich, Warszawa 2012.
- Kotarbiński T., *Traktat o dobrej robocie*, Ossolineum, Wrocław 1973.
- Nogalski B., *Kultura organizacyjna. Duch organizacji*, Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz 1998.
- Peszko A., *Podstawy zarządzania organizacjami*, Skrypty uczelniane AGH, nr 1485, Wydawnictwa AGH, Kraków 1997.
- Pilch T., Bauman T., *Zasady badań pedagogicznych: strategie ilościowe i jakościowe*, wyd. Żak, Warszawa 2001.
- Sikorski Cz., *Kultura organizacyjna*, C.H. Beck, Warszawa 2002.
- Słownik terminów z zakresu bezpieczeństwa narodowego*, „Myśl Wojskowa” 2002, nr 6.
- Urbanek P. (red.), *Ekonomia i zarządzanie w teorii i praktyce*, WUŁ, Łódź 2011.
- Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005.
- Wróblewski D. (red.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014.
- Wróblewski D., Poleć B., *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, D. Majchrzak (red.), AON, Warszawa 2014.

Akty prawne

- Zarządzenie nr 80 Wojewody Mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

Normy i standardy

- AS/NZS 4360:2004 Risk Management.
- CAN/CSA-Q850-97 (2009) Risk Management: Guidelines for Decision-makers.
- ISO 31000:2009 Risk Management – Principles and Guidelines.
- ISO Guide 73:2009 Risk Management – Vocabulary.
- ISO/IEC 31010:2009 Risk Management – Risk Assessment Techniques.

- PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.
PN-EN ISO/IEC 17021:2011 Ocena zgodności. Wymagania dla jednostek prowadzących audyty i certyfikację systemów zarządzania.
PN-ISO 26000:2012 Wytyczne dotyczące społecznej odpowiedzialności.
PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.
PN-ISO 9000:2006 System zarządzania jakością. Podstawy i terminologia.
PN-ISO 9004:2009 Zarządzanie ukierunkowane na trwały sukces organizacji. Podejście wykorzystujące zarządzanie jakością.
Risk Management Guidelines Companion to AS/NZS 4360:2004.

Słowniki, leksykony i encyklopedie

- Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2008.
Wielki słownik języka polskiego, Instytut Języka Polskiego PAN: http://www.wsjp.pl/index.php?id_hasla=33068&ind=0&w_szukaj=awaria.

Dokumenty elektroniczne, strony internetowe i inne

- AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, Australian Government, August 2010, Fact Sheet [dok. elektr.], http://www.finance.gov.au/sites/default/files/COV_216905_Risk_Management_Fact_Sheet_FA3_23082010_0.pdf.
- Fabrizi L., Struckl M., Wood M., *Guidance on the Preparation of a Safety Report to Meet the Requirements of Directive 96/82/EC as Amended by Directive 2003/105/EC (Seveso II)*, European Communities, 2005.
<http://mfiles.pl>.
<http://wartowiedziec.org>.
<http://www.wsjp.pl>.
- IIF Report Reform In the Financial Services Industry: Strengthening Practices for a More Stable System, Institute of International Finance, 2009.
- Knight K.W., The New Standard For Risk Management, materiał przygotowany na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, Warszawa 2010.
- Maas P., *Wiedza praktyczna: Zarządzanie poprzez cele*, wyd. Verlag Dashofer, Warszawa 2004 [dok. elektr.], <http://www.dashofer.pl/przyklady/ED-ZPC.pdf>.
- Mitkowski P.T., Ocena ilościowa ryzyka: analiza drzewa błędu (konsekwencji), materiały dydaktyczne, Politechnika Poznańska.
- Wnioski wypływające z kryzysu finansowego z perspektywy nadzorczej, prezentacja ze spotkania szefów banków działających w Polsce z kierownictwem UKNF (Warszawa, 25 lutego 2011 r.) [dok. elektr.], http://www.knf.gov.pl/Images/Wnioski_wplywajace_z_kryzysu_tcm75-25681.pdf.

CZEŚĆ III

ZARZĄDZANIE RYZYKIEM NA SZCZEBLU UNII EUROPEJSKIEJ

WPROWADZENIE

Unia Europejska podejmuje na swoim poziomie prace w zakresie oceny zagrożeń i ryzyka, na które narażeni są obywatele UE w różnych obszarach życia i działalności. Niemal każdy obszar funkcjonowania UE można powiązać z koniecznością dokonania oceny ryzyka wystąpienia danego zagrożenia, np.: możliwy wypadek przy przepływie statków przez Morze Bałtyckie, zagrożenie piractwem morskim u wybrzeży Afryki, zagrożenie terroryzmem, kryzys migracyjny, zagrożenia przestępczością zorganizowaną czy handlem ludźmi w UE, ryzyko wystąpienia katastrof naturalnych lub technologicznych.

Unia Europejska w pracach związanych z oceną ryzyka i zagrożeń korzysta z wypracowanych metodyk – w tym z norm Międzynarodowej Organizacji Normalizacyjnej, terminologii ustalonej podczas forum Organizacji Narodów Zjednoczonych, metodologii państw członkowskich oraz innych metod opracowanych w wyniku analiz, sama też proponuje państwom członkowskim terminologię, która dotyczy analizy ryzyka i oceny zagrożeń. Liczba katastrof rośnie, w latach 1994–2013 na całym świecie doszło do 6 873 katastrof naturalnych, które pochłonęły 1,35 mln ofiar, co oznacza średnio ok. 68 000 ofiar rocznie. ONZ szacuje, że straty gospodarcze spowodowane przez katastrofy naturalne w latach 2005–2015 wyniosły 1,3 bln dolarów¹. Dlatego tym bardziej zrozumiałe są prace prowadzone na forum UE czy międzynarodowym, mające na celu ograniczanie możliwości występowania katastrof, lepsze przygotowywanie się na ich wypadek czy zarządzanie ich skutkami.

W *Strategii bezpieczeństwa wewnętrznego UE* z 2010 r. podkreślono, że należy opracować wytyczne diagnozowania, oceniania i analizowania zagrożeń i ryzyka oraz dokonywać przeglądu zagrożeń naturalnych i wynikających z działalności ludzkiej, przed którymi może w przyszłości stanąć Unia. Wspierający realizację tej strategii Fundusz Bezpieczeństwa Wewnętrznego przyjmuje, że „zarządzanie ryzykiem i zarządzanie kryzysowe – oznacza każdy środek dotyczący oceny, zapobiegania, środków gotowości oraz zarządzania następstwami terroryzmu, przestępczości zorganizowanej oraz innych zagrożeń dla bezpieczeństwa. Jako priorytety strategiczne UE wskazano środki podnoszące odporność Unii na sytuacje kryzysowe i katastrofy, w szczególności projekty promujące rozwój spójnej polityki Unii w dziedzinie

¹ Europejski Trybunał Obrachunkowy, Sprawozdanie specjalne nr 33/2016, Unijny Mechanizm Ochrony Ludności – koordynacja reagowania na klęski żywiołowe poza terytorium UE była zasadniczo skuteczna, s. 8; za: Ramy z Sendai dotyczące ograniczania ryzyka klęsk żywiołowych na lata 2015–2030, UNISDR, Genewa 2015.

zarządzania ryzykiem, która łączy ocenę zagrożenia i ryzyka z procesem decyzyjnym, jak również projekty wspierające skuteczne i skoordynowane reagowanie na sytuacje kryzysowe poprzez połączenie istniejącego potencjału, ośrodków wiedzy eksperckiej oraz ośrodków wiedzy na temat sytuacji (w poszczególnych sektorach), w tym w sektorze zdrowia, ochrony ludności i przeciwdziałania terroryzmu”².

Kwestie oceny ryzyka uregulowała także decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności. Zgodnie z jej zapisami państwa członkowskie zostały zobligowane do opracowania oceny ryzyka na szczeblu krajowym lub odpowiednim niższym szczeblu oraz udostępnienia Komisji streszczenia istotnych elementów tych ocen do 22 grudnia 2015 r.³ Ponadto ustanowiono, że kraje te miały przygotować plany zarządzania ryzykiem związanym z klęskami i katastrofami na szczeblu krajowym lub odpowiednio niższym, stale je doskonaląc. Komisja Europejska do końca 2014 r. opracowała wspólnie z państwami członkowskimi wytyczne w sprawie treści, metodologii i struktury tych ocen. Kontynuacją była publikacja wyników prac KE w dniu 23 maja 2017 r. *Overview of Natural and Man-made Disaster Risks the European Union may face* (Przegląd zagrożeń w UE), który będzie omówiony w dalszej części pracy.

W tej części publikacji po opisanu pojęć funkcjonujących w ramach UE, a dotyczących zarządzania ryzykiem w ramach analizy przepisów, zostaną przedstawione przykłady przepisów odnoszących się do zarządzania ryzykiem, powiązanych z zapobieganiem, przygotowaniem, reagowaniem oraz odbudową po wystąpieniu sytuacji kryzysowej w UE. Analizy przepisów w zakresie oceny ryzyka nie można dokonać w oderwaniu od instytucji unijnych, które ją przeprowadzają. Przedstawienie przykładów agencji czy roli instytucji będzie miało na celu pokazanie sektorowego podejścia UE do kwestii zarządzania ryzykiem na wypadek potencjalnych sytuacji kryzysowych. W niniejszej części diagnozy zostaną przedstawione standardy i definicje uznane przez Unię Europejską i zapisane w dokumentach unijnych, rozporządzeniach, wytycznych oraz dyrektywach.

W materiale przeprowadzona zostanie analiza metodyk oceny ryzyka dla poszczególnych rodzajów zagrożeń odnoszących się do wielu dziedzin aktywności UE. Dotychczas Unia prowadziła działania w zakresie oceny zagrożeń i ryzyk w sektorach oraz obszarach. W niniejszej części przybliżona zostanie organizacja zarządzania ryzykiem na szczeblu UE z uwzględnieniem roli instytucji unijnych i agencji z nimi współpracujących. Omówione zostaną przykłady zarządzania ryzykiem w obszarze bezpieczeństwa wewnętrznego, a także w skróconej wersji zostanie przedstawiona ocena ryzyka prowadzona w dziedzinie bezpieczeństwa

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 513/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego oraz uchylające decyzję Rady 2007/125/WSiSW, (Dz. Urz. UE L 150 z 20.05.2014, s. 93).

³ A następnie co 3 lata.

zewnątrznego. W odniesieniu do bezpieczeństwa wewnętrznego działania UE w poszczególnych obszarach zostaną przedstawione na przykładzie: zarządzania ryzykiem powodziowym, zagrożeń wypadkami chemicznymi, testów wytrzymałościowych, transgranicznych zagrożeń zdrowia, zagrożeń związanych z żywnością, ochrony granic zewnętrznych Unii, a także Unijnego Mechanizmu Ochrony Ludności. W końcowej części rozdziału przywołana zostanie również aktywność naukowo-badawcza UE w zakresie projektów zgłębiających tematykę oceny ryzyka. Ostatnią część rozdziału stanowią podsumowanie i wnioski. W tej części zostaną zaakcentowane wnioski dotyczące przepisów oraz przybliżone problemy i wyzwania, z którymi musi się zmierzyć Unia Europejska w obszarze zarządzania ryzykiem na wypadek sytuacji kryzysowych możliwych do wystąpienia na jej terytorium, jak i w otoczeniu gospodarczym czy geopolitycznym.

Rozważania w rozdziale zostały oparte w głównej mierze o wyniki badań zawarte w sprawozdaniach pt. *Analiza metodyk oceny ryzyka i zagrożeń ujętych w przepisach UE związanych z zarządzaniem ryzykiem – diagnoza stanu oraz Analiza przepisów unijnych związanych z zarządzaniem ryzykiem* autorstwa Małgorzaty Trzcńskiej, powstałe w ramach projektu badawczo-rozwojowego pt. „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne” nr DOBR/0016/R/ID2/2012/03.

1. ZARZĄDZANIE RYZYKIEM W UNII EUROPEJSKIEJ

Niemal we wszystkich dziedzinach funkcjonowania UE można znaleźć odniesienia do zagadnienia zarządzania ryzykiem: w sektorze finansowym, celnym, żywnościowym, bezpieczeństwie w pracy, bezpieczeństwie żywnościowym, zdrowotnym, zarządzaniu ryzykiem na wypadek wystąpienia katastrof. Z niniejszej analizy wyłączone zostaną obszary niepowiązane z zarządzaniem kryzysowym, które jest rozumiane jako działania z zakresu: zapobiegania, przygotowania oraz reagowania na sytuacje kryzysowe oraz odbudowy w różnych obszarach funkcjonowania UE, zarówno w wymiarze wewnętrznym, jak i zewnętrznym.

W niniejszej analizie przedstawiono przepisy, które regulują zarządzanie ryzykiem w UE, a także przepisy regulujące role instytucji unijnych oraz współpracujących agencji unijnych w zakresie zarządzania ryzykiem. Zostały opisane także unijne prace nad zarządzaniem ryzykiem w obszarze bezpieczeństwa wewnętrznego oraz zewnętrznego UE. Nie da się rozłączyć tych obszarów np. w kwestii zarządzania ryzykiem na wypadek zagrożeń globalnych (terroryzm, transgraniczne zagrożenia zdrowotne), które mają swoje implikacje w dziedzinie bezpieczeństwa wewnętrznego oraz zewnętrznego. Aby jednak rozpocząć analizę przepisów i przedstawić unijne analizy ryzyka, punktem wyjściowym jest zdefiniowanie pojęć.

2. POJĘCIE ZARZĄDZANIA RYZYKIEM W UNII EUROPEJSKIEJ

Zarządzanie ryzykiem powiązane jest z teorią zarządzania i jest częścią składową procesu zarządzania. Każda organizacja jest narażona na ryzyko np. utraty płynności finansowej, straty w wyniku awarii przemysłowej czy katastrofy naturalnej, ataku terroru czy sabotażu. Proces zarządzania ryzykiem składa się z wielu elementów: po pierwsze ważne jest zrozumienie wykonywanej działalności przez daną firmę, identyfikacja zagrożeń w jej wnętrzu i otoczeniu, dokonanie analizy ryzyka oraz jego oceny punktowej (tzw. *scoring*), potem hierarchizowanie ryzyka oraz zarządzanie (sterowanie) nim. W niniejszej analizie zarządzanie ryzykiem będzie rozumiane jako proces łączący wyżej wymienione elementy oraz jako sterowanie, sposób zarządzania, podejmowania działań i decyzji, których celem jest poradzenie sobie z danym ryzykiem.

Zarządzanie ryzykiem doczekało się standaryzacji w normie ISO 31000:2009 *Risk management – Principles and guidelines*, której polskim odpowiednikiem jest norma PN-ISO 31000:2012. Norma ISO zawiera opis skoordynowanych działań dotyczących kierowania i nadzorowania organizacją w odniesieniu do ryzyka. ISO 31000 to międzynarodowy standard zapewniający reguły i ogólne wskazówki wprowadzania zarządzania ryzykiem. Norma 31010 dookreśla pojęcia istotne z punktu widzenia niniejszej analizy:

- **ryzyko** jest kombinacją skutków zdarzenia (zagrożenia) oraz związanego z nimi prawdopodobieństwa/możliwości ich wystąpienia;
- **ocena ryzyka** jest całościowym procesem obejmującym identyfikację ryzyka, analizę ryzyka i ewaluację ryzyka;
- **identyfikacja ryzyka** jest procesem poszukiwania, rozpoznawania i opisywania ryzyk;
- **analiza ryzyka** jest procesem zrozumienia natury ryzyka w celu określenia poziomu ryzyka;
- **ewaluacja ryzyka** jest procesem porównywania wyników analizy ryzyka z kryteriami ryzyka w celu ustalenia, czy ryzyko i/lub jego wielkość jest akceptowalne lub tolerowane.

Z uwagi na fakt, że zarządzanie ryzykiem jest powiązane z teorią zarządzania, Unia Europejska też nie może w ramach swojego funkcjonowania tego obszaru pominąć. Rządy i służby publiczne w państwach Unii Europejskiej coraz częściej udostępniają informacje o sposobie i zakresie inwestycji w zarządzanie ryzykiem.

W 2005 r. Komisja Europejska przyjęła dokument *Ku skutecznemu i spójnemu zarządzaniu ryzykiem w służbach Komisji (SEC/2005/1327)*. Można zadać pytanie, dlaczego takie procesy mają miejsce? Wymusza to bowiem rzeczywistość i potencjalne zagrożenia. Obecnie jednym z zadań organizacji jest ograniczanie ryzyka i związanych z nim skutków, np. zapobieganie korupcji, przygotowanie się na wystąpienie potencjalnej sytuacji kryzysowej i działań – zarówno w czasie kryzysu, jak i fazy pokryzysowej. Konieczność funkcjonowania firm czy przedsiębiorstw w globalnym świecie naraża je na skutki zdarzeń już nie tylko na terytorium jednego kraju, ale także Unii Europejskiej czy nawet całego świata w odniesieniu do firm działających globalnie. Ryzyko wystąpienia zagrożeń czy sytuacji kryzysowych może wymuszać konieczność podejmowania działań przez inne kraje (np. w przypadku katastrofy w Fukushima w obliczu ryzyka skażenia żywności w UE czy zagrożenia pandemią, wirusem ebola lub zika w wymiarze globalnym).

Wyróżnia się następujące etapy procesu zarządzania ryzykiem:

- identyfikacja ryzyka;
- analiza i pomiar ryzyka;
- sterowanie ryzykiem;
- monitorowanie i kontrola ryzyka.

Glosariusz Międzynarodowych Standardów Profesjonalnej Praktyki Audytu Wewnętrznego wydany przez Auditorów Wewnętrznych określa ryzyko jako możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów. Proces zarządzania ryzykiem powinien być wsparty solidną bazą informacyjną, obejmującą identyfikację ryzyka, analizę ryzyka, punktową ocenę ryzyka (ang. *risk scoring*) oraz hierarchizację ryzyka.

Poprzez ryzyko wystąpienia katastrof (ang. *disaster risk*) UE rozumie: „możliwą utratę życia, szkody, zniszczone lub uszkodzone zasoby, które mogą wystąpić w systemie, społeczeństwie, wspólnocie w danym przedziale czasowym; określone z uwzględnieniem zagrożenia (naturalnego lub spowodowanego działalnością człowieka), ryzyka, podatności oraz wymiaru” (tłum. własne)⁴. Z kolei ocena ryzyka wystąpienia katastrof (ang. *assessment of risks of disasters*) odnosi się do: „całościowego międzysektorowego procesu identyfikacji ryzyka, analizy ryzyka i jego oceny” (tłum. własne)⁵. Definicje pozostałych terminów dotyczących oceny ryzyka oraz mapowania ryzyka i opracowane na poziomie ONZ lub w ramach normy ISO 31010 zestawiono w wytycznych KE.

⁴ *Disaster risk: potential loss of life, injury, destroyed or damaged assets which could occur to a system, society or community in a specific period of time, determined by taking into account hazard (both natural and man-made), exposure, vulnerability and capacity*; Źródło: Komisja Europejska, Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final z dnia 23 maja 2017, s. 13.

⁵ *Assessment of risks of disasters: overall cross-sectorial process of risk identification, risk analysis, and risk evaluation*; Źródło: Tamże.

Z perspektywy niniejszej analizy warto zwrócić uwagę na rozumienie pojęć ryzyko oraz zagrożenie. W Traktacie z Lizbony stanowi się, że „Unia zachęca do współpracy między państwami członkowskimi w celu zwiększenia skuteczności systemów zapobiegania klęskom żywiołowym lub katastrofom spowodowanym przez człowieka i ochrony przed nimi. Działanie Unii zmierza do:

- a) wspierania i uzupełniania działań państw członkowskich na poziomie krajowym, regionalnym i lokalnym w zakresie zapobiegania zagrożeniom, przygotowania personelu ochrony ludności w państwach członkowskich i reagowania na klęski żywiołowe lub katastrofy spowodowane przez człowieka na terytorium Unii;
- b) wspierania szybkiej i skutecznej współpracy operacyjnej krajowych służb ochrony ludności na terytorium Unii;
- c) wspierania spójności międzynarodowych działań w zakresie ochrony ludności”⁶.

Pojęcia ryzyko i zagrożenie nie są tożsame w języku polskim i w innych wersjach językowych dokumentu, choć w niemieckiej wersji językowej Traktatu mówi się *Risikoprävention*, natomiast we francuskiej *prévention des risques*, z kolei w angielskiej *risk prevention*. W polskiej wersji Traktatu mówi się o „zapobieganiu zagrożeniom”. W niniejszej analizie celem nie będzie rozstrzygnięcie różnic terminów *ryzyko* oraz *zagrożenie* występujących w Traktacie, a jedynie zwrócenie uwagi na rozbieżność, która może wprowadzić pewne utrudnienie w zrozumieniu siatki pojęciowej UE w tym zakresie z perspektywy państw członkowskich. Angielskiego pojęcia *risk* oraz polskiego *zagrożenie* używa się w Traktacie wymiennie.

Podsumowując, na potrzeby niniejszej analizy przyjmuje się tezę o sektorowym podejściu UE do kwestii zarządzania ryzykiem związanym z występowaniem danych zagrożeń.

⁶ Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz. Urz. UE C 306 z 17.12.2007); data wejścia w życie: 01.12.2009.

3. ANALIZA PRZEPISÓW UNIJNYCH ZWIĄZANYCH Z ZARZĄDZANIEM RYZYKIEM

Analiza przepisów unijnych w zakresie zarządzania ryzykiem zostanie przedstawiona na przykładach istniejącego prawodawstwa UE w tym zakresie (rozporządzeń, dyrektyw i decyzji).

3.1. Rozporządzenia

Rozporządzenia są wiążącym aktem prawnym i muszą być stosowane w całości na całym obszarze UE. Rozporządzenia wydaje Rada UE oraz Komisja Europejska lub wspólnie Parlament Europejski i Rada UE. Przykłady dokumentów z obszaru zarządzania ryzykiem:

1. Rozporządzenie Rady (EWG) nr 793/93 z dnia 23 marca 1993 r. w sprawie oceny i kontroli ryzyk stwarzanych przez istniejące substancje¹.
2. Rozporządzenie (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności².
3. Rozporządzenie Rady (EWG) nr 793/93 z dnia 23 marca 1993 r. w sprawie oceny i kontroli ryzyk stwarzanych przez istniejące substancje³.

3.2. Dyrektywy

Dyrektywa jest aktem prawnym, którego cele muszą osiągnąć wszystkie państwa UE, jednak sposób ich osiągnięcia określają państwa członkowskie. Przykłady dyrektyw z obszaru zarządzania ryzykiem:

¹ Dz. Urz. WE L 84 z 05.04.1993, s. 1 z późn. zm.; Rozporządzenie (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. (Dz. Urz. UE L 284 z 31.10.2003, s. 1) stosuje się do oceny ryzyk stwarzanych przez istniejące substancje dla człowieka, w tym dla pracowników i konsumentów, jak i dla środowiska, w celu zapewnienia lepszego zarządzania tymi ryzykami w ramach przepisów wspólnotowych.

² Dz. Urz. WE L 31 z 01.02.2002, s. 1–24.

³ Dz. Urz. WE L 84 z 05.04.1993, s. 1–75.

1. Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim⁴.
2. Dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE⁵.
3. Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony⁶.

3.3. Decyzje

Decyzja jest wiążąca dla tych podmiotów, do których jest skierowana (np. państwa UE lub pojedynczego przedsiębiorstwa) i jest stosowana bezpośrednio. Przykłady decyzji:

1. Decyzja Rady z dnia 12 lutego 2007 r. ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa.
2. Decyzja Rady UE z dnia 8 listopada 2007 r. ustanawiająca wspólnotowy mechanizm ochrony ludności (przekształcenie) (2007/779/WE, Euratom)⁷.
3. Wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia⁸.
4. Decyzja nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE⁹.

⁴ Dz. Urz. UE L 288 z 06.11.2007, s. 27–34.

⁵ Dz. Urz. UE L 197 z 27.04.2012, s. 1–37.

⁶ Dz. Urz. UE L 345 z 23.12.2008, s. 75–82.

⁷ Dz. Urz. UE L 314 z 01.12.2007, s. 9–19.

⁸ Komisja Europejska, wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 final z dnia 08 grudnia 2011.

⁹ Decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE (Dz. Urz. UE L 293/1 z 05.11.2013).

4. ROLA INSTYTUCJI UNIJNYCH W ZAKRESIE ZARZĄDZANIA RYZYKIEM

Instytucje unijne takie jak Komisja Europejska (KE), Rada Unii Europejskiej, Europejska Służba Działań Zewnętrznych (ESDZ) uczestniczą w różny sposób w procesie zarządzania ryzykiem w Unii Europejskiej. Biorąc pod uwagę np. samą Komisję Europejską, jak pokaże niniejsza analiza, dokonuje ona oceny ryzyka poprzez swoje Dyrekcje Generalne, natomiast zarządza nim już jako Komisja Europejska na poziomie decyzji, które zapadają w jej władzach. Jako przykład, który będzie dokładniej przedstawiony w dalszej części pracy, posłuży np. rola agencji FRONTEX. Agencja ta prowadzi analizy ryzyka wystąpienia zagrożeń na granicach zewnętrznych UE. W przypadku identyfikacji zagrożeń bądź eskalacji zdarzeń informuje o nich zarówno KE (np. kanałem ARGUS do Sekretariatu Generalnego Komisji Europejskiej), jak i państwa członkowskie oraz inne agencje unijne czy też Europejską Służbę Działań Zewnętrznych. Decyzje strategiczne dla danego ryzyka będą zapadać na forum FRONTEX oraz Komisji Europejskiej, ESDZ czy Rady Unii Europejskiej.

Powiązania, role i zadania poszczególnych instytucji unijnych w zakresie analizy ryzyka oraz zarządzania ryzykiem na forum UE pokaże dokładniej przypadek katastrofy jądrowej w Japonii, która nastąpiła w wyniku trzęsienia ziemi i tsunami w dniu 11 marca 2011 r. Od samego początku w ramach działań KE np. w tym DG ds. Energii, DG ds. Środowiska, Dyrekcja Generalna ds. Zdrowia i Konsumentów oraz Dyrekcja Generalna ds. Pomocy Humanitarnej i Ochrony Ludności (DG ECHO) prowadziły monitoring sytuacji. W ramach prac w UE wykorzystano z możliwości systemów np. ECURIE (ang. *European Community Urgent Radiological Information Exchange*), EURDEP (ang. *European Radiological Data Exchange Platform*) czy innej platformy CECIS (ang. *Common Emergency Communication and Information System*). Z uwagi na brak formalnej prośby o pomoc ze strony rządu Japonii, UE nie mogła podjąć w pierwszych dniach zdarzenia innego rodzaju zaangażowania. W tym czasie część państw członkowskich UE wysłało pomoc w ramach umów bilateralnych. Po katastrofie w Fukushima w 2011 r. po kilku dniach od formalnego wyrażenia przez rząd Japonii prośby o pomoc rozpoczęła się organizacja wsparcia materialnego państw członkowskich dla ofiar katastrofy w Japonii. DG ECHO wyłoniło grupę ekspertów, którzy pojechali do Japonii wspierać koordynację działań oraz przygotować kanały dystrybucji dla pomocy

świadczonej przez UE. Już w dniach 24–25 marca 2011 r. Rada Unii Europejskiej przyjęła konkluzje, a tym samym liderzy UE podjęli decyzję, w której podkreślili znaczenie oceny ryzyka do oceny bezpieczeństwa elektrowni atomowych w UE (tzw. *stress tests* / testy wytrzymałościowe). Szczególnie obawy o ewentualny atak terrorystyczny na elektrownie atomowe w Europie wymuszały pilne prace po stronie Komisji Europejskiej, która miała podjąć się zdefiniowania zasad, na jakich będą dokonywane testy wytrzymałościowe. Z drugiej strony Rada Europejska miała dokonać oceny wyników tej analizy. Plan działania Europejskiej Grupy Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego ENSREG został zatwierdzony w dniu 1 sierpnia 2012 r. W 2012 r. wydano komunikat Komisji (COM(2012)0571)¹ z dnia 4 października 2012 r. dotyczący kompleksowych ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych. Wypadek w elektrowni Fukushima w Japonii w następstwie trzęsienia ziemi i tsunami w marcu 2011 r. uwypuklił wyzwania dotyczące zapewnienia bezpieczeństwa jądrowego. Wydarzenie to pokazało, że reaktory jądrowe muszą być chronione nawet przed wypadkami, które zostały ocenione jako wysoce nieprawdopodobne.

Rolę Parlamentu w tym przypadku widać w Rezolucji Parlamentu Europejskiego w sprawie ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych (2012/2830(RSP)). Rezolucję w tej sprawie przyjęto 14 marca 2013 r. Parlament przyjął do wiadomości komunikat Komisji w sprawie testów wytrzymałościowych i ich wyników po wypadku w Fukushima. Z zadowoleniem przyjął on także wysiłki podjęte przez Komisję i Europejską Grupę Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego (ENSREG) po wypadku w Fukushima na rzecz przeprowadzenia testów wytrzymałościowych 145 reaktorów w UE i 20 reaktorów poza UE. PE wezwał Komisję i państwa członkowskie do zachęcania krajów spoza UE, które mają elektrownie jądrowe, w szczególności krajów sąsiadujących z UE, do przeprowadzenia takich testów wytrzymałościowych i podzielenia się ich wynikami. Podkreśla on także znaczenie zwiększenia międzynarodowych norm bezpieczeństwa jądrowego i ochrony jądrowej oraz ich właściwego wdrażania. Ponadto zauważa, że katastrofy naturalne, takie jak trzęsienia ziemi i tsunami, mogą zagrozić bezpieczeństwu istniejących lub budowanych elektrowni jądrowych na terenie Unii i w krajach sąsiadujących, w których występuje wysokie ryzyko trzęsień ziemi i tsunami, jak na przykład w Akkuyu w Turcji. Ponadto podkreśla również, że oprócz środków, jakie mają zostać wdrożone w odniesieniu do elektrowni jądrowych, należy podjąć wszelkie stosowne działania na szczeblu Unii i państw członkowskich, aby nie dopuścić do składowania odpadów promieniotwórczych w obszarach wysokiego ryzyka.

¹ Komisja Europejska, komunikat Komisji do Rady i Parlamentu Europejskiego dotyczący kompleksowych ocen ryzyka i bezpieczeństwa („testów wytrzymałościowych”) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych, COM(2012) 571 final z dnia 4 października 2012.

Przypadek katastrofy w Japonii i zaangażowanie UE są na tyle wielowymiarowe (katastrofa naturalna, technologiczna, wymiar globalny, pomoc ratownicza, pomoc humanitarna, skażenie wody oraz żywności, ewakuacja masowa, bezpieczeństwo elektrowni atomowych), że nie sposób w tej analizie przedstawić wszystkich powiązań na szczeblu UE. Jednak widoczne jest podejmowanie decyzji i działań na poziomie Komisji Europejskiej, Rady Unii Europejskiej oraz pewnych działań określających kierunek prac UE na poziomie Parlamentu Europejskiego oraz oceny ryzyka i oceny sytuacji na poziomie roli i zadań np. w ramach zadań sieci RASFF: System Wczesnego Ostrzegania o Niebezpiecznych Produktach Spożywczych i Środkach Żywnienia Zwierząt (ang. *Rapid Alert System for Food and Feed*) czy ówczesnego MIC w DG ECHO (obecnie ERCC: *Emergency Response Coordination Centre*) w DG ECHO oraz innych centrach Dyrekcji Generalnych Komisji Europejskiej.

Nową jakością w zarządzaniu ryzykiem w wymiarze zewnętrznym po wprowadzeniu Traktatem z Lizbony funkcji Wysokiego Przedstawiciela UE ds. zagranicznych i polityki bezpieczeństwa oraz utworzeniu Europejskiej Służby Działań Zewnętrznych jest proces analizy ryzyka prowadzony przez ESDZ. Te nowe role wpisały się w proces zarządzania ryzykiem w UE. W ramach ESDZ utworzono nową strukturę z części Sekretariatu Generalnego Rady UE oraz Komisji Europejskiej, której zdaniem jest m.in. przeprowadzanie oceny ryzyka zewnętrznego UE oraz dla misji zewnętrznych prowadzonych przez Unię Europejską. W przypadku np. omawianego wcześniej przypadku bezpieczeństwa jądrowego w UE Komisja Europejska będzie współpracowała z Europejską Służbą Działań Zewnętrznych w celu jak najlepszego wykorzystania istniejących w tym obszarze instrumentów współpracy zewnętrznej, w szczególności Instrumentu Współpracy w dziedzinie Bezpieczeństwa Jądrowego, Instrumentu na rzecz Stabilności w zakresie, w jakim jest on poświęcony ograniczaniu ryzyka chemicznego, biologicznego, radiologicznego i jądrowego oraz Instrumentu Pomocy Przedakcesyjnej. Przykład ten pokazuje powiązanie poziomu politycznego z konkretnymi instrumentami służącymi realizacji polityki zewnętrznej UE. Szerzej zadania ESDZ zostaną omówione na koniec analizy.

Inną instytucją uczestniczącą w procesie analizy ryzyka jest Rada Europejska, która po wejściu w życie Traktatu z Lizbony zyskała status instytucji unijnej. Rada Europejska wskazuje Unii Europejskiej ogólny kierunek działań politycznych i wytycza jej ogólne priorytety. W celu umożliwienia podjęcia skutecznych działań przez Unię i jej państwa członkowskie, Rada Europejska systematycznie ocenia zagrożenia dla Unii.

Podsumowując, o ile działania i decyzje, dokumenty wypracowywane przez Komisję Europejską, Radę Unii Europejskiej, Europejską Służbę Działań Zewnętrznych, Radę Europejską oraz Parlament Europejski można powiązać z elementem zarządzania (sterowania) ryzykiem, to prace agencji unijnych w ramach Komisji

Europejskiej, Dyrekcje Generalne Komisji prowadzących monitoring zagrożeń czy przygotowanie na wypadek wystąpienia danego kryzysu będą powiązane z poziomem oceny ryzyka. Podział na poziom oceny oraz poziom decyzji ws. działań na wypadek wystąpienia ryzyk musi być oddzielony, niemniej jeden nie może istnieć bez drugiego.

5. ZARZĄDZANIE RYZYKIEM W OBSZARZE BEZPIECZEŃSTWA WEWNĘTRZNEGO UNII EUROPEJSKIEJ

Zgodnie z zapisami *Strategii bezpieczeństwa wewnętrznego Unii Europejskiej. Dążąc do europejskiego modelu bezpieczeństwa*¹, działania UE w zakresie ochrony ludności muszą być zorientowane na zwiększanie odporności na katastrofy i w tym celu należy opracować strategiczne podejście do zapobiegania katastrofom i do ich uprzedzania. Powinno się także dalej zwiększać gotowość i optymalizować reagowanie, uznając jednocześnie indywidualną odpowiedzialność każdego państwa. Należy opracować wytyczne diagnozowania, oceniania i analizowania zagrożeń i ryzyka oraz dokonać przeglądu zagrożeń naturalnych i antropogenicznych, które mogą w przyszłości pojawić się przed UE. Ogólnounijna analiza ryzyka powinna stać się podstawą inicjatyw współpracy między zagrożonymi państwami członkowskimi a UE w dziedzinie ochrony ludności i planowaniu zdolności. Należy zidentyfikować nowe niebezpieczeństwa i zagrożenia, takie jak niedobór energii, awarie informacyjno-komunikacyjne oraz pandemie. W polityce prewencyjnej należy uwzględnić troskę o odporność obywateli oraz sektora publicznego i prywatnego na skutki katastrof².

Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa stanowią zasadnicze aspekty ochrony ludzi i infrastruktury krytycznej w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W zmienionej decyzji z 2 grudnia 2004 r. Rada przyjęła zmieniony *Program Solidarności Unii Europejskiej na temat skutków zagrożeń i ataków terrorystycznych*. Podkreśliła znaczenie oceny ryzyka i zagrożenia, ochrony infrastruktury krytycznej, mechanizmów wykrywania i identyfikacji zagrożeń terrorystycznych, oraz politycznej i operacyjnej gotowości i zdolności w zakresie zarządzania skutkami. Program ma na celu ochronę ludności i infrastruktury krytycznej, w szczególności poprzez: „stymulowanie, promowanie i wspieranie ocen ryzyka dotyczących infrastruktury krytycznej w celu modernizacji systemów bezpieczeństwa oraz stymulowanie, promowanie i wspieranie opracowywania metodologii ochrony infrastruktury krytycznej, w szczególności metodologii

¹ Komisja Europejska, komunikat Komisji do Parlamentu Europejskiego i Rady, Strategia bezpieczeństwa wewnętrznego Unii Europejskiej. Dążąc do europejskiego modelu bezpieczeństwa, COM(2010) 673 final.

² Tamże.

w zakresie oceny ryzyka. (...) Główna odpowiedzialność za ochronę infrastruktury krytycznej spoczywa na państwach członkowskich, właścicielach, operatorach i użytkownikach (użytkowników definiuje się, jako organizacje eksploatujące i wykorzystujące infrastrukturę do celów gospodarczych i do celów świadczenia usług). (...) Odpowiedzialność za przeprowadzanie ocen ryzyka i zagrożenia spoczywa zatem głównie na państwach członkowskich. Ponadto w ramach tego programu uznaje się za użyteczne i właściwe wspieranie projektów realizowanych w państwach członkowskich, o ile mogą one dostarczyć przydatnego doświadczenia i wiedzy w kontekście dalszych działań na szczeblu wspólnotowym, w szczególności ocen ryzyka i zagrożenia”³.

W ramach programu ogólnego *bezpieczeństwo i ochrona wolności* Unia Europejska ustanowiła na lata 2007–2013 specjalny program mający na celu wspieranie projektów w zakresie zapobiegania, gotowości i zarządzania skutkami ataków terrorystycznych i innymi rodzajami ryzyka dla bezpieczeństwa. Program obejmował okres od dnia 1 stycznia 2007 r. do dnia 31 grudnia 2013 r.⁴ Nowy instrument wsparcia finansowego na rzecz współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego, w ramach Funduszu Bezpieczeństwa Wewnętrznego, został ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 513/2014 na okres od 1 stycznia 2014 r. do 31 grudnia 2020 r.⁵ Ma on wspierać realizację *Strategii bezpieczeństwa wewnętrznego UE*, współpracę w zakresie stanowienia prawa oraz zarządzanie na zewnętrznych granicach UE. Ogólnym celem instrumentu jest przyczynianie się do zapewnienia wysokiego poziomu bezpieczeństwa w Unii. „Jednym z celów szczegółowych jest zwiększanie zdolności państw członkowskich i Unii do skutecznego zarządzania ryzykami związanymi z bezpieczeństwem i zarządzania kryzysowego oraz przygotowanie i ochrona ludzi i infrastruktury krytycznej przed atakami terrorystycznymi i innymi zdarzeniami związanymi z zagrożeniem dla bezpieczeństwa”⁶.

W rozwinięciu toczących się prac w zakresie oceny ryzyka oraz w celu zagwarantowania skutecznej współpracy na państwa członkowskie został w 2011 r. we *wniosku dotyczącym decyzji Parlamentu Europejskiego i Rady w sprawie unijnego Mechanizmu Ochrony Ludności* został nałożony obowiązek przekazania do końca 2016 r. ich planów zarządzania zagrożeniami (art. 6). „Plany zarządzania

³ Decyzja Rady z dnia 12 lutego 2007 r. ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa” 2007/124/WE, Euratom (Dz. Urz. UE L 58 z 24.02.2007); wygaszony z końcem 2013 r.

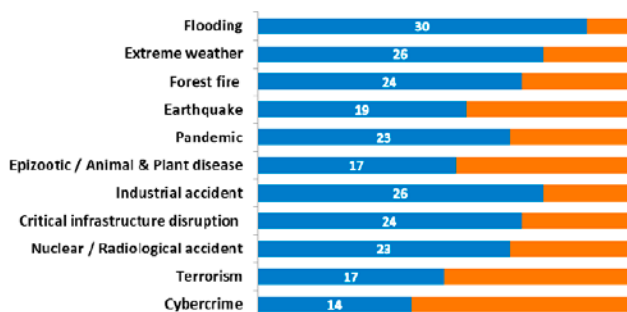
⁴ Tamże.

⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 513/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego oraz uchylające decyzję Rady 2007/125/WSiSW (Dz. Urz. UE L 150/93 z 20.05.2014).

⁶ Tamże.

zagrożeniem uwzględniają krajowe oceny zagrożenia oraz inne właściwe oceny zagrożenia i są spójne z innymi właściwymi planami obowiązującymi w danym państwie członkowskim”⁷. W końcu 2015 r. KE uruchomiła internetowe centrum wiedzy o zarządzaniu ryzykiem związanym z klęskami żywiołowymi, które świadczy usługi na potrzeby lepszej wymiany wiedzy i budowania zdolności w państwach uczestniczących w Unijnym Mechanizmie Ochrony Ludności⁸.

W dniu 23 maja 2017 r. Komisja opublikowała dokument *Overview of Natural and Man-made Disaster Risks the European Union may face* (Przegląd zagrożeń w UE), który podsumowuje prace KE nad krajowymi planami zarządzania zagrożeniami. Dokument skupia się na 11 głównych zagrożeniach, które zostały zaczerpnięte z dokumentów krajowych: powódzie, ekstremalne zagrożenia powodziowe, pożary lasów, trzęsienia ziemi, pandemie, zagrożenia epizoiczne, wypadki przemysłowe, załamania infrastruktury krytycznej, wypadki nuklearne i radiologiczne cyberprzestępstwo i terroryzm (zob. rys. 1).



Rys. 1. Ocena ryzyka wystąpienia danego zagrożenia w krajach UE uczestniczących w Unijnym Mechanizmie OL

Źródło: Komisja Europejska, *Overview of Natural and Man-made Disaster Risks the European Union may face*, SWD(2017) 176 final z dnia 23 maja 2017, s. 4.

W *Sprawozdaniu Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny śródkresowej funkcjonowania Unijnego Mechanizmu Ochrony Ludności w latach 2014–2016* za konieczne uznaje się „lepsze powiązanie Mechanizmu z innymi unijnymi politykami zewnętrznymi (np. pomocą rozwojową) i narzędziami, biorąc pod uwagę, że w ramach Unijnego Mechanizmu Ochrony Ludności coraz częściej prowadzi się interwencje poza UE (np. w przypadku epidemii eboli, trzęsienia ziemi w Nepalu, kryzysu migracyjnego) w rejonach, w których powtarzające się klęski i katastrofy mogą spłacać się z innymi czynnikami ryzyka, takimi jak konflikt i niestabilność. Podkreśla się, że należałoby również zwrócić uwagę na transgraniczne działania

⁷ Komisja Europejska, wniosek w sprawie decyzji Parlamentu Europejskiego i Rady w sprawie unijnego Mechanizmu Ochrony Ludności, COM(2011) 934 final z dnia 20 grudnia 2011, s. 20.

⁸ Disaster Risk Management Knowledge Centre platform, <http://drmkc.jrc.ec.europa.eu> [dostęp: wrzesień 2017].

z zakresu zapobiegania i gotowości, usprawniając tym samym zarządzanie ryzykiem w europejsko-krajowo-regionalno-lokalnym łańcuchu. Ponadto na poziomie polityki Komisja zobowiązała się do zapewnienia spójności i stałości swoich działań w zakresie ochrony ludności zgodnie z porozumieniami międzynarodowymi, w tym ramami z Sendai dotyczącymi ograniczania ryzyka klęsk żywiołowych w latach 2015–2030⁹.

Konkretne działania, które mają na celu poprawę zwalczania globalnych zagrożeń bezpieczeństwa wewnętrznego UE, finansowane są również poza UE w ramach unijnego Instrumentu na rzecz Stabilności, Instrumentu Pomocy Przedakcesyjnej oraz inicjatyw flagowych PPRD-South, PPRD-East. Celem jest wypracowanie na forum UE przeglądu ryzyk dla Unii Europejskiej. Drugie edycje ww. inicjatyw, w tym program PPRD-South realizowany był w latach 2013–2016 na rzecz państw: Algieria, Egipt, Izrael, Jordania, Liban, Libia, Maroko, Palestyna, Syrii. Z kolei program PPRD-East (listopad 2014–grudzień 2018) objął kraje: Armenia, Azerbejdżan, Białoruś, Gruzja, Mołdawia, Ukraina. Głównym celem tych inicjatyw była i jest budowa i wzmacnianie zdolności do radzenia sobie z przygotowaniem do reagowania na katastrofy, poprzez prewencję do usuwania skutków katastrof.

5.1. Zarządzanie ryzykiem powodziowym

Z powodziami mamy w Europie do czynienia od wieków. Wiele państw walczyło z nimi na swoich terenach, ale w przypadku rzek i dorzeczy na terenach przygranicznych niejednokrotnie nawiązywała się współpraca bilateralna. Wartością jednoczącą się Europy była także wspólna walka z powodziami. Katastroficzne w skutkach dla naszego regionu były powodzie w dorzeczach Dunaju i Elby w latach 2002 oraz 2005. To one wywarły wpływ na UE, aby działania związane z zarządzaniem ryzykiem powodziowym były bardziej skoordynowane.

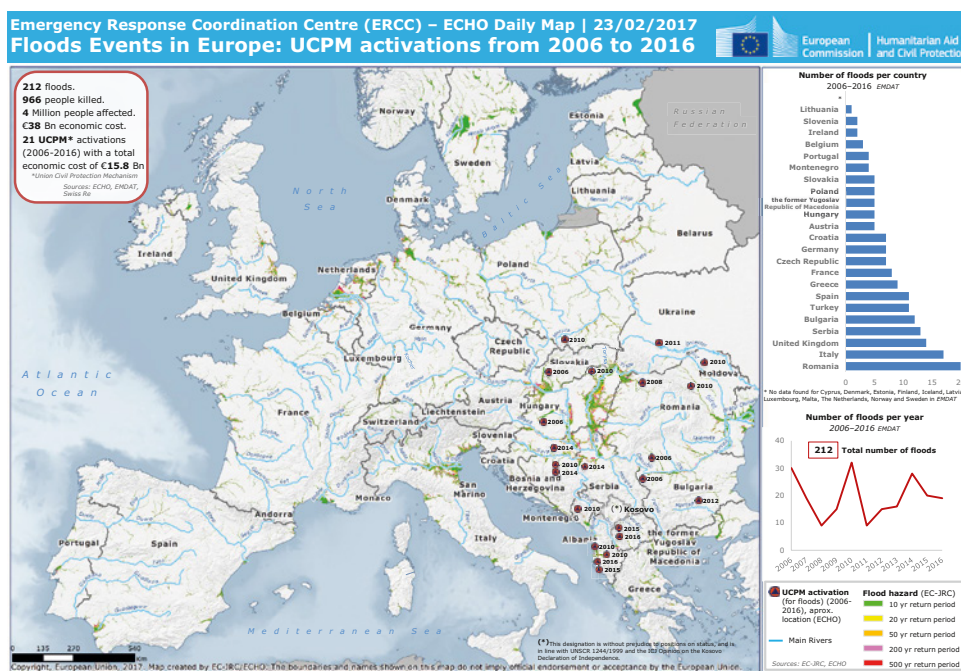
W latach 1998–2009 powodzie w Europie spowodowały śmierć 1126 osób, konieczność ewakuacji ponad pół miliona ludzi i straty ekonomiczne na poziomie co najmniej 52 mld EUR¹⁰. W raporcie Europejskiej Agencji Środowiskowej szacuje się, że koszt szkód spowodowanych przez powodzie rzeczne może przekraczać 10 mld EUR rocznie¹¹. Powodzie występują w wielu krajach UE. Regularnie nawiedzają kraje Europy Środkowej i Niemcy. Mimo wielu skoordynowanych działań UE nie udaje się zapobiec im w takim stopniu, aby można było mówić o wygranej walce. Od początku lat 80. XX wieku Komisja Europejska wspiera badania nad zjawiskami powodziowymi, w formie kolejnych ramowych programów badań i rozwoju technologicznego. Powodzie obejmują często Europę Środkową, w szczególności Polskę,

⁹ Komisja Europejska, sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny śródkresowej funkcjonowania Unijnego Mechanizmu Ochrony Ludności w latach 2014–2016, COM(2017) 460 final z dnia 30 sierpnia 2017.

¹⁰ Dane Europejskiej Agencji Środowiskowej.

¹¹ Europejska Agencja Środowiskowa, 2015, *Życie w zmieniającym się klimacie*, za: www.eea.europa.eu/soer-2015/europe/climate-changeimpacts-and-adaptation (original source PESETA study by JRC).

Republikę Czeską, Słowację, Węgry, Rumunię i Francję. Zagrożenie powodzią to jedno z największych zagrożeń w UE. Na poziomie 34¹² krajów UE uczestniczących w Unijnym Mechanizmie OL, zagrożenie wystąpienia w UE to aż 30% ryzyka¹³. Ostatnie aktywacje Mechanizmu bardzo często dotyczą powodzi: Była Jugosłowiańska Republika Macedonii i Albania (2015, 2016), Bośnia i Hercegowina, Serbia, Chorwacja (2014), Wielka Brytania i Słowenia (2014), Sardynia, Francja, Słowacja, Austria, Niemcy, Czechy (2013). W latach 2006–2016 miało miejsce 212 powodzi, które pochłonęły życie 966 osób. 4 miliony ludzi zostało dotkniętych skutkami tych zdarzeń, zarejestrowano 38 mld euro strat ekonomicznych oraz 21 aktywacji (2006–2016), które kosztowały 15,8 mld euro. Dane KE dot. powodzi z lat 2006–2016 w poszczególnych krajach UE przedstawia mapa ERCC z 23 lutego 2017 roku (rys. 2)¹⁴.



Rys. 2. Powodzie w Europie: aktywacje Unijnego Mechanizmu OL w latach 2006–2016, mapa z 23.02.2017

Źródło: <https://reliefweb.int/map/serbia/floods-events-europe-ucpm-activations-2006-2016-echo-daily-map-23022017>.

¹² 28 krajów UE oraz Islandia, Norwegia, Serbia, Montenegro, Była Jugosłowiańska Republika Macedonii oraz Turcja.

¹³ Komisja Europejska, *Overview of Natural and Man-made Disaster Risks the European Union may face*, SWD(2017) 176 final z dnia 23 maja 2017.

¹⁴ <http://erccportal.jrc.ec.europa.eu/getdailymap/docId/1969>; za: ECHO, EMDAT, Swiss Re [dostęp: wrzesień 2017].

Unia zajmuje się powodzią od wielu lat, jednak dopiero Komunikat Komisji z dnia 12 lipca 2004 r. dla Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów Zarządzanie zagrożeniem powodziowym – zapobieganie powodziom, ochrona przeciwpowodziowa i ograniczanie skutków powodzi¹⁵ zawierał opartą na analizie koncepcję zarządzania ryzykiem powodziowym na poziomie Wspólnoty. Raport stwierdzał, że uzgodnione i skoordynowane działanie na tym szczeblu przyniosłoby znaczne korzyści i przyczyniłoby się do poprawy ogólnego poziomu ochrony przeciwpowodziowej. „Wiele państw członkowskich już wprowadza środki ochrony przeciwpowodziowej, jednak uzgodnione i skoordynowane działanie na poziomie Unii Europejskiej przyniosłoby znaczną wartość dodaną i przyczyniłoby się do poprawy ogólnego poziomu ochrony przeciwpowodziowej, biorąc pod uwagę potencjalne zagrożenie ludzkiego życia, dóbr gospodarczych i środowiska”¹⁶. Co warto podkreślić, już w 2004 r. w komunikacie wspomina się o efekcie domina: „z dotychczasowych doświadczeń wynika, że lokalne środki ochrony przeciwpowodziowej, podejmowane w jednym miejscu, będą wywoływały efekt domina w obszarach położonych w górnym/dolnym biegu rzek. Jeżeli na przykład w obrębie jednego obszaru zostaną zastosowane rozwiązania inżyniersko-techniczne w celu odprowadzenia w możliwie najkrótszym czasie wody na należącym do niego odcinku rzeki, jest oczywiste, że pojawi się ona szybciej na sąsiednich terenach w jej dolnym biegu. Z tego względu koniecznością jest podejmowanie działań w zakresie ochrony przeciwpowodziowej w sposób uzgodniony i skoordynowany wzdłuż całego biegu rzeki”¹⁷.

Komunikat Zarządzanie zagrożeniem powodziowym – zapobieganie powodziom, ochrona przeciwpowodziowa i ograniczanie skutków powodzi przygotował UE oraz państwa członkowskie do przyjęcia dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim. Dyrektywa, która była propozycją Komisji Europejskiej przedstawioną 18 stycznia 2006 r., weszła w życie 26 listopada 2007 r. Co ważne, potwierdzała możliwość osiągnięcia większych efektów w walce z powodzią w przypadku podjęcia działań na poziomie Wspólnoty. Zadanie to uznano za pożądane oraz wykonalne. Z uwagi na zasady wprowadzania dyrektyw (dyrektywa jest aktem prawnym, którego cele muszą osiągnąć wszystkie państwa UE) sposób ich osiągnięcia pozostawiono do określenia państwom członkowskim. Wyznaczenie celów zarządzania ryzykiem powodziowym również pozostawiono państwom członkowskim, uznając, że cele państw powinny opierać się na warunkach lokalnych i regionalnych.

¹⁵ Komisja Europejska, komunikat Komisji dla Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Zarządzanie zagrożeniem powodziowym – zapobieganie powodziom, ochrona przeciwpowodziowa i ograniczanie skutków powodzi, COM(2004) 472 final z dnia 12 lipca 2004.

¹⁶ Tamże.

¹⁷ Tamże.

W powyższej dyrektywie zostały określone zobowiązania nakładane na państwa, które obejmowały¹⁸:

- opracowanie wstępnej oceny ryzyka powodziowego (do 22.12.2011 r.);
- opracowanie map zagrożenia powodziowego i map ryzyka powodziowego (do 22.12.2013 r.);
- opracowanie planów zarządzania ryzykiem powodziowym (do 22.12.2015 r.).

Wstępna ocenę ryzyka powodziowego przeprowadza się w oparciu o dostępne lub łatwe do uzyskania informacje, takie jak rejestry i długofalowe analizy rozwoju wydarzeń, dotyczące zwłaszcza wpływu zmian klimatycznych na występowanie powodzi.

Dyrektywa powodziowa wymaga od państw członkowskich identyfikacji obszarów potencjalnego ryzyka wystąpienia tego zjawiska. W ocenie należy wziąć pod uwagę m.in.: minione powodzie, zdolność ochrony infrastruktury przed powodzią czy długoterminową politykę w obszarze zagospodarowania przestrzennego czy zmian klimatu. Dla tych obszarów przygotowuje się oceny zagrożenia powodziowego oraz mapy ryzyka powodziowego, które uwzględniają potencjalne konsekwencje dla ludzkiego zdrowia, działalności ekonomicznej, dziedzictwa kulturowego i środowiska w poszczególnych scenariuszach. Ostatnim krokiem w celu unikania i ograniczania negatywnych skutków powodzi na danym obszarze jest przygotowanie planów zarządzania ryzykiem powodziowym, które powinny uwzględniać jego cele oraz zawierać zhierarchizowane środki służące ich osiągnięciu. W planach zarządzania na wypadek powodzi szczególny nacisk powinno się położyć na zapobieganie, ochronę i przygotowanie. Celem „dyrektywy jest ustanowienie ram dla oceny ryzyka powodziowego i zarządzania nim, w celu ograniczania negatywnych konsekwencji dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej, związanych z powodzią na terytorium Wspólnoty”¹⁹.

Na potrzeby dalszych prac w państwach członkowskich przyjęto definicję ryzyka powodziowego, które oznacza „kombinację prawdopodobieństwa wystąpienia powodzi i związanych z powodzią potencjalnych negatywnych konsekwencji dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej”²⁰.

5.1.1. Wstępna ocena ryzyka powodziowego

Wstępna ocena ryzyka powodziowego dokonywana przez państwa członkowskie, opisana w art. 4 ww. dyrektywy, powinna obejmować co najmniej:

¹⁸ Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz. Urz. UE L. 288 z 06.11.2007, s. 27–33).

¹⁹ Tamże, art. 1.

²⁰ Tamże.

- „mapy obszaru dorzecza w odpowiedniej skali, zawierające granice dorzeczy, zlewni i – jeżeli takowe istnieją – obszarów wybrzeża, ukazujące topografię i zagospodarowanie przestrzenne;
- opis powodzi, które wystąpiły w przeszłości i miały znaczące negatywne konsekwencje dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej, jeżeli prawdopodobieństwo wystąpienia podobnych zjawisk w przyszłości (uwzględniając zasięg powodzi i trasy przejścia fali powodziowej) jest nadal duże, jak i ocenę wywołanych przez nie negatywnych skutków;
- opis istotnych powodzi, do których doszło w przeszłości, jeżeli można przewidzieć, że podobne zjawiska w przyszłości będą miały znaczące negatywne skutki;

a w zależności od specyficznych potrzeb państw członkowskich:

- ocenę potencjalnych negatywnych konsekwencji przyszłych powodzi dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej, z jak najszerszym uwzględnieniem takich kwestii, jak: topografia, położenie cieków wodnych i ich ogólne cechy hydrologiczne oraz geomorfologiczne, w tym obszarów zalewowych jako naturalnych obszarów retencyjnych, skuteczność istniejącej, wybudowanej przez człowieka infrastruktury przeciwpowodziowej, położenie obszarów zamieszkałych, obszarów działalności gospodarczej oraz prognozę długofalowego rozwoju wydarzeń, w tym wpływu zmian klimatu na występowanie powodzi²¹.

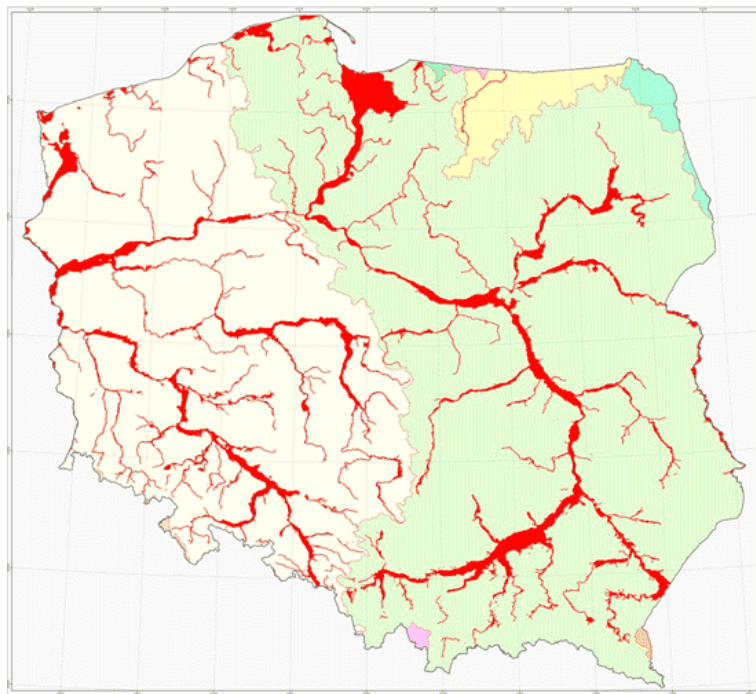
Metodyka wstępnej oceny ryzyka powodziowego zakłada wyodrębnienie obszarów narażonych na niebezpieczeństwo powodzi w dwóch etapach:

1. Przeprowadzenie analiz dla obszarów potencjalnie zagrożonych powodzią poprzez przyjęcie następujących kryteriów, w podanej niżej hierarchii:
 - bezpośredni wpływ powodzi na życie i zdrowie ludzi;
 - wpływ powodzi na obszary działalności gospodarczej wraz z infrastrukturą;
 - skuteczność istniejących budowli przeciwpowodziowych;
 - wpływ rozwoju zagospodarowania przestrzennego na wzrost ryzyka powodziowego.
2. Określenie punktacji ryzyka powodziowego dla każdego obszaru spełniającego kryteria wydzielenia oraz przyjęcie wartości granicznej punktacji, pozwalającej na wskazanie obszarów narażonych na niebezpieczeństwo powodzi.

Po podliczeniu wartości punktów w raporcie z oceny zostaje określone, czy w poszczególnych regionach wodnych istnieje prawdopodobieństwo wystąpienia powodzi i jeśli tak, to jakie – procentowo. Państwa członkowskie miały dokonać wstępnej oceny ryzyka powodziowego do 22 grudnia 2011 r. W Polsce za przygotowanie wstępnej oceny ryzyka powodziowego (WORP) odpowiadał Prezes Krajowego Zarządu Gospodarki

²¹ Tamże.

Wodnej. W ramach projektu ISOK, do końca 2013 r., wykonano mapy zagrożenia powodziowego i mapy ryzyka powodziowego dla 253 rzek o łącznej długości 14 481 km²². Przykład mapy ze wstępnej oceny ryzyka powodziowego przedstawia rys. 4.



Rys. 4. Obszary w Polsce narażone na niebezpieczeństwo powodzi wskazane we wstępnej ocenie ryzyka powodziowego

Źródło: www.isok.gov.pl.

5.1.2. Mapy zagrożenia powodziowego i mapy ryzyka

Mapy zagrożenia powodziowego i mapy ryzyka²³ miały być przygotowane przez państwa członkowskie do 22 grudnia 2013 r. „Mapy zagrożenia powodziowego obejmują obszary geograficzne, na których może wystąpić powódź, zgodnie z jednym z następujących scenariuszy:

- niskie prawdopodobieństwo powodzi lub scenariusze zdarzeń ekstremalnych;
- średnie prawdopodobieństwo powodzi (częstotliwość występowania ≥ 100 lat);
- wysokie prawdopodobieństwo powodzi, w odpowiednich przypadkach”²⁴.

²² <http://www.isok.gov.pl/pl/wstepna-ocena-ryzyka-powodziowego> [dostęp: wrzesień 2017].

²³ Por. definicje i przykłady: część IV, rozdział 3, podrozdziały 3.1–3.2.

²⁴ Art. 6 ust. 3 dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz. Urz. UE L 288 z 06.11.2007).

Dla każdego ze scenariuszy przedstawia się następujące elementy:

- „zasięg powodzi;
- głębokość wody lub – w odpowiednich przypadkach – poziom zwierciadła wody;
- tam, gdzie jest to właściwe, prędkość przepływu wody lub odnośny przepływ wody”²⁵.

Metodyka przyjęta do opracowania map ryzyka powodziowego uwzględnia potencjalnie negatywne konsekwencje związane z powodzią, która wystąpiła zgodnie z jednym ze scenariuszy, wyrażone w następujący sposób:

- „szacunkowa liczba mieszkańców potencjalnie dotkniętych powodzią,
- rodzaj działalności gospodarczej prowadzonej na obszarze potencjalnie dotkniętym powodzią,
- instalacje, o których mowa w załączniku I do dyrektywy Rady 96/61/WE z dnia 24 września 1996 r., dotyczącej zintegrowanego zapobiegania zanieczyszczeniom i ich kontroli (1), które mogłyby spowodować przypadkowe zanieczyszczenie w przypadku powodzi oraz potencjalnie dotknięte powodzią obszary chronione określone w załączniku IV pkt 1 ppkt (i), (iii) i (v) do dyrektywy 2000/60/WE,
- inne informacje uważane przez państwo członkowskie za przydatne, takie jak wskazanie obszarów, na których mogą wystąpić powodzie, którym towarzyszy transport dużej ilości osadów i rumowiska, oraz informacje o innych istotnych źródłach zanieczyszczenia”²⁶.

5.1.3. Plany zarządzania ryzykiem powodziowym

Ustalenie celów zarządzania ryzykiem powodziowym powierzono państwom członkowskim, przy czym w analizie tej szczególny nacisk powinny kłaść one na ograniczenie potencjalnych negatywnych konsekwencji powodzi dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego i działalności gospodarczej oraz, jeżeli zostanie to uznane za właściwe, na działania nietechniczne lub na zmniejszenie prawdopodobieństwa wystąpienia powodzi.

„Plany zarządzania ryzykiem powodziowym obejmują wszystkie aspekty zarządzania ryzykiem powodziowym, kładąc szczególny nacisk na zapobieganie, ochronę i stan należytego przygotowania, w tym prognozowanie powodzi i systemy wczesnego ostrzegania, a także uwzględniając cechy danego dorzecza lub zlewni. Plany zarządzania ryzykiem powodziowym mogą również obejmować działania na rzecz zrównoważonego zagospodarowania przestrzennego, skuteczniejszą retencję

²⁵ Tamże, art. 6 ust. 4.

²⁶ Tamże, art. 6 ust. 5.

wód oraz kontrolowane zalewanie niektórych obszarów w przypadku wystąpienia powodzi²⁷.

„Przy opracowaniu planów zarządzania ryzykiem powodziowym uwzględnia się takie aspekty, jak: koszty i korzyści, zasięg powodzi i trasy przejścia fali powodziowej oraz obszary o potencjalnej retencji wód powodziowych – takie jak naturalne obszary retencyjne, cele środowiskowe, gospodarowanie gruntami i wodą, planowanie przestrzenne, zagospodarowanie terenu, ochrona przyrody, nawigacja i infrastruktura portowa²⁸. Są to aspekty, które wskazują na konieczność uwzględnienia czynników geograficznych, historycznych, ekonomicznych, gospodarki przestrzennej i infrastruktury.

Państwa członkowskie miały opracować i opublikować plany zarządzania ryzykiem powodziowym do 22 grudnia 2015 r. Harmonogram dalszych prac na forum UE oraz w państwach członkowskich przedstawia się następująco²⁹:

1. Wstępne oceny ryzyka powodziowego lub ocena i decyzje poddawane są przeglądowi i w razie potrzeby aktualizowane do 22 grudnia 2018 r., a następnie co 6 lat.
2. Mapy zagrożenia powodziowego i mapy ryzyka powodziowego są poddawane przeglądowi i w razie potrzeby aktualizowane do 22 grudnia 2019 r., a następnie co 6 lat.
3. Plany zarządzania ryzykiem powodziowym są poddawane przeglądowi i w razie potrzeby aktualizowane do 22 grudnia 2021 r., a następnie co 6 lat.

Dodatkowe informacje na temat zarządzania ryzykiem powodziowym zawarto w rozdziale 3 części V publikacji.

5.2. Kontrola zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi – SEVESO III

Dyrektywa SEVESO III – tj. dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE³⁰ weszła w życie z dniem 13 sierpnia 2012 r. Krajowa transpozycja miała nastąpić do 31 maja 2015 r., natomiast całkowita implementacja miała zakończyć się do dnia 1 czerwca 2015 r. Jednym z kluczowych powodów przyjęcia nowej regulacji była konieczność uwzględnienia zmian dotyczących klasyfikowania substancji i mieszanin chemicznych. Dyrektywa była kolejnym krokiem UE w osiągnięciu większego bezpieczeństwa w obrębie jej granic, wezwała bowiem państwa członkowskie do podejmowania określonych działań na wypadek poważnych awarii z udziałem substancji chemicznych.

²⁷ Tamże, art. 7 ust. 3.

²⁸ Tamże.

²⁹ Tamże, art. 14.

³⁰ Dz. Urz. UE L 197 z 24.07.2012, s. 1–37.

Awarie w zakładach przemysłowych, w których wykorzystywane są substancje niebezpieczne, często pociągają za sobą poważne konsekwencje zarówno dla człowieka, jak i środowiska. Dowodem na to są m.in. awarie w Seveso (1976, Włochy), Bhopalu (1984, Indie), Schweizerhalle (1986, Szwajcaria), Enschede (2000, Niemcy), Tuluzie (2001, Francja) i Buncefield (2005, Wielka Brytania). Skutki awarii mogą być odczuwalne poza granicami danego państwa, a to przemawia tym bardziej za koniecznością zapewnienia właściwych działań zapobiegawczych, które zagwarantują wysoki poziom ochrony obywateli, społeczności i środowiska w całej Unii.

Na potrzeby przepisu przyjęto definicje „zakładu o zwiększonym ryzyku” oraz „zakładu o dużym ryzyku”, w którym znajdują się substancje niebezpieczne w ilościach określonych w zapisach dyrektywy. Dla dalszej analizy ważne będą dwie kluczowe definicje: zagrożenia i ryzyka. Zagrożenie oznacza samoistną właściwość substancji niebezpiecznej lub warunki fizyczne, które mogą spowodować szkody dla zdrowia ludzkiego lub środowiska. Ryzyko natomiast oznacza prawdopodobieństwo wystąpienia określonego skutku w określonym czasie lub w określonych okolicznościach.

Na podstawie dyrektywy Komisja, opierając się na zawiadomieniu państwa strony, dokonuje oceny zagrożenia poważną awarią dla określonej substancji niebezpiecznej. Systematyczna ocena zagrożeń w przypadku kontroli w danych zakładach opiera się co najmniej na następujących kryteriach:

- potencjalnym wpływie zakładów na zdrowie ludzkie i środowisko;
- historii zgodności z wymogami niniejszej dyrektywy.

Art. 10 dyrektywy daje możliwość nałożenia przez państwa członkowskie na prowadzącego zakład o dużym ryzyku obowiązku przygotowania raportu o bezpieczeństwie. „Raport o bezpieczeństwie powinien zawierać szczegółowe informacje na temat zakładu, znajdujących się w nim substancji niebezpiecznych, instalacji lub obiektów magazynowych, prawdopodobnych scenariuszy poważnych awarii i analizy ryzyka środowiskowego, środków zapobiegawczych i interwencyjnych oraz dostępnych systemów zarządzania, mając na względzie zapobieganie poważnym awariom i ograniczenie ryzyka ich wystąpienia oraz umożliwienie podjęcia niezbędnych działań w celu ograniczenia skutków takich awarii. Ryzyko poważnej awarii może być większe ze względu na prawdopodobieństwo wystąpienia klęsk żywiołowych związanych z położeniem zakładu. Należy to uwzględnić przy opracowywaniu scenariuszy poważnych awarii”³¹.

Minimalny zakres danych i informacji, które muszą zostać wzięte pod uwagę w raporcie o bezpieczeństwie, określa załącznik II do Dyrektywy. W zakresie

³¹ Dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE (Dz. Urz. UE L 197 z 24.07.2012, s. 1–37).

identyfikacji i analizy zagrożeń awariami oraz metod zapobiegawczych prowadzący zakład w raporcie o bezpieczeństwie uwzględnia:

- „szczegółowy opis scenariuszy poważnych awarii, które mogą się zdarzyć, oraz ich prawdopodobieństwo lub warunki, w jakich takie awarie mogą się zdarzyć, wraz ze streszczeniem przypadków mogących przyczynić się do rozpoczęcia każdego scenariusza, bez względu na to, czy przyczyny będą tkwić wewnątrz, czy na zewnątrz instalacji; w tym w szczególności:
 - przyczyny operacyjne;
 - przyczyny zewnętrzne, takie jak przyczyny związane z efektem domina, z obiektami, które nie są objęte zakresem stosowania niniejszej dyrektywy, obszarami i zabudowaniami, które mogą być źródłem zagrożenia poważną awarią lub które mogą zwiększyć takie zagrożenie lub jego skutki;
 - przyczyny naturalne, na przykład trzęsienia ziemi lub powódzie;
- ocenę zasięgu i skali skutków zidentyfikowanych poważnych awarii, w tym mapy, zobrazowania lub, stosownie do potrzeb, równoważne opisy ukazujące obszary, które mogą zostać dotknięte takimi awariami mogącymi powstać w zakładzie;
- przegląd wcześniejszych awarii i zdarzeń z takimi samymi wykorzystywanymi substancjami i procesami, uwzględnienie zdobytych w związku z nimi doświadczeń i wyraźne odniesienie do konkretnych działań podjętych w celu zapobiegania takim awariom;
- opis parametrów technicznych i sprzętu użytego do celów bezpieczeństwa instalacji”³².

Załącznik IV określa z kolei dane i informacje, które należy uwzględnić w planach operacyjno-ratowniczych, o których mowa w art. 12 dyrektywy. W przypadku wewnętrznych planów operacyjno-ratowniczych powinny one objąć także ustalenia związane z ograniczaniem ryzyka dla osób znajdujących się na miejscu, w tym sposób ostrzegania oraz działania, jakie osoby ostrzeżone mają podjąć.

W dyrektywie przyjęto także zapisy o efekcie domina. „Aby zmniejszyć ryzyko efektu domina w przypadku zakładów ułożonych w taki sposób lub tak blisko siebie, że wzrasta prawdopodobieństwo poważnych awarii lub nasilenia ich skutków, prowadzący zakłady powinni współpracować w zakresie wymiany odpowiednich informacji i informowania społeczności, z uwzględnieniem sąsiednich zakładów, które mogą odczuć skutki takich awarii”³³. Przyjęcie takiego

³² Tamże, załącznik II.

³³ Dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE z dnia 9 grudnia 1996 r. (Dz. Urz. UE L 197 z 24.7.2012, s. 1–37).

podejścia w UE jest wynikiem analizy skutków katastrofy w Japonii, która miała miejsce w 2011 r.

Kryteria zgłaszania Komisji poważnej awarii obejmują m.in. pożar czy uwolnienie substancji niebezpiecznej (zgodnie z zakresem wskazanym w dyrektywie), szkody i obrażenia doznane przez ludzi i szkody w nieruchomościach, jeżeli: awaria spowodowała bezpośrednie szkody w środowisku, wystąpiły szkody w mieniu lub doszło do wystąpienia zniszczeń o zasięgu transgranicznym. Komisji należy zgłaszać ponadto „awarie lub sytuacje bliskie awariom, które państwa członkowskie uznają za szczególnie interesujące z technicznego punktu widzenia w kontekście zapobiegania poważnym awariom oraz ograniczania ich skutków, które nie spełniają podanych powyżej kryteriów ilościowych”³⁴.

Dyrektywa w pkt 19 zapewnia dostęp do informacji na temat środowiska: (...) „należy poprawić poziom i jakość informacji udostępnianych społeczeństwu. W szczególności osoby, które mogą być narażone na skutki poważnej awarii powinny uzyskać wystarczające informacje o właściwych działaniach, które należy podjąć w takiej sytuacji (...)”. Co istotne jest to wymuszona transparentność działań, która z perspektywy procesu zarządzania ryzykiem także została wzięta pod uwagę przez UE. Społeczność ma być poinformowana za pośrednictwem ogłoszeń publicznych lub innych odpowiednich środków, w tym mediów elektronicznych.

Zgodnie z przyjętym w dyrektywie harmonogramem państwa członkowskie miały wprowadzić w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania danej dyrektywy w terminie do 31 maja 2015 r. Państwa członkowskie mają stosować niniejsze przepisy od dnia 1 czerwca 2015 r.

5.3. Zarządzanie ryzykiem związanym z elektrowniami jądrowymi – testy wytrzymałościowe

W wyniku trzęsienia ziemi, do którego doszło 11 marca 2011 r. w Japonii, poniosło śmierć wielu ludzi. Efekt domina, w którym jedno zdarzenie może spowodować wystąpienie innego czy wielu innych zdarzeń. W przypadku tej katastrofy przerósł on oceny ryzyka dokonane przez zakład jądrowy. Trzęsienie ziemi spowodowało powstanie fali tsunami, która doprowadziła do wypadku w elektrowni jądrowej Fukushima-Daiichi. Skutki tego wydarzenia były odczuwalne nawet w Stanach Zjednoczonych, gdzie służby ratownicze badały dryfujące po oceanie szczątki zmiecionych z powierzchni ziemi, skażonych domów, statków i drzew, które stanowiły zagrożenie dla środowiska naturalnego. Służby w Europie badały na lotniskach osoby powracające z Japonii pod kątem skażenia. Nikt nie zakładał takiego scenariusza wydarzeń dla elektrowni w Fukushima ani skali organizacji

³⁴ Tamże, załącznik IV.

pomocy w Japonii. Przerosła ona zdolności reagowania służb kraju dotkniętego kaskadową katastrofą³⁵.

Po katastrofie jądrowej w 2011 r. w japońskiej elektrowni jądrowej Fukushima-Daiichi, Rada Unii Europejskiej w dniach 24–25 marca 2011 r. przyjęła konkluzje Rady. Tym samym liderzy UE podjęli decyzję o konieczności przeglądu bezpieczeństwa wszystkich unijnych elektrowni jądrowych na podstawie kompleksowych, przejrzystych ocen ryzyka i bezpieczeństwa (testy wytrzymałościowe, testy warunków skrajnych tzw. *stress tests*). Obawy o ewentualny atak terrorystyczny na elektrownie atomowe w Europie wymusiły pilne prace po stronie Komisji Europejskiej, która miała podjąć się określenia zasad, na jakich będą dokonywane tzw. *stress tests*.

W listopadzie 2011 r. Komisja przedstawiła komunikat do Rady i Parlamentu Europejskiego dotyczący sprawozdania okresowego na temat kompleksowych ocen ryzyka i bezpieczeństwa w odniesieniu do elektrowni jądrowych w Unii Europejskiej (testy wytrzymałościowe)³⁶. Wezwała do dokonania „przeglądu bezpieczeństwa wszystkich unijnych elektrowni jądrowych na podstawie kompleksowych i przejrzystych ocen ryzyka i bezpieczeństwa („testy warunków skrajnych”)³⁷. Zasady dokonywania testów miały określić wspólnie Europejska Grupa Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego (European Nuclear Safety Regulatory Group ENSREG) oraz Komisja Europejska, szczególnie na bazie doświadczeń i wniosków po katastrofie w Japonii oraz przy pełnym zaangażowaniu państw członkowskich. „Oceny te będą przeprowadzane przez niezależne organy krajowe oraz w ramach wzajemnej oceny, a informacje na temat ich wyniku oraz wszelkich późniejszych środków, które zostaną podjęte, powinny być udostępniane Komisji i na forum ENSREG oraz podawane do wiadomości publicznej”³⁸. Rada Europejska do końca 2011 r. miała ocenić wstępne wyniki ocen prowadzonych na podstawie raportu Komisji Europejskiej z państw członkowskich.

Szczególnego charakteru nabrała także kwestia zapewnienia bezpieczeństwa dla elektrowni pozostających w sąsiedztwie UE oraz na świecie, bowiem katastrofa

³⁵ Katastrofy kaskadowe – zdarzenia ekstremalne, w których skutki kaskadowe nasilają się w czasie i powodują niespodziewane, silne zdarzenia wtórne. Te ostatnie są co najmniej równie poważne, jak zdarzenie pierwotne i wywierają silny wpływ na całkowity okres utrzymywania się skutków katastrofy. Wtórne i niespodziewane zdarzenia mogą mieć poważniejszy wymiar wskutek naruszenia konstrukcji i funkcji społecznych, które są od nich zależne (np. obiekty infrastruktury krytycznej) lub poprzez nieadekwatność zastosowanych strategii łagodzących (takich jak procedury ewakuacji, planowanie zagospodarowania przestrzennego i strategii zarządzania kryzysowego). Katastrofy kaskadowe uwiadcniają nierozwiązane problemy podatności w społeczeństwach. W katastrofach kaskadowych można wyróżnić jedno lub więcej zdarzeń wtórnych, które odróżniają się od pierwotnego źródła katastrofy; Źródło: G. Pescaroli, D. Alexander, *A definition of cascading disasters and cascading effects: Going beyond the “toppling dominos” metaphor*, „Planet@Risk” 2015, 3(1), s. 58-67 (tłum. własne).

³⁶ COM(2011) 784 final z dnia 24 listopada 2011.

³⁷ Tamże.

³⁸ COM(2012) 571 final z dnia 4 października 2012.

w Japonii osiągnęła globalne skutki – dryfujące szczątki po tsunami, obawa skażenia wody pitnej, kwestia bezpieczeństwa żywności dostarczanej z UE, kwestia skażenia obywateli UE wracających z Japonii do Europy. „Priorytetowe znaczenie zapewnienia bezpieczeństwa elektrowni jądrowych nie może oczywiście obowiązywać wyłącznie w obrębie naszych granic; UE wystąpi o przeprowadzenie podobnych „testów warunków skrajnych” w państwach sąsiednich i na całym świecie – w odniesieniu zarówno do istniejących, jak i planowanych elektrowni; w tym względzie należy w pełni zaangażować odpowiednie organizacje międzynarodowe; najwyższe standardy bezpieczeństwa jądrowego należy wdrażać i ustawicznie podnosić w UE i promować w wymiarze międzynarodowym”³⁹.

Rada Europejska miała natomiast dokonać oceny wyników tej analizy. Plan działania Europejskiej Grupy Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego ENSREG zatwierdzono 1 sierpnia 2012 r. 4 października 2012 r. Komisja wydała komunikat (COM(2012) 0571)⁴⁰ dotyczący kompleksowych ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych. „Wypadek w elektrowni Fukushima w Japonii w następstwie trzęsienia ziemi i tsunami w marcu 2011 r. uwytkłił wyzwania związane z zapewnianiem bezpieczeństwa jądrowego. Wydarzenie to pokazało, że reaktory jądrowe muszą być chronione nawet przed wypadkami, które zostały ocenione jako wysoce nieprawdopodobne. Wydarzenia w Fukushima uwidoczniły dobrze znane i powracające problemy: wady konstrukcyjne, niedoskonałe systemy rezerwowe, błędy ludzkie, nieodpowiednie plany awaryjne oraz słabą komunikację. UE musi wyciągnąć wnioski z tego, co stało się w Fukushima, aby bardziej ograniczyć ryzyko incydentów jądrowych w Europie”⁴¹. Zadania sprawdzające określono jako celowane testy wytrzymałościowe marginesów bezpieczeństwa elektrowni jądrowych w świetle wniosków wyciągniętych z wydarzeń w Fukushima, związanych z ekstremalnymi zjawiskami naturalnymi, stanowiącymi zagrożenie dla funkcji bezpieczeństwa elektrowni (np. powodziami, trzęsieniem ziemi, ekstremalnymi zjawiskami atmosferycznymi).

Metodologia zastosowana w testach była wspólna i wykorzystywana dwutorowo. Testy pokazały, że:

- „w czterech reaktorach (znajdujących się w dwóch różnych krajach) operatorzy mają niespełna godzinę na przywrócenie funkcji bezpieczeństwa w razie utraty całego zasilania elektrycznego lub ostatecznego ujścia ciepła;
- w 10 reaktorach nie zainstalowano przyrządów do pomiaru aktywności sejsmicznej wykorzystywanych na miejscu;

³⁹ Konkluzje Rady Europy (24–25 marca 2011), EUCO 10/1., s. 11.

⁴⁰ Komisja Europejska, komunikat Komisji do Rady i Parlamentu Europejskiego dotyczący kompleksowych ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych, COM(2012) 571 final z dnia 4 października 2012.

⁴¹ Tamże.

- cztery kraje stosują obecnie dodatkowe systemy bezpieczeństwa w pełni niezależne od zwykłych systemów bezpieczeństwa, zlokalizowane w obszarach dobrze chronionych przed zdarzeniami zewnętrznymi, np. systemy bezpieczeństwa zabezpieczone przed zagrożeniami zewnętrznymi (ang. *bunkered systems*) lub wzmocniony rdzeń systemów bezpieczeństwa (ang. *hardened core systems*), a piąty kraj bierze tę opcję pod uwagę;
- sprzęt przenośny, zwłaszcza generatory dieslowe, potrzebne w razie całkowitej utraty zasilania, zdarzeń zewnętrznych lub poważnych awarii, są już dostępne w siedmiu krajach i będą instalowane w większości innych⁴².

Kluczowe wyniki testów przedstawiały się następująco:

1. **„Brakowało spójności oceny zewnętrznych zagrożeń dla bezpieczeństwa obiektów i zarządzania tymi zagrożeniami.** Na przykład wytyczne Międzynarodowej Agencji Energii Atomowej dotyczące obciążeń sejsmicznych lub wytyczne dotyczące powodzi nie były wdrażane przez wszystkie państwa członkowskie.
2. **Zakres i dogłębność probabilistycznych ocen bezpieczeństwa (PSA),** stosowanych do określania bezpieczeństwa reaktorów jądrowych, bardzo się różniły i w niektórych państwach członkowskich powinny zostać niezwłocznie dostosowane do przyjętych norm międzynarodowych.
3. **Wytyczne dotyczące zarządzania poważnymi awariami** (ang. Severe Accident Management Guidelines, SAMG), obejmujące wszystkie rodzaje sytuacji, powinny być dostępne we wszystkich elektrowniach jądrowych. Testy wytrzymałościowe wykazały, że w kilku państwach członkowskich istnieje potrzeba aktualizacji i jak najszybszego pełnego wdrożenia SAMG.
4. **Konieczna jest poprawa kultury bezpieczeństwa**⁴³. Istnieją luki w **zapewnianiu kompleksowego i przejrzystego systemu identyfikacji oraz zarządzania kluczowymi kwestiami bezpieczeństwa.** Jaskrawy przykład Fukushima pokazuje, że zagrożenie ze strony tsunami było zaniżone, głównie w wyniku działania czynników ludzkich, systemowych i organizacyjnych⁴⁴.

⁴² Tamże.

⁴³ Por. kultura bezpieczeństwa – wzór podstawowych założeń, wartości, norm, reguł, symboli i przekonań wpływających na sposób postrzegania wyzwań, szans i (lub) zagrożeń, a także sposób odczuwania bezpieczeństwa i myślenia o nim oraz związany z tym sposób zachowania i działania (współdziałania) podmiotów, w różny sposób przez te podmioty wyuczonych i wyartykułowanych w procesach szeroko rozumianej edukacji, w tym również w naturalnych procesach wewnętrznej integracji i zewnętrznej adaptacji oraz w innych procesach organizacyjnych, a także w procesie umacniania szeroko (nie tylko militarnie) rozumianej obronności, służących w miarę harmonijnemu rozwojowi tych podmiotów i osiągnięciu przez nie najszerzej rozumianego bezpieczeństwa, z pożytkiem dla siebie, ale i otoczenia. Źródło: M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, wyd. AP, Siedlce 2011, s. 210.

⁴⁴ Komisja Europejska, komunikat Komisji do Rady i Parlamentu Europejskiego dotyczący kompleksowych ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych, COM(2012) 571 final z 4 października 2012.

W 2012 r. Parlament przyjął do wiadomości komunikat Komisji w sprawie testów wytrzymałościowych i ich wyników po wypadku w Fukushima. Parlament Europejski 14 marca 2013 r. przyjął rezolucję Parlamentu Europejskiego w sprawie ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych (2012/2830(RSP)). Z zadowoleniem przyjął także wysiłki podjęte przez Komisję i Europejską Grupę Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego (ENSREG) na rzecz przeprowadzenia testów wytrzymałościowych dla 145 reaktorów w UE i 20 reaktorów poza UE⁴⁵. „Wezwał Komisję i państwa członkowskie do zachęcania krajów spoza UE, które mają elektrownie jądrowe, w szczególności krajów sąsiadujących z UE, do przeprowadzenia testów wytrzymałościowych i do podzielenia się ich wynikami. Podkreślił także znaczenie międzynarodowych norm bezpieczeństwa jądrowego i ochrony jądrowej oraz ich właściwego wdrażania. Zauważając, że katastrofy naturalne, takie jak trzęsienia ziemi i tsunami, mogą zagrozić bezpieczeństwu istniejących lub budowanych elektrowni jądrowych na terenie Unii i w krajach sąsiadujących, w których występuje wysokie ryzyko trzęsień ziemi i tsunami, jak na przykład w Akkuyu w Turcji, dodatkowo zwrócił uwagę, że należy podjąć wszelkie stosowne działania na szczeblu Unii i państw członkowskich, aby nie dopuścić do składowania odpadów promieniotwórczych w obszarach wysokiego ryzyka”⁴⁶.

„Głównym czynnikiem gwarantującym wysoką jakość życia w społeczeństwie europejskim oraz ochronę naszej infrastruktury krytycznej stało się bezpieczeństwo, polegające na zapobieganiu wspólnym zagrożeniom i ich usuwaniu”⁴⁷.

5.4. Zarządzanie ryzykiem w dziedzinie zdrowia Unii Europejskiej

UE prowadzi działania mające na celu zapewnienie bezpieczeństwa zdrowotnego obywateli UE. Ocena możliwości wystąpienia zagrożenia prowadzona jest w ramach prac DG SANKO oraz wielu agencji UE.

Traktat o funkcjonowaniu Unii Europejskiej⁴⁸ przyznaje jej kompetencje do prowadzenia działań mających na celu wspieranie, koordynowanie lub uzupełnianie działań państw członkowskich w obszarze ochrony i poprawy zdrowia ludzkiego. Traktat z Lizbony w art. 168 odnosi się do zdrowia publicznego. Co ważne, ustosunkowuje się także do dowodów naukowych, danych, jako podstawy oraz uzasadnienia dla prowadzonej polityki czy wprowadzanych środków. Art. 168 określa dokładniej „działanie Unii, które uzupełnia polityki krajowe, nakierowane jest na poprawę zdrowia publicznego, zapobieganie chorobom i dolegliwościom

⁴⁵ Rezolucja Parlamentu Europejskiego w sprawie ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych (2012/2830(RSP)).

⁴⁶ Tamże.

⁴⁷ Strategia bezpieczeństwa wewnętrznego UE, s. 13.

⁴⁸ Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 83/123 z 30.03.2010).

ludzkim oraz usuwanie źródeł zagrożeń dla zdrowia fizycznego i psychicznego. Działanie to obejmuje zwalczanie epidemii, poprzez wspieranie badań nad ich przyczynami, sposobami ich rozprzestrzeniania się oraz zapobiegania im, jak również informacji i edukacji zdrowotnej, a także monitorowanie poważnych transgranicznych zagrożeń dla zdrowia, wczesne ostrzeganie w przypadku takich zagrożeń i ich zwalczanie⁴⁹. Co więcej, Parlament Europejski i Rada (stanowiąc zgodnie ze zwykłą procedurą ustawodawczą i po konsultacji z Komitetem Ekonomiczno-Społecznym i Komitetem Regionów) mogą również ustanowić środki zachęcające, skłaniające do podejmowania działań w obszarze ochrony i poprawy zdrowia ludzkiego, w szczególności do zwalczania epidemii transgranicznych oraz środki dotyczące monitorowania poważnych transgranicznych zagrożeń dla zdrowia, wczesnego ostrzegania w przypadku takich zagrożeń, a także ich zwalczania, z wyłączeniem jakiegokolwiek harmonizacji przepisów ustawowych i wykonawczych państw członkowskich⁴⁹.

W zakresie ryzyk związanych ze zdrowiem i bezpieczeństwem żywności UE kieruje się zasadami, które oparte są na następujących dokumentach referencyjnych:

- *EU Commission: Communication on Consumer Health and Food Safety* (1997);
- *EU Commission: Communication on Collection and Use of Expertise* (2002),
- *EU Food Law* (2002);
- *EU Commission Decision establishing Scientific Committees in the field of Consumer Safety, Public health and the Environment* (2004, revised 2008);
- Decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE (2013).

W ramach prac KE (DG SANKO) oraz OECD odbywają się konferencje *The EU Risk Analysis Approach and the Perspectives for a Global Risk Assessment Dialogue*, których celem jest dostarczenie rzetelnej informacji na temat zasad, priorytetów oraz struktury zarządzania ryzykiem na poziomie UE.

Koncepcja oceny ryzyka i zarządzania ryzykiem w dziedzinie zdrowia w UE obejmuje następujące elementy⁵⁰:

- ocenę ryzyka (ang. *risk assessment*);
- zarządzanie ryzykiem (ang. *risk management*);
- przekazywanie informacji o ryzyku (ang. *risk communication*).

W ramach niniejszej analizy skupiono się na ocenie ryzyka. W reagowaniu na transgraniczne kryzysy zdrowotne ocena ryzyka jest pierwszym działaniem. Inicjatywa UE dot. bezpieczeństwa zdrowotnego ma na celu szybkie uruchomienie

⁴⁹ Tamże, art. 168.

⁵⁰ Por. Komisja Europejska, wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 final z dnia 08 grudnia 2011 oraz decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE (Dz. Urz. UE L 293 z 05.11.2013, s. 1–15).

mechanizmów jego oceny. W ramach tej inicjatywy uaktywniany jest proces tworzenia ekspertyz przez agencje unijne związane ze zdrowiem. Mają one zapewnić UE najlepsze wsparcie eksperckie i naukowe w procesie zarządzania ryzykiem. Komisję wspierają w tym procesie następujące agencje unijne i międzynarodowe:

1. Europejskie Centrum ds. Zapobiegania i Kontroli Chorób – European Centre for Diseases Prevention and Control (ECDC),
2. Europejski Urząd ds. Bezpieczeństwa Żywności – European Food Safety Authority (EFSA),
3. Światowa Organizacja Zdrowia – World Health Organisation (WHO).

Propozycja wniosku – decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia z dnia 8 grudnia 2011 r.⁵¹ była odpowiedzią UE na potrzebę działań w obszarze bezpieczeństwa zdrowotnego. Unia sformułowała wnioski z doświadczeń po kryzysach zdrowotnych, które wydarzyły się w latach: 2009 (pandemia H1N1), 2010 (chmura pyłu wulkanicznego nad terytorium UE po wybuchu wulkanu Eyjafjallajökull w południowej Islandii) oraz 2011 (skażenie żywności bakterią *E. coli*), co pozwoliło jej lepiej zarządzać ryzykiem w przypadku wirusa ebola w latach 2014–2015. Już w 2013 r. Parlament Europejski i Rada przyjęły decyzję nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylającą decyzję nr 2119/98/WE⁵². Z powyższej decyzji wynika, że „poważne transgraniczne zagrożenie zdrowia oznacza zagrażające życiu lub w innym stopniu poważne ryzyko dla zdrowia o pochodzeniu biologicznym, chemicznym, środowiskowym lub nieznanym, które rozprzestrzenia się lub wiąże ze znacznym ryzykiem rozprzestrzenienia się ponad granicami krajowymi państw członkowskich i które może wymagać koordynacji na szczeblu unijnym, aby zagwarantować wysoki poziom ochrony zdrowia ludzkiego. Decyzja przyznaje, że państwa członkowskie odpowiadają za zarządzanie na szczeblu krajowym kryzysami w dziedzinie zdrowia publicznego. Jednak środki podejmowane indywidualnie przez państwa członkowskie mogą zaszkodzić interesom innych państw członkowskich, jeśli będą niespójne ze sobą lub oparte na rozbieżnych ocenach ryzyka. Cel koordynacji reagowania na poziomie unijnym powinien zatem dążyć do zagwarantowania, między innymi, że środki podejmowane na poziomie krajowym będą proporcjonalne i ograniczone do ryzyka dla zdrowia publicznego związanego z poważnymi transgranicznymi zagrożeniami zdrowia”. Zapowiedzią późniejszej współpracy przy wybuchu wirusa eboli były niniejsze zapisy: „należy propagować współpracę z państwami trzecimi i organizacjami międzynarodowymi w dziedzinie zdrowia publicznego; jest ona szczególnie ważna dla zagwarantowania wymiany ze WHO informacji na temat środków podjętych

⁵¹ Komisja Europejska, wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 final z dnia 08 grudnia 2011.

⁵² Decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE (Dz. Urz. UE L 293/1 z 05.11.2013).

na podstawie niniejszej dyrektywy. W szczególności w interesie Unii może być zwłaszcza zawieranie umów o współpracy międzynarodowej z państwami trzecimi lub organizacjami międzynarodowymi, w tym WHO, aby sprzyjać wymianie odpowiednich informacji z systemów monitorowania i ostrzegania o poważnych transgranicznych zagrożeniach zdrowia”.

Wzmocnienie roli UE w reagowaniu na kryzysy zdrowotne (2009–2011) było więc sumą doświadczeń, w tym pandemii H1N1, reagowania na chmurę pyłu wulkanicznego nad terytorium UE po wybuchu wulkanu Eyjafjallajökull oraz skażenia żywności bakterią *E. coli*, a decyzja z 2013 r. zawierała propozycje spójnych ram reagowania ze strony UE w razie poważnej sytuacji kryzysowej dotyczącej zdrowia publicznego.

Wejście w życie Traktatu z Lizbony wzmocniło podstawy prawne UE do przeciwdziałania poważnym transgranicznym zagrożeniom zdrowia na szczeblu unijnym. Obecnie UE może podejmować działania w tym obszarze, z wyłączeniem jakiegokolwiek harmonizacji przepisów ustawowych i wykonawczych państw członkowskich. Aby usprawnić przekazywanie między państwami członkowskimi istotnych informacji i danych do oceny ryzyka innego niż choroba oraz monitorowania pojawiających się zagrożeń, ustanowiony został system wczesnego ostrzegania i reagowania – sieć doraźna na potrzeby takiej sytuacji. W decyzji rozszerzono zakres istniejącego systemu wczesnego ostrzegania i reagowania tak, aby obejmował on wszystkie poważne zagrożenia zdrowia, a nie wyłącznie choroby zakaźne, jak to miało miejsce wcześniej. Wprowadzono koordynację opracowywania krajowych i europejskich ocen ryzyka dla zdrowia publicznego w sytuacji kryzysowej w przypadku zagrożeń biologicznych, chemicznych, środowiskowych oraz tych nieznanego pochodzenia⁵³.

Wniosek Komisji bazował na współpracy istniejących struktur, jednak proponował rozszerzenie dokonywanej oceny ryzyka oraz koordynację środków tak, aby poza chorobami zakaźnymi obejmowały one wszystkie zagrożenia zdrowotne wywołane czynnikami biologicznymi, chemicznymi lub środowiskowymi. Na przykład istniejącą sieć nadzoru epidemiologicznego nad chorobami zakaźnymi, do której włączone są KE, Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) oraz organy krajowe, we wniosku rozszerzono o inne poważne transgraniczne zagrożenia dla zdrowia: „w celu przekazywania istotnych informacji i danych do oceny ryzyka oraz monitorowania pojawiających się zagrożeń ustanowiona zostanie sieć doraźna na potrzeby sytuacji, w których państwo członkowskie powiadamia o poważnym zagrożeniu innym niż choroba zakaźna”⁵⁴. We wniosku wprowadzono koordynację opracowywania krajowych i europejskich ocen ryzyka dla zdrowia publicznego w sytuacji kryzysowej w przypadku zagrożeń biologicznych, chemicznych, środowiskowych oraz nieznanego pochodzenia.

⁵³ Komisja Europejska, wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 final z dnia 8 grudnia 2011, s. 3.

⁵⁴ Tamże.

Uzasadnienie UE bazuje na wiedzy o lukach w systemie bezpieczeństwa zdrowotnego. Unia oceniła sytuację i stwierdziła, że „istnieją krajowe oceny ryzyka dla zdrowia, ale mogą nie być kompleksowe i spójne, jeśli rozważać je z perspektywy UE, i nie istnieje obecnie mechanizm umożliwiający skoordynowane podejście na szczeblu UE. Brak oceny ryzyka dla zdrowia publicznego na poziomie UE prowadzi do rozbieżności pomiędzy państwami członkowskimi w ocenie ryzyka związanego z danym zagrożeniem, dokonywania oddzielnych ocen ryzyka przez poszczególne państwa i stosowania niespójnych środków na szczeblu UE. Aby ocena ryzyka dla zdrowia publicznego na poziomie unijnym powodowanego przez poważne transgraniczne zagrożenia była spójna, a także kompleksowa z perspektywy zdrowia publicznego, należy w skoordynowany sposób zgromadzić dostępne zasoby wiedzy specjalistycznej poprzez odpowiednie kanały lub struktury, zależnie od rodzaju zagrożenia. Ocena ryzyka powinna być oparta na solidnych dowodach naukowych oraz niezależnej wiedzy specjalistycznej i przekazywana przez agencje unijne zgodnie z ich misją lub przez grupy ekspertów ustanowione przez Komisję”⁵⁵.

Ponadto wcześniejsze rozporządzenie (WE) nr 851/2004 Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. ustanawiało Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC). Ma ono kompetencje nadzoru i oceny ryzyka zagrożeń dla zdrowia ludzkiego ze strony chorób zakaźnych i chorób nieznanego pochodzenia. W zakresie zapobiegania transgranicznym zagrożeniom zdrowia Komisja Europejska współpracuje z rządami państw członkowskich. Swoistą rolę w zarządzaniu ryzykiem odgrywa Komitet Bezpieczeństwa Zdrowia⁵⁶, którego zadaniem jest skoordynowanie środków w zakresie bezpieczeństwa zdrowotnego podejmowanych w UE. Komitet powołano w 2011 r. po atakach terrorystycznych. Komitet ds. Bezpieczeństwa koordynuje ocenę ryzyka dla zdrowia publicznego i zarządzanie w przypadku poważnych transgranicznych zagrożeń zdrowia⁵⁷. Monitorowanie poważnych transgranicznych zagrożeń zdrowia innych niż choroby zakaźne opiera się jednak na systemach monitorowania państw członkowskich, a dostępne informacje są wymieniane za pośrednictwem EWRS.

Jak stwierdza się w raporcie Europejskiego Trybunału Obrachunkowego⁵⁸: „wybuch epidemii eboli w Afryce Zachodniej stanowił nietypową klęskę żywnościową z punktu widzenia Unijnego Mechanizmu Ochrony Ludności. Komisja i agencje UE zareagowały szybko na pierwsze doniesienia o eboli: Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) rozesłało szybką ocenę ryzyka w marcu 2014 r.; Europejskie Mobilne Laboratorium zostało zainstalowane w regionie w kwietniu; między kwietniem a sierpniem 2014 r. epidemia stanowiła kilkakrotnie

⁵⁵ Tamże.

⁵⁶ Komitet ustanowiony podstawie konkluzji prezydencji z dnia 15 listopada 2001 r. w sprawie bioterroryzmu.

⁵⁷ Tamże.

⁵⁸ Europejski Trybunał Obrachunkowy, Sprawozdanie specjalne nr 33/2016, Unijny Mechanizm Ochrony Ludności – koordynacja reagowania na klęski żywiołowe poza terytorium UE była zasadniczo skuteczna.

przedmiot dyskusji na forum Komitetu ds. Bezpieczeństwa Zdrowia, a szereg głównych podmiotów partnerskich DG ECHO szybko zmobilizowało środki finansowe. ECDC wniosło istotny wkład w działania podjęte przez UE w związku z wybuchem epidemii eboli, dokonując tzw. szybkich ocen ryzyka oraz koordynując oddelegowanie ekspertów ds. epidemiologii z ECDC i państw członkowskich do regionu dotkniętego tą katastrofą⁵⁹. Jednak w dniu 8 sierpnia 2014 r. WHO ogłosiło stan zagrożenia zdrowia publicznego o zasięgu międzynarodowym. KE aktywowała w dniu 14 sierpnia 2014 r. Unijny Mechanizm Ochrony Ludności na prośbę WHO. Wniosek obejmował m.in. zespoły medyczne (*Foreign Medical Teams FMTs*), w pełni wyposażone centra do opieki zarażonych wirusem ebola, ambulansy, lekarzy oraz materiały medyczne. W dniu 30 sierpnia 2014 r. Rada Europejska wezwała do większej koordynacji i przyjęcia kompleksowych ram reagowania na zagrożenie ebolą. Dopiero w październiku 2014 r. powołano do życia grupę zadaniową ds. boli, a pod koniec października Rada Europejska mianowała komisarza ds. pomocy humanitarnej i zarządzania kryzysowego koordynatorem UE ds. eboli. Jego zadaniem było zapewnienie koordynacji działań dot. tego kryzysu na szczeblu politycznym. Na zwieńczenie prac UE w zakresie zwalczania wirusa eboli w marcu 2015 r. w Brukseli została zorganizowana konferencja darczyńców. Celem było podsumowanie prac nad zwalczaniem wirusa, określenie dalszych kroków w jego eliminacji oraz przedyskutowanie procesu odnowy w państwach dotkniętych jego skutkami. W dniach 12–14 października 2015 r. w Luksemburgu zorganizowano kolejną konferencję *Lessons learned for public health from the Ebola outbreak in West Africa – how to improve preparedness and response in the EU for future outbreaks*. Reagowanie na kryzys wywołany wirusem ebola pozwoliło UE wypracować nowe techniki zarządzania kryzysowego. W opinii komisarza ds. zdrowia i bezpieczeństwa żywności, kryzys wywołany wirusem ebola był testem dla systemu przygotowania UE na sytuacje kryzysowe, które określała decyzja PE i Rady 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia.

Obecny program UE w dziedzinie zdrowia zawiera wiele działań związanych z ostrzeganiem, oceną ryzyka i monitorowaniem niektórych zagrożeń zdrowia. Od 2014 r. działa program „Zdrowie na rzecz wzrostu gospodarczego” na lata 2014–2020, w którym w celu szczegółowym nr 4, mówiącym o ochronie obywateli przed transgranicznymi zagrożeniami dla zdrowia, Komisja przyznała, że w jej opinii należy zwiększyć poziom gotowości i koordynacji w sytuacjach kryzysowych związanych z transgranicznymi zagrożeniami dla zdrowia. Przyjęte w 2014 r. rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 282/2014 z dnia 11 marca 2014 r. w sprawie ustanowienia 3. Programu działań Unii w dziedzinie zdrowia (2014–2020)⁵⁹ wskazało, że „program powinien wspierać skoordynowane środki

⁵⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 282/2014 z dnia 11 marca 2014 r. w sprawie ustanowienia 3. Programu działań Unii w dziedzinie zdrowia (2014–2020) oraz uchylające decyzję nr 1350/2007/WE (1) (Dz. Urz. UE L 86/3, t. 57 z 21.03.2014, s. 1).

publiczne przeznaczone na zdrowie na szczeblu Unii, aby odnieść się do różnych aspektów transgranicznych zagrożeń zdrowia, bazując na planowaniu i reagowaniu, rzetelnej i wiarygodnej ocenie ryzyka, a także solidnym schemacie zarządzania ryzykiem i sytuacjami kryzysowymi⁶⁰.

5.5. Zarządzanie ryzykiem na wypadek kryzysów związanych z żywnością

Rozporządzenie (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r.⁶¹ ustanowiło ogólne zasady i wymagania prawa żywnościowego, powołało Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanowiło procedury w zakresie bezpieczeństwa żywności⁶². Jednym z obszarów objętych rozporządzeniem jest analiza ryzyka, w ramach której przyjęto następującą terminologię:

- „ryzyko oznacza niebezpieczeństwo zaistnienia negatywnych skutków dla zdrowia oraz dotkliwość takich skutków w następstwie zagrożenia;
- analiza ryzyka oznacza proces składający się z trzech powiązanych elementów: oceny ryzyka, zarządzania ryzykiem i informowania o ryzyku;
- ocena ryzyka oznacza proces wsparty naukowo, składający się z czterech etapów: identyfikacji zagrożenia, charakterystyki niebezpieczeństwa, oceny ekspozycji i charakterystyki ryzyka;
- zarządzanie ryzykiem oznacza proces, różniący się od oceny ryzyka, polegający na zbadaniu alternatywy polityki w porozumieniu z zainteresowanymi stronami, wzięciu pod uwagę oceny ryzyka i innych prawnie uzasadnionych czynników, i w razie potrzeby – na wybraniu stosownych sposobów zapobiegania i kontroli;
- informowanie o ryzyku oznacza interaktywną wymianę informacji i opinii podczas procesu analizy ryzyka, dotycząca zagrożeń i ryzyka, czynników związanych z ryzykiem i postrzeganiem ryzyka, między oceniającymi ryzyko, zarządzającymi ryzykiem, konsumentami, przedsiębiorstwami żywnościowymi i paszowymi, środowiskiem naukowym i innymi zainteresowanymi stronami, z uwzględnieniem wyjaśnienia wniosków z oceny ryzyka i powodów decyzji w zakresie zarządzania ryzykiem;
- zagrożenie oznacza czynnik biologiczny, chemiczny lub fizyczny w żywności lub paszy, bądź stan żywności lub paszy, mogący powodować negatywne skutki dla zdrowia⁶³.

⁶⁰ Tamże.

⁶¹ Dz. Urz. L 31 z 01.02.2002.

⁶² Tamże, s. 1.

⁶³ Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (Dz. Urz. UE L 31 z 01.02.2002, s. 1–24).

W przypadku, gdy Komisja zidentyfikuje zaistnienie poważnego bezpośredniego lub pośredniego ryzyka dla zdrowia ludzkiego, pochodzącego z żywności i pasz, a ryzyku temu nie można zapobiec, wyeliminować je lub zredukować poprzez obowiązujące przepisy, lub w przypadku, gdy ryzyko nie może być adekwatnie uregulowane wyłącznie w drodze stosowania art. 53 i 54⁶⁴, to Komisja Europejska powiadamia niezwłocznie państwa członkowskie i Urząd ds. Bezpieczeństwa Żywności. Powołany Europejski Urząd ds. Bezpieczeństwa Żywności jest niezależnym naukowym źródłem porad, informacji i informowania o ryzyku w celu polepszenia zaufania konsumenta. Aby promować spójność między funkcjami oceny ryzyka, zarządzaniem ryzykiem i informowaniem o ryzyku, wzmocnione powinno być powiązanie między oceniającymi ryzyko i zarządzającymi nim.

System Wczesnego Ostrzegania o Niebezpiecznych Produktach Spożywczych i Środkach Żywnienia Zwierząt (*Rapid Alert System for Food and Feed – RASFF*) powstał w 1979 r. Jego celem jest wymiana informacji pomiędzy kompetentnymi instytucjami zajmującymi się bezpieczeństwem żywności. W sytuacjach potencjalnie kryzysowych i kryzysowych pozwala komunikować się w czasie rzeczywistym pomiędzy DG SANKO a państwami członkowskimi. W 2002 r. istniejący System szybkiego alarmowania utworzony w ramach dyrektywy Rady 92/59/EWG z dnia 29 czerwca 1992 r. w sprawie ogólnego bezpieczeństwa produktów rozszerzono o pasze. Natomiast w wyniku kryzysów w 2011 r. (zakażenie bakterią e-coli, skutki awarii w elektrowni Fukushima) Komisja Europejska usprawniła system RASFF poprzez uruchomienie iRASFF – platformy powiadamiania online, która pozwala skuteczniej przygotować się do sytuacji kryzysowej i nią zarządzać⁶⁵.

Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawia ogólne zasady i wymagania prawa żywnościowego, powołuje Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawia procedury w zakresie bezpieczeństwa żywności. Zgodnie z art. 17 tego rozporządzenia „w przypadku, gdy prawo żywnościowe ma na celu redukcję, wyeliminowanie lub uniknięcie ryzyka utraty zdrowia, trzy powiązane ze sobą składniki analizy zagrożeń – ocena zagrożeń, zarządzanie zagrożeniami i komunikacja zagrożeń

⁶⁴ Art. 53 mówi o środkach nadzwyczajnych dla żywności i pasz pochodzących ze Wspólnoty lub przywożonych z państwa trzeciego, natomiast art. 54 o innych środkach nadzwyczajnych podejmowanych przez państwa członkowskie. Rozporządzenie (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 (Dz. Urz. UE L 31 z 01.02.2002, s. 1–24).

⁶⁵ Istotna statystyka: W 2011 r. w ramach RASFF złożono 9 157 powiadomień dotyczących niezgodności z unijnymi przepisami dotyczącymi żywności, z czego 617 dotyczyło poważnych zagrożeń. Większość powiadomień stanowiła działania następcze (5 345), lecz zarejestrowano także 3 812 nowych powiadomień. (...) Spośród 3 812 nowych powiadomień: 3 139 dotyczyło żywności, 361 – pasz, zaś 312 – materiałów przeznaczonych do kontaktu z żywnością. Niektóre z najczęściej zgłaszanych problemów odnosiły się do aflatoksyn w paszach, suszonych owoców i orzechów oraz migracji substancji chemicznych z wyrobów kuchennych pochodzących z Chin – informacja prasowa służb Komisji Europejskiej 12/806.

– zapewniają systematyczną metodologię dla określenia efektywnych, współmierzalnych i skierowanych we właściwym kierunku środków lub innych działań, mających na celu ochronę zdrowia”⁶⁶. Jednak „uważa się, że naukowa ocena ryzyka nie może, w pewnych przypadkach, samodzielnie dostarczyć wszystkich informacji, na których należy opierać decyzję w zakresie zarządzania ryzykiem oraz, że inne czynniki związane z rozpatrywaną sprawą powinny być brane pod uwagę w sposób prawnie uzasadniony, łącznie z czynnikami społecznymi, gospodarczymi, związanymi z tradycją, etycznymi i środowiskowymi oraz możliwością ich kontroli”⁶⁷.

5.6. Zarządzanie ryzykiem nielegalnej imigracji – FRONTEX

Analiza ryzyka jest podstawą działania agencji FRONTEX. Analizuje ona dane dotyczące bezpieczeństwa, sytuacji politycznej, ekonomicznej, socjologicznej, rozwoju technologii, prawa oraz czynników środowiskowych, które to wszystkie mogą mieć wpływ na bezpieczeństwo na granicach zewnętrznych UE. FRONTEX otrzymuje dane z państw członkowskich, prowadzi monitoring mediów, korzysta także z innych źródeł, w tym spoza UE. Celem tych wszystkich działań jest uzyskanie przez UE jak najbardziej rzeczywistej i rzetelnej oceny sytuacji na granicach zewnętrznych UE.

Agencja FRONTEX opracowała własny zintegrowany model analizy ryzyka⁶⁸, tzw. CIRAM (*Common Integrated Risk Analysis Model*). Jego idea powstała podczas spotkania Rady UE w Sewilli w 2002 r. Do opracowania wspólnego modelu oceny ryzyka, pozwalającego stworzyć wspólny zintegrowany model analizy ryzyka, który służyłby zwalczaniu nielegalnej imigracji, wzywał szczególnie pkt 32. konkluzji Rady. Celem było prowadzenie systematycznej oceny sytuacji w zakresie kontroli na granicy. Propozycja ta została uzgodniona w Elsinore 22 lipca 2002 r. z Komitetem SCIFA+ (Strategic Committee on Immigration, Frontiers and Asylum), z udziałem szefów służb zajmujących się kontrolą graniczną.

Wspólny zintegrowany model analizy ryzyka (CIRAM) powstał w 2002 r. w ramach prac grupy roboczej Sekretariatu Generalnego Rady Unii Europejskiej i przyczynił się do powstania Helsinki Risk Analysis Centre, któremu powierzono połączenie wspólnych ocen ryzyka na szczeblu Unii Europejskiej. CIRAM był opracowywany pod auspicjami Finlandii, prace w systemie rozpoczęto 28 stycznia 2003 r.⁶⁹

⁶⁶ Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (Dz. Urz. UE L 31 z 01.02.2002).

⁶⁷ Tamże, art. 19.

⁶⁸ Agencja FRONTEX w ramach CIRAM umożliwia ocenę względnego ryzyka stwarzanego przez różne zagrożenia, dokonując ich identyfikacji i analizy.

⁶⁹ Za: S. Carrera, *The EU Border Management Strategy FRONTEX and the challenges of irregular immigration in the Canary Islands*, CEPS Working Document, nr 261, 2007.

CIRAM stwarza agencji FRONTEX podstawę do koordynacji działań dla wspólnie prowadzonych operacji na granicach zewnętrznych UE. Ocena sytuacji jest kluczowa dla podjęcia reakcji przez FRONTEX. CIRAM jest stosowany przez agencję, jak i inne państwa członkowskie. W zależności od poziomu, w systemie współpracują służby graniczne, celne w ramach systemu Schengen, jak i krajowe instytucje współpracujące z krajami sąsiadującymi z UE. Analiza ryzyka jest stosowana nie tylko do przygotowania operacji FRONTEX. Jest także wykorzystywana jako system wspierania decyzji, wyznaczania priorytetów pracy oraz rozwijania polityki prac agencji. FRONTEX w ramach analizy ryzyka prowadzi analizę strategiczną i analizę operacyjną. Analiza strategiczna prowadzona jest na podstawie informacji z różnych źródeł z państw członkowskich i spoza UE, agencji UE, organizacji międzynarodowych, mediów. Na ich podstawie FRONTEX opracowuje obraz sytuacji, próbuje przeanalizować jej rozwój, trendy nielegalnej migracji czy przestępczości zorganizowanej, w tym handlu ludźmi. W razie konieczności podjęcia działań przez UE FRONTEX we współpracy z państwami członkowskimi może rozpocząć konkretne działania czy operację. Analiza ryzyka w ramach CIRAM obejmuje trzy wyznaczniki: zagrożenie (ang. *threat*), podatność (ang. *vulnerability*), rozumianą jako zdolność systemu do uniknięcia zagrożenia oraz wpływ (ang. *impact*), który jest określany jako potencjalna konsekwencja zagrożenia.

Analiza zagrożenia jest prowadzona pod kątem jego natężenia (ang. *magnitude*) oraz prawdopodobieństwa (ang. *likelihood*) wystąpienia. Elementami branymi pod uwagę przy analizie zagrożenia są tzw. *modus operandi*, fakty, informacje typu: kto, kiedy, gdzie oraz opis trendów i przypuszczeń (ang. *trends and predictions*) w ujęciu: wzrost, spadek, sytuacja stabilna, dane historyczne. Kolejne elementy obejmują tzw. *push factors*, czyli czynniki wywołujące nielegalną migrację w krajach pochodzenia imigrantów oraz trasy przekraczania granic czy przerzutu pod kątem ich trudności i odległości. Ostatni element to tzw. *access to facilitation*, czyli dostęp do możliwości nielegalnego przekroczenia granicy.

Zależności pomiędzy poszczególnymi elementami badane są ze względu na poziom podatności⁷⁰ (ang. *level of vulnerability*) dla Unii Europejskiej, danego wjazdu do państwa członkowskiego oraz miejsca opuszczenia UE. W tym obszarze bada się np. stopień szczelności granicy ze względu na obszar, infrastrukturę, możliwości oraz ruch. Badane są także działania operacyjne pod kątem personelu, szkolenia, interoperacyjności⁷¹ oraz efektywność zastosowanych środków, jak i tzw. *pull factors* – czynników zachęcających do migracji (np. dostęp do pracy, bezpłatna opieka medyczna, bezpłatny dostęp do szkół).

⁷⁰ Poziom podatności – wartość podatności lub suma podatności.

⁷¹ Interoperacyjność – możliwość współdziałania różnych odrębnych organizacji na rzecz osiągnięcia uzgodnionych i korzystnych dla wszystkich stron celów, przy jednoczesnym dzieleniu się informacjami i wiedzą pomiędzy tymi organizacjami. Źródło: na podstawie art. 2 decyzji nr 922/2009/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie rozwiązań interoperacyjnych dla europejskich administracji publicznych (ISA) (Dz. Urz. UE L 260 z 3.10.2009).

W analizie ryzyka pod kątem wpływu rozpatruje się sytuację na granicy i sytuację wewnętrzną danego kraju członkowskiego (ang. *border and internal security*), zdolności do poradzenia sobie z ruchem osób (ang. *ability to manage legitimate passenger flow at border*) oraz wpływ czynników ludzkich (ang. *humanitarian impact*). Zależności te przedstawia rys. 5.



Rys. 5. Analiza ryzyka w ramach CIRAM

Źródło: FRONTEX, Western Balkans, Annual Risk Analysis 2012.

Najbardziej istotnym wydarzeniem w rozwoju systemu CIRAM 2.0 było przyjęcie w 2011 r. podejścia zarządczego do wykonywanej w agencji FRONTEX analizy ryzyka, które zdefiniowano jako funkcję zagrożenia, podatności oraz wpływu.

W ramach działającego systemu ICONet w Sieci Analizy Ryzyka FRONTEX (FRAN) przyjęto następujące wskaźniki dla dokonywanych przez FRONTEX analiz ryzyka FRAN:

- 1A: wykrycie prób nielegalnego przekroczenia granicy pomiędzy punktami kontroli granicznej,
- 1B: wykrycie prób nielegalnego przekroczenia granicy na punktach kontroli granicznej,
- 2: wykrycie podejrzanych sprawców,
- 3: wykrycie nielegalnego pobytu,
- 4: odmowy wjazdu,
- 5: aplikacje o azyl,
- 6: fałszywe dokumenty (EDF-RAN),
- 7A: decyzje o odesłaniu nielegalnie przebywających obywateli krajów trzecich,
- 7B: skuteczne odesłanie nielegalnie przebywających obywateli krajów trzecich.

Państwa członkowskie co miesiąc uzupełniają dane w załącznikach przygotowanych przez Dział Analizy Ryzyka FRONTEX (ang. *FRONTEX Risk Analysis Unit*). FRONTEX przygotowuje także tzw. *tailored risk analysis* (specjalnie dostosowaną analizę ryzyka, która może dotyczyć np. skutków nielegalnej imigracji z danego kraju, regionu itp.).

Analiza operacyjna FRONTEX prowadzona jest stale także poprzez system raportowania wydarzeń na granicach zewnętrznych UE. Eksperti FRONTEX poprzez wyznaczone centra koordynacyjne w państwach członkowskich przesyłają informacje dotyczące danych operacji i podejmowanych działań. Wszelkie dane tego rodzaju, miejsce, czas, ocena sytuacji na miejscu są wykorzystywane w *Tactical Focused Assessment* (TFA), który ma wspomóc najlepszy sposób realizacji misji *Search And Rescue* (SAR) w zakresie nielegalnych imigrantów.

W ramach analizy ryzyka FRONTEX współpracuje operacyjnie z innymi krajami np. w ramach FRAN z krajami spoza UE, w ramach WB RAN z krajami Bałkanów Zachodnich oraz EB RAN Ekstern Borders Risk Analysis Network z krajami graniczącymi z UE na Wschodzie UE. Te sieci współpracy umożliwiają dokonywanie regularnego przeglądu ryzyka na granicach zewnętrznych UE w cyklu półrocznym oraz rocznym. Z kolei współpracujące agencje spoza UE mogą korzystać z wiedzy oraz metodologii FRONTEX w procesie zarządzania ryzykiem.

W podsumowaniu dot. implementacji zapisów *Strategii bezpieczeństwa wewnętrznego* ujęto zadania Frontex, który w „ścisłej współpracy ze służbami państw członkowskich odpowiedzialnymi za zarządzanie granicami, rozwija sieć analizy ryzyka oraz dostarcza regularne i doraźne analizy ryzyka w odniesieniu do nielegalnej migracji na granicach zewnętrznych UE”⁷². Prowadzenie analiz operacyjnych jest podstawą do podjęcia decyzji i działań na poziomie strategicznym dla samej agencji FRONTEX, Komisji Europejskiej, państw członkowskich, międzynarodowych

⁷² Komisja Europejska, komunikat Komisji do Parlamentu Europejskiego i Rady, Drugie sprawozdanie na temat realizacji strategii bezpieczeństwa wewnętrznego UE, COM(2013) 179 final z dnia 10.04.2013.

instytucji stojących na straży prawa, zajmujących się kwestiami nielegalnych imigrantów czy handlu ludźmi.

W grudniu 2011 r. Komisja przedstawiła wniosek ustawodawczy w sprawie europejskiego systemu nadzoru granic (EUROSUR), który ma zapewnić państwom członkowskim oraz agencjom UE wspólne ramy wymiany informacji w czasie zbliżonym do rzeczywistego oraz ramy współpracy między różnymi organami na poziomie krajowym i europejskim w celu zwalczania nielegalnej migracji i przestępczości transgranicznej. EUROSUR przyczyni się również do wzmocnienia ochrony i ratowania życia migrantów. Uruchomienie sieci EUROSUR było zaplanowane na 1 października 2013.

5.7. Mechanizm Ochrony Ludności

W decyzji Rady z dnia 8 listopada 2007 r. ustanawiającej wspólnotowy mechanizm ochrony ludności (przekształcenie) znalazły się zapisy, że ogólnym celem mechanizmu jest zapewnienie – na wniosek – wsparcia w przypadku poważnych sytuacji nadzwyczajnych oraz ułatwienie lepszej koordynacji interwencji pomocowych podejmowanych przez państwa członkowskie i Wspólnotę, z uwzględnieniem szczególnych potrzeb odizolowanych, najbardziej oddalonych i innych regionów lub wysp na terenie Wspólnoty. W 2011 r. we wniosku dotyczącym decyzji Parlamentu Europejskiego i Rady w sprawie unijnego Mechanizmu Ochrony Ludności przypisano zapobieganiu znaczenie równorzędne z działaniami służącymi zapewnieniu gotowości oraz reagowaniem i zawarto przepisy mające na celu dalszy rozwój oceny ryzyka w dziedzinie strategii ochrony ludności. Wniosek wprowadza nowy rozdział poświęcony zapobieganiu w celu zwiększenia znaczenia unijnych ram politycznych w zakresie zapobiegania oraz skutecznego połączenia ich z działaniami na rzecz zapewnienia gotowości i działaniami w zakresie reagowania. W ramach rozwijania toczących się prac w zakresie oceny ryzyka oraz w celu zagwarantowania skutecznej współpracy w zakresie mechanizmu na państwa członkowskie nałożony zostaje obowiązek przekazania Komisji Europejskiej planów zarządzania zagrożeniami do końca 2016 r. (art. 6).

1. Aby zapewnić skuteczną współpracę w ramach Mechanizmu państwa członkowskie przekazują Komisji swoje plany zarządzania zagrożeniem.
2. Plany zarządzania zagrożeniem uwzględniają krajowe oceny zagrożenia oraz inne właściwe oceny zagrożenia i są spójne z innymi właściwymi planami obowiązującymi w danym państwie członkowskim.
3. Państwa członkowskie zapewniają najpóźniej do końca 2016 r. przygotowanie swoich planów zarządzania zagrożeniem oraz przekazanie ich Komisji w najbardziej aktualnej formie⁷³.

⁷³ Art. 6. wniosku w sprawie decyzji Parlamentu Europejskiego i Rady w sprawie unijnego Mechanizmu Ochrony Ludności, COM(2011) 934 final z dnia 20 grudnia 2011.

Plany te stanowią istotny instrument planistyczny oraz przyczyniają się do spójnej polityki zarządzania zagrożeniami nakreślonej w unijnej *Strategii bezpieczeństwa wewnętrznego*. Zgodnie z planem przegląd zagrożeń dokonany na szczęblu Unii Europejskiej w oparciu o krajowe oceny ryzyka zapewni wartość dodaną w formie udoskonalonego planowania scenariuszy i planowania ewentualnościowego w celu optymalnej koordynacji europejskich działań w zakresie reagowania, zapewnienia gotowości i zapobiegania. Wartością dodaną UE jest zwiększona skuteczność działań dzięki wyższej gotowości oraz bardziej spójnej polityce zarządzania ryzykiem wystąpienia klęsk i katastrof.

6. ZARZĄDZANIE RYZYKIEM W OBSZARZE BEZPIECZEŃSTWA ZEWNĘTRZNEGO UNII EUROPEJSKIEJ

W grudniu 2003 r. Rada Europejska przyjęła *Europejską strategię bezpieczeństwa*, w której zostały zawarte następujące trzy podstawowe cele UE: wniesienie wkładu w stabilizację i dobre rządzenie w najbliższym sąsiedztwie Unii, tworzenie porządku międzynarodowego opartego na efektywnym multilateralizmie oraz przeciwdziałanie zagrożeniom – zarówno nowym, jak i tradycyjnym. W *Strategii* podkreślono, że UE ponosi odpowiedzialność za bezpieczeństwo międzynarodowe i powinna odgrywać ważną rolę w jego zapewnianiu. Jako zagrożenia, jakim Unia musi się przeciwstawić, wymieniono konflikty regionalne, terroryzm, proliferację broni masowego rażenia oraz możliwość jej użycia przeciw terytorium UE, upadające państwa i wybuchające w nich oraz w ich sąsiedztwie konflikty, a także przestępczość zorganizowaną¹. Od czasu przyjęcia *Strategii* nastąpiło wiele zmian instytucjonalnych, przyjęto Traktat z Lizbony oraz włączono do UE nowe państwa. Zmieniło się także otoczenie oraz rodzaj zagrożeń wokół UE. Skutki wiosny arabskiej były odczuwalne w Europie. W obliczu zagrożeń częściowo pochodzących spoza obszaru UE zasadnicze znaczenie dla prowadzenia skutecznej polityki bezpieczeństwa ma wzmocniona współpraca z podmiotami z obszaru bezpieczeństwa zewnętrznego, państwami trzecimi i organizacjami.

W takiej sytuacji istotna staje się rola ESDZ, utworzonej zgodnie z zapisami Traktatu z Lizbony. Zgodnie z mandatem określonym dla Wysokiego Przedstawiciela UE ds. do spraw wspólnej polityki zagranicznej i bezpieczeństwa oraz dla Europejskiej Służby Działań Zewnętrznych, aby umożliwić Wysokiemu Przedstawicielowi prowadzenie europejskiej polityki bezpieczeństwa i obrony (EPBiO), struktury zarządzania kryzysowego UE miały zostać częścią służby, z pełnym uwzględnieniem ich cech charakterystycznych. Struktury te miały stworzyć jednostkę, która będzie bezpośrednio podlegać wysokiemu przedstawicielowi i pozostanie pod jego kierownictwem. Zmiany te dokonywały się od 2010 r. i zgodnie z decyzją Rady z dnia 26 lipca 2010 r. (2010/427/UE) Dyrekcja ds. zarządzania i planowania kryzysowego, Komórka Planowania i Prowadzenia Operacji Cywilnych, Sztab Wojskowy Unii Europejskiej i Centrum Sytuacyjne Unii Europejskiej (SITCEN) podlegają

¹ http://www.ms.gov.pl/pl/c/MOBILE/polityka_zagraniczna/polityka_bezpieczenstwa/europejska_polityka_bezpieczenstwa_i_obrony_esdp/europejska_strategia_bezpieczenstwa/ [dostęp: październik 2017].

bezpośrednio Wysokiemu Przedstawicielowi². Dawniej w ramach Sekretariatu Generalnego Rady UE w strukturze zarządzania kryzysowego funkcjonował m.in. Joint SITCEN (Wspólne Centrum Sytuacyjne), w którym dokonywano oceny ryzyka na potrzeby działań prowadzonych także poza UE. Dawne komórki „kryzysowe” Sekretariatu Generalnego Rady UE zostały przeniesione do ESDZ: Dyrekcja ds. Zarządzania Kryzysowego i Planowania (CMPD), Komórka Planowania i Prowadzenia Operacji Cywilnych (CPCC), Sztab Wojskowy Unii Europejskiej (SWUE), Działy bezpośrednio podlegające dyrektorowi generalnemu Sztabu Wojskowego Unii Europejskiej (DGEUMS), Dyrekcja ds. Koncepcji i Zdolności, Dyrekcja ds. Wywiadu, Dyrekcja ds. Operacji, Dyrekcja ds. Logistyki, Dyrekcja ds. Systemów Łączności i Informacji, Centrum Sytuacyjne Unii Europejskiej (SITCEN). Ponadto z Dyrekcji Generalnej ds. Stosunków Zewnętrznych do ESDZ włączono platformę kryzysową i koordynację polityczną w ramach WPZiB. W strukturze Crisis Response and Operational Coordination w ESDZ funkcjonowały Crisis Response Planning and Operations, EU Situation Room, Consular Crisis Management oraz INTCEN EU Intelligence Analysis Centre (działy: Analysis oraz General and External Relations). Nastąpiła ewolucja dawnego SITCEN, które zajmowało się oceną ryzyka w ramach zadań ESDZ, niemniej jednak jednym z obszarów powiązanych jest także prowadzony monitoring sytuacji wewnętrznej UE. „Europejska Służba Działań Zewnętrznych dysponuje strukturami rozporządzającymi oceną sytuacji, informacjami w zakresie danych wywiadowczych lub spraw wojskowych, jak również siecią przedstawicielstw, które mogą pomóc przeciwdziałać zagrożeniom oraz klęskom lub katastrofom na terytorium państw członkowskich lub sytuacjom kryzysowym o wymiarze zewnętrznym”³. INTCEN składało się z dwóch wydziałów:

- Wydziału Analiz – który jest odpowiedzialny za dostarczanie strategicznej analizy bazującej na wkładzie dostarczanym przez agencje wywiadowcze i informacyjne w państwach członkowskich. Wydział podzielony jest na obszary tematyczne oraz geograficzne;
- Działu Reakcji Ogólnych i Zewnętrznych, zajmującym się zapytaniami administracyjnymi oraz czerpiącym informacje z ogólnodostępnych źródeł.

Zadania INTCEN były takie jak dawnego SITCEN w Sekretariacie Generalnym Rady Unii Europejskiej⁴. Ponadto rola EU INTCEN była związana przede wszystkim z przygotowywaniem ocen ryzyka i zagrożeń dla bezpieczeństwa zewnętrznego UE. Jednak jak pokazały kryzysy bezpieczeństwo zewnętrzne (np.

² Decyzja Rady z dnia 26 lipca 2010 r. określająca organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych 2010/427/UE (Dz. Urz. UE L 201 z 03.08.2010).

³ Wspólny wniosek Decyzja Rady w sprawie ustaleń dotyczących zastosowania przez Unię klauzuli solidarności JOIN/2012/039 final–2012/0370 (NLE).

⁴ Z wyłączeniem następujących: kwestie konsularne przeniesiono do Crisis Response; Operational Coordination Managing Directorate także włączono do Crisis Response, z kolei Operational coordination Managing Directorate (zwane ComCen) przesunięto do Managing Directorate for Resources (Dział IT).

kryzys migracyjny) ma wpływ na bezpieczeństwo wewnętrzne, dlatego też z analiz ESDZ korzystają też inne instytucje UE: Komisja Europejska oraz państwa członkowskie. ESDZ kieruje się podejściem konieczności poinformowania o zagrożeniach strony zainteresowane – oczywiście z poszanowaniem zasad udostępniania informacji niejawnych (limited lub SECRET UE/EU SECRET). Ponadto EU INTCEN było częścią tzw. Single Intelligence Analysis Capacity (SIAC), która łączyła wywiad cywilny EU INTCEN oraz wywiad wojskowy EUMS INT DIR. W ramach SIAC zarówno wkład przygotowywany przez stronę cywilną, jak i wojskową był wykorzystywany do całościowej analizy ryzyka. Wszystkie państwa członkowskie były proszone o przekazywanie informacji do EU INTCEN w zależności od możliwości wywiadowczych oraz woli współpracy z EU INTCEN. Informacje były przygotowane do poziomu TRES SECRET UE/EU TOP SECRET. INTCEN czerpie także informacje z Rady Unii Europejskiej, Komisji oraz delegacji UE. W trakcie prac w 2012 r. w ESDZ ustanowiono również bliższe powiązania między Europejską Służbą Działań Zewnętrznych a odpowiednimi organami (takimi jak np. Europol i FRONTEX).

W 2017 r. w SDZ w ramach EU Intelligence and Situation Centre funkcjonują 4 wydziały: Open Source Intelligence, Situation Room, Consular Crisis Management.

7. PRZYKŁADOWE PROJEKTY BADAWCZE Z ZAKRESU OCENY RYZYKA

„Od 2007 r. Komisja wydała w sumie na 7. Program Ramowy w dziedzinie badań nad bezpieczeństwem kwotę rzędu 1,4 mld euro. Wsparcie finansowe otrzymało ponad 250 projektów, dotyczących między innymi ochrony ludności przed zagrożeniami związanymi z materiałami chemicznymi, biologicznymi, radiologicznymi, jądrowymi i wybuchowymi (CBRJW) i sytuacjami wywołanymi działalnością człowieka lub klęskami żywiołowymi, ochrony infrastruktury krytycznej, zdolności w zakresie zarządzania kryzysowego czy inteligentnego nadzorowania granic na morzu i lądzie”¹.

UE przeznacza także znaczne środki na projekty badawcze, które obejmują badania nad poszczególnymi rodzajami zagrożeń występującymi w Europie, np. powodzią, pożarami lasów, osuwiskami ziemi, suszami, trzęsieniem ziemi, aktywnością wulkanów. Z perspektywy niniejszej analizy istotne są przykłady trzech projektów, które obejmują złożone oceny ryzyka:

- KULTURisk – Knowledge-based approach to develop a cULTUre of RISK prevention;
- MATRIX – New Multi-HAZard and MulTi-RISk Assessment MethodS for Europe;
- CATALYST – Capacity Development for Hazard Risk Reduction and Adaptation.

7.1. KULTURisk

Projekt KULTURisk (2011–2013) zakładał zastosowanie naukowego podejścia do rozwoju obszaru prewencji ryzyka (ang. *risk prevention*). Tragiczne w skutkach wydarzenia i katastrofy wzmocniły przekonanie o konieczności zajęcia się tym obszarem, w celu ograniczenia strat w ludziach oraz zmniejszenia szkód ekonomicznych. KULTURisk miał wypracować metodologię i przedstawić korzyści wynikające z położenia nacisku na techniki prewencji, zastosowane w różnych przypadkach o zróżnicowanym kontekście socjoekonomicznym, w których występują zagrożenia związane z wodą. Metoda wypracowana w ramach projektu miała pomóc ocenić, do

¹ Informacja prasowa KE, http://europa.eu/rapid/press-release_IP-13-317_pl.htm?locale=FR. [dostęp: marzec 2015].

jakiego stopnia działania prewencyjne będą efektywniejsze niż pomoc udzielana po wystąpieniu zdarzenia i działania naprawcze. Projekt miał na celu rozwój kultury rozumianej jako myślenie i działanie w obszarze ryzyka, aby dzięki zastosowaniu odpowiednich środków unaocznic korzyści z zajęcia się oceną ryzyka. Rozwój kultury prewencji wymaga pamięci o przeszłych katastrofach i wiedzy na ich temat, komunikacji i zrozumienia możliwości aktualnych i przyszłych zagrożeń, świadomości włączenia analiz ryzyka do działań oraz przygotowania na przyszłe zdarzenia.

Szczegółowe cele projektu:

1. Przegląd środków zapobiegania w obszarze zagrożeń związanych z wodą, ze szczególnym naciskiem na techniki komunikacji.
2. Rozwój metodologii związanej z ryzykiem do oceny różnych środków prewencyjnych na wypadek występowania różnych zdarzeń.
3. Udowodnienie, że stosowanie środków prewencji jest efektywniejsze z punktu widzenia czynników społecznych i ekonomicznych w przypadku różnego rodzaju zagrożeń związanych z wodą (powodzie, osuwiska ziemi).
4. Promowanie kultury prewencji poprzez użycie przykładów z projektu:
 - a) zwiększenie w społeczeństwie świadomości ryzyka poprzez lepszą komunikację,
 - b) wykształcenie w mieszkańcach poprawnej, odpowiedzialnej postawy w kontekście postrzegania ryzyka,
 - c) szkolenia dla ekspertów, służące doskonaleniu tworzenia oceny socjoekonomicznej i uczące jej uwzględniania w analizie ryzyka dla zagrożeń związanych z wodą.

Analiza zlewni dwóch rzek, które przepływają przez wiele krajów Europy: Soczy-Isonzo i Dunaju pozwoliła na analizę aspektów transgranicznych. W tym projekcie widać podejście UE, które polega na rozpatrywaniu całościowo dorzeczy oraz zlewni, a nie tylko na zapobieganiu powodzi na danym odcinku rzeki w jednym z krajów członkowskich. W ramach projektu analizie poddano sześć przypadków, które zostały wykorzystane do pokazania wartości włączenia analizy ryzyka, także na poziomie Unii Europejskiej, do polityki zapobiegania katastrofom naturalnym. Zastosowane w projekcie środki, techniki oraz metodologia miały pozwolić na uwzględnienie zmian w zakresie użytkowania terenu, gospodarki przestrzennej oraz wpływu zmian klimatu.

7.2. MATRIX

Projekt MATRIX – New Multi-Hazard and Multi-Risk Assessment Methods for Europe, realizowany w latach 2010–2013 w ramach 7. Programu Ramowego przez Narodowe Centrum Badawcze Nauki o Ziemi, miał na celu wypracowanie narzędzi do analizy zagrożeń i oceny ryzyka na potrzeby Unii Europejskiej. W skład konsorcjum weszło 12 instytucji z 10 krajów UE. Główne cele projektu obejmowały

określenie oraz przedstawienie, w jakich warunkach złożona ocena ryzyka (ang. *multi-type risk assessment*) przynosi lepsze efekty od analizy ryzyka danego zagrożenia (ang. *single-type hazards*) oraz dostarczenie bazy wiedzy do przeprowadzania złożonej oceny ryzyka w Europie.

Zgodnie z obserwacjami założeń projektu poczynionymi przez jego realizatorów pewne obszary w Europie są narażone na ryzyko wystąpienia katastrof naturalnych i zdarzeń w określonych kombinacjach. Analiza oraz ocena zagrożeń i ryzyka nie powinny opierać się na jednostkowej ocenie jednego zagrożenia, ale zawsze uwzględniać także inne zagrożenia z nim powiązane. Trzęsienie ziemi, erupcje wulkanu, osuwiska ziemi, tsunami, pożary, śnieżyce czy powodzie mogą być wywołane jednymi czynnikami i wpływać na wystąpienie kolejnych. Obecnie zjawiska te są traktowane przez naukowców w oderwaniu od innych, a jak pokazuje rzeczywistość, występują także w połączeniach, np. silne opady deszczu powodują osuwiska ziemi. Ponadto zjawiska naturalne występują na określonych obszarach, w określonym czasie, a dodatkowo są trudne do przewidzenia. Miejsca występowania danych zdarzeń (powodzie, trzęsienia ziemi, erupcje wulkanów) są łatwiejsze do określenia. Szczególnie ważne dla projektu będzie zaś zebranie i zharmonizowanie elementów trudnych do przewidzenia. W projekcie badane są następujące obszary:

1. Porównywalność zagrożeń i ryzyk (ang. *comparability of hazards and risks*) – w ramach MATRIX zaplanowano rozwinięcie metod, które pozwolą na analizę ilościową ryzyka powiązanego z różnymi zagrożeniami.
2. Efekt domina/efekt kaskadowy (ang. *domino/cascade effects*) – w tym przypadku jedno zdarzenie może spowodować wystąpienie innego czy wielu innych zdarzeń. Projekt badał relacje pomiędzy różnymi typami zdarzeń oraz dokonał ich pomiaru.
3. Podatność wystąpienia zdarzenia w czasie² (ang. *time-dependent vulnerability*) – ta kwestia jest szczególnie ważna w przypadku, kiedy uważa się, że różne typy ekstremalnych zdarzeń mogą po sobie następować i że kolejne będą powodowały zwiększenie szkód na obszarach, które zostały już dotknięte poprzednimi zdarzeniami.

Spodziewane efekty projektu objęły wypracowanie narzędzi do oceny różnych rodzajów ryzyka, które mogą być stosowane przez badaczy zajmujących się katastrofami naturalnymi czy organy ochrony ludności w poszczególnych krajach. Dokonano przeglądu scenariuszy zdarzeń kaskadowych na bazie minionych katastrof (m.in. trzęsienia ziemi oraz tsunami) i stworzono bazę wiedzy, która jest dostępna dla badaczy i kadry zarządzającej w przypadku katastrof. Wypracowano także wytyczne do oceny różnych rodzajów ryzyka w Europie. Projekt MATRIX zakładał rozwinięcie metod i narzędzi badawczych, które będą przydatne w kontekście europejskim.

² Podatność wystąpienia zdarzenia w czasie – oznacza zmienność charakterystyk podatności w czasie, <https://crisma-cat.ait.ac.at/glossary/time-dependent-vulnerability> [dostęp: marzec 2015].

7.3. Catalyst

Projekt Catalyst: *Capacity Development for Hazard Risk Reduction and Adaptation* miał dzięki współpracy badaczy i stron zainteresowanych zidentyfikować wiedzę i praktyki związane ze zmniejszaniem ryzyka katastrof i naturalnych zagrożeń (ang. *natural hazards/disaster risk reduction*). Nadrzędnym celem było zwiększenie możliwości rozwoju tego obszaru poprzez umożliwienie wymiany wiedzy i poprawę współpracy naukowej, identyfikację luk pomiędzy występowaniem naturalnych zagrożeń oraz zmniejszaniem ryzyka katastrof a stroną badawczą. Projekt miał zapewnić wsparcie europejskich i międzynarodowych sieci współpracy, a także zwiększyć możliwości włączenia organizacji pozarządowych (ang. *NGO*) oraz małych i średnich przedsiębiorstw (ang. *SME*) do działań w tych obszarach. Kluczowym działaniem Catalyst było zebranie stron zainteresowanych, w tym praktyków oraz badaczy w *think tank*, który umożliwił wymianę wiedzy w obszarach wyłonionych jako problematyczne (np. metodologiczne ograniczenia, braki danych, wymiana najlepszych praktyk). Działania wspierane były poprzez wymianę informacji, m.in. na stronie internetowej, która będzie stanowiła miejsce wymiany wiedzy i zostanie udostępniona zainteresowanym ekspertom, badaczom i praktykom.

PODSUMOWANIE I WNIOSKI

Globalizacja np. łańcuchów dostaw różnego rodzaju produktów przemysłowych czy żywności, terroryzm, wypadki technologiczne, katastrofy naturalne, pandemie, zmiany klimatu, stwarzają zagrożenia m.in. dla Unii Europejskiej. Ryzyko wystąpienia pewnych zdarzeń wymaga wzmożonej współpracy i spójności UE oraz świata naukowego w zakresie analiz służb dbających o bezpieczeństwo obywateli. Ryzyko może być odczuwalne w wymiarze globalnym (terroryzm, pandemie, skażenie żywności, zmiany klimatu, skutki katastrofy jądrowej), w wymiarze wewnętrznym UE (terroryzm, napływ nielegalnych imigrantów do UE), w wymiarze transgranicznym (powodzie, pożary lasów, awaria elektrowni atomowej w sąsiedztwie UE).

Zmieniająca się rzeczywistość, w której obecnie funkcjonują rozwinięte społeczeństwa wymusza na Unii Europejskiej także działanie w wymiarze wirtualnym. Pewne zdarzenia dziejące się w rzeczywistości mogą być inicjowane w świecie wirtualnym. Przykładami są np. tzw. *flashmob* czy zapraszanie kilku tysięcy osób na urodziny poprzez portal. Z drugiej strony nowe formy komunikacji w sytuacjach kryzysowych (np. przekazywanie sobie informacji o miejscu zagrożenia lub o swoim miejscu przebywania za pośrednictwem Twittera, Facebooka lub SMS-a) otwierają nowe kanały wymiany informacji, możliwe do wykorzystania przez służby porządkowe i ratownicze. Zmiany w zapisach dyrektywy Seveso III oraz informowanie społeczeństwa o zagrożeniach w ramach testów wytrzymałościowych jest wynikiem realizacji zapisów *konwencji z Aarhus*, dotyczącej dostępu społeczeństwa do informacji środowiskowych, które kładą duży nacisk na otwartość i przejrzystość tych informacji. „Zgodnie z konwencją z Aarhus skuteczny udział społeczeństwa w podejmowaniu decyzji jest konieczny, aby umożliwić zainteresowanej społeczności wyrażanie, a decydentowi uwzględnianie, opinii i obaw, które mogą być istotne dla tych decyzji, zwiększając w ten sposób odpowiedzialność w ramach procesu podejmowania decyzji i jego przejrzystość oraz przyczyniając się do zwiększenia świadomości publicznej w zakresie środowiska oraz poparcia dla podjętych decyzji”³.

³ Dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE, (Dz. Urz. UE L 197 z 24.07.2012, s. 1–37).

Już w 2008 r. KE potwierdziła, że Unia Europejska potrzebuje większej zdolności podejmowania ogólnych wyzwań w obszarze zapobiegania katastrofom, ograniczania ich skutków i reagowania. Kompleksowość i zakres tych wielowymiarowych wyzwań wymaga szeroko zakrojonego podejścia UE do całokształtu zagadnień związanych z oceną ryzyka wystąpienia katastrofy, prognozami, zapobieganiem, gotowością i ograniczeniem skutków (przed katastrofą i po jej wystąpieniu), koordynacją różnych obszarów polityki, instrumentów i usług⁴. W grudniu 2010 r. KE wydała *Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management*, przedstawiając w nim wytyczne dla państw członkowskich w zakresie oceny ryzyka oraz mapowania ryzyka, zbierając i porządkując metodologię, ale pozostawiając państwom wskazówki. Ocena ryzyka jest kluczowa dla zapobiegania katastrofom w państwach członkowskich, może wspomóc zapobieganie oraz wzmocnić planowanie zasobów na wypadek reagowania na katastrofy. Wytyczne mają na celu poprawę spójności ocen ryzyka podejmowanych w państwach członkowskich oraz możliwości ich porównywania. Ułatwi to współpracę np. w obszarach przygranicznych w przypadku wystąpienia podobnego ryzyka dla danego terenu. Co ważne, w wytycznych tych porusza się szereg opcji, np. oceny pojedynczego ryzyka oraz ryzyka uwzględniającego wiele zagrożeń, efektu domina i scenariuszy. Wprowadza się też zmienne do mierzenia ryzyka w postaci skutków dla obszaru.

UE sięga do metodologii, które stosują państwa członkowskie, ale także do doświadczeń innych krajów – USA, Kanady, Nowej Zelandii. W 2011 r. w Brukseli odbyła się druga międzynarodowa konferencja poświęcona ocenie ryzyka – *Global Risk Assessment Dialogue*. Jej celem było umożliwienie dyskusji na temat priorytetów oceny ryzyka, metod oceny i zasad jej prowadzenia. Spotkanie odbyło się w ramach współpracy UE z USA i Kanadą. W wyniku spotkań na forum *Global Risk Assessment Dialogue* Unii Europejskiej udaje się w wymiarze globalnym osiągnąć przegląd systemów oraz rozumienia oceny ryzyka, wyłonić istotne kwestie oraz określić wyzwania dla przyszłych ocen ryzyka, znaleźć obszary dla dialogu i współpracy, a także wyznaczyć priorytety dla przyszłych inicjatyw w tym obszarze.

Zarządzanie ryzykiem w UE jest koniecznością z uwagi na wymóg zapewniania obywatelom oraz mieszkańcom UE bezpieczeństwa w wymiarze wewnętrznym i zewnętrznym. UE rozumie rolę zaplecza naukowego oraz analizy naukowej, które są niezbędnym elementem poprawnego procesu zarządzania ryzykiem. Zasadne jest włączenie innowacji, wyników badań oraz technologii do zarządzania ryzykiem. Przykładowo nieprzeprowadzenie analizy naukowej zdarzenia lub przeprowadzenie jej w nieprawidłowy sposób może spowodować, że społeczeństwo utraci zaufanie do wydawanych komunikatów. Przykładem kryzysu, którego analiza naukowa była źle

⁴ Komisja Europejska, komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie wzmocnienia zdolności Unii do reagowania w przypadku katastrof, COM(2008) 130 final z 5 marca 2008, s. 3.

zinterpretowana, był kryzys związany z BSE w Wielkiej Brytanii. Z kolei niepewność co do czynnika powodującego zgony oraz konieczność przeprowadzenia kolejnych badań naukowych nad czynnikiem wywołującym kryzys – jak się okazało w 2011 r. bakterii *E. coli* – wprowadzała nieufność wśród społeczeństw UE oraz doprowadziła do znacznych strat finansowych.

Ocena ryzyka powinna być oparta na dowodach naukowych np. w zakresie ochrony zdrowia ludzkiego i ekosystemów, w przypadku których narażenie na wystąpienie negatywnych skutków dla zdrowia musi być potwierdzone przez analizę czynników powodujących dane zagrożenie.

Należy zaznaczyć, że widoczne jest oddzielenie oceny ryzyka (ang. *risk assessment*) od zarządzania ryzykiem (ang. *risk management*). Szczególnie widoczne jest to w podziale, i zadaniach i roli poszczególnych instytucji unijnych, które dokonują ocen ryzyka za pośrednictwem agencji unijnych, np. FRONTEx, czy w przypadku ryzyka kryzysu w dziedzinie zdrowia: EFSA-EMEA-EEA-ECD-C-ECHA-SCENIHR/SCCP/SCHER oraz SCOEL. Z kolei poziom zarządzania ryzykiem i decyzji jest wprowadzony na poziomie Komisji Europejskiej, Rady Unii Europejskiej, Europejskiej Służby Działań Zewnętrznych oraz Parlamentu Europejskiego.

Ocena ryzyka ma zawierać elementy prawdopodobieństwa wystąpienia określonego zdarzenia, jego skutków oraz skali. Jednym z elementów, który jest rozpatrywany w analizach ryzyka jest tzw. ocena wpływu (ang. *impact assessment*). Plany na wypadek wystąpienia danego typu ryzyka muszą być przygotowywane na największe ryzyko, być na tyle elastyczne, aby móc w ich ramach reagować na większe zdarzenia. Ryzyko wystąpienia zdarzeń rzadkich, o dużej skali oddziaływania, jest kwestią, która obecnie szczególnie po katastrofie w 2011 r. w Fukushimie była przedmiotem debat na forum UE. Jednak powinna być poddana dalszej analizie. Nie da się przygotować żadnej organizacji, nawet ratowniczej, na wszelkie rodzaje kryzysu. Pewien stopień rzadkich i nietypowych zdarzeń zawsze będzie stanowił ułamek standardowo prowadzonych operacji. Podobnie będzie w przypadku UE. Nie mniej jednak w komunikacie (COM(2012)0571)⁵ z dnia 4 października 2012 r. dotyczącym kompleksowych ocen ryzyka i bezpieczeństwa („testów wytrzymałościowych”) Komisja stwierdza: „Wydarzenie to pokazało, że reaktory jądrowe muszą być chronione nawet przed wypadkami, które zostały ocenione, jako wysoce nieprawdopodobne”. W tym celu powinna zostać nawiązana ściślejsza współpraca pomiędzy Komisją, państwami członkowskimi, instytucjami zajmującymi się zapewnianiem bezpieczeństwa w przypadku zdarzeń czy wypadków jądrowych, a także służbami ratowniczymi.

⁵ Komisja Europejska, komunikat Komisji do Rady i Parlamentu Europejskiego dotyczący kompleksowych ocen ryzyka i bezpieczeństwa („testów wytrzymałościowych”) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych, COM(2012) 571 final z dnia 4 października 2012.

Na poziomie UE wypracowano metodyki oceny ryzyka i zagrożeń m.in. w stosunku do zagrożenia powodziowego, suszy, awarii przemysłowych i ochrony infrastruktury krytycznej. Przykłady ważniejszych opracowań zostały omówione w niniejszej analizie w odniesieniu do: powodzi, awarii chemicznych oraz infrastruktury krytycznej, zagrożeń związanych z bezpieczeństwem na granicach zewnętrznych oraz bezpieczeństwem zdrowotnym. Prace w obszarze oceny ryzyka, oceny zagrożeń i zarządzania ryzykiem widać w podejściu sektorowym. W Unii Europejskiej obserwować już można proces podejmowania działań w obszarze tzw. ocena ryzyka uwzględniająca wiele rodzajów zagrożeń (ang. *multi-risk assessment*). Dokumenty strategiczne UE mówią o tym obszarze jako o wyzwaniu. Ponadto Unia Europejska, sama zainteresowana zagadnieniem i zobligowana dokumentami do dokonania całościowej analizy zagrożeń dla swojego obszaru, wspiera się pracami badawczymi. Dotyczą one nie tylko poszczególnych zagrożeń naturalnych czy technologicznych, ale jak widać w niniejszej analizie – także ocen bardziej złożonych, które przedstawione zostały na przykładzie projektów KULTURisk, MATRIX i Catalyst.

Kluczowa dla zrozumienia prac na forum UE w tym obszarze jest zasada pomocniczości, określona w art. 5 Traktatu. „Zgodnie z zasadą pomocniczości, w dziedzinach, które nie należą do jej wyłącznej kompetencji, Unia podejmuje działania tylko wówczas i tylko w takim zakresie, w jakim cele zamierzonego działania nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, zarówno na poziomie centralnym, jak i regionalnym oraz lokalnym, i jeśli ze względu na rozmiary lub skutki proponowanego działania możliwe jest lepsze ich osiągnięcie na poziomie Unii”⁶. Zasada pomocniczości ma na celu określenie odpowiedniego poziomu interwencji w dziedzinach kompetencji dzielonych między UE a państwami członkowskimi. Ochrona ludności jest na przykład domeną państw członkowskich, a zadanie UE stanowi wspieranie, koordynowanie lub uzupełnianie ich działań. Zasada pomocniczości dotyczy działań na szczeblu europejskim, krajowym lub regionalnym. W każdym z przypadków Unia może interweniować tylko wówczas, jeśli jest w stanie działać skuteczniej niż państwa członkowskie. Przepisy UE w zakresie oceny ryzyka powodziowego oraz zarządzania nim są właśnie takim przykładem: „Jako że cel niniejszej dyrektywy, a mianowicie stworzenie ram dla środków mających na celu ograniczenie ryzyka wystąpienia szkód powodziowych, nie może być osiągnięty w wystarczającym stopniu przez państwa członkowskie, a ze względu na rozmiary i skutki działania możliwe jest jego lepsze osiągnięcie na poziomie Wspólnoty, Wspólnota może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu (...)”⁷.

Kolejną zasadą jest zasada proporcjonalności. Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka

⁶ Art. 5 Traktatu o funkcjonowaniu Unii Europejskiej.

⁷ Dyrektywa 2007/60/WE PE i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz. Urz. UE L 288/27 z 06.11.2007).

powodziowego i zarządzania nim nie wykracza poza to, co jest konieczne do osiągnięcia tego celu. „Zgodnie z zasadą proporcjonalności zakres i forma działania Unii nie wykraczają poza to, co jest konieczne do osiągnięcia celów Traktatów. Instytucje Unii stosują zasadę proporcjonalności zgodnie z Protokołem w sprawie stosowania zasad pomocniczości i proporcjonalności”⁸. Podobnie jest w przypadku dyrektywy Seveso III, zastosowano w niej ten sam zapis: „Ponieważ cel niniejszej dyrektywy, mianowicie zapewnienie wysokiego poziomu ochrony zdrowia ludzkiego i środowiska, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Stanowi ona, że niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu”⁹.

W toku prac problematyczną kwestią okazała się porównywalność danych, analiz ryzyka i metodologii stosowanych przez poszczególne państwa członkowskie w ocenach ryzyka. Dlatego prace UE zmierzają do zapewnienia możliwości porównywania danych, koncentrują się na dokonywaniu analiz ryzyka, które nie rozpatrują już tylko jednego zagrożenia, np. wystąpienia powodzi czy pożarów lasów, ale coraz częściej poruszają tzw. efekt domina dla łańcucha zdarzeń – wywołanego jednym zdarzeniem, które implikuje wystąpienie kolejnego. Efekt domina znalazł się w zapisach w przyjętej w 2012 r. dyrektywie Seveso III. „Aby zmniejszyć ryzyko efektu domina w przypadku zakładów ulokowanych w taki sposób lub tak blisko siebie, że wzrasta prawdopodobieństwo poważnych awarii lub nasilenia ich skutków, prowadzący zakłady powinni współpracować w zakresie wymiany odpowiednich informacji i informowania społeczności, z uwzględnieniem sąsiednich zakładów, które mogą odczuć skutki takich awarii”¹⁰. Z kolei niewykluczonym działaniem Komisji może być opracowanie wytycznych dotyczących bezpiecznych odległości oraz efektu domina (art. 24). W kontekście efektu domina i zawarcia takich przepisów w dyrektywie trzeba wziąć pod uwagę także doświadczenia UE po katastrofie w Japonii w 2011 r.

Analizy zagrożeń oraz oceny ryzyka wykonują także agencje unijne, w ramach własnych kompetencji. Poszczególne agencje wypracowały metodyki oceny ryzyka i zagrożeń w swoich obszarach kompetencyjnych, np. agencja FRONTEX w zakresie oceny bezpieczeństwa na granicach zewnętrznych, kryzysu migracyjnego, DG HOME w zakresie analizy zagrożeń UE terroryzmem, DG SANCO w zakresie zagrożeń związanych ze zdrowiem, Europejska Służba Działań Zewnętrznych w zakresie oceny ryzyka i zagrożeń związanych z bezpieczeństwem zewnętrznym Unii Europejskiej.

⁸ Art. 5 Traktatu o funkcjonowaniu Unii Europejskiej.

⁹ Dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE (Dz. Urz. UE L 197/1 z 24.07.2012).

¹⁰ Tamże, art. 9.

Mimo że w niektórych politykach unijnych zawarto kwestie dotyczące analiz ryzyka lub rozpoczęto prace nad nimi, większy wysiłek na poziomie UE należy skupić na przyjęciu podejścia zintegrowanego zarządzania ryzykiem (ang. *Integrated Risk Management* – IRM), które obejmuje prewencję, przygotowanie, reagowanie oraz odbudowę w przypadku wszystkich zagrożeń w Europie.

Jak udowodniła niniejsza analiza zarządzanie ryzykiem w UE jest ugruntowanym zagadnieniem i praktyką, która jest widoczna w ujęciu sektorowym w pracy poszczególnych agencji UE, jak i samych instytucji unijnych. Zarządzanie ryzykiem ma dwa wymiary, z jednej strony jest to zadanie instytucji unijnych, które stosują zarządzanie ryzykiem w ramach swojej organizacji, jako element systemu zarządzania. Z drugiej strony zarządzanie ryzykiem jest powiązane z rolą i zadaniami powierzonymi instytucjom unijnym np. oceną ryzyka w ramach bezpieczeństwa wewnętrznego UE czy bezpieczeństwa zewnętrznego UE.

W dokonanej analizie przedstawiono podejście UE do zarządzania ryzykiem powiązane z obszarem zarządzania kryzysowego. Jest ono jak najbardziej sektorowe, co pokazał przegląd działań w ramach Komisji Europejskiej (zarządzanie ryzykiem w dziedzinie zdrowia, żywności, bezpieczeństwa na granicach zewnętrznych, katastrof naturalnych i technologicznych) oraz szczególnego przypadku oceny zagrożeń prowadzonym przez ESDZ w wymiarze bezpieczeństwa zewnętrznego UE. Niemniej jednak opisany w zakresie współpracy instytucji unijnych przypadek katastrofy jądrowej pokazuje konieczność ponadsektorowej oraz ponadinstytucjonalnej współpracy w Unii Europejskiej.

Do 2016 r. UE opracowała analizę zagrożeń, na które jest narażona UE. Służyć temu też miał wymóg przekazania Komisji Europejskiej przez państwa członkowskie planów zarządzania zagrożeniami do końca 2016 r. – zgodnie z zapisami Wniosku dotyczącym decyzji Parlamentu Europejskiego i Rady w sprawie unijnego Mechanizmu Ochrony Ludności. Celem tego przeglądu nie było zwolnienie ani instytucji UE ani państw członkowskich z dalszych prac nad przygotowaniem się na wypadek danych zagrożeń i reagowaniem na nie. Jej wyniki zawarto w dokumencie KE z dnia 23 maja 2017 r. *Overview of Natural and Man-made Disaster Risks the European Union may face* (Przegląd zagrożeń w UE). Jednym z wniosków wskazano, że lepsze zrozumienie regionalnego wymiaru pewnych zagrożeń poprzez przygotowanie ocen oraz planowanie na wypadek ich wystąpienia na poziomie regionu, mogłoby wzmocnić wartość współpracy krajów UE w zakresie zarządzania na wypadek katastrof, w tym takich zagrożeń jak pandemie, zagrożenia epizootyczne, terroryzm i przestępstwa cybernetyczne. Ponadto zwracanie uwagi na zależności, powiązania oraz efekty kaskadowe ryzyka wystąpienia danych zdarzeń, mogłoby poprawić zarządzanie kompleksowymi katastrofami poprzez zbliżanie instytucji, które są odpowiedzialne za reagowanie i zarządzanie w przypadku wystąpienia danych katastrof. Tu w dokumencie KE podaje się przypadki załamania kluczowej infrastruktury, zdarzeń epizoicznych czy ekstremalne zdarzenia pogodowe. Dodatkowo

KE wskazuje na konieczność zwiększania świadomości, także poprzez prowadzenie badań oraz foresight nt. zmieniającego się otoczenia oraz ryzyk, do których KE zaliczyła m.in. nagły napływ emigrantów i migracje, zagrożenia terrorystyczne, także pogodę kosmiczną czy utratę różnorodności. O ile wpływ zmian klimatu w perspektywie średniookresowej pojawia się jako zagrożenie, to w perspektywie długoterminowej w państwach uczestniczących w Mechanizmie OL, poświęca się temu zagadnieniu jeszcze mało uwagi¹¹.

Przegląd prac w zakresie analizy ryzyka i zagrożeń pokazuje także zmianę podejścia UE, podejmowane próby osiągnięcia celów oraz możliwości oceny zagrożeń w kontekście efektu domina czy zagrożeń powiązanych, mających wpływ na wiele sfer (np. powódzie, obecny kryzys migracyjny w UE). Unia zmierza do dokonywania oceny ryzyka wynikającego z zagrożeń naturalnych i wywołanych działalnością człowieka, które mogą wystąpić w Europie, ale także tych, na które narażone są państwa członkowskie czy sąsiadujące regiony. W ramach realizacji tego celu Unia korzysta ze współpracy na forum międzynarodowym, a także korzysta z wyników prac poszczególnych państw członkowskich oraz wiedzy wypracowywanej w ramach polityki badawczej, w tym także obecnego programu Horyzont 2020.

¹¹ Komisja Europejska, Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final z dnia 23 maja 2017, s. 71.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

- Cieślarczyk M., *Kultura bezpieczeństwa i obronności*, wyd. AP, Siedlce 2011.
- Carrera S., *The EU Border Management Strategy FRONTEX and the challenges of irregular immigration in the Canary Islands*, „CEPS Working Document” nr 261, 2007.
- Pescaroli G., Alexander D., *A definition of cascading disasters and cascading effects: Going beyond the „toppling dominos” metaphor*, „Planet@Risk” 2015, 3(1).

Akty prawne

- Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 83/123 z 30 marca 2010).
- Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz. Urz. UE C 306 z 17.12.2007).
- Dyrektywa 2007/60/WE PE i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz. Urz. UE L 288/27 z 06.11.2007).
- Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345 z 23.12.2008).
- Dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE (Dz. Urz. UE L 197 z 27.04.2012).
- Rozporządzenie Rady (EWG) nr 793/93 z dnia 23 marca 1993 r. w sprawie oceny i kontroli ryzyk stwarzanych przez istniejące substancje (Dz. Urz. WE L 84 z 05.04.1993, s. 1 z późn. zm.)
- Rozporządzenie (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. dostosowujące do decyzji Rady 1999/468/WE przepisy odnoszące się do komitetów, które wspomagają Komisję w wykonywaniu jej uprawnień wykonawczych ustanowionych w instrumentach podlegających procedurze określonej w art. 251 Traktatu WE (Dz. Urz. UE L 284 z 31.10.2003).
- Rozporządzenie (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 282/2014 z dnia 11 marca 2014 r. w sprawie ustanowienia Trzeciego Programu działań Unii w dziedzinie zdrowia (2014–2020) oraz uchylające decyzję nr 1350/2007/WE (1) (Dz. Urz. UE L 86/3, t. 57

- z 21 marca 2014).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 513/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego oraz uchylające decyzję Rady 2007/125/WSiSW (Dz. Urz. UE L 150 z 20.05.2014, s. 93).
- Rezolucja Parlamentu Europejskiego w sprawie ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych (2012/2830(RSP)).
- Decyzja Rady z dnia 12 lutego 2007 r. ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa” 2007/124/WE, Euratom (Dz. Urz. UE L 58 z 24.02.2007).
- Decyzja Rady UE z dnia 8 listopada 2007 r. ustanawiająca wspólnotowy mechanizm ochrony ludności (przekształcenie) (2007/779/WE, Euratom) (Dz. Urz. UE L 314 z 01.12.2007).
- Decyzja Parlamentu Europejskiego i Rady nr 922/2009/WE z dnia 16 września 2009 r. w sprawie rozwiązań interoperacyjnych dla europejskich administracji publicznych (ISA) (Dz. Urz. UE L 260 z 3.10.2009).
- Decyzja Rady z dnia 26 lipca 2010 r. określająca organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych 2010/427/UE (Dz. Urz. UE L 201 z 03.08.2010).
- Wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 final z dnia 8 grudnia 2011.
- Decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE (Dz. Urz. UE L 293/1 z 05.11.2013).
- Komunikat Komisji dla Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Zarządzanie zagrożeniem powodziowym – zapobieganie powodziom, ochrona przeciwpowodziowa i ograniczanie skutków powodzi, COM(2004) 472 final z dnia 12 lipca 2004.
- Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie wzmocnienia zdolności Unii do reagowania w przypadku katastrof, COM(2008) 130 final z dnia 5 marca 2008 r.
- Komunikat Komisji do Parlamentu Europejskiego i Rady, Strategia bezpieczeństwa wewnętrznego Unii Europejskiej. Dążąc do europejskiego modelu bezpieczeństwa, COM(2010) 673 final.
- Komunikat Komisji do Rady i Parlamentu Europejskiego dotyczący kompleksowych ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych, COM(2012) 571 final z dnia 4 października 2012.
- Komunikat Komisji do Parlamentu Europejskiego i Rady, Drugie sprawozdanie na temat realizacji strategii bezpieczeństwa wewnętrznego UE, COM(2013) 179 final z dnia 10.04.2013.
- Komisja Europejska, Overview of Natural and Man-made Disaster Risks the European Union may face, SWD(2017) 176 final z dnia 23 maja 2017.
- Wniosek – decyzja Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 final z dnia 8 grudnia 2011.

- Wniosek dotyczący decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 final z dnia 8 grudnia 2011.
- Wniosek w sprawie decyzji Parlamentu Europejskiego i Rady w sprawie unijnego Mechanizmu Ochrony Ludności, COM(2011) 934 final z dnia 20 grudnia 2011.
- Wspólny wniosek Decyzja Rady w sprawie ustaleń dotyczących zastosowania przez Unię klauzuli solidarności JOIN/2012/039 final–2012/0370 (NLE).
- Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny śródkre-sowej funkcjonowania Unijnego Mechanizmu Ochrony Ludności w latach 2014–2016, COM(2017) 460 final z dnia 30 sierpnia 2017.
- Sprawozdanie specjalne nr 33/2016, Unijny Mechanizm Ochrony Ludności – koordynacja reagowania na klęski żywiołowe poza terytorium UE była zasadniczo skuteczna.
- Konkluzje Rady Europy (24–25 marca 2011), EUCO 10/1.
- Risk Assessment and Mapping Guidelines for Disaster Management, Commission Staff Working Paper, SEC(2010) 1626 final z dnia 21 grudnia 2010.

Dokumenty elektroniczne, strony internetowe i inne

- Disaster Risk Management Knowledge Centre platform, <http://drmkc.jrc.ec.europa.eu>.
- Frontex, Western Balkans, Annual Risk Analysis 2012.
<http://europa.eu>.
- <https://crisma-cat.ait.ac.at/glossary>.
- <http://erccportal.jrc.ec.europa.eu/getdailymap/docId/1969>.
- <http://www.isok.gov.pl/pl/wstepna-ocena-ryzyka-powodziowego>.
- http://www.msz.gov.pl/pl/c/MOBILE/polityka_zagraniczna/polityka_bezpieczenstwa/europejska_polityka_bezpieczenstwa_i_obrony_esdp/europejska_strategia_bezpieczenstwa/.
- http://europa.eu/rapid/press-release_IP-13-317_pl.htm?locale=FR.
- <https://crisma-cat.ait.ac.at/glossary/time-dependent-vulnerability>.
- www.eea.europa.eu/soer-2015/europe/climate-changeimpacts-and-adaptation.

CZEŚĆ IV

ZARZĄDZANIE RYZYKIEM W WYBRANYCH PAŃSTWACH

WPROWADZENIE

W części III niniejszego opracowania zawarta została analiza metodyk¹ oceny ryzyka stosowanych w innych krajach. Badania literaturowe objęły rozwiązania przyjęte w Australii, Irlandii, Niemczech, Szwecji oraz Wielkiej Brytanii. Ich wybór był determinowany doświadczeniem tych państw w wypracowywaniu własnej metodyki oceny ryzyka na potrzeby planowania kryzysowego. Poddane analizie dokumenty mają postać przewodników (wytycznych), opisujących podejście poszczególnych krajów do tej problematyki. Wzięto również pod uwagę dokumenty uwzględniające wyniki ocen ryzyka przeprowadzanych na szczeblu krajowym. W ramach dokumentów poddanych analizie znalazły się:

1. *National Emergency Risk Assessment Guidelines. Commonwealth of Australia and Each of its States and Territories 2010*, październik 2010 (Australia).
2. *A National Risk Assessment for Ireland*, Office of Emergency Planning, grudzień 2012 (Irlandia).
3. *A Framework for Major Emergency Management. A Guide to risk Assessment in Major Emergency Management*, styczeń 2010 (Irlandia).
4. *Method of Risk Analysis for Civil Protection 2011*, Federal Office of Civil Protection and Disaster Assistance, 2011 (Niemcy).
5. *Guide to risk and Vulnerability Analyses*, Swedish Civil Contingencies Agency, 2012 (Szwecja).
6. *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012 (Szwecja).
7. *The National Risk Register of Civil Emergencies 2010*, (NRR), Cabinet Office, 2010 (Wielka Brytania).
8. *National Risk Register for Civil Emergencies 2013* (NRR), Cabinet Office, 2013 (Wielka Brytania).

Omawiane metodyki różnią się szczegółowością prezentowanych treści, niemniej jednak zawarte w nich podstawowe założenia odnoszące się do rozwiązań w zakresie oceny ryzyka pozwoliły na prezentację podejścia poszczególnych państw oraz przeprowadzenie analizy porównawczej metodyk oceny ryzyka stosowanych w poszczególnych krajach, w której wzięte zostały pod uwagę ich mocne i słabe strony.

¹ W przeciwieństwie do omówionych w części I metod i zgodnie z definicjami tam zawartymi w tej części należy mówić o metodykach, ponieważ zebrano tu zbiory zasad, sposobów postępowania (metod) niezbędnych do realizacji zadań z zakresu zarządzania ryzykiem poszczególnych państw.

Umożliwiły również wskazanie korzyści z ich zastosowania, z uwzględnieniem potrzeb planowania cywilnego w Polsce. Rozważone zostały zarówno koncepcje przyjętych metodyk, jak i stosowane techniki i metody oceny ryzyka.

1. ZARZĄDZANIE RYZYKIEM W AUSTRALII

Przyczynami katastrof i zdarzeń niekorzystnych są zjawiska naturalne lub związane z działalnością człowieka. W obu przypadkach oddziałują podobnie: zagrażają życiu, zdrowiu, mieniu i środowisku. Naruszają równowagę otoczenia bezpieczeństwa. Finansowe skutki takich zdarzeń są niekiedy bardzo poważne – zarówno dla ludzi, jak i ekosystemu. Za tym podążają straty ekonomiczne, społeczne, kulturalne i polityczne. W Australii koszty katastrof naturalnych na przestrzeni 40 lat – 1950–1990 wzrosły piętnastokrotnie. W latach 1967–1999 rocznie wynosiły średnio 1,14 mld AUD. Trend wzrostowy utrzymywał się i w 2008 r. straty z tego powodu osiągnęły wielkość 2,49 mld AUD.

Zmiany te wymagały nowego podejścia, ponieważ wyczerpały się już środki techniczne i organizacyjne. Władze zostały zmuszone do udzielenia odpowiedzi, jak ograniczyć zdarzenia niekorzystne¹ i ich konsekwencje. Rząd Australii zdecydował się na wstępie zintensyfikować działania na rzecz zapobiegania i odbudowy, co poszerzyło domenę zainteresowań zarządzania kryzysowego. Oceniono, że zwiększenie bezpieczeństwa wymaga podjęcia 12 reform i wypełnienia 66 rekomendacji i zobowiązań, w tym ograniczenia ryzyka i szkód powstających z powodu katastrof naturalnych w przeszłości.

Taka koncepcja budowania bezpieczeństwa zmuszała do wyjścia poza reagowanie i udzielanie pomocy. Należało podjąć zdecydowane działania, uwzględniając analizę kosztów i korzyści², zmniejszenie wrażliwości ekspozycji³, uodpornienie

¹ Patrz: definicja na s. 139.

² Analiza kosztów i korzyści (ang. *Cost-Benefit Analysis*, CBA) – metoda oceny efektywności inwestycji i projektów biorąca pod uwagę całość przewidywanych korzyści i kosztów, z uwzględnieniem kosztów zewnętrznych (np. środowiskowych, społecznych). Źródło: A. Boardman, D. Greenberg, A. Vining, D. Weimer, *Cost-Benefit Analysis: concepts and practice*, Prentice Hall 2010. Wszystkie korzyści i straty są wyrażane w jednostkach finansowych i z uwzględnieniem zmiany w czasie (wartość bieżąca netto). Do wyceny kosztów i korzyści społecznych stosuje się społeczną stopę dyskontową. CBA to systematyczny proces obliczania i porównywania korzyści i kosztów projektu, decyzji lub polityki publicznej (odtąd nazywanej projektem). CBA ma dwa cele: 1) ustalić, czy inwestycja lub decyzja jest sensowna (uzasadnienie/wykonalność), 2) zapewnić podstawy do porównywania projektów. Cel ten obejmuje porównanie całości oczekiwanego kosztu każdej z opcji do całości oczekiwanych korzyści – aby zobaczyć, czy korzyści przeważają nad kosztami, a jeśli tak, to w jakim stopniu. Źródło: http://www.governica.com/Analiza_koszt%C3%B3w_i_korzy%C5%9Bci [dostęp: marzec 2015].

³ Patrz: definicja na s. 115.

społeczeństwa na zagrożenia i wybór przedsięwzięć umożliwiających zminimalizowanie kosztów strat – a to wymagało zdecydowanej zmiany w podejściu do zarządzania ryzykiem. Rozdział ten przedstawia kierunki, w jakich podążyły te rozwiązania – od formalnoprawnych do praktyki.

1.1. Narodowe ramy oceny ryzyka

Ważne zmiany w zakresie zarządzania ryzykiem i informowania o nim podjęto w 2007 r. Określono wtedy *Narodowe ramy oceny ryzyka*⁴. Ich produktem tych są *Narodowe wytyczne oceny ryzyka zdarzeń kryzysowych*. Kolejnym krokiem było sporządzenie i wdrożenie planu oraz metodyki zarządzania ryzykiem, co znacząco wsparło podjęte reformy w skali krajowej. Takie podejście zapewniło:

- zwiększanie świadomości ryzyka zagrożeń w społeczeństwie i wdrażanie przedsięwzięć odpowiedniego postępowania z ryzykiem⁵,
- standaryzację oceny ryzyka⁶ i doskonalenie alternatywnych propozycji ograniczania ryzyka⁷,
- wzrost przejrzystości procesu, co ułatwiło jego realizację w zakresie ocen, kontroli i modelowania ryzyka w wyniku zdobywania wiedzy i informacji,
- poprawę spójności, pozwalającą na czytelne porównanie różnych obszarów geograficznych i kategorii zagrożeń.

Dokument miał służyć zwiększeniu spójności i jednolitości metodyki oceny ryzyka, poprawie jakości opracowywanych informacji o ryzyku oraz zwiększeniu baz analizy ryzyka. Celem poradnika jest dostarczenie metodyki oceny ryzyka, która:

- umożliwi skupienie uwagi na ryzyku zarówno na szczeblu samorządu, jak i na wyższych szczeblach,
- jest użyteczna zarówno z perspektywy ryzyka wynikającego „z” (konkretnego zagrożenia), jak i ryzyka „dla” (danej wartości chronionej), np. ryzyka pożaru dla danej infrastruktury bez względu na źródło pochodzenia ryzyka,
- pozwala wykorzystać podejście scenariuszowe⁸,

⁴ *Narodowe ramy oceny ryzyka* stanowią istotny punkt odniesienia w procesie realizacji przez rząd Australii zadań z zakresu zarządzania ryzykiem w kontekście zdarzeń kryzysowych. Jako dokument koncepcyjny określają cele i wytyczne w zakresie zarządzania ryzykiem.

⁵ Patrz: definicja na s. 106.

⁶ Patrz: definicja na s. 107.

⁷ Ograniczanie ryzyka – proces zmniejszający ryzyko bądź przez zmniejszenie prawdopodobieństwa, bądź/i skutków wystąpienia zdarzenia stwarzającego zagrożenie Źródło: J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 177.

⁸ Podejście opisano w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 2 *Metody wykorzystywane w ocenie ryzyka*, podrozdział 2.13 *Analiza scenariuszowa*.

- umożliwia klasyfikację ryzyka⁹ w zakresie wiarygodnych poziomów konsekwencji,
- pozwala identyfikować występujące ryzyka będące pod kontrolą oraz te, które wymagają wdrożenia dodatkowej kontroli lub wzmocnienia istniejącej,
- zapewnia podstawy dla jakościowej oceny ryzyka oraz uruchomienie bardziej szczegółowej analizy,
- umożliwia ewaluację ryzyka¹⁰ na różnych poziomach pewności,
- zapewnia wyniki porównywalne do tych, które wynikają z wymogów dotyczących ograniczania ryzyka.

Australijską metodykę oceny ryzyka rozpoczyna identyfikacja zagrożeń i ich klasyfikacja. Zasadniczo we wszystkich państwach przyjmuje się od 55 do 65 rodzajów zagrożeń, zaklasyfikowanych według źródeł ich powstawania: jako naturalne i powodowane działalnością człowieka. Zagrożenia w tych dwóch kategoriach dzielone są na mniejsze grupy i w grupach lub według rodzaju przyporządkowywane samorządom, regionom, ministerstwom lub rządowi. Zapewnia to przejrzystość, precyzuje kompetencje i odpowiedzialność.

Zarządzanie ryzykiem w Australii instytucjonalnie sięga 1995 r. i miało do tychczas kilka etapów rozwoju, w latach: 2000, 2004, 2005, 2008, 2009 i 2010. Każdy z etapów skutkowało wprowadzeniem lub doprecyzowaniem standardów w zakresie: zasad, ram (struktur) i procesów zarządzania ryzykiem opisanych w AS/NZS ISO 31000:2009.

Zasady:

1. Kreowanie i ochrona wartości. Zarządzanie ryzykiem, służąc realizacji przedsięwzięć w obszarze ochrony ludności, pozwala osiągnąć bezpieczny i stabilny poziom życia w przyjaznym środowisku, sprzyjając gospodarce, administracji i infrastrukturze.
2. Integracja ze wszystkimi procesami organizacyjnymi. Zarządzanie ryzykiem stanowi główny nurt aktywności, najskuteczniejszy w integracji standardów aktywności gospodarczej organizacji, władzy i społeczeństwa.
3. Informowanie o podejmowanych decyzjach. Zarządzanie ryzykiem wspiera w świadomym podejmowaniu decyzji i ustaleniu priorytetów względem ograniczonych zasobów dla działań redukujących ryzyko¹¹.
4. Dokładne adresowanie niepewności. Poprawnie realizowane zarządzanie ryzykiem pozwala ograniczać niepewność.
5. Systematyczność, określoność i terminowość. Czynniki te gwarantują spójność, elastyczność i adekwatność rezultatów.

⁹ Patrz: definicja na s. 154.

¹⁰ Patrz: definicja na s. 114.

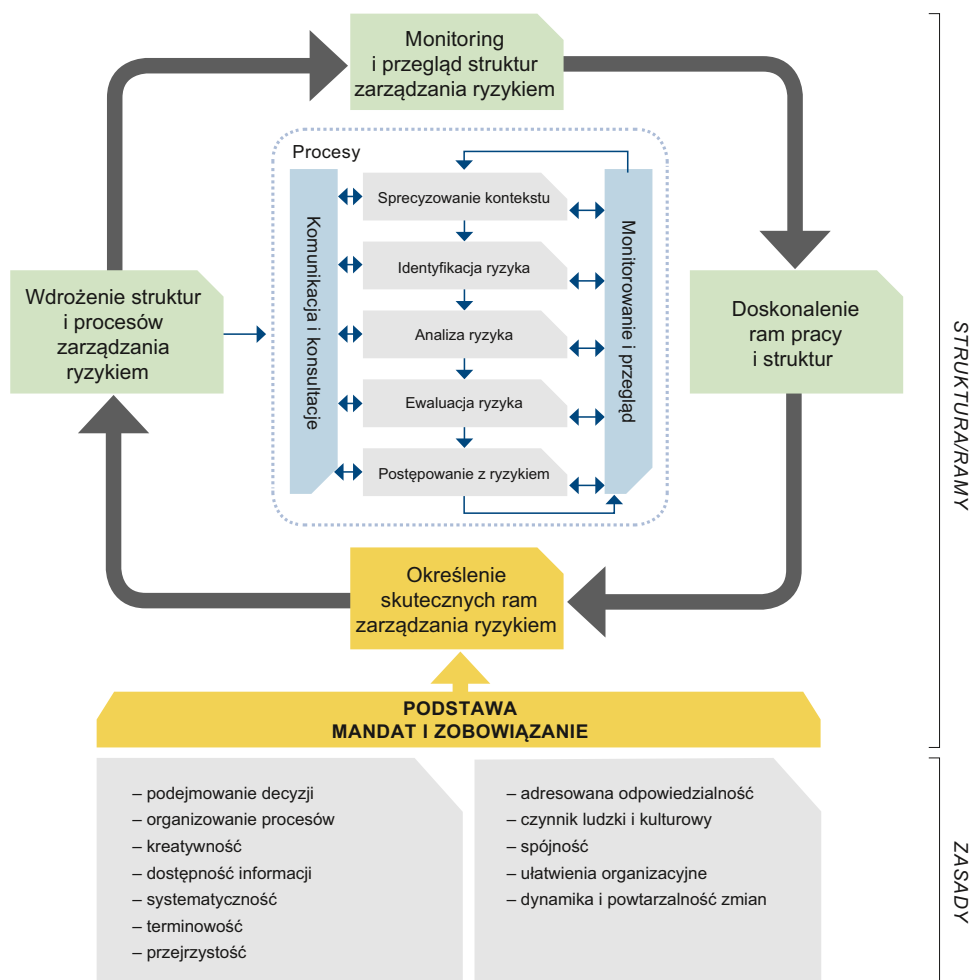
¹¹ Patrz: ograniczanie ryzyka, s. 238.

6. Dostępność najlepszych informacji¹². Informacje gromadzone są w bazach danych. Gromadzi się i opracowuje dostępne dane o zagrożeniach, wrażliwości ekspozycji na różne czynniki w ujęciu historycznym i perspektywicznym oraz zmiany i obserwacje społeczeństwa z udziałem ekspertów. Decydenci powinni być świadomi ograniczonych możliwości baz i zróżnicowania opinii ekspertów (recenzentów), w zależności od ich merytorycznego przygotowania do wykonywania stawianych przed nimi zadań.
7. Dopasowanie. Metodyka zarządzania ryzykiem zapewnia zrównanie potrzeb społecznych w zakresie profilu ryzyka¹³.
8. Uwzględnienie czynników ludzkich i kulturowych. W zarządzaniu ryzykiem należy uwzględniać zdolności percepcyjne zarówno jednostek, jak i powołanych do tego zadania zespołów.
9. Transparentność i ogólność. Zapewnienie skuteczności zarządzania ryzykiem zależy od angażowania wszystkich interesariuszy¹⁴, w tym decydentów, w odpowiednim zakresie i kolejności.
10. Dynamika, powtarzalność i reagowanie na zmiany. Zarządzanie ryzykiem zagrożeń reaguje na zmiany profilu ryzyka, informacje o zagrożeniach i wrażliwości ekspozycji. Skuteczny monitoring pozwala te zmiany identyfikować i odpowiednio wcześniej na nie reagować.
11. Ułatwienie ciągłego doskonalenia. Skuteczne zarządzanie ryzykiem steruje doskonaleniem i wdrażaniem strategii, które podnoszą na wyższy poziom organizację zarządzania ryzykiem w społeczeństwie i organach władzy. Takie podejście zapewnia elastyczność i możliwości adaptacyjne społeczności.

¹² Zgodnie z ISO 31000: pełny przekrój dostępnych danych oraz informacji na potrzeby bieżących oraz przyszłych działań.

¹³ Patrz: agregacja ryzyka, s. 120.

¹⁴ Patrz: definicja na s. 117.



Rys. 1. Relacje pomiędzy zasadami, strukturą ramową i procesem zarządzania ryzykiem
Źródło: Opracowanie własne na podstawie State Emergency Service, *National Emergency Risk Assessment Guidelines*, Hobart 2010, s. 7.

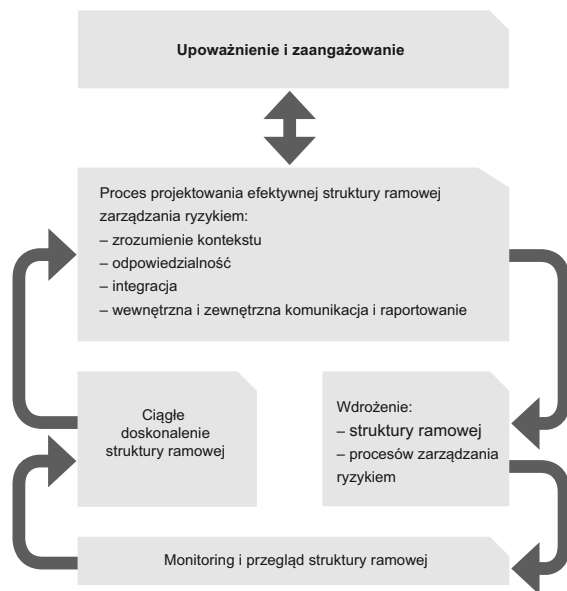
Ramy zarządzania ryzykiem

Skuteczność zarządzania ryzykiem zależy od efektywności struktury zarządzania, zapewniającej podstawy organizacyjne, które gwarantują sukcesy na wszystkich szczeblach organizacyjnych państwa. Właściwie dopasowana struktura zapewnia poprawność obiegu informacji o ryzyku i wykorzystanie jej w podejmowaniu decyzji na wszystkich szczeblach. Struktura ramowa zarządzania ryzykiem jest

przeznaczona do wsparcia integracji zarządzania ryzykiem i jego rezultatów z polityką kierownictwa, systemem zarządzania i podejmowanymi działaniami. Struktura ramowa zarządzania ryzykiem obejmuje (patrz rys. 2):

- upoważnienie i zaangażowanie kierownictwa,
- procesy ukierunkowane na projektowanie skutecznej struktury ramowej zarządzania ryzykiem,
- programy wdrażania struktury i procesów zarządzania ryzykiem,
- programy pozwalające monitorować i analizować tę działalność,
- procesy ciągłego wdrażania tej działalności.

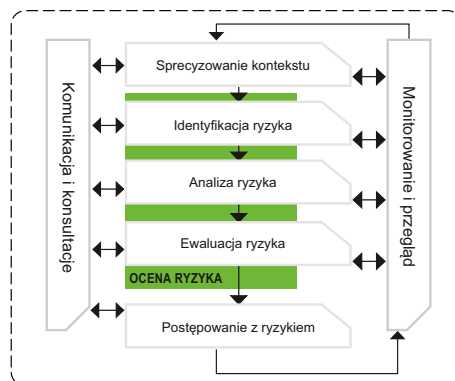
Proces zarządzania ryzykiem jest opisany w normie ISO 31000:2009 i zgodnie z nią powinien być integralną częścią zarządzania¹⁵. Powinien być także zintegrowany z praktyką, kulturą organizacyjną, organizacją społeczeństwa i jego profilem ryzyka. W kontekście zarządzania kryzysowego zarządzanie ryzykiem jest procesem obejmującym postępowanie z ryzykiem będącym wynikiem zdarzeń kryzysowych. Proces zarządzania ryzykiem jest natomiast usystematyzowaną metodą identyfikacji, analizy i ewaluacji ryzyka w ramach całego procesu oceny ryzyka oraz podejmowaniem powtarzalnych, racjonalnych i skutecznych działań w ramach postępowania z ryzykiem, wynikającego z przyjętej strategii zarządzania ryzykiem.



Rys. 2. Struktura ramowa zarządzania ryzykiem

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 9.

¹⁵ Standard zarządzania ryzykiem wyraźnie rozgranicza zarządzanie i decydowanie.



Rys. 3. Ogólny schemat procesu zarządzania ryzykiem

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 9.

Proces zawiera pięć głównych składowych (rys. 3), wspieranych przez komunikowanie i konsultacje oraz monitorowanie i przegląd. Ma zastosowanie w każdej sytuacji, dotyczącej dowolnego zagrożenia.

Zrozumienie (określenie) kontekstu¹⁶ polega na zdefiniowaniu parametrów, w jakich będzie realizowane zarządzanie ryzykiem. Definiuje się je na podstawie możliwości organizacji lub społeczności w całym przekroju zarządzania ryzykiem. Użyteczność tych działań polega na wspólnym zrozumieniu zakresu procesu i kryteriów ryzyka¹⁷, na podstawie których ryzyko zostanie zmierzone. Zrozumienie kontekstu obejmuje szereg działań, w tym: określenie wyniku, celów i zadań, zdefiniowanie zakresów odpowiedzialności, wskazanie kluczowych elementów, zidentyfikowanie kluczowych działań i procesów oraz stosowanych metod. Określenie kontekstu (związków) potwierdza ocena skuteczności procesu, rozważenie decyzji, które trzeba będzie podjąć i wskazanie dostępnych badań, włącznie z oszacowaniem potrzebnych zasobów. Zrozumienie kontekstu jest ważne dla identyfikacji, analizy, ewaluacji ryzyka i kolejnych kroków zarządzania ryzykiem. Zapewnia również, że przyjęte podejście jest dopasowane do celu i odpowiednie dla społeczności i jej profilu ryzyka.

Identyfikacja ryzyka¹⁸ opiera się na bazie informacji odpowiednio wysokiej jakości, wiedzy oraz doświadczeniu kadr i personelu organizacji. Pod uwagę bierze się zarówno zagrożenia, jak i wrażliwość ekspozycji na konkretne ryzyko, które jest badane i opisywane. Rozważane są źródła ryzyka¹⁹, zdarzenia i ich przyczyny, obszary ich wpływu, a także możliwe konsekwencje. Systematyczne i kompleksowe podejście do tych działań zapewnia, że żadne istotne ryzyko nie zostanie

¹⁶ Patrz: definicja na s. 109.

¹⁷ Patrz: definicja na s. 115.

¹⁸ Patrz: definicja na s. 106.

¹⁹ Patrz: definicja na s. 119.

przypadkowo wykluczone. Zwraca się uwagę na udział ekspertów w tworzeniu scenariuszy możliwych zdarzeń kryzysowych. Scenariusze te mogą uwzględniać dane historyczne lub odwzorowywać podobne zdarzenia. Identyfikacja obejmuje wszystkie możliwe ryzyka, bez względu na to, czy są one pod kontrolą, czy nie, a także wszystkie problemy – istniejące i potencjalne, które wymagają rozwiązań w zakresie ograniczenia ryzyka.

Analiza ryzyka²⁰ stanowi ten element procesu zarządzania ryzykiem, który pozwala określić poziom ryzyka²¹. Wiedza, będąca rezultatem analizy ryzyka, jest bardzo ważna dla określenia jego istoty i podjęcia decyzji co do dalszego postępowania. W tej fazie uwzględnia się możliwe konsekwencje, prawdopodobieństwo ich wystąpienia oraz istniejące mechanizmy kontroli, które wpływają na ograniczenie ryzyka. Stopień zaufania do metody określania poziomu ryzyka ocenia się tu, uwzględniając takie czynniki, jak różnorodność opinii ekspertów, niepewność, dostępność, jakość, liczbę oraz przydatność danych i informacji lub ograniczenia w modelowaniu wyników zdarzeń. W tej fazie należy dokonać wartościowania ryzyka przy wykorzystaniu rekomendowanych metod, co umożliwi poddanie ich dalszej klasyfikacji i hierarchizacji²², a najważniejsze z nich objąć właściwą kontrolą.

Ewaluacja ryzyka to etap, w ramach którego poziom ryzyka jest porównywany z kryteriami ryzyka zatwierdzonymi na początku procesu, gdy został ustanowiony kontekst. Wynik i cele samego procesu muszą uwzględniać punkt widzenia wszystkich interesariuszy, jak również brać pod uwagę skumulowany efekt serii zdarzeń, które mogą wystąpić jednocześnie. Podkreśla się również, że ewaluacja ryzyka jest punktem wyjścia do podejmowania decyzji w kwestii dodatkowych analiz ryzyka. Wyniki ewaluacji wskażą, które ryzyko wymaga wzmożonej czujności, a które nie potrzebuje szczególnej uwagi. Pozwala to określić ryzyka, którymi należy się zająć – i w jakim stopniu, oraz te, które mogą być monitorowane i podlegać przeglądowi w ramach istniejących mechanizmów kontroli.

Postępowanie z ryzykiem polega na dokonaniu wyboru i oceny środków w celu modyfikacji ryzyka²³ oraz przygotowaniu i wdrożeniu planów postępowania z ryzykiem, które albo dostarczają nowych środków kontroli, albo modyfikują istniejące. Oznacza to zidentyfikowanie i zaprojektowanie alternatywnych, właściwych działań, ewaluację i ocenę ich wyniku oraz wpływu, a także wdrożenie planów postępowania z ryzykiem. Ważne jest przy tym rozważenie wszystkich bezpośrednich i pośrednich kosztów i korzyści, zarówno materialnych, jak i niematerialnych, dokonując przy tym ich pomiaru w aspekcie finansowym lub pod kątem innego kryterium. Wskazane jest rozważanie kilku opcji postępowania z ryzykiem, razem bądź łącznie. Przedsięwzięcia w zakresie postępowania z ryzykiem obejmują: unikanie,

²⁰ Patrz: definicja na s. 109.

²¹ Patrz: definicja na s. 115.

²² Patrz: definicja na s. 154.

²³ Modyfikacja ryzyka – działania podejmowane samodzielnie lub w kombinacji w celu ograniczenia ryzyka. Źródło: opracowanie autorskie.

podjęcie lub zwiększenie ryzyka, usunięcie źródła ryzyka, zmianę (konsekwencji lub prawdopodobieństwa), optymalizację, przeniesienie, dzielenie oraz zatrzymanie ryzyka. Wdrożenie procesu postępowania z ryzykiem oznacza, że dane ryzyko musi zostać włączone do zestawu stałego monitorowania i przeglądu.

Komunikacja i konsultacje²⁴ dotyczą wszystkich wewnętrznych i zewnętrznych interesariuszy na wszystkich etapach procesu zarządzania ryzykiem i stanowią jego nierozłączny, podstawowy element. Ważne jest, by upewnić się, że wszyscy ci, którzy powinni być zaangażowani w te działania (m.in. osoby odpowiedzialne za konkretny proces lub jego wynik), są nie tylko informowani, ale także włączani do udziału w tym procesie, aby mogli zrozumieć, jak podejmowane są decyzje.

Monitorowanie²⁵ i przegląd²⁶ to jedne z najważniejszych czynników zarządzania ryzykiem i są działaniem permanentnym. Pozwalają potwierdzić skuteczność istniejących mechanizmów kontroli lub ją zakwestionować. Monitorowanie i przegląd kończą cykl zarządzania ryzykiem i stanowią dopełnienie słuszności przyjętych metod, źródeł danych, rezultatów i przyczyn podejmowanych decyzji, które podlegają regularnej kontroli. Regularność i systematyczność kontroli ryzyka pozwala utrzymać aktualne plany działania. Pomocne na tym etapie mogą być działania prowadzone w różnych obszarach aktywności, np. systemie ubezpieczeń. Rezultaty kontroli z kolei są pomocne w analizie ryzyka oraz w całym procesie oceny ryzyka. Pozwalają określić wpływ wrażliwości ekspozycji na poziom ryzyka i ocenić skuteczność podejmowanych działań w tym zakresie. Monitoruje się również zmiany w otoczeniu, zagrożenia i inne zdarzenia niekorzystne. Wymaga się, aby odpowiedzialność za kontrolę i monitoring była jasno zdefiniowana, a wszystkie działania dokumentowane i okresowo lub w zależności od sytuacji rejestrowane i raportowane w ramach procesu przeglądu zarządzania ryzykiem.

1.2. Opis procesu zarządzania ryzykiem

Metodyka oceny ryzyka to ogół zasad (metod) stosowanych w tym procesie, system jasno sprecyzowanych reguł i procedur pomocnych w ocenie ryzyka. Proces ten pod wpływem doświadczeń jest ciągle doskonalony.

Metodyka oceny ryzyka jest zintegrowana w procesie zarządzania ryzykiem. Takie podejście determinuje uzyskanie ostatecznego efektu, czyli oceny ryzyka w drodze realizacji algorytmów i przestrzegania wymaganych procedur postępowania z ryzykiem.

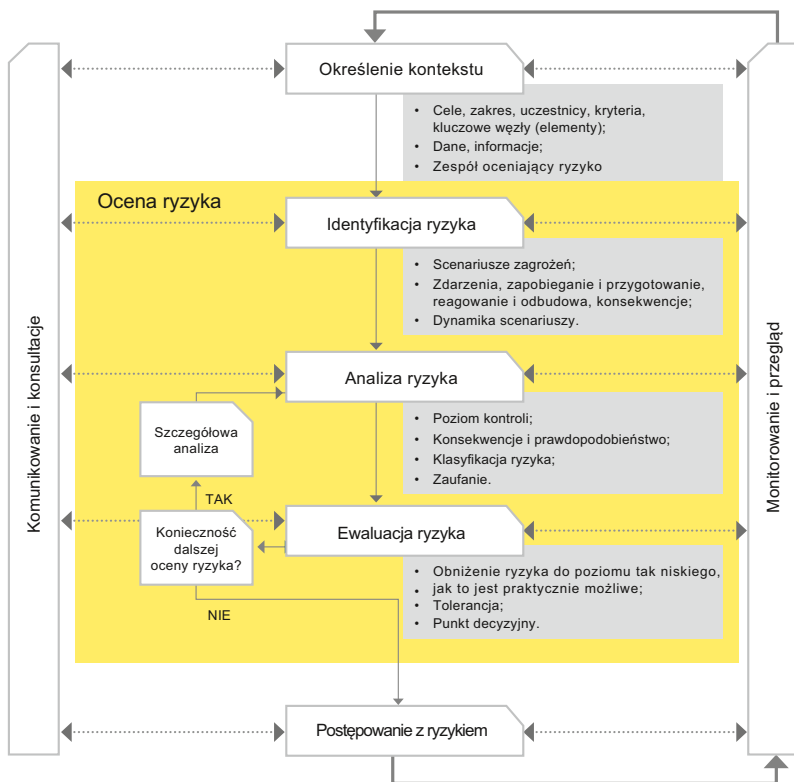
Metodyka australijska jest w całości zgodna z normą zarządzania ryzykiem ISO 31000:2009, co daje gwarancję, że ocena ryzyka może prowadzić do decyzji o podjęciu dalszych analiz, w razie istnienia takiej potrzeby (rys. 4). Punktem wyjścia

²⁴ Patrz: definicja na s. 116.

²⁵ Patrz: definicja na s. 113.

²⁶ Patrz: definicja na s. 113.

do podejmowania decyzji jest wprowadzenie elementu metodycznego określającego stopień zaufania do wyniku ewaluacji ryzyka i w konsekwencji uzyskanej oceny. Ważne jest przy tym, że przyjęcie decyzji w związku z koniecznością realizacji dodatkowej analizy wiąże się z konkretną oceną sytuacji. Jeżeli szacunki wskazują na wyjątkowo wysoki poziom potencjalnych strat związanych z konkretnym zdarzeniem niekorzystnym lub wysoki poziom kosztów koniecznych dla obniżenia ryzyka do poziomu dopuszczalnego lub tolerowanego, podjęcie decyzji o szczegółowej analizie jest koniecznością.



Rys. 4. Metodyka oceny ryzyka wystąpienia zdarzeń niekorzystnych

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 13.

Metodyka oceny ryzyka prezentowana jest jako dwuetapowe podejście do tej działalności, polegające na zbudowaniu jakościowej bazy oceny, która może być uzupełniona analizami różnych szczebli decyzyjnych, jeżeli wyniknie taka potrzeba.

1. Ocena bazowa w celu identyfikacji i szybkiego ukazania ryzyka. Ocena ta będzie stosunkowo prosta, jednak procedury mogą zostać przeprowadzone przez osoby o zróżnicowanym poziomie umiejętności technicznych i dysponujące czasem w różnym wymiarze.

2. Szczegółowa analiza (gdym jest konieczna) wzmacnia zaufanie do oceny w ogóle i pozwala sporządzić dokładną klasyfikację ryzyka, a także dokonać ewaluacji ryzyka i opracowania projektu wdrażania strategii postępowania z ryzykiem. Szczegółowa analiza może jednak wymagać specjalnych metod w postaci wykorzystania rekomendowanych modeli lub scenariuszy zdarzeń. Znaczną ich część przedstawiono w rozdziale 2 części I publikacji.

Ponieważ takie podejście pozwala na skalowanie przestrzenne, metodyka może być stosowana na wszystkich szczeblach administracyjnych. Inne kluczowe cechy metodyki wymienione są poniżej:

- stosowanie scenariuszy zdarzeń w całym procesie oceny ryzyka,
- usystematyzowane podejście do identyfikacji mechanizmów kontroli i możliwość zastosowania adekwatnych rozwiązań – przyjęcie takich rozwiązań pozwala na lepsze zrozumienie ewentualnego wpływu na społeczeństwo pojedynczego lub wielu zagrożeń i zastosowanie ścieżek wyjścia od zagrożeń do konsekwencji, umożliwiając szybką identyfikację właściwych przedsięwzięć w zakresie postępowania z ryzykiem,
- dobór ryzyka w zakresie wiarygodnego poziomu konsekwencji dla określonego ryzyka – dobór prawdopodobieństwa w zakresie wiarygodnych konsekwencji pozwala zrozumieć profil ryzyka danej społeczności lub organizacji w odniesieniu do poszczególnych źródeł ryzyka,
- wystandaryzowane zestawienie opisu konsekwencji i prawdopodobieństw do zastosowania przez wszystkich użytkowników; takie podejście pozwala uzyskać spójne wyniki w formie klasyfikacji zidentyfikowanych ryzyk z określeniem ścieżek krytycznych i środków postępowania z ryzykiem,
- zastosowanie mechanizmu wyznaczania stopnia zaufania do procesu oceny ryzyka w celu zidentyfikowania i określenia niepewności oraz wzmocnienia procesu podejmowania decyzji w zakresie potrzeb szczegółowej analizy ryzyka lub wyboru środków postępowania z ryzykiem; ten mechanizm pomaga uniknąć błędnych rezultatów, wynikających np. z subiektywnego postrzegania,
- wystandaryzowane zestawienie matryc tolerancji, co może znaleźć zastosowanie u wszystkich uczestników procesu oceny ryzyka; pomaga to oszacować ryzyko w różnym stopniu zaufania i pewności.

Ocena ryzyka według wytycznych obowiązujących w Australii jest najbardziej efektywna, gdy jest realizowana w formie warsztatów, podczas których uczestnicy (sektor publiczny, prywatny, organizacje pozarządowe, przedstawiciele społeczności i niektóre osoby – autorytety, jednostkowo) prezentują zagadnienia kluczowe dla sporządzenia wszechstronnej listy ryzyk, wynikających z bieżącej działalności i zdarzeń kryzysowych – potencjalnych źródeł zagrożeń.

Przygotowania do warsztatów są kierowane przez kontekst, który będzie musiał zostać ustalony przed oceną. Aby zapewnić maksymalną efektywność procesu, każdy członek zespołu musi zrozumieć tło oceny, specyfikę właściwego scenariusza

awaryjnego, podejście warsztatowe i jego rolę w procesie. Dlatego też, po starannym przygotowaniu oceny, warsztaty muszą podsumować podjęte decyzje, kiedy został ustanowiony kontekst, a gromadzone i weryfikowane informacje wpłynęły na rozwój potencjału oddziaływania. Zrozumienie tych uwarunkowań w poważnym stopniu przybliży cały zespół do zamierzonego celu, czyli w miarę obiektywnej oceny ryzyka.

Same warsztaty powinny zapewnić:

- zgromadzenie wiedzy specjalistycznej odpowiadającej zakresowi tematu warsztatów,
- prawidłowość zastosowania oraz dyscyplinę w przebiegu procesu oceny ryzyka,
- dostęp do właściwych informacji i baz danych (jeszcze przed warsztatami),
- kreatywność i zaangażowanie podmiotów oraz środowiska w ramach prac zespołów studyjnych.

Podkreślono, że prowadzący warsztaty powinien być doświadczoną, obiektywną osobą, która nie jest zaangażowana w szczegóły tematu i nie należy zespołu badawczego. Pozwoli to zwiększyć obiektywność i pomóc w rozwiązywaniu kolejnych zagadnień.

Warsztaty powinny skutkować: pogłębieniem wiedzy o poszczególnych etapach oceny ryzyka, zdobywaniem doświadczenia w rozwiązywaniu złożonych zagadnień w ramach analizowanych scenariuszy zagrożeń, doskonaleniem pracy zespołowej, przygotowaniem personelu – zarówno uczestników warsztatów, jak i obserwatorów.

Proces oceny ryzyka według wytycznych australijskich w praktyce prowadzony jest według algorytmu. Określone działania są wykonywane w ściśle sprecyzowanej kolejności, a realizacja kolejnego jest kontynuacją poprzedniego. Proces oceny ryzyka poprzedza określenie kontekstu (związków). To pierwszy krok w kierunku oceny ryzyka, a jego rzetelna realizacja będzie miała wpływ na rezultaty oceny. Określenie kontekstu pozwala sprecyzować cele organizacji i opisać zarówno wewnętrzne, jak i zewnętrzne otoczenie brane pod uwagę podczas oceny ryzyka. Na tym etapie określa się kryteria ryzyka i przyjmuje poziomy ryzyka (dopuszczalny, tolerowany i inne, jeżeli jest taka potrzeba). Określając kontekst, trzeba akcentować przede wszystkim zapewnienie osiągnięcia celów organizacji czy społeczeństwa. Ocenia się przy tym możliwość realizacji zadań i kluczowych elementów, niezbędnych do przeprowadzenia badań ryzyka przed jego właściwą oceną.

Na etapie określenia kontekstu właściciele procesu powinni rozważyć właściwości i uwarunkowania środowiska, uwzględniając: geografię, klimat, populację, przemysł, niezbędne usługi i infrastrukturę krytyczną, a na drugim biegunie – gotowość kryzysową²⁷ czy możliwości sprostania potencjalnym zagrożeniom. Wspólne zrozumienie celów tej oceny jest najważniejsze dla zapewnienia, że wszystkie istotne ryzyka zostały uwzględnione. Potwierdzenie celów będzie wspierało inne aspekty

²⁷ Gotowość kryzysowa państwa – oznacza stan zorganizowania państwa, wszystkich jego struktur, władz, ludności i terenu do sprostania każdej katastrofie z wojną włącznie. Adekwatną do zagrożeń gotowość kryzysową państwa zapewnia wysoki potencjał bezpieczeństwa. Organizacyjnie obejmuje dyplomację i gotowość obronną w składzie gotowości cywilnej i militarnej. Źródło: J. Gołębiowski, *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, SA PSP, Kraków 2011, s. 339–340.

etapu ustalania kontekstu: określenie zakresu, identyfikację interesariuszy oraz określenie kluczowych elementów na potrzeby oceny ryzyka.

Określenie potrzebnych danych wymaga odpowiedniego uwzględnienia zakresu oceny ryzyka. Ponieważ zarządzanie ryzykiem zdarzeń kryzysowych może dotyczyć wielu zagrożeń, opis zakresu powinien obejmować szereg zagrożeń dla jednego lub większej liczby zdarzeń, które są istotne dla organizacji bądź społeczności, wraz z ich ramami czasowymi, prawnymi oraz granicami geograficznymi.

Zarządzanie ryzykiem w kontekście danego państwa dotyczy wszystkich zagrożeń w granicach administracyjnych, a w pewnym stopniu również poza tymi granicami. Oznacza to, że należy wziąć pod uwagę wszystkie zdarzenia, które mogą być źródłem zagrożeń dla społeczeństwa o określonym stopniu podatności.

Kolejnym zagadnieniem jest sprecyzowanie kryteriów ryzyka, które wykorzystuje się podczas analizy i ewaluacji ryzyka. Zalicza się do nich:

- definicje konsekwencji (charakter i rodzaj oraz sposób pomiaru),
- definicje prawdopodobieństw (rodzaj oraz sposób pomiaru),
- kategorie poziomu ryzyka (sposób ustalenia),
- definicje stopnia ufności,
- kategorie ewaluacji (określenie poziomu ryzyka akceptowalnego lub tolerowanego).

Kryteria (opublikowane w *Narodowych Wytocznych Oceny Ryzyka Zdarzeń Kryzysowych*²⁸) stanowią bazę do oceny ryzyka, która powinna być wykorzystywana podczas rozważania każdego kryterium.

Bardzo ważnym zagadnieniem jest określenie elementów kluczowych, które zapewnią wysoką efektywność całego procesu oceny ryzyka. Powinny być one dobrane zgodnie z zakresem i stanowić przedmiot najwyższej uwagi zespołu oceniającego ryzyko. Te elementy to przede wszystkim: źródła ryzyka, rodzaje konsekwencji, wrażliwość ekspozycji, podatność społeczeństwa. Elementy kluczowe bądź ich podzbiory powinny być możliwe do zdefiniowania, by umożliwić identyfikację każdego istotnego ryzyka.

Proces oceny ryzyka

Pierwszym krokiem oceny ryzyka jest jego identyfikacja, obejmująca zdefiniowanie źródeł ryzyka, zdarzeń niekorzystnych i potencjalnych konsekwencji. W tym procesie wykorzystuje się informacje historyczne, wiedzę zatrudnionego personelu, wiedzę ekspertów, analizy obliczeniowe, opinie specjalistów, doświadczenie ludzi starszych i potrzeby odbiorców (społeczeństwa). Ujawnia się przy tym dynamika scenariuszy potencjalnych sytuacji kryzysowych. Znaczącym ułatwieniem są bazy danych oraz wcześniej przygotowane materiały do wykorzystania podczas warsztatów.

Na etapie identyfikacji ryzyka wykorzystuje się wszystkie dostępne informacje, prezentacje, wiedzę, doświadczenie i materiały zebrane w inny sposób, np. badania ankietowe społeczeństwa. Dużą pomocą może być otwarta dyskusja prowadzona

²⁸ Opublikowane w Australii w 2010 r.

w formie zorganizowanej lub w mediach²⁹. Dyskusje mogą się toczyć na różnych poziomach wiedzy, doświadczenia, przygotowania i w różnych perspektywach, a niekiedy i w obszarze różnych interesów – w celu zebrania możliwie najbardziej wszechstronnego materiału na potrzeby interpretacji wniosków.

W identyfikacji ryzyka istotne jest ujawnienie powiązań źródeł ryzyka i konsekwencji potencjalnych zagrożeń. Przydatne narzędzie stanowi diagram muchy i rejestr ryzyka (tabela 1).

Tabela 1. Rejestr ryzyka (przykład)

Nr ryzyka	Ryzyko	Źródło	Kategoria	Fazy zarządzania kryzysowego	
				zapobieganie/ przygotowanie	reagowanie/ odbudowa
1	możliwość wystąpienia powodzi w regionie...	duże opady deszczu	ludzie infrastruktura	spuścić wodę ze zbiorników, wzmocnić wały	gotowość, wnioski, poprawność planów
2	możliwość gołoledzi...	poważne oziębienie	ludzie	umowy, plany, służby	gotowość, wnioski, weryfikacja
itd.					

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 27.

Rekomenduje się wykorzystanie diagramu muchy, w którym ujęte zostają źródła ryzyka, ich charakter, przyczyny (warunki wystąpienia zagrożenia), skala (wypadek, incydent, katastrofa), kategoria (wpływ dla ludzi, środowiska, infrastruktury, gospodarki, administracji, społeczności) oraz środki kontroli umożliwiające ograniczenie ryzyka (bariery).

Następnie sporządza się rejestr ryzyka, podając źródło, kategorię i konsekwencje, np. potencjalna powódź spowodowana nadmiernymi opadami... może wystąpić w dorzeczu... na obszarze (a) ha, zatapiając (b) miejscowości, w tym (c) miasteczek i (d) większych miast. Pod wodą może znaleźć się (e) zakładów przemysłowych, w tym..., (f) oczyszczalni ścieków, (g) stacji paliw i (h) składów śmieci. Powódź może objąć (i) ha upraw rolników, (j) lasów i (k) nieużytków. Uszkodzeniu może ulec (l) km dróg, w tym (m) autostrad i dróg szybkiego ruchu, (n) mostów, w tym (o) kolejowych itd. Przewiduje się, że powódź może spowodować straty w wysokości (xx) mln zł, w tym w produkcji..., w rolnictwie..., infrastrukturze..., środowisku..., ochronie zdrowia..., handlu..., szkolnictwie... itd. Zastosowanie prostych przedsięwzięć

²⁹ Dyskusja w mediach jest bardzo ważnym elementem komunikacji kryzysowej. Rola mediów w kreowaniu bezpieczeństwa ma dziś dwoisty charakter. Przede wszystkim media zapewniają możliwość szybkiego rozprzestrzenienia się informacji, co ma wpływ na skuteczne ostrzeganie i alarmowanie ludności. Wspomagają również zapobieganie zagrożeniom poprzez edukację. Z drugiej jednak strony, poprzez rozposzechnienie niezaweryfikowanej informacji, same mogą doprowadzić do trudnego do opanowania kryzysu.

zapobiegawczych i odpowiedniej gotowości może ograniczyć straty w (y) %. Należy przedsięwziąć natychmiast... oraz zapewnić gotowość następujących ogniw systemu... itd. (dla każdego zagrożenia ta treść może być inna, zależna od wielu czynników). W zakończeniu powinno się określić formy prowadzenie skutecznych kontroli: rutynowe, proceduralne lub systemowe określając zakres każdej z proponowanych.

Drugim poważnym przedsięwzięciem procesu oceny ryzyka jest analiza ryzyka. Jest to działalność praktyczna i usystematyzowana, pozwalająca zrozumieć otoczenie i przewidzieć poziom ryzyka. Podczas analizy wykorzystuje się wcześniej sporządzone tzw. diagramy muchy, rejestry ryzyka, tablice, matryce i wystandaryzowane kryteria ryzyka w ramach *Narodowych Wytycznych Oceny Ryzyka Zdarzeń Kryzysowych*. Wybór metody analizy ryzyka jest wcześniej określony przez kontekst, dostępne źródła informacji i zastosowany sposób ich obiegu. Zazwyczaj stosuje się metody ilościowe, jakościowe lub ilościowo-jakościowe, rzadziej półilościowe.

Metody jakościowe polegają na wykorzystaniu tablic, matryc, nomogramów i wykresów. Ilościowe angażują matematyków, wymagają uruchomienia programów, kalkulacji i przeliczeń, które pozwolą określić i zrozumieć wiele parametrów ryzyka prezentowanych liczbowo. Doświadczenie potwierdza, że częściej wykorzystuje się metody jakościowe, ponieważ są bardziej praktyczne, zdecydowanie prostsze i bazują na ściśle sprecyzowanych procedurach.

W tabeli 2 przedstawiono rodzaje prawdopodobieństwa będące punktem odniesienia dla oceny ryzyka zdarzeń kryzysowych. Opisana została częstotliwość zdarzenia i prawdopodobieństwo jego konsekwencji. W zestawieniu ujęto także wystąpienie źródła ryzyka i poszczególnych konsekwencji w zakresie średniego interwału ponownego wystąpienia i rocznego prawdopodobieństwa nasilenia.

Tabela 2. Tabela prawdopodobieństwa

Poziom prawdopodobieństwa	Częstotliwość	Średni cykl nawrotu	Roczne prawdopodobieństwo nasilenia
prawie pewne	raz lub więcej na rok	< 3 lat	> 0,3
prawdopodobne	raz na 10 lat	3–30 lat	0,031–0,3
możliwe	raz na 100 lat	31–300 lat	0,0031–0,03
mało prawdopodobne	raz na 1000 lat	301–3000 lat	0,00031–0,003
rzadkie	raz na 10 000 lat	3001–30 000 lat	0,000031–0,0003
bardzo rzadkie	raz na 100 000 lat	30.001–300 000 lat	0,0000031–0,00003
niewiarygodne	mniej niż raz na 1 mln lat	>300 000 lat	<0,0000031

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 33.

Perspektywa 1% rocznego prawdopodobieństwa nasilenia oznacza, że dane wydarzenie ma 1% szans wystąpienia lub nasilenia każdego roku. Podczas gdy wydłuża się czas, szansa wystąpienia lub nasilenia zdarzenia o takiej skali wzrasta, jak wskazano w tabeli 3. Istnieje również możliwość wystąpienia więcej niż jednego z tych zdarzeń kryzysowych w tym samym roku. Tabela zawiera podsumowanie prawdopodobieństwa wystąpienia zdarzeń dla 1% rocznego prawdopodobieństwa nasilenia w różnych przedziałach czasowych.

Tabela 3. Procentowy rozkład prawdopodobieństwa nasilenia w latach przy szansie 1%

Roczne prawdopodobieństwo nasilenia dla szansy wynoszącej 1%	W roku	W okresie 10 lat	W okresie 50 lat	W okresie 100 lat
nie wystąpi	99%	90,4%	60,5%	36,6%
tylko raz	1%	9,1%	30,5%	37,0%
dwa razy	–	0,4%	7,6%	18,5%
trzy razy	–	0,01%	1,2%	6,1%
więcej niż trzy razy	–	–	0,2%	1,8%

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 34.

Matryca ryzyka (tabela 4) prezentuje kombinację konsekwencji zdarzenia i jego prawdopodobieństwa służącą określeniu poziomu ryzyka. Poziom ryzyka wraz z ufnością w całym procesie oceny i innymi czynnikami określa potrzebę szczegółowej analizy i informuje o postępowaniu z ryzykiem. Dzięki wykorzystaniu matrycy ryzyka wszystkie poziomy ryzyka są odnotowywane w rejestrze ryzyka.

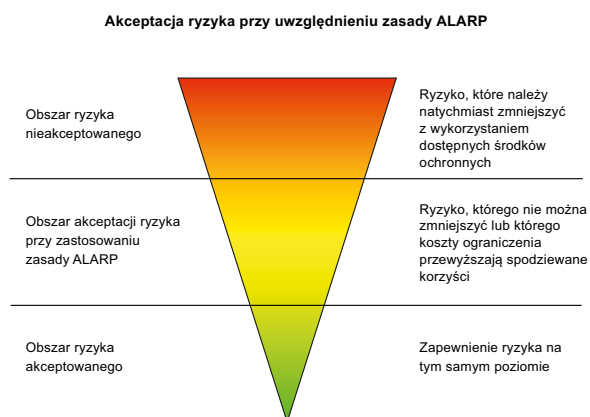
Tabela 4. Matryca ryzyka

Prawdopodobieństwo	Konsekwencje				
	nieznaczne	małe	średnie	wysokie	katastrofalne
prawie pewne	średni	średni	wysoki	ekstremalny	ekstremalny
prawdopodobne	niski	średni	wysoki	wysoki	ekstremalny
możliwe	niski	niski	średni	wysoki	wysoki
nieprawdopodobne	niski	niski	średni	średni	wysoki
rzadkie	niski	niski	niski	średni	średni
bardzo rzadkie	niski	niski	niski	niski	średni
niewiarygodne	niski	niski	niski	niski	niski

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 35.

Trzeci w kolejności krok oceny ryzyka stanowi ewaluacja. Jest to działanie polegające na porównaniu wyniku analizy ryzyka z przyjętymi kryteriami w celu zakwalifikowania ryzyka do odpowiedniej kategorii (poziomu ryzyka akceptowalnego, tolerowanego, nietolerowanego). Celem nadrzędnym jest dostarczenie danych

stanowiących podstawę do podjęcia decyzji o dalszym postępowaniu z ryzykiem (pozostawić, czy zajmować się nim, a jeżeli tak, to w jakim zakresie). Ewaluacja ryzyka jest podsumowaniem dotychczasowych działań (identyfikacji i analizy) i wskazaniem, którym ryzykiem czy grupą ryzyk zajmować się dalej, a które wymagają wyłącznie dotychczasowych środków kontroli. Ewaluacja, tak jak identyfikacja i analiza, zależy od wiarygodności zebranych informacji³⁰. Zgodnie z zasadą ALARP (rys. 5) ryzyko akceptowalne powinno trafić do poziomu szeroko akceptowanego ryzyka na wykresie ALARP. Niektóre ryzyka mogą być tolerowane, pod warunkiem, że są tak niskie, jak to praktycznie możliwe i wchodzą do poziomu tolerowanego (z zastrzeżeniem ALARP).



Źródło: <http://www.ryzykozawodoweonline.pl/proces-oceny-ryzyka-id64.html>, [dostęp: marzec 2015].

Dwoma czynnikami, które należy uwzględnić przy określaniu, czy ryzyko jest nietolerowane, tolerowane z zastrzeżeniem ALARP lub szeroko akceptowane, są ocena ryzyka oraz stopień ufności. Ich powiązanie przedstawiono na matrycach tolerancji (tabela 5, 6, 7). Poszczególne matryce tolerancji należy stosować w zależności od stopnia ufności dla konkretnego ryzyka.

Tabela 5. Ewaluacja ryzyka – wysoki poziom wiarygodności

Poziom prawdopodobieństwa	Poziom konsekwencji				
	nieznaczny	mały	średni	wysoki	katastrofalny
prawie pewne	tolerowane	tolerowane	tolerowane	nietolerowane	nietolerowane
prawdopodobne	akceptowane	tolerowane	tolerowane	tolerowane	nietolerowane

³⁰ Kryteria informacji opisano w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 1 *Zarządzanie ryzykiem według normy ISO 31000*, podrozdział 1.4 *Proces zarządzania ryzykiem*.

Poziom prawdopodobieństwa	Poziom konsekwencji				
	nieznaczny	mały	średni	wysoki	katastrofalny
możliwe	akceptowane	akceptowane	tolerowane	tolerowane	tolerowane
nieprawdopodobne	akceptowane	akceptowane	tolerowane	tolerowane	tolerowane
rzadkie	akceptowane	akceptowane	akceptowane	tolerowane	tolerowane
bardzo rzadkie	akceptowane	akceptowane	akceptowane	akceptowane	tolerowane
niewiarygodne	akceptowane	akceptowane	akceptowane	akceptowane	akceptowane

Źródło: Opracowanie własne na podstawie State Emergency Service, *National...*, dz. cyt., s. 40.

Tabela 6. Ewaluacja ryzyka – średni poziom wiarygodności

Poziom prawdopodobieństwa	Poziom konsekwencji				
	nieznaczny	mały	średni	wysoki	katastrofalny
prawie pewne	tolerowane	tolerowane	nietolerowane	nietolerowane	nietolerowane
prawdopodobne	tolerowane	tolerowane	tolerowane	nietolerowane	nietolerowane
możliwe	akceptowane	tolerowane	tolerowane	tolerowane	nietolerowane
nieprawdopodobne	akceptowane	akceptowane	tolerowane	tolerowane	tolerowane
rzadkie	akceptowane	akceptowane	tolerowane	tolerowane	tolerowane
bardzo rzadkie	akceptowane	akceptowane	akceptowane	tolerowane	tolerowane
niewiarygodne	akceptowane	akceptowane	akceptowane	akceptowane	tolerowane

Źródło: Tamże.

Tabela 7. Ewaluacja ryzyka – niski poziom wiarygodności

Poziom prawdopodobieństwa	Poziom konsekwencji				
	nieznaczny	mały	średni	wysoki	katastrofalny
prawie pewne	tolerowane	tolerowane	nietolerowane	nietolerowane	nietolerowane
prawdopodobne	tolerowane	tolerowane	nietolerowane	nietolerowane	nietolerowane
możliwe	tolerowane	tolerowane	tolerowane	nietolerowane	nietolerowane
nieprawdopodobne	akceptowane	tolerowane	tolerowane	tolerowane	nietolerowane
rzadkie	akceptowane	akceptowane	tolerowane	tolerowane	tolerowane
bardzo rzadkie	akceptowane	akceptowane	tolerowane	tolerowane	tolerowane
niewiarygodne	akceptowane	akceptowane	akceptowane	tolerowane	tolerowane

Źródło: Tamże.

Ostatnim krokiem oceny ryzyka, a właściwie jej rezultatem, jest podjęcie decyzji o dalszym postępowaniu z ryzykiem. Punkt decyzyjny wynika z rejestru ryzyka, który powstał w wyniku oceny ryzyka i jest stale aktualizowany. Decyzja jest tylko aktem zatwierdzenia wybranej metody postępowania z ryzykiem. Przede wszystkim decyduje się o tym, które ryzyka wymagają pogłębionej analizy, a to może wynikać z różnych przyczyn: dynamiki zmian w otoczeniu, w organizacji, zmian priorytetów, ale przede wszystkim ze zbyt wysokiego poziomu niepewności, niskiego stopnia zaufania do informacji czy do oceniających, nadmiernych konsekwencji wystąpienia zdarzenia lub kosztów modelowania ryzyka. Na ostateczną decyzję umożliwiającą postępowanie z ryzykiem składa się wiele zmiennych, które mają wpływ na dobór odpowiednich kryteriów, np. zmiana kategorii wiarygodności informacji (tabela 5–7).

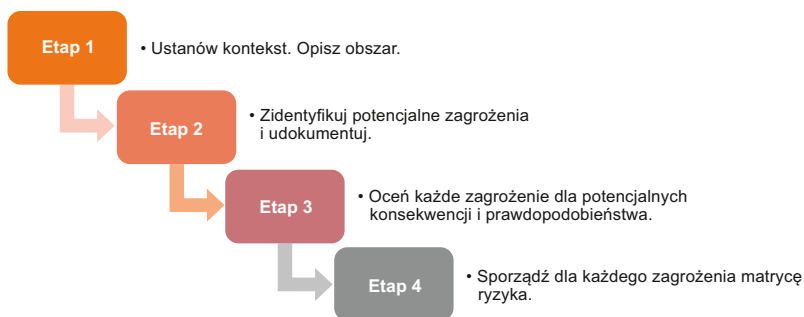
2. ZARZĄDZANIE RYZYKIEM W IRLANDII

W ostatnich latach w Irlandii opracowano na potrzeby zarządzania kryzysowego, w tym planowania cywilnego, dwa zasadnicze dokumenty: *Ramy zarządzania poważnymi sytuacjami kryzysowymi* oraz *Narodową ocenę ryzyka Irlandii*¹. Pierwszy dokument, o charakterze wytycznych, obszernie opisuje zakres oraz formę przeprowadzania przez organy właściwe w sprawach zarządzania kryzysowego procesu oceny występujących zagrożeń. Drugi dokument uwzględnia wyniki oceny ryzyka na szczeblu krajowym, przeprowadzonej zgodnie z wypracowaną metodyką.

W niniejszym rozdziale zaprezentowano irlandzkie doświadczenia w zakresie wypracowania i zastosowania elementów procesu zarządzania ryzykiem. Celem rozważań było wskazanie cennych praktyk tego i podkreślenie zalet przyjętego podejścia.

2.1. Ramy zarządzania poważnymi sytuacjami kryzysowymi

Narodowa ocena ryzyka Irlandii została przygotowana zgodnie z metodyką opisaną w dokumencie *A Framework for Major Emergency Management* z 2010 r. Obejmuje ona cztery etapy (rys. 1):



Rys. 1. Schemat procesu oceny ryzyka

Źródło: Opracowanie własne na podstawie *A Framework...*, dz. cyt., s. 21.

¹ Ramy zarządzania poważnymi sytuacjami kryzysowymi stanowią istotny punkt odniesienia w zakresie realizacji przez rząd Irlandii procesu oceny ryzyka w kontekście zdarzeń kryzysowych. *Narodowa ocena ryzyka* stanowi zaś wynik zastosowania powyższej metodyki.

Przedstawiony powyżej schemat procesu oceny ryzyka² w metodyce irlandzkiej zawiera trzy podstawowe elementy tego podprocesu, występującego w normie ISO 31000 jako komponent procesu zarządzania ryzykiem. Są to: w etapie drugim – identyfikacja ryzyka³, w etapie trzecim – analiza ryzyka⁴ oraz w etapie czwartym – ewaluacja ryzyka⁵. W irlandzkim procesie oceny ryzyka jako pierwszy etap oceny wykorzystano ustalenie kontekstu, który stanowi pierwszy krok w procesie zarządzania ryzykiem zawartym w normie.

Cel pierwszego etapu stanowi opisanie terenu/obszaru, dla którego przygotowuje się ocenę ryzyka. Jest to istotny element, ponieważ podczas jego realizacji dochodzi do określenia (zrozumienia), jaka jest jego podatność⁶ i odporność⁷ w sytuacji zagrożenia. Zadanie to, podobnie jak w poprzednich przykładach, jest realizowane przez zespół ekspertów.

Proces rozpoczyna się od ustalenia warunków, w których podejmuje się ocenę ryzyka (stan wyjściowy/wejście). Jednym z założeń jest wskazanie, że zespół wykonujący analizę powinien brać pod uwagę krajowe, regionalne i lokalne warunki mające wpływ na zarządzanie kryzysowe w ich okolicy (na obszarze administrowanym przez organ, na rzecz którego zespół pracuje). Istotne jest także, aby zespół w trakcie badania mógł nawiązać współpracę z podmiotami mogącymi zapewnić mu pomoc i dostarczyć niezbędnych informacji w procesie analizy ryzyka takimi jak: straż pożarna, inspektor ochrony środowiska czy instytucje sanitarne. Dokument zwraca uwagę, że w tej fazie należy wziąć pod uwagę czynniki: społeczne, środowiskowe, przemysłowe (infrastruktura) oraz lokalizację potencjalnych zagrożeń.

Drugi etap to identyfikacja zagrożeń⁸. Część zagrożeń jest zdefiniowana z góry i traktowana jako pewnik występujący w każdym regionie (pożary, wypadki drogowe itp.). Niemniej jednak zaleca się, aby w analizie skupiać się na co najmniej dużych zagrożeniach, czyli obejmujących zdarzenia nierutynowe, w których podejmowane przez służby działania wymagają uruchomienia znacznych sił i środków. Celem na tym etapie jest dokonanie przeglądu i określenie ogólnych/typowych zagrożeń, a następnie dodanie tych, które są charakterystyczne dla danego regionu. Generalnie zagrożenia podzielić można na cztery rodzaje:

- naturalne,
- w transporcie,

² Patrz: definicja na s. 107.

³ Patrz: definicja na s. 106.

⁴ Patrz: definicja na s. 109.

⁵ Patrz: definicja na s. 114.

⁶ Podatność – patrz: część II *Zarządzanie ryzykiem na szczeblu UE*, rozdział 5 *Zarządzanie ryzykiem nielegalnej imigracji* – FRONTEX, s. 208.

⁷ Odporność – termin stosowany do opisu nieodłącznej zdolności społeczności, służb i infrastruktury oparcia się konsekwencjom zdarzenia i przywrócenia stanu normalności. Źródło: A Framework..., dz. cyt., s. 29. Por.: definicja, s. 115.

⁸ Por.: identyfikacja ryzyka wg PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem* – Terminologia.

- technologiczne,
- cywilne⁹.

Do każdego zidentyfikowanego zagrożenia w kolejnym kroku przypisuje się podmioty, które są na nie narażone.

Etap trzeci – ocena ryzyka to faza, w której zespół podejmuje się rozważenia całościowego ryzyka związanego ze zdefiniowanymi uprzednio zagrożeniami. Podproces ten odpowiada działaniom prowadzonym w ramach analizy ryzyka, zgodnie z normą ISO 31000. Ocena ryzyka rozpoczyna się od analizy potencjalnego wpływu (dotkliwość skutków dla życia i zdrowia, mienia i infrastruktury oraz ochrony środowiska) stwierdzonych zagrożeń. Prawdopodobieństwo wystąpienia zagrożenia należy rozważyć i przedstawić na macierzy.

Rodzaj i charakter zjawiska może być rozpatrywany w trzech aspektach:

- wpływu na życie, zdrowie i dobrobytu społeczności,
- wpływu na gospodarkę w zakresie kosztów/zniszczeń infrastruktury, jak również kosztów odbudowy lub utraty produkcji gospodarczej,
- społecznych/oddziaływania na środowisko.

W uwagach metodyka wskazuje, jak ważne jest uwzględnienie możliwości eskalacji zdarzenia lub jego kombinacji z innymi zagrożeniami. Mimo tego zastrzeżenia i tak wszystkie wyniki analizy pozostają jedynie subiektywnymi ocenami specjalistów / członków zespołu. Metodyka nie zakłada stosowania żadnych matematycznych rozwiązań związanych z rachunkiem prawdopodobieństwa (analizą ilościową).

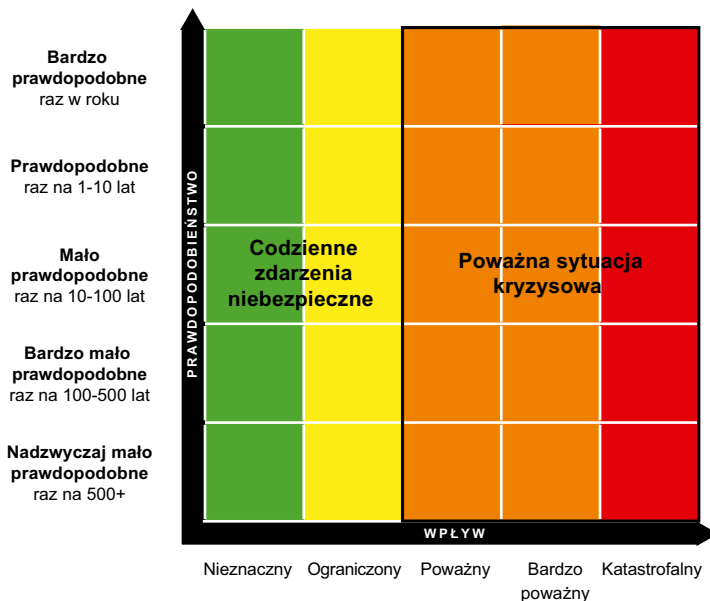
Podobnie jak w przypadku kilku innych metodyk stosowanych przez poszczególne państwa, w ostatnim – czwartym etapie następuje prezentacja wyników poprzez umieszczenie każdego z zagrożeń na macierzy ryzyka (5 x 5), uwzględniającej prawdopodobieństwo wystąpienia zdarzenia (od bardzo rzadkiego – raz na 500 lat do bardzo prawdopodobnego – raz na rok) oraz jego rozmiary/skutki (od znikomych do katastrofalnych). W normie ISO 31000 etapem porównania poziomów ryzyka¹⁰ w celu ułatwienia podjęcia decyzji jest ewaluacja ryzyka. Dokument ten nie narzuca jednak zastosowania w tym celu macierzy ryzyka. Macryca irlandzka dodatkowo podzielona jest według dwóch stref (rys. 2) – pierwsza dotyczy zdarzeń umiarkowanych, druga zaś zdarzeń, które wymagają najwyższego stopnia gotowości.

Ocena ryzyka zapewnia podstawę do określenia czynników determinujących kolejne kroki (w późniejszych etapach zarządzania kryzysowego), zwłaszcza w zakresie planowania cywilnego oraz ograniczania skutków zdarzeń. Ocena ryzyka pomaga także w wyborze priorytetów działań prewencyjnych w obszarach, w których ryzyko wystąpienia zdarzenia jest bardzo prawdopodobne, a jego konsekwencje będą katastrofalne. Porównując powyższe z podejściem ISO 31000,

⁹ A Framework..., dz. cyt., s. 23.

¹⁰ Patrz: definicja na s. 115.

dostrzegamy ograniczenia zastosowane w metodyce irlandzkiej. Celem zasadniczym, na co wskazuje również tytuł dokumentu opracowanego przez rząd Irlandii, jest położenie nacisku na ocenę ryzyka i wypracowanie priorytetów postępowania z ryzykiem wynikającym z poważnych sytuacji kryzysowych. W przypadku normy dotyczy to wszystkich zagrożeń, które mogą wpływać na osiągnięte cele. Natomiast sam proces, choć uboższy, jest bardzo zbliżony do wprowadzonego przez ISO 31000.



Rys. 2. Strefy matrycy ryzyka

Źródło: Opracowanie własne na podstawie *A Framework...*, dz. cyt., s. 26.

2.2. Narodowa ocena ryzyka Irlandii

Dokument *A National Risk Assessment for Ireland (NRA)* z 2012 r. przedstawia rezultaty krajowej oceny ryzyka. Celem opracowania jest dokonanie analizy eksperckiej w poszczególnych sektorach i dziedzinach działalności państwa, ukazującej proces rozwoju narodowego postrzegania ryzyka. Analiza ta ma:

- przyczynić się do stworzenia kompleksowej oceny ryzyka i wspólnego rozumienia wyzwań narodowych/społecznych,
- wesprzeć w porównaniu różnych rodzajów zagrożeń z punktu widzenia narodowego/społecznego, pozwalając na ocenę ryzyka według wcześniej zdefiniowanych kryteriów prawdopodobieństwa i wpływu¹¹,

¹¹ Wpływ – w odniesieniu do normy ISO 31000: konsekwencje.

- stanowić podstawę do ustalenia priorytetów w zarządzaniu kryzysowym, które ułatwią koordynację międzysektorową i zapewnią równowagę środków na potrzeby zapobiegania i/lub ograniczania ryzyka¹²,
- zapewnić zgodność z wymaganiami Unii Europejskiej, aby państwa członkowskie, opracowując krajowe strategie zarządzania ryzykiem, wspierały podejście UE do zapobiegania katastrofom naturalnym i spowodowanym przez człowieka i zarządzania nimi.

Korzystając z metodyki przygotowanej w ramach *Framework for Major Emergency Management*, przeprowadzono narodową ocenę ryzyka. Opracowanie dokumentu koordynowało Biuro Planowania Kryzysowego. Narodowa ocena ryzyka jest zatwierdzana przez Grupę Zadaniową ds. Planowania Kryzysowego wyznaczoną przez rząd Irlandii.

Pierwszym działaniem była identyfikacja zagrożeń, którą przeprowadzono w grupach tematycznych. Zidentyfikowane zagrożenia poddano ocenie ryzyka. Zgodnie z wytycznymi metodyki irlandzkiej zagrożenia podzielono na cztery kategorie: zagrożenia w transporcie, naturalne, technologiczne oraz cywilne. Do kolejnego etapu zaangażowane zostały zespoły eksperckie, mające przeprowadzić analizę całościowego ryzyka, by móc rozpocząć proces oceny ryzyka. Proces ten prowadzą zespoły tematyczne składające się z ekspertów poszczególnych ministerstw i agencji państwowych. Kluczem prawidłowości przebiegu procesu oceny ryzyka jest ocena prawdopodobieństwa wystąpienia zagrożenia oraz zbadanie konsekwencji (rozumianych jako konsekwencje wystąpienia zdarzenia niebezpiecznego, wyrażone w postaci negatywnego wpływu na dobro człowieka, szkody dla środowiska lub infrastruktury lub innych późniejszych konsekwencji – przyp. autora) zidentyfikowanych zagrożeń. Oszacowano go na podstawie możliwie najgorszego scenariusza. Klasyfikację wpływu i prawdopodobieństwa przedstawiono w poniższych tabelach, które wykorzystane zostały jako baza do podejmowania decyzji w odniesieniu do względnego ryzyka każdego zidentyfikowanego zagrożenia. W kontekście wpływu kryteria oceny zostały przeskalowane, w celu odzwierciedlenia sytuacji kryzysowych wymagających koordynacji na poziomie krajowym.

Tabela 1. Klasyfikacja prawdopodobieństwa

Lp.	Klasyfikacja	Prawdopodobieństwo
1.	skrajnie 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 niepotwierdzone incydenty i/lub bardzo niewiele incydentów w organizacjach, obiektach i komunikacji; mała szansa wystąpienia, może wystąpić raz na 100–500 lat

¹² Patrz: definicja na s. 238.

Lp.	Klasyfikacja	Prawdopodobieństwo
3.	nieprawdopodobne	może wystąpić od czasu do czasu i/lub niewiele razy; rzadko, losowo zarejestrowane przypadki, słabo potwierdzone incydenty lub niektóre incydenty w jednostkach stowarzyszonych lub podobnych organizacjach na całym świecie; pewna szansa, sposobność lub możliwość wystąpienia – może wystąpić raz na 10–100 lat
4.	prawdopodobne	prawdopodobnie wystąpi, regularnie rejestrowane zdarzenia i potwierdzone incydenty; prawdopodobne wystąpienie – raz na 1–10 lat
5.	bardzo prawdopodobne	bardzo prawdopodobne, wysoki poziom odnotowanych zdarzeń i/lub wiele potwierdzonych incydentów; prawdopodobnie będzie występowało częściej niż raz w roku

Źródło: Opracowanie własne na podstawie *A National Risk Assessment for Ireland*, dz. cyt., s. 15.

Tabela 2. Klasyfikacja wpływu

Lp.	Klasyfikacja	Wpływ	Opis
1.	bardzo mały wpływ	życie, zdrowie, opieka środowisko infrastruktura społeczeństwo	ograniczona liczba osób dotkniętych; 0–4 ofiary śmiertelne i ograniczona liczba drobnych urazów wymagających leczenia lub pierwszej pomocy nieznaczne, miejscowe zanieczyszczenia poniżej 4 mln EUR miejscowe zakłócenie usług społecznych lub infrastruktury (< 48 godz.)
2.	niewielki wpływ	życie, zdrowie, opieka środowisko infrastruktura społeczny	4–8 ofiar śmiertelnych, znaczna liczba rannych; poważne urazy hospitalizacyjne, leczenie wymagane; miejscowe przemieszczenia znacznej liczby osób przez 2–8 dni; wsparcie realizowane przez lokalne jednostki samorządu terytorialnego zanieczyszczenie regionalne, skutki krótkotrwałe od 4-24 mln EUR społeczność funkcjonuje w znacznych niedogodnościach

Lp.	Klasyfikacja	Wpływ	Opis
3.	umiarkowany wpływ cd.	życie, zdrowie, opieka środowisko infrastruktura społeczny	znaczna liczba osób w obszarze zagrożonym – wiele wypadków śmiertelnych (8–20), wiele poważnych i rozległych urazów (20), znaczna hospitalizacja; duża liczba osób przesiedlonych przez 2–8 dni; do 4000 ewakuowanych; zasoby regionalne wymagane do wsparcia osobistego duże skutki, skażenia miejscowe w dość długim okresie 24–80 mln EUR społeczność działa tylko częściowo, dostępne tylko niektóre usługi
4.	duży wpływ	życie, zdrowie, opieka środowisko infrastruktura społeczny	20 do 50 wypadków śmiertelnych, do 100 poważnych obrażeń, do 16 000 ewakuowanych duże zanieczyszczenia, w długim okresie 80–200 mln EUR społeczność działa słabo, minimalne usługi zapewnione
5.	bardzo duży wpływ	życie, zdrowie, opieka środowisko infrastruktura społeczny	duża liczba osób miała w obszarze zagrożonym – znaczna liczba zgonów (> 50), znaczne obrażenia, ponad 16 000 ewakuowanych bardzo duże zanieczyszczenia, rozległe, długotrwałe skutki powyżej 200 mln EUR poważne uszkodzenia infrastruktury powodujące znaczne zakłócenia lub utratę, kluczowych usług przez dłuższy okres; społeczność nie może funkcjonować bez znaczącego wsparcia

Źródło: Opracowanie własne na podstawie *A National Risk Assessment for Ireland*, dz. cyt., s. 16–17.

Kryteria ryzyka¹³ (mniej lub bardziej szczegółowe) nie są narzucone przez normę ISO, zaleca ona jedynie ich adekwatny dobór, według potrzeb. W metodyce irlandzkiej zarówno wpływ, jak i prawdopodobieństwo sklasyfikowano w sposób jakościowy oraz ilościowy, stosując wystarczająco precyzyjny opis.

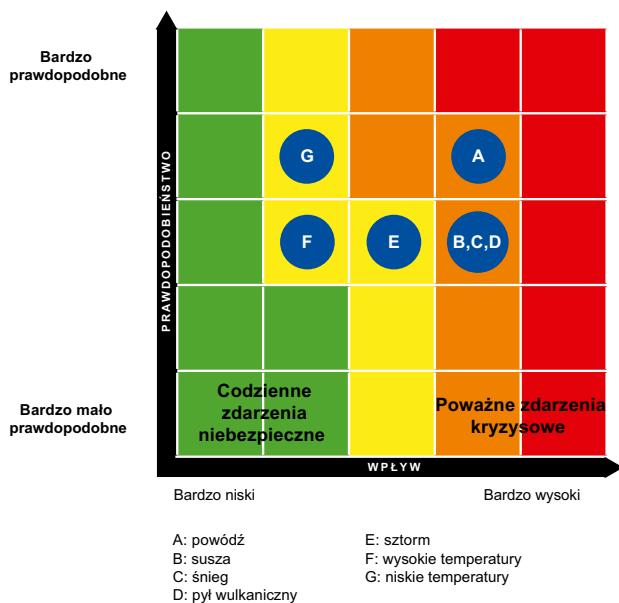
Wynik oceny ryzyka stanowi podstawę dla skutecznego zarządzania w sytuacjach kryzysowych. Takie podejście, oparte na ocenie eksperckiej i interpretacji reprezentatywnych i rzetelnych danych, świadczy o stosowaniu dobrych praktyk w zakresie analizy zagrożeń. Wykorzystanie informacji dotyczących analizy

¹³ Patrz: definicja na s. 115.

zagrożeń od regionalnych grup sterujących w połączeniu z danymi zespołu eksperckiego ze szczebla centralnego przynosi równowagę w ocenie analizy zagrożeń. Pełna ekspertyza daje solidne podstawy do twierdzenia, że całościowa matryca ryzyka jest wiarygodna.

Krajowy rejestr ryzyka (National Risk Register – NRR)

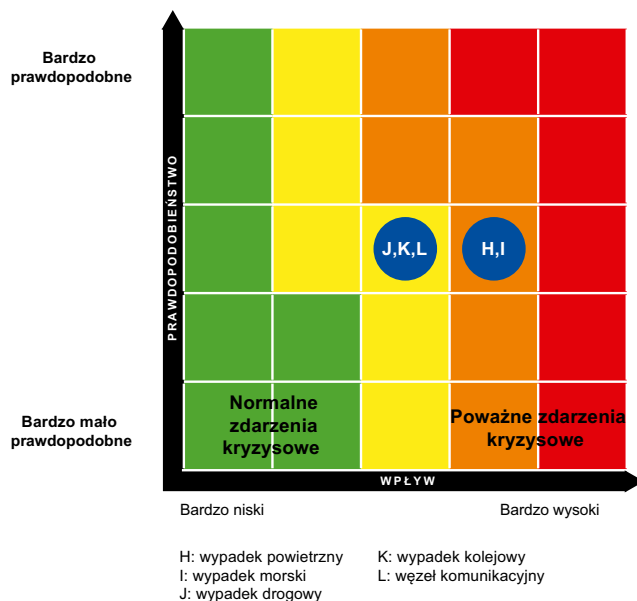
Matryce dla każdej kategorii zagrożeń (naturalnych, w transporcie, technologicznych, cywilnych), jak również zbiorcza matryca ryzyka zostały przedstawione poniżej. W przeciwieństwie do zaleceń dokumentowania ryzyk zawartych w normie ISO 31000 Krajowy rejestr ryzyka ma odmienne cele. Dla normy dokumentowanie stanowi – poza możliwością identyfikacji podjętych działań – formę doskonalenia procesu oraz wykorzystywanych w nim metod i narzędzi. Dokument irlandzki oprócz inwentaryzacji zidentyfikowanych i poddanych ocenie ryzyk oraz podjętych działań wobec najważniejszych zagrożeń dla Irlandii stanowić ma podstawę do uruchomienia działań związanych z łagodzeniem ryzyka¹⁴, a także planowaniem i przygotowaniem odpowiedzi na nie.



Rys. 3. Narodowa matryca ryzyka – zagrożenia naturalne

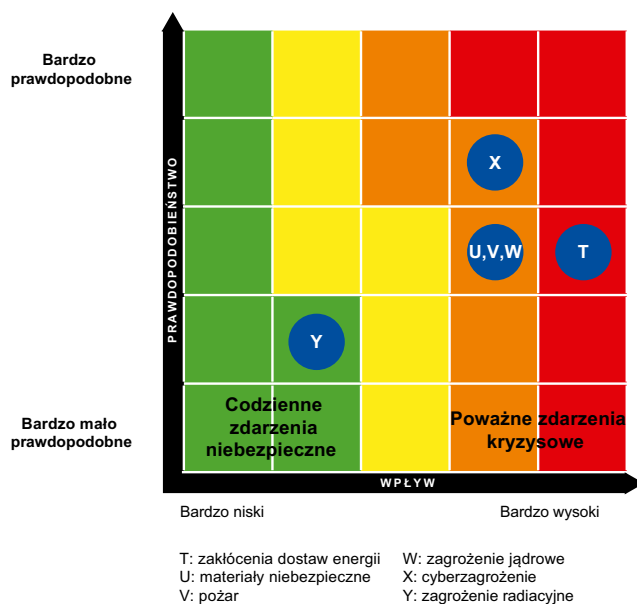
Źródło: Opracowanie własne na podstawie *A National Risk Assessment for Ireland*, dz. cyt., s. 18.

¹⁴ Patrz: definicja na s. 140.



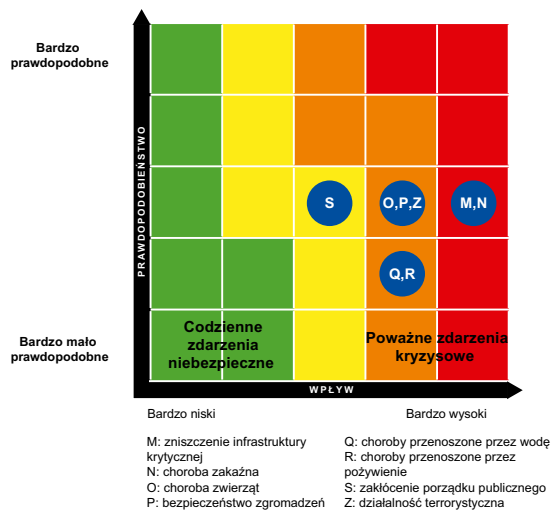
Rys. 4. Narodowa matryca ryzyka – zagrożenia w transporcie

Źródło: Opracowanie własne na podstawie *A National Risk Assessment for Ireland*, dz. cyt., s. 22.



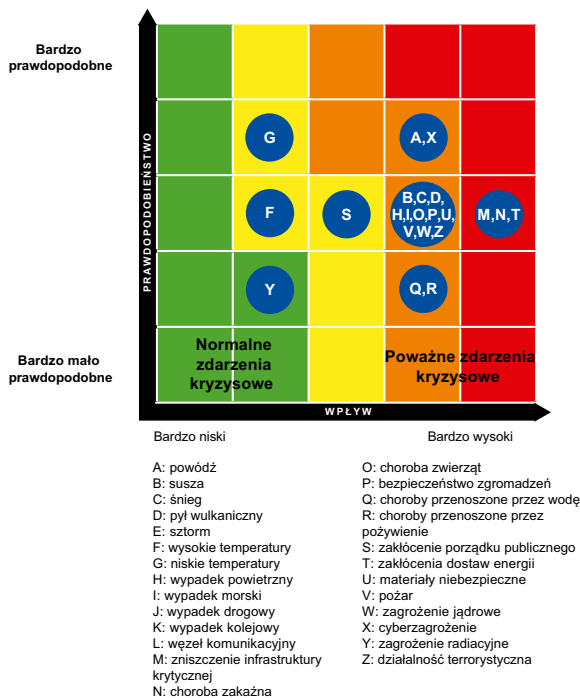
Rys. 5. Narodowa matryca ryzyka – zagrożenia technologiczne

Źródło: Opracowanie własne na podstawie *A National Risk Assessment for Ireland*, dz. cyt., s. 24.



Rys. 6. Narodowa matryca ryzyka – zagrożenia cywilne

Źródło: Opracowanie własne na podstawie *A National Risk Assessment for Ireland*, dz. cyt., s. 28.



Rys. 7. Narodowa matryca ryzyka – wszystkie zagrożenia

Źródło: Opracowanie własne na podstawie *A National Risk Assessment for Ireland*, dz. cyt., s. 32.

Aktualna ocena

Dane z czterech pojedynczych matryc ryzyka zagrożeń zostały skonsolidowane w narodowej matrycy ryzyka (rys. 7). Matryca prezentuje bieżącą ocenę względnych ryzyk dla kluczowych zagrożeń w Irlandii. Opiera się ona na opinii ekspertów i interpretacji danych, dostępnych m.in. dzięki współpracy ze służbami. Matryca ta powinna być używana do prowadzenia działań związanych z łagodzeniem ryzyka, planowaniem i przygotowaniem na poziomie krajowym i regionalnym. Jest corocznie aktualizowana, w odpowiedzi na zmiany w otoczeniu ryzyka.

3. ZARZĄDZANIE RYZYKIEM W REPUBLICE FEDERALNEJ NIEMIEC

Niemiecką metodę analizy ryzyka (rozumianą jako systematyczna procedura określająca prawdopodobieństwo wystąpienia pewnych uszkodzeń obiektu podlegającego ochronie, z uwzględnieniem potencjalnego stopnia zniszczeń – przyp. autora) Federalne Biuro Ochrony Ludności i Wsparcia Katastrof (BBK) przyjęło w dokumencie *Method of Risk Analysis for Civil Protection* z 2011 r. Jest ona zarówno wynikiem badań Biura Federalnego, jak i efektem wymiany doświadczeń pomiędzy władzami federalnymi oraz ośrodkami naukowymi. Zaproponowane podejście jest zgodne ze standardami międzynarodowymi związanymi z zarządzaniem ryzykiem oraz oceną ryzyka¹, tj. normami ISO 31000 oraz ISO 31010. Cel przygotowanego dokumentu to wsparcie praktycznego zastosowania metody analizy ryzyka dla ochrony ludności.

W niniejszym rozdziale zawarto analizę rozwiązań zaproponowanych w niemieckiej metodzie analizy ryzyka. Celem rozważań było wskazanie cennych praktyk tego kraju w omawianym zakresie oraz bliższe przyjrzenie się niemieckiemu podejściu do problematyki ochrony ludności.

3.1. Metoda analizy ryzyka w ochronie ludności

Dokument *Method of Risk Analysis for Civil Protection* określa na wstępie warunki niezbędne do zastosowania powyższej metody. Po pierwsze, podkreśla się, że integralnymi elementami ryzyka są prawdopodobieństwo i wpływ². Prawdopodobieństwo odnosi się do niebezpiecznych zdarzeń o pewnym natężeniu³, wpływ dotyczy się zaś różnorodnych zniszczeń obiektów chronionych, które są spodziewane, jeśli ryzykowne zdarzenie wystąpi. Po drugie, proces analizy ryzyka⁴ powinien wykorzystywać najlepsze dane i informacje, w tym badania naukowe, dane statystyczne oraz szacunki eksperckie zapewniające możliwie najwyższy poziom

¹ Patrz: definicja na s. 107.

² Wpływ – w odniesieniu do normy ISO 31000: konsekwencje.

³ Natężenie – stopień nasilenia czegoś, intensywność. Źródło: <http://sjp.pl/nat%C4%99%C5%BCenie> [dostęp: marzec 2015].

⁴ Patrz: definicja na s. 109.

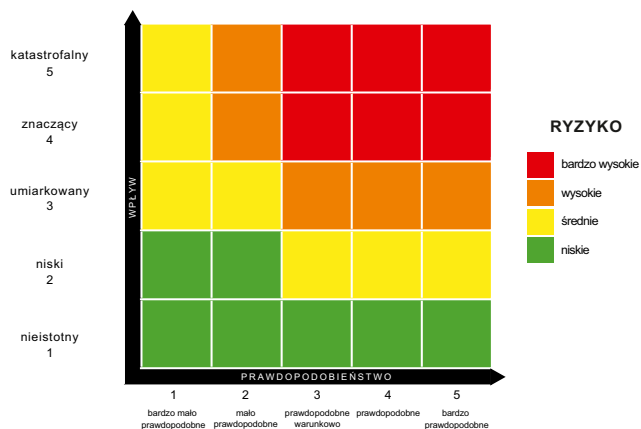
wiarygodności. Po trzecie, wszystkie kroki procesu analizy ryzyka powinny być wnikliwie dokumentowane w celu zagwarantowania uzyskania jej rezultatów. Po czwarte, za dopuszczalne uważa się ograniczenie analizy do tych ryzyk, które konfrontowałyby szczebel administracyjny z tak znacznymi wyzwaniami, w których poradzenie sobie ze zniszczeniami lub podjęcie odpowiednich środków zapobiegawczych wymagałoby wsparcia poziomu centralnego. Po piąte, analiza ryzyka powinna rozważać także zagrożenia, które mogą mieć swoje źródło na zewnątrz zidentyfikowanego obszaru, jak i te, które mogą mieć wpływ na obszar odpowiedzialności danej jednostki. Po szóste, analiza ryzyka dla ochrony ludności jest zadaniem ustawicznym. Zastosowana metoda powinna mieć zdolność adaptacji do nowych warunków działania w każdym czasie. Po siódme, metoda jest instrukcją do praktycznego dokonywania analizy ryzyka. Ewaluacja rezultatów oceny ryzyka i ich implementacji przez administrację są kolejnymi krokami w procesie zarządzania ryzykiem. Po ósme, analiza ryzyka stanowi część kompleksowego procesu zarządzania ryzykiem, który zawiera: analizę, ewaluację⁵, postępowanie z ryzykiem⁶ oraz monitorowanie⁷ ryzyk.

Celem analizy ryzyka w obszarze ochrony ludności jest porównanie różnych rodzajów zagrożeń za pomocą matrycy ryzyka (rys. 1) i stanowi podstawę dla procesu planowania cywilnego. Ryzyko definiowane jest w tym dokumencie w odniesieniu do: ludności, środowiska, gospodarki, zaopatrzenia (w tym dostaw: prądu, gazu, wody, usług telekomunikacyjnych) i wartości niematerialnych (dóbr kultury czy zdolności utrzymania władzy). Niemiecka metoda, podobnie jak opisana w części trzeciej szwedzka (rozdział 4 *Zarządzanie ryzykiem w Szwecji*, podrozdział 4.2. *Szwedzka narodowa ocena ryzyka 2012*), opiera się przede wszystkim na scenariuszach i odnosi się do procesu oceny ryzyka dla określonych/zdefiniowanych obiektów lub miejsc. Scenariusze przedstawione w metodzie niemieckiej różnią się diametralnie od ich rozumienia w przypadku analizy scenariuszowej i jej charakterystyki, opisanej w części I. W metodzie niemieckiej, gdy mówimy o scenariuszu, mamy na myśli proces obejmujący założenie możliwych zdarzeń lub sekwencji zdarzeń i ich skutków dla podmiotów chronionych.

⁵ Patrz: definicja na s. 114.

⁶ Patrz: definicja na s. 106.

⁷ Patrz: definicja na s. 113.



Rys. 1. Matryca ryzyka wykorzystywana przez niemieckie Federalne Biuro Ochrony Ludności
Źródło: Opracowanie własne na podstawie Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 22.

Budowa scenariusza opiera się na odpowiedziach na zdefiniowane wcześniej pytania dotyczące przedstawionych poniżej parametrów, które stanowią pewien substytut dla podprocesu identyfikacji ryzyka⁸ w normie ISO 31000.

Tabela 1. Parametry i centralne pytania do opisu scenariusza

Parametr	Pytania
Zagrożenie	Jaki typ zdarzenia jest rozpatrywany?
Miejsce wystąpienia	Gdzie zdarzenie ma miejsce?
Wymiar przestrzenny	Jaki teren jest objęty zdarzeniem?
Natężenie	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 przewidywalne? 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 są dotknięte zdarzeniem? (ludzie, środowisko, obiekty itp.)
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 Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 26.

⁸ Patrz: definicja na s. 106.

Tabela 1 opisuje jedynie wstępny proces, który pozwala ustalić, co ma wpływ na wydarzenie. Prawdopodobieństwo oraz konsekwencje zostają określone w kolejnych etapach analizy ryzyka.

Określenie prawdopodobieństwa opiera się na pięciostopniowej skali. Klasyfikacja obejmuje kategorie od „bardzo mało prawdopodobne” do „bardzo prawdopodobne”, którym przypisuje się odpowiadające im statystyczne prawdopodobieństwo (zgodnie z tabelą 2).

Tabela 2. Przykładowy model klasyfikacji 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 Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 27.

O ile określenie prawdopodobieństwa wystąpienia zagrożenia stanowi mało złożony proces (pod warunkiem, że dysponuje się odpowiednimi danymi), wskazanie konsekwencji zdarzenia jest bardziej złożone.

Pierwszym krokiem analizy ryzyka w tym zakresie jest dokładny opis miejsca, dla którego będzie ona przygotowana (według określonych parametrów – przykładowe parametry ukazuje poniższa tabela).

Tabela 3. Przykładowe parametry charakteryzujące miejsce

Klasa	Informacja	Możliwe źródła informacji
Ludność	liczba mieszkańców	biura statystyczne główny urząd statystyczny
	gęstość zaludnienia	
	liczba gospodarstw domowych	
Środowisko	obszar chroniony (rezerwaty przyrody, rezerwaty biosfery, parki narodowe i krajobrazowe)	ministerstwo środowiska biura ochrony środowiska
	obszary rolne	władza/administracja właściwa w obszarze rolnictwa biura statystyczne
Gospodarka	wydajność gospodarki	władza/administracja właściwa ds. ekonomicznych biura statystyczne
	wpływy podatkowe	

Klasa	Informacja	Możliwe źródła informacji
Zaopatrzenie	dostawy wody	władza/administracja właściwa ds. ekonomicznych dostawca
	dostawy energii elektrycznej	władza/administracja właściwa ds. ekonomicznych dostawca
	dostawy gazu	władza/administracja właściwa ds. ekonomicznych dostawca
	dostawy usług telekomunikacyjnych	władza/administracja właściwa ds. ekonomicznych dostawca
Wartości niematerialne	dobra kultury	konserwator zabytków

Źródło: Opracowanie własne na podstawie Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 30–31.

Kolejnym krokiem jest opisanie atrybutów zdarzenia (według określonych parametrów – patrz tabela 4).

Tabela 4. Przykładowe parametry charakteryzujące zdarzenie⁹

Kategoria	Rodzaj szkody	Opis	Jednostka miary
Ludność	ofiary	liczba osób, które poniosły śmierć w wyniku zdarzenia	liczba
	ranni	osoby ranne w wyniku zdarzenia oraz osoby chore w wyniku zdarzenia	liczba
	osoby poszkodowane oczekujące pomocy pow. 14 dni	osoby potrzebujące pomocy publicznej dłużej niż 14 dni	liczba
	osoby poszkodowane oczekujące pomocy do 14 dni	osoby potrzebujące pomocy publicznej dłużej niż 14 dni	liczba
Środowisko	straty w obszarach chronionych	obszary chronione zniszczone w wyniku zdarzenia (rezerwaty przyrody, rezerwaty biosfery, parki narodowe i krajobrazowe)	ha

⁹ Źródło: opracowanie własne na podstawie Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 30–31.

Kategoria	Rodzaj szkody	Opis	Jednostka miary
Środowisko cd.	straty w zbiornikach wodnych	obszar wód powierzchniowych i mórz „zniszczone” w wyniku zdarzenia	km/ha
	straty w wodach gruntowych	wody gruntowe zanieczyszczone w wyniku zdarzenia	ha
	straty w gruntach rolnych	grunty rolne zniszczone w wyniku zdarzenia	ha
Gospodarka	straty fizyczne	suma wartości strat zadanych bezpośrednio przez zdarzenie	waluta
	straty wtórne	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	konsekwencje dla bezpieczeństwa i porządku publicznego	rozmiary konsekwencji incydentu na bezpieczeństwo publiczne (np. protesty publiczne, przemoc wobec osób, ataki na obiekty)	zasięg
	konsekwencje polityczne	zakres skutków incydentu na sektor polityczno-administracyjnych (np. wezwanie przez społeczeństwo struktur państwa do podjęcia działań lub do rezygnacji z nich)	zasięg

Kategoria	Rodzaj szkody	Opis	Jednostka miary
	konsekwencje psychologiczne	stopień utraty zaufania publicznego do organów władzy (np. rządu lub administracji)	zasięg
	zniszczenia dóbr kultury	zniszczenia dóbr kultury w wyniku incydentu (np. będących pod ochroną konwencji haskiej)	liczba uszkodzonych obiektów i stopień tych uszkodzeń

Źródło: Tamże.

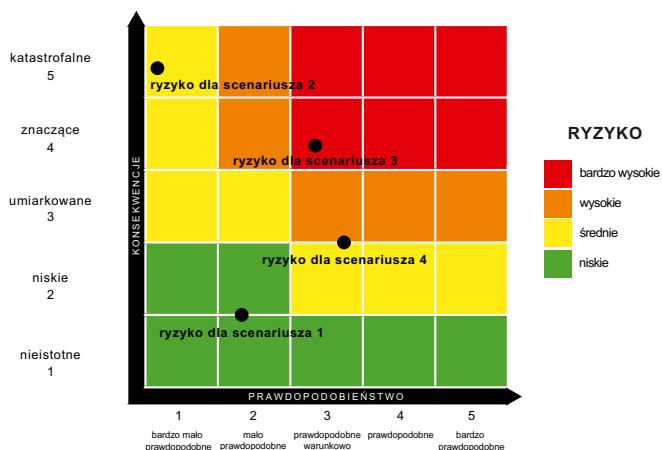
Kolejnym krokiem jest przypisanie właściwych poziomów konsekwencji, zgodnie ze wskazaną jednostką miary. Tabela 5 wskazuje przykładowy model bez wskazania wartości (symbol „_” pokazuje miejsce wskazania wartości).

Tabela 5. Model klasyfikacji 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 > _ godz./dni
4	znaczące	_ _ _	_ _ _	_ _ _	_ _ _ osób przez _ _ _ godz./dni
3	umiarkowane	_ _ _	_ _ _	_ _ _	_ _ _ osób przez _ _ _ godz./dni
2	niskie	_ _ _	_ _ _	_ _ _	_ _ _ osób przez _ _ _ godz./dni
1	nieistotne	= lub < _	= lub < _	= lub < _	= lub < _ osób przez = lub < _ godz./dni

Źródło: Opracowanie własne na podstawie Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., dz. cyt., s. 33.

Po określeniu (zgodnie z powyżej wskazanymi zasadami) wartości wpływu i prawdopodobieństwa wyniki analizy ryzyka są wizualizowane na matrycach ryzyka, w których ryzyka dla poszczególnych scenariuszy, warunkowane przez czynniki prawdopodobieństwa i wpływu, ujęte zostały jako punkty.



Rys. 2. Przykładowe zestawienie porównawcze różnorodnych zagrożeń w macierzy
Źródło: Opracowanie własne na podstawie Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 41.

Wizualizacja ryzyka dla poszczególnych scenariuszy jest ostatnim etapem analizy ryzyka. Stanowi ona punkt wyjścia dla procesu planowania cywilnego. Niemniej jednak dokument zaznacza, że analiza ryzyka nie jest celem samym w sobie, ale jednym z aspektów całościowego zarządzania ryzykiem. Proces zarządzania ryzykiem jest zwykle przedstawiany jako cykl, ponieważ po wdrożeniu odpowiednich środków (planów i procedur – przyp. autora) dokonywana jest ponowna ocena, która pozwala określić, czy zamierzony cel został osiągnięty¹⁰. Ujęcie analizy ryzyka jako centralnego elementu zarządzania ryzykiem prezentuje rys. 3.



Rys. 3. Analiza ryzyka jako centralny element zarządzania ryzykiem (na podstawie ISO 31000)

Źródło: Opracowanie własne na podstawie Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 45.

¹⁰ Federal Office of Civil Protection and Disaster Assistance, *Method...*, dz. cyt., s. 45.

Należy podkreślić, że zasady zarządzania ryzykiem, którymi posługuje się Federalne Biuro Ochrony Ludności (zgodnie z powyższym rysunkiem), bazują na normach wskazanych w implementowanej w Polsce normie PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*.

W dokumencie *Method of Risk Analysis for Civil Protection* podkreślono, że w kontekście procesu zarządzania ryzykiem zadaniem organów odpowiedzialnych za ochronę ludności jest dostarczenie aktualnych i wiarygodnych informacji na temat zagrożeń, ryzyk i dostępnych zdolności w ramach zarządzania kryzysowego. Mają one stanowić pomoc dla decydentów w podjęciu decyzji odnoszących się do zarządzania ryzykiem (np. ustalenie priorytetowych środków do minimalizacji ryzyka¹¹), planowania kryzysowego (przygotowania na nieuchronne incydenty) oraz zarządzania kryzysowego (dostarczania niezbędnych sił i środków). Zalecaną praktyką jest również dialog między kompetentnymi służbami, światem nauki, polityki i sferą publiczną, w tym obywatelami, mający doprowadzić do identyfikacji ryzyk, służący również późniejszej dyskusji o wynikach analizy ryzyka oraz ewaluacji.

Ponadto w metodyce niemieckiej rekomenduje się i potwierdza możliwość zastosowania metody na wszystkich szczeblach administracyjnych. Ze względu na porównywanie wyników analizy ryzyka na poszczególnych szczeblach oraz ich sumowanie na szczeblu centralnym konieczne jest wykorzystywanie wystandaryzowanych scenariuszy, atrybutów opisu wpływu, wskaźników dla ich operacjonalizacji, jak również złożoności wartości progowych dla klasyfikacji prawdopodobieństwa i wpływu. Pod rozwagę poddano decydentom ponadto kwestię wsparcia analizy ryzyka przez technologie informatyczne, tj. użycie GIS. Mają one pozwolić m.in. na stworzenie przestrzennych analiz i wizualizację danych na mapach.

¹¹ Patrz: definicja na s. 238.

4. ZARZĄDZANIE RYZYKIEM W SZWECJI

W niniejszym rozdziale omówione zostaną wydane w 2012 r. dwa istotne dokumenty: *Przewodnik po analizie ryzyka i podatności*¹ oraz *Szwedzka narodowa ocena ryzyka*². Odnoszą się one do zarządzania ryzykiem w Szwecji – szczególnie w kontekście zarządzania kryzysowego, a w tym planowania cywilnego.

Przewodnik stanowi źródło wiedzy i wsparcia dla organów administracji rządowej oraz samorządowej, zobligowanych do przeprowadzania oceny ryzyka i podatności, a także innych podmiotów zainteresowanych tą problematyką. Dokument przedstawia w klarowny sposób, jak zarządzać tym procesem analitycznym.

Szwedzka narodowa ocena ryzyka przedstawia rezultaty przeprowadzonej w tym państwie krajowej oceny ryzyka. Efekty jej prac były następujące:

- identyfikacja 27 zdarzeń narodowych – na podstawie analiz ryzyka i podatności przeprowadzonych w latach 2010–2011 przez odpowiednie organy,
- 11 scenariuszy opartych na tych zdarzeniach,
- analiza oraz ocena 7 zdarzeń,
- opracowanie procesu i metodologii przeprowadzenia oceny,
- udokumentowanie pracy i doświadczeń Szwedzkiej Agencji ds. Cywilnych Sytuacji Kryzysowych (MSB) oraz podmiotów zaangażowanych w zarządzanie kryzysowe.

Analiza podejścia szwedzkiego do zarządzania ryzykiem oraz podkreślenie wartościowych praktyk i narzędzi stosowanych w tym kraju determinowały strukturę i cele niniejszego rozdziału.

4.1. Przewodnik po analizie ryzyka i podatności

Wprowadzając w tematykę, przewodnik opisuje ogólne cele przygotowania społeczeństwa na wystąpienie sytuacji kryzysowych oraz rolę analizy ryzyka i podatności^{3,4} w zarządzaniu przygotowaniem na stan kryzysowy. Przedstawia także

¹ Swedish Civil Contingencies Agency, *Guide to risk and vulnerability analyses*, Karlstad 2012, <https://www.msb.se/RibData/Filer/pdf/26267.pdf>.

² Swedish Civil Contingencies Agency, *Swedish National Risk Assessment 2012*, Karlstad 2012.

³ Patrz: definicja na s. 209.

⁴ Autorzy przewodnika stosują i konsekwentnie podkreślają w dokumencie istotne dla nich elementy: analizę ryzyka (jako najważniejszy podproces oceny ryzyka) i analizę podatności (jako

cel przewodnika i docelowe grupy jego odbiorców. Główne cele bezpieczeństwa społeczeństwa, które zgodnie z dokumentem należy chronić, to:

- życie i zdrowie populacji,
- funkcjonowanie społeczne,
- zdolność do utrzymania podstawowych wartości, takich jak demokracja, rządy, prawa i wolności człowieka.

Do powyższych elementów zalicza się np. zapewnienie opieki zdrowotnej, systemów informacyjnych i komunikacyjnych, dostaw energii, przepływu dóbr i usług oraz inne funkcje społeczne, które są warunkami funkcjonowania społeczeństwa i nie można dopuścić do ich załamania.

Cele osiągnięte poprzez przygotowanie społeczeństwa na wystąpienie sytuacji kryzysowych to:

- redukcja ryzyka⁵ oraz skutków poważnych zakłóceń, kryzysów i wypadków,
- zapewnienie zdrowia i bezpieczeństwa dzieci, kobiet i mężczyzn,
- zapobieganie powstawaniu szkód w mieniu lub środowisku i ograniczanie ich.

Zarządzanie kryzysowe małymi zdarzeniami może stanowić podstawę do zarządzania sytuacjami nadzwyczajnymi. W przypadku zdarzeń drobnych źródło informacji stanowią codzienne incydenty, natomiast dla zdarzeń dużych trudno jest pozyskać ważne informacje, które stanowiłyby podstawę do oceny. Codzienne wypadki to częste zdarzenia z nieznacznymi bądź niewielkimi konsekwencjami, np. wypadki w pracy, wypadki drogowe. Takie sytuacje są w dużym stopniu przewidywalne i informacje o nich można czerpać ze zgłoszeń lub badań statystycznych.

Podmioty zaangażowane muszą również opierać się na różnych dokumentach normatywnych, które zawierają wymagania wobec analiz ryzyka. Dotyczą one często konkretnych rodzajów zagrożeń, ryzyka, zdarzeń i sytuacji kryzysowych. W pracy wstępnej nad analizą ważne jest ustalenie i zdefiniowanie jej punktów wyjściowych.

Analizy mogą być opracowywane według niżej wymienionych dokumentów. Bardzo istotna jest prawidłowa identyfikacja ryzyka, ponieważ determinuje ona właściwy dobór dokumentu normatywnego, na którym analiza ma się opierać (dla zdarzeń nieprzewidzianych ustawodawstwem autorzy opracowują własne narzędzia):

1. *Government Authority Risk Management Ordinance* (SFS 1995:1300).
2. *Internal Governance and Control Ordinance* (SFS 2007:603).
3. *Security Protection Act* (SFS 1996:627) i *Security Protection Ordinance* (1996:633).
4. *Civil Protection Act* (2003:778) i *Civil Protection Ordinance* (2003:789).

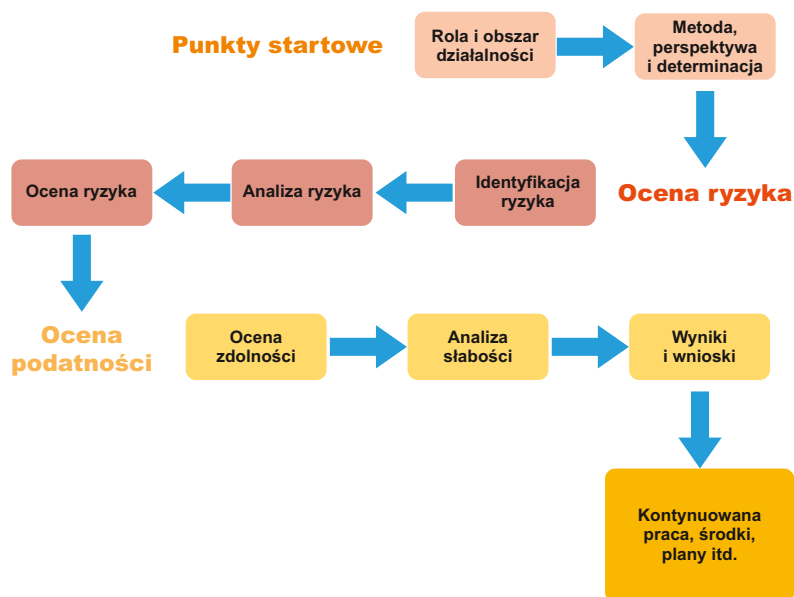
najważniejszy podproces oceny podatności). W dalszej części rozdziału dokonano próby ich charakterystyki.

⁵ Patrz: definicja na s. 238.

5. Swedish National Board of Health and Welfare regulations and general guidelines on disaster medicine preparedness.

6. Agency regulations in the field of information security.

Poniżej przybliżony został cały proces zarządzania ryzykiem, którego ważny element stanowi analiza ryzyka i podatności.



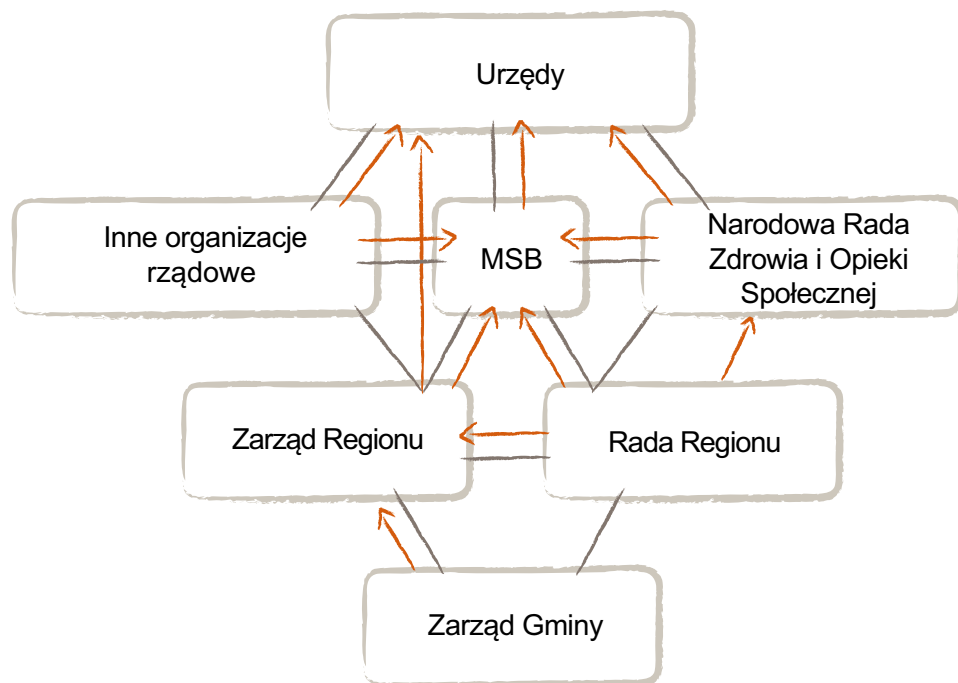
Rys. 1. Proces zarządzania ryzykiem

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 14.

Schemat Szwedzkiej Agencji ds. Cywilnych Sytuacji Kryzysowych (rys. 1) bazuje na wzorze trzonu procesu zarządzania ryzykiem, który został opracowany w ramach normy ISO 31000. Dodane zostały jednak elementy własne. Punkty startowe (wyjściowe) to nic innego, jak elementy podprocesu ustalenie kontekstu. Proces oceny ryzyka⁶ z kolei przeniesiono, zgodnie z wytycznymi normy. Nowum stanowi tutaj wprowadzenie oceny podatności społeczności i podmiotów w postaci oceny gotowości (zdolności do przewyciężenia konsekwencji danego zdarzenia kryzysowego) oraz analizy podatności (czyli określenia, w jakim stopniu dana wartość chroniona narażona na konkretne ryzyko jest w stanie odeprzeć bądź zniwelować konsekwencje jego wystąpienia). Wyniki i wyciągnięte wnioski z tak przeprowadzonych, następujących po sobie kroków umożliwiają przejście do etapu (w normie ISO 31000: podprocesu) postępowania z ryzykiem⁷, w którym wiodącą rolę przejmują decydenci właściwi dla danego obszaru administracyjnego.

⁶ Patrz: definicja na s. 107.

⁷ Patrz: definicja na s. 106.



– Informacja – Sprawozdawczość

Rys. 2. Graficzny opis obiegu informacji na temat analizy ryzyka

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 17.

Cel oceny ryzyka i podatności

Autorzy przewodnika wyjaśniają, w jakim celu przeprowadza się oceny ryzyka i podatności, a powód zbliżony jest do tych ujętych w normie ISO 31000 – przede wszystkim nadrzędnego, jakim jest realizacja celów organizacji (w tym przypadku państwa na rzecz bezpieczeństwa społeczeństwa) oraz m.in.:

- zapewnienie społeczeństwu informacyjnej bazy dotyczącej zagrożeń społecznych,
- zapewnienie podstaw do podjęcia decyzji decydujących oraz osobom odpowiedzialnym za działania operacyjne,
- zapewnienie podstawowych informacji dla społecznego planowania,
- wniesienie wkładu w określenie profilu ryzyka dla całego społeczeństwa.

Autorzy informują o możliwości utajnienia zawartości analiz ryzyka i podatności, gdy informacje o słabościach mogą zostać wykorzystane na szkodę agencji. Wspominają także o konflikcie pomiędzy potrzebą utajnienia dokumentu a funkcją budowania świadomości w społeczeństwie.

Przeprowadzenie analizy ryzyka i podatności jest obowiązkiem każdego z podmiotów zaangażowanych w proces zarządzania ryzykiem (agencji rządowych, rządów regionów, gmin i rad regionów). Przewodnik omawia role podmiotów zaangażowanych i podział obowiązków w tym obszarze.

Administracja rządowa – analiza ryzyka i podatności

Każda agencja rządowa ma określony obszar działań, a także obszar (resort), za który jest odpowiedzialna. Właśnie za analizę ryzyka i podatności tych obszarów odpowiada administracja rządowa.

Obowiązki agencji dotyczące przygotowania do sytuacji kryzysowych uregulowane są głównie przez dokument *Emergency Preparedness Ordinance*, jak również w ramach wytycznych od rządu.

Podmioty administracji rządowej podzielone są na sześć obszarów współpracy:

- infrastruktura techniczna,
- transport,
- substancje niebezpieczne,
- bezpieczeństwo ekonomiczne,
- geograficzny obszar odpowiedzialności,
- ochrona, ratownictwo i opieka.

Każda agencja co roku (*Emergency Preparedness Ordinance* SFS 2006:942) analizuje, czy w obszarze jej działalności pojawiły się słabe punkty, zagrożenia, które mogłyby ograniczyć jej zdolność do prowadzenia powierzonych jej zadań. Agencje muszą wziąć szczególnie pod uwagę:

- sytuacje, które pojawiają się szybko, niespodziewanie i bez ostrzeżenia, lub czy istnieje zagrożenie bądź ryzyko, że tego typu sytuacja wyniknie,
- sytuacje, które wymagają natychmiastowych decyzji i współpracy z innymi podmiotami,
- potrzebę utrzymania najważniejszych funkcji społecznych,
- zdolność do zwalczania niezwykle trudnych sytuacji w zakresie odpowiedzialności agencji.

Zadaniem agencji rządowych jest ocena oraz opracowanie analizy ryzyka i podatności. Agencje o szczególnej odpowiedzialności zgodnie z dokumentem EPD (2006:942) i agencje wyznaczone przez Agencję ds. Cywilnych Sytuacji Kryzysowych zobligowane są przekazać raport opracowany na podstawie analizy rządowi.

Zarząd regionu – analiza ryzyka i podatności

Obszar odpowiedzialności zarządu regionu⁸ w kwestii opracowania analizy ryzyka i podatności dzieli się na dwie części: obszar własnej działalności oraz geograficzny obszar odpowiedzialności.

Geograficzne obszary odpowiedzialności znajdują się na poziomie lokalnym, regionalnym i krajowym. Na poziomie lokalnym należy do gminy, na poziomie regionalnym do zarządu regionu, na poziomie krajowym do rządu.

Zarząd regionu zbiera informacje od gmin w celu przeprowadzenia własnej analizy. Pełni rolę wspierającą w tworzeniu analizy ryzyka i podatności przez gminy. Zarząd regionu współpracuje z gminami, radą regionu, agencjami rządowymi i partnerami biznesowymi w regionie. Wszystkie gminy przekazują analizę ryzyka i podatności do zarządu regionu i od tego momentu region pracuje nad tymi samymi scenariuszami⁹, a analizy gmin stanowią bazę do ogólnej analizy regionu.

Gmina – analiza ryzyka i podatności

Punktem wyjściowym do analizy ryzyka przez gminę jest jej obszar działalności oraz obszar odpowiedzialności geograficznej. Gmina musi utrzymać niezbędne funkcje społeczne niezależnie od skali i charakteru sytuacji kryzysowej, a także zapewnić zaspokojenie specjalnych potrzeb informacyjnych i wsparcie jednostki w czasie kryzysu.

Gmina powinna przeanalizować, jakie sytuacje nadzwyczajne mogą zdarzyć się na jej terenie w czasie pokoju i jak mogą oddziaływać na jej obowiązki. Powinna zidentyfikować i przeanalizować ryzyko oraz podatność w obrębie swojego obszaru geograficznego. To daje jej bazę do pracy nad:

- 1) różnymi podmiotami współpracującymi w gminie i przejmowaniem koordynacji w działaniach przygotowawczych i planowaniu,
- 2) koordynowaniem działań podejmowanych przez różne podmioty w czasie zdarzenia,
- 3) koordynowaniem przepływu informacji do wiadomości publicznej w takich warunkach.

Analizy muszą zakładać cały wachlarz zdarzeń – incydent, kryzys, wojnę. Cel wyjściowy to zdolność do odparcia poważnych zakłóceń w funkcjonowaniu społeczeństwa. Gmina powinna dysponować planem zarządzania, opartym na wynikach analizy podatności. Plan ten musi zostać zatwierdzony przez wszystkich członków rady gminy co najmniej raz w czasie trwania całej kadencji.

Rada regionu – analiza ryzyka i podatności

Rada regionu odpowiedzialna jest za zadania wspólne dla dużych obszarów geograficznych, co wymaga dużych nakładów finansowych. Najważniejsze obszary działalności to:

⁸ Odpowiednik zarządu województwa w Polsce.

⁹ Scenariusze w znaczeniu analogicznym do scenariuszy niemieckich, patrz: s. 270.

- służba zdrowia,
- kontrola zachorowań (80% wydatków),
- usługi stomatologiczne,
- edukacja pielęgniarek,
- kultura,
- wsparcie przedsiębiorców z terenu regionu,
- odpowiedzialność za rozwój regionalny.

Rada może sama wypełniać zadania lub je zlecać.

Analiza ryzyka zawiera m.in. odpowiedzi na trzy najważniejsze pytania:

- co może się stać?
- dlaczego może to nastąpić i jak często?
- jakie będą konsekwencje dla społeczeństwa?

Prace nad analizą ryzyka i podatności

Analiza ryzyka i podatności to proces. Istotne jest, by proces ten był kontrolowany przez koordynatora, który wyznaczy terminy i którego zadaniem będzie praca na granicy zarządzania i działań operacyjnych. Analiza musi uwzględniać działania wszystkich zaangażowanych podmiotów. Dobrym rozwiązaniem jest utworzenie grupy zarządzania ryzykiem – złożonej z reprezentantów każdego z podmiotów.

Przed rozpoczęciem oceny ryzyka i podatności należy ustalić:

- role i obszary odpowiedzialności,
- metody i narzędzia pracy,
- zakres prowadzonej oceny ryzyka i podatności,
- oczekiwane perspektywy, problemy do rozwiązania.

Elementy oceny ryzyka i podatności

Aby uruchomić cały proces oceny ryzyka, należy upewnić się, że właściwie wyznaczono role i obszary odpowiedzialności, odpowiednio dobrano metody i narzędzia pracy, ustalono jasny zakres oceny i postawiono cel całego działania, który umożliwi rozwiązanie po drodze zidentyfikowanych problemów.

Identyfikacja ryzyka¹⁰

Należy ustalić, co może się wydarzyć, określić źródła ryzyka¹¹, proces analizy musi być udokumentowany. Jako wsparcie w tym działaniu można wykorzystać wiele dostępnych metod oceny ryzyka.

Warto rozpocząć od opisu systemu, który można przedstawić na trzy sposoby: model strukturalny (podział na poszczególne elementy składowe organizacji), model funkcjonalny (podział na obszary działalności) oraz model mieszany. Dla tak opisanego systemu należy dokonać identyfikacji wewnętrznych oraz zewnętrznych czynników, które mogą zaburzyć system z podziałem na grupy, np. wypadki,

¹⁰ Patrz: definicja na s. 106.

¹¹ Patrz: definicja na s. 119.

katastrofy itp. Dokładnie w ten sam sposób ujmuje to norma ISO 31000, dodając, że bardzo ważnym elementem pozwalającym na zestawienie pełnej listy ryzyk jest wykorzystanie jak najbardziej aktualnej i rzetelnej informacji.

Analiza ryzyka

Analiza ryzyka opiera się na odpowiedziach na zadane wcześniej pytania: co się może zdarzyć? na ile jest to prawdopodobne? jakie mogą być skutki? Na pierwsze pytanie częściowo odpowiada się przy identyfikacji ryzyka. W fazie analizy istotne jest udoskonalanie opisu scenariusza oraz ocena, jakie jest prawdopodobieństwo jego urzeczywistnienia. Tak jak przyjęto to w zaleceniach normy ISO 31000, etap ten prowadzi do zebrania wiedzy umożliwiającej przeprowadzenie w dalszym kroku ewaluacji ryzyka¹² i podjęcie decyzji co do postępowania z nim.

Ocena prawdopodobieństwa

Na potrzeby oceny prawdopodobieństwa również stosuje się szereg metod, które zawierają różnie przyjętą skalę dla wystąpienia danego zagrożenia. Wykorzystywane metody pogrupowane są w cztery grupy:

- opis jakościowy prawdopodobieństwa wystąpienia zdarzenia,
- opis jakościowy za pomocą skali,
- opis ilościowy za pomocą skali i podziałów,
- opis ilościowy z wykorzystaniem statystyki.

Ocena skutków

Ocena skutków to ważny element oceny ryzyka. Bez informacji o konsekwencjach danego scenariusza trudno jest wykorzystać analizę jako podstawę do podjęcia decyzji. Metody wykorzystywane do oceny skutków pogrupowane są w cztery grupy:

- opis jakościowy skutków wystąpienia zdarzenia,
- opis jakościowy z pomocą skali,
- opis ilościowy z pomocą skali i podziałów,
- opis ilościowy.

Tabela 1. Opis jakościowy z pomocą skali

Poziom	Konsekwencje	Opis
1	bardzo ograniczone	mały bezpośredni wpływ na ziemię, bardzo ograniczone zakłócenia funkcji społecznych, nieufność wobec pojedynczych instytucji społecznych, bardzo ograniczone szkody majątkowe i środowiskowe
2	ograniczone	umiarkowany bezpośredni wpływ na zdrowie, ograniczone zakłócenia funkcji społecznych, przejściowa nieufność wobec kilku instytucji społecznych, ograniczone szkody majątkowe i środowiskowe

¹² Patrz: definicja na s. 114.

Poziom	Konsekwencje	Opis
3	poważne	znaczący bezpośredni lub umiarkowany pośredni wpływ na ziemię, poważne zakłócenia funkcji społecznych, dalsza nieufność wobec kilku instytucji społecznych lub zmiana zachowania, poważne szkody majątkowe i środowiskowe
4	bardzo poważne	bardzo duży bezpośredni lub znaczący pośredni wpływ na zdrowie, bardzo poważne zakłócenia funkcji społecznych, dalsza nieufność wobec kilku instytucji społecznych lub zmiana zachowania, bardzo poważne szkody majątkowe i środowiskowe
5	katastrofalne	Katastrofalny bezpośredni lub bardzo duży pośredni wpływ na ziemię, ekstremalne zakłócenia funkcji społecznych, stała nieufność wobec instytucji społecznych i ogólna niestabilność, katastrofalne szkody majątkowe i środowiskowe

Źródło: Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 48.

Tabela 2. Wyniki ilościowej analizy ryzyka

Analiza ryzyka		
Scenariusz	Częstotliwość (rocznie)	Konsekwencje
scenariusz 1	0,1	10 ofiar śmiertelnych
scenariusz 2	0,01	50 ofiar śmiertelnych
scenariusz 3	0,005	200 ofiar śmiertelnych

Źródło: Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 50.

Ocena ryzyka¹³

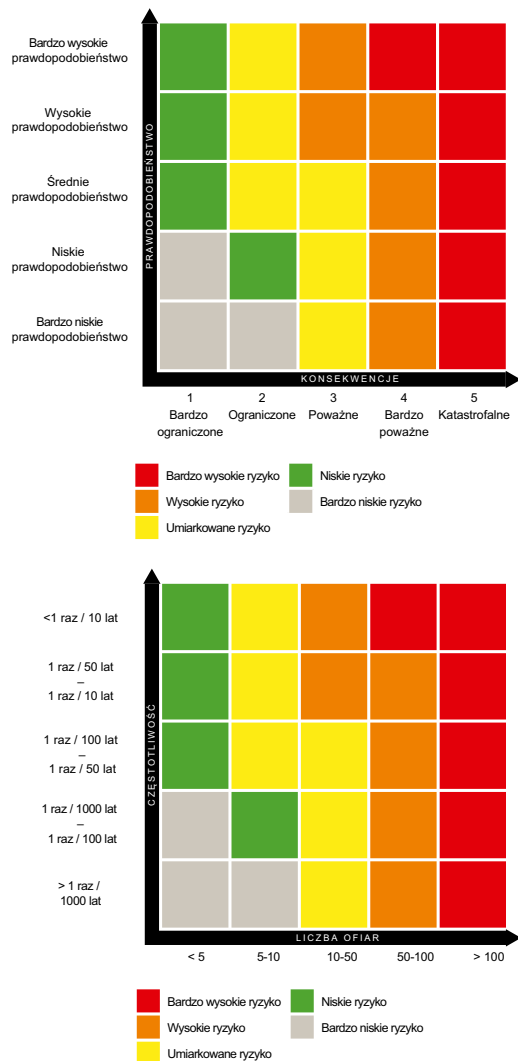
Ocena ryzyka oznacza analizę pozwalającą na określenie, czy poziom danego ryzyka¹⁴ jest akceptowalny, czy nie. Stanowi właściwą podstawę do planowania oraz wdrażania środków ograniczających ryzyko. Ocena powinna zawierać analizę zalet i wad proponowanych rozwiązań i zostać uzupełniona o niezbędne wnioski: czy dane rozwiązanie powinno zostać zastosowane, czy też nie, a także jak znaczący

¹³ W dokumencie zastosowano pojęcie oceny ryzyka, jednak etap ten odpowiada ewaluacji ryzyka, zgodnie z definicją i opisem w normie ISO 31000.

¹⁴ Patrz: definicja na s. 115.

będzie spadek ryzyka i jakie będą związane z tym koszty. Norma ISO 31000 dodatkowo podkreśla istotę tego etapu, który wymaga wielkiej dokładności i rzetelności w porównaniu z kryteriami ryzyka, a w obu przypadkach prowadzi do wypracowania najkorzystniejszych możliwych rozwiązań dla danego ryzyka.

Matryce ryzyka stanowią powszechne narzędzie ewaluacji ryzyka. Składają się one z dwóch połączonych (najczęściej pięciostopniowych) skali: prawdopodobieństwa i skutków, pozwalając na określenie poziomu akceptowalności danego ryzyka.

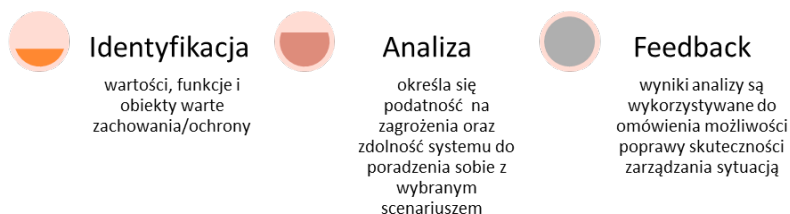


Rys. 3. Przykładowe matryce ryzyka

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 52.

Metodyka stosowana przez Szwedzką Agencję ds. Cywilnych Sytuacji Kryzysowych bazuje na wielowymiarowej analizie aktywności (MVA)¹⁵. Metoda ta opiera się na tzw. społecznej perspektywie, co oznacza, że podstawą oceny skutków zdarzenia jest ich wpływ na społeczeństwo, przy czym ryzyko definiuje się dla konkretnych, poszczególnych obiektów.

Jest to metoda oparta na procesie budowania scenariuszy na wypadek wystąpienia zagrożeń. Stanowi niejako udoskonaloną analizę scenariuszową przedstawioną w części I, którą dodatkowo można wspomagać specjalnym oprogramowaniem¹⁶. Praca jest podzielona i realizowana podczas trzech seminariów, poświęconych: identyfikacji, analizie i feedbackowi.



Rys. 4. Metoda MVA

Źródło: Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 62.

W trakcie pierwszego seminarium grupa robocza definiuje wartości, funkcje i obiekty warte zachowania/ochrony. Na tym etapie przywiązuje się dużą wagę do identyfikacji różnych dziedzin aktywności, np. dostępnych zasobów czy zaopatrzenia technicznego systemu. Następnie inwentaryzowane są zdarzenia niekorzystne¹⁷ – wraz ze szczegółową analizą ich konsekwencji, źródła ryzyka, wskazywane są zagrożone obiekty. Ostatnim krokiem tego etapu jest wyliczenie prawdopodobieństwa wystąpienia tych zdarzeń oraz ocena konsekwencji zidentyfikowanych wcześniej zagrożeń.

Druga faza koncentruje się na analizie, podczas której szczegółowo przedstawia się podatność na zagrożenia oraz odporność¹⁸ systemu, czyli jego zdolność do poradzenia sobie z wybranym scenariuszem. Poza określeniem przebiegu zdarzenia i następujących po sobie szczegółowych sytuacji scenariusz powinien wskazywać możliwe konsekwencje zdarzenia. Proces tworzenia scenariusza podzielony jest na trzy etapy. W pierwszym opisuje się dokładnie scenariusz, następnie określa się dla niego konieczne zasoby (dostępne siły i środki) oraz obowiązki i możliwości poszczególnych podmiotów zaangażowanych w zdarzenie. W ostatnim etapie, przed przystąpieniem do trzeciego seminarium, określa się niepożądane zmiany,

¹⁵ Źródło: opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 62–63.

¹⁶ Por.: część I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 2 *Metody wykorzystywane w ocenie ryzyka*, podrozdział 2.13 *Analiza scenariuszowa*.

¹⁷ Patrz: definicja na s. 139.

¹⁸ Patrz: definicja na s. 115.

jakie mogą nastąpić w trakcie trwania zdarzenia (instytucjonalne, organizacyjne i społeczne).

Ostatnią fazą jest feedback (tzw. informacja zwrotna), w trakcie którego wyniki analizy są wykorzystywane do omówienia możliwości poprawy skuteczności zarządzania sytuacją w przypadku przeanalizowanego konkretnego scenariusza.

Kolejnym narzędziem wykorzystywanym przez szwedzki system ochrony ludności jest analiza ryzyka i podatności (ROSA)¹⁹. Metoda ta kładzie duży nacisk na proces zarządzania ryzykiem²⁰. Jej cel stanowi przede wszystkim ocena zdolności podmiotu do zarządzania niepożądanym zjawiskiem. Wskazuje się również, że jest ona determinantem poprawy skuteczności zadań realizowanych w ramach zarządzania kryzysowego. Metoda ta w swoich głównych założeniach odwołuje się do postulatu stworzenia stale funkcjonującego systemu zarządzania kryzysowego (system ten jest inaczej definiowany niż w Polsce, bardziej zbliżony do procesów określanych w Polsce mianem ciągłości działania), który powinien być integralną częścią normalnej działalności podmiotu (ryzyko odwołuje się do procesów zachodzących w organizacji).

Pierwszym krokiem jest otrzymanie wsparcia od kierownictwa. Analiza zaczyna się od identyfikacji ryzyka i przypisanych im zagrożeń. Oceny opierają się na wiedzy grupy eksperckiej pracującej nad danym scenariuszem, a zatem omawiany proces jest analizą jakościową.

Każdy przedstawiciel w grupie zapisuje scenariusze, które mogą być zidentyfikowane, a następnie obrazuje je prostą metodą prawdopodobieństwa i konsekwencji w pięciostopniowej skali (matryca ryzyka). Opisy stają się bazą dla dalszej fazy, czyli pogłębionej analizy.

Dysponując katalogiem scenariuszy (wraz z przypisanym im ryzykiem), grupa decyduje, które z nich mają zostać poddane dalszej analizie. Odrzucone scenariusze mogą zostać oznaczone jako:

- 1) zdarzenia typowe, czyli występujące dosyć często (a więc dla których istnieją standardowe procedury postępowania),
- 2) takie, których wystąpienie jest na tyle mało prawdopodobne, że z punktu widzenia systemu nie jest ekonomiczne podejmowanie jakichkolwiek działań dotyczących ryzyka.

Wyniki szczegółowych analiz są przygotowane i przedstawiane przez grupę ds. zarządzania ryzykiem. Następnym krokiem jest zebranie wszystkich analizowanych scenariuszy i stworzenie profilu ryzyka²¹ podmiotu (systemu lub obiektu), wraz ze wskazaniem istniejących słabych punktów (podatności). Aby wizualnie przedstawić

¹⁹ Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 63–65.

²⁰ Fundament tej metody zakorzeniony jest w procesie zarządzania ryzykiem normy ISO 31000. Patrz szerzej: tamże, s. 190–203.

²¹ Patrz: definicja na s. 303.

wyniki, używa się trzech kolorów (dokument nie określa koloru) odpowiadających trzem poziomom oceny:

- bardzo dobrej,
- dobrej,
- niewystarczającej.



Rys. 5. Metoda ROSA

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 64.

Następnie wyniki przedstawiane są kierownictwu, które decyduje, jakie podjąć kroki. Metoda ta jest dość popularna, szczególnie w małych gminach. Zaletą jest to, że nie wymaga od twórców dogłębnej znajomości metod analizy ryzyka.

Wskazane wyżej narzędzia nie są jedynymi, które wykorzystuje szwedzka agencja. Na potrzeby zarządzania ryzykiem wykorzystywane są ponadto:

- 1) IBERO – narzędzie przygotowane przez Stockholm County Administrative Board przy współpracy z Emergency Preparedness Authority, Swedish Defence Research Agency oraz Lund University. Wykorzystuje ono przeznaczony dla poszczególnych jednostek administracyjnych system teleinformatyczny oraz bazodanowy i oparte jest na modułach: ocenie gotowości dla indywidualnego podmiotu (jednostki administracyjnej), ocenie gotowości dla kilku podmiotów, katalogu zinwentaryzowanych ryzyk i dostępnych zasobów (sił i środków) oraz raportowaniu. Metoda bazuje na analizie scenariuszowej²² i jest najbliższa metodzie wypracowanej przez stronę niemiecką²³;
- 2) wstępna analiza ryzyka (*Preliminary Risk Analysis* oraz *Broad Analysis*) – ogólna analiza jakościowa stosowana przy sporządzaniu map ryzyka, skoncentrowana na identyfikacji i scenariuszu ryzyka. Analiza ta jest często stosowana w wielu innych metodach, jako ich pierwsza faza, stanowiąca podstawę dla ustalania priorytetów do dalszych prac analitycznych. Nie daje pełnego obrazu ryzyka i nie wskazuje żadnych luk ani zdolności systemu. Za jej pomocą można wskazać jedynie ogólne scenariusze oparte na

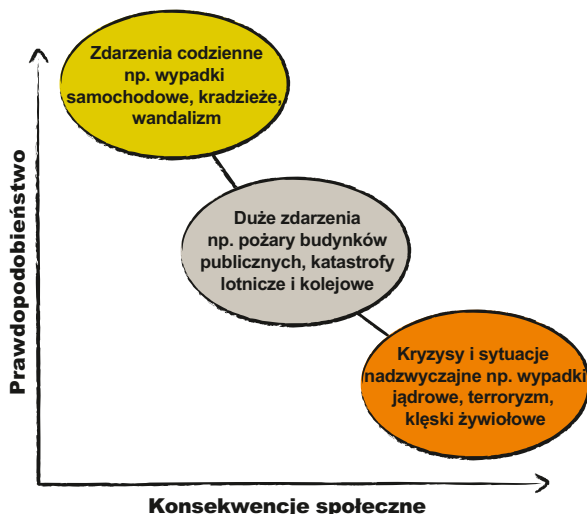
²² Patrz szerzej: Swedish Civil Contingencies Agency, *Guide...*, s. 65–66.

²³ Patrz: s. 271.

zidentyfikowanych zagrożeniach, ich możliwe przyczyny i konsekwencje, dokonać ewaluacji ryzyka oraz przedstawić ogólne rekomendacje działań redukujących konsekwencje²⁴;

3) analiza „co, jeśli?” oraz drzewa błędów.

W swojej metodyce Szwedzi zwracają uwagę na jeszcze jeden istotny element, który pozwala na umiejscowienie poszczególnych grup sytuacji (zdarzenia codzienne, duże zdarzenia, kryzysy) na wykresie ryzyka. Zależności pomiędzy tymi sytuacjami a kategoriami ryzyka: prawdopodobieństwem i konsekwencjami wskazuje rys. 6.



Rys. 6. Zależność pomiędzy skalą ryzyka a rodzajami zdarzeń

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Guide...*, dz. cyt., s. 12.

4.2. Szwedzka narodowa ocena ryzyka 2012

Szwedzka narodowa ocena ryzyka to dokument uwzględniający wyniki oceny ryzyka na szczeblu krajowym, przeprowadzonej zgodnie z wypracowaną metodyką. Jest częścią procesu rozwoju zbiorowej zdolności do zapobiegania szczególnym i niekorzystnym zdarzeniom oraz zarządzania nimi na każdym poziomie organizacji szwedzkiego społeczeństwa. Szwedzka ocena ryzyka jest bardziej szczegółową analizą i rozwinięciem identyfikacji ryzyka przeprowadzonej w 2011 r. Na analizę składa się praca gmin, rad regionów, zarządów regionów i innych organów publicznych, w tym Szwedzkiej Agencji ds. Cywilnych Sytuacji Kryzysowych (MSB), która jest także odpowiedzialna za koordynację pozostałych uzupełniających analiz, nieprzeprowadzanych przez wymienione instytucje. *Narodowa ocena ryzyka*

²⁴ Patrz szerzej: Swedish Civil Contingencies Agency, *Guide...*, s. 67–68.

została opracowana we współpracy z Unią Europejską i jest oparta na wspólnych wytycznych dla państw członkowskich, których celem jest stworzenie możliwości do rozwinięcia współpracy i wymiany doświadczeń w tym obszarze. Zawiera analizę i ocenę siedmiu zdarzeń. Wstępnie MSB wybrała 200 zdarzeń, opartych głównie na analizach ryzyka i podatności przeprowadzonych w Szwecji przez podmioty zaangażowane w zarządzanie sytuacjami kryzysowymi z lat 2010–2011. Zdarzenia najpierw zostały ocenione pod kątem chronionych wartości narodowych, a wskutek tej oceny wyodrębniono 40 zdarzeń. Grupę zdarzeń oceniono pod względem prawdopodobieństwa, konsekwencji i niepewności. 40 zdarzeń ogólnych rozpatrzono pod kątem kryteriów zdarzenia narodowego i tym sposobem wyodrębniono 27 zdarzeń narodowych. Na podstawie 27 zdarzeń opracowano 11 scenariuszy.

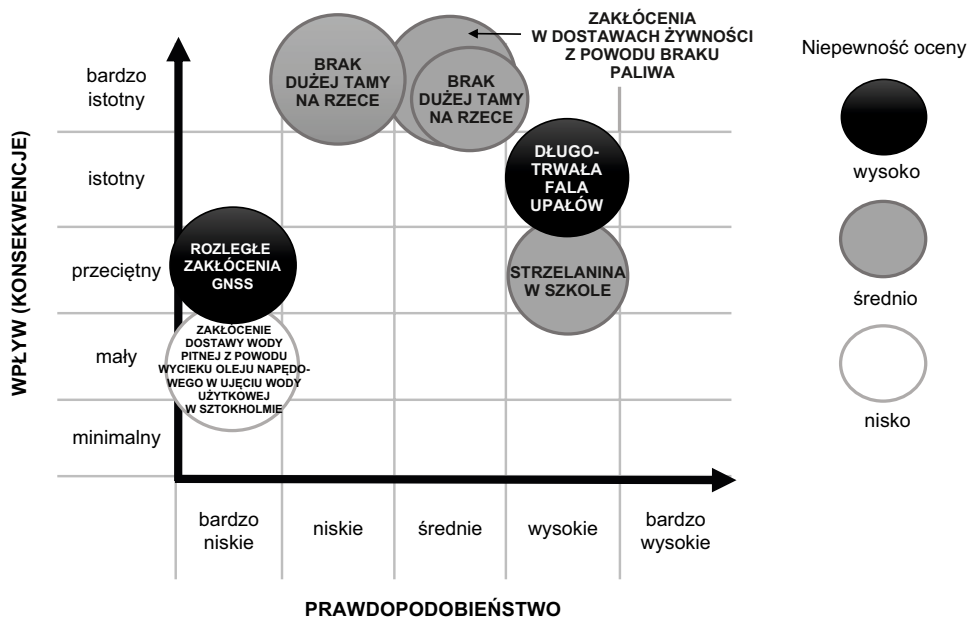
Scenariusze opisują zdarzenia zróżnicowane pod względem miejsca wystąpienia na terenie Szwecji. Każdy ze scenariuszy wskazuje na zagrożenie co najmniej jednej chronionej wartości narodowej, natomiast ogół scenariuszy musi uwzględnić zagrożenia wszystkich z tych wartości.

Są to tzw. czarne scenariusze, co oznacza, że zakładają zdarzenia, które mogą powodować poważne lub bardzo poważne skutki i są uważane za realne na podstawie wiedzy eksperckiej w dziedzinie, której scenariusz dotyczy. Scenariusze powstające w ramach *Szwedzkiej narodowej oceny ryzyka* są spójne z elementami analizy scenariuszowej opisanej w ramach części I i przydatne zarówno w identyfikacji ryzyka, analizie ryzyka, jak i ewaluacji. Mają jednak również za zadanie sprawdzić funkcjonowanie różnych elementów szwedzkiego systemu ochrony ludności.

W odniesieniu do wytycznych Komisji Europejskiej²⁵ ocenione scenariusze prezentowane muszą być w postaci matrycy ryzyka. Pozycja danego scenariusza na matrycy zależy przede wszystkim od ocen, na podstawie których zdarzenie zostało opracowane. Bardziej szczegółowe analizy w przyszłości mogą dać nowe, odmienne wyniki. Matryca ryzyka dla narodowej oceny ryzyka daje obraz połączonej oceny: prawdopodobieństwa, konsekwencji, niepewności²⁶ (prawdopodobieństwa i konsekwencji) dla każdego zdarzenia. Taka matryca nazywana jest matrycą 5×5, ponieważ składa się z pięciu kolumn i pięciu rzędów z 25 możliwymi kombinacjami oceny prawdopodobieństwa i wpływu (zob. rys. 7).

²⁵ European Commission, Commission Staff Working Paper, Risk Assessment and Mapping Guidelines for Disaster Management, 2010, SEC(2010) 1626 wersja ostateczna (17899/10).

²⁶ Niepewność – stan, również częściowy, braku informacji związanej ze zrozumieniem lub wiedzą na temat zdarzenia, jego następstw lub prawdopodobieństwa. Źródło: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, definicja 1.1, uwaga 5.



Rys. 7. Matryca ryzyka analizowanych scenariuszy w Narodowej ocenie ryzyka 2012

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Swedish...*, dz. cyt., s. 23.

Poniżej przedstawiono jakościową skalę matrycy ryzyka dla prawdopodobieństwa i konsekwencji, ze wskaźnikami ilościowymi, z wyjątkiem skutków politycznych i społecznych, które są opisane wyłącznie w sposób jakościowy.

Tabela 3. Skala prawdopodobieństwa

Skala jakościowa (matryca ryzyka)	Skala ilościowa oceny prawdopodobieństwa		
	dolna granica	środek przedziału	górną granicą
bardzo wysokie	$\geq 0,2$ w ujęciu rocznym ($\geq 0,5$ raz na 5 lat)	1 w ujęciu rocznym (raz do roku)	1 (raz do roku)
wysokie	$\geq 0,02$ w ujęciu rocznym (\geq raz na 50 lat)	0,1 w ujęciu rocznym (raz na 10 lat)	$< 0,2$ w ujęciu rocznym ($<$ raz na 5 lat)
średnie	$\geq 0,002$ w ujęciu rocznym (\geq raz na 500 lat)	0,0001 w ujęciu rocznym (raz na 1000 lat)	$< 0,02$ w ujęciu rocznym ($<$ raz na 50 lat)

Skala jakościowa (matryca ryzyka)	Skala ilościowa oceny prawdopodobieństwa		
	dolna granica	środek przedziału	górną granicą
niskie	≥ 0,0002 w ujęciu rocznym (≥ raz na 5000 lat)	0,0001 w ujęciu rocznym (raz na 1000 lat)	< 0,002 w ujęciu rocznym (< raz na 500 lat)
bardzo niskie	≥ 0	0,0001 w ujęciu rocznym (raz na 10000 lat)	< 0,0002 w ujęciu rocznym (< raz na 5000 lat)

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Swedish...*, dz. cyt., s. 23.




Tabela 4. Skala konsekwencji

Skala oceny konsekwencji (matryca ryzyka)	Skala dla każdego rodzaju konsekwencji		
	Skala ilościowa: konsekwencje dla człowieka	Skala ilościowa: konsekwencje ekonomiczne/dla środowiska	Skala jakościowa: konsekwencje polityczne/społeczne
bardzo istotne	≥ 50 martwych > 100 ciężko rannych	> SEK 1 bln	bardzo poważny
istotne	10–49 martwych i/lub 50–100 ciężko rannych	SEK 500 mln – SEK 1 bln	poważny
przeciętne	2–9 martwych i/lub 10–49 ciężko rannych	SEK 100–499 mln	poważny
nieznaczące	1 martwy i/lub 1–9 ciężko rannych	SEK 20–99 mln	nieznaczący
minimalne	brak martwych lub ciężko rannych, kilka drobnych urazów	< SEK 20 mln	minimalny

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Swedish...*, dz. cyt., s. 24.

Niepewność odzwierciedla wiarygodność danych pomocniczych, na których zostały oparte wcześniejsze oceny, czyli szacowany jest poziom zaufania do trafności oceny prawdopodobieństwa i konsekwencji. Dla każdego zdarzenia niepewność została oceniona zgodnie ze skalą, która ma trzy poziomy w matrycy – czarny (wysoki), szary (średni) i biały (niski).

Tabela 5. Skala niepewności

Oznakowanie w macyryzy ryzyka	Oznaczenie niepewności	Wyjaśnienie, uzasadnienie oceny
	wysoka	Jest niewiele statystyk i danych, na których może bazować ocena i występuje znaczny margines błędu
	średnia	Są dostępne statystyki i dane. Ekspertcy rozważają ocenę jako najbardziej zasadną, ale istnieje margines błędu
	niska	Ocena jest oparta na solidnym doświadczeniu, statystykach i innych danych. Możliwe, że ocena jest niedokładna, ale to mało prawdopodobne

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Swedish...*, dz. cyt., s. 24.

Długa fala upałów i ostrzał z broni na terenie szkoły zostały ocenione wśród wybranych zdarzeń jako zdarzenia o wysokim prawdopodobieństwie. Oszacowanie prawdopodobieństwa dla długiej fali upałów zostało oparte głównie na danych dotyczących zmian klimatycznych. W ciągu ostatnich 20 lat (1991–2010) odnotowano w Szwecji zwiększoną liczbę ciepłych miesięcy w porze letniej i fal upałów w porównaniu do poprzedzających ten okres 30 lat (1960–1990). Oszacowanie prawdopodobieństwa strzelaniny w szkole podobnej do tej opisanej w scenariuszu jest oparte na odnotowanych już zdarzeniach: przemoc w szkole ze skutkiem śmiertelnym w Szwecji (na dyskotecę szkolnej w 1961 r. – jedna ofiara śmiertelna) oraz dwie strzelaniny w szkołach w Finlandii. Strzelaninę udaremniono również w szwedzkich szkołach (w Malmö i w Sztokholmie). Ponadto wzięto pod uwagę częstotliwość tego typu zdarzeń poza granicami Szwecji (w Europie i na świecie). Wysoka ocena prawdopodobieństwa strzelaniny w szkole wynika również z niewielkich nakładów potrzebnych do przeprowadzenia takiego zdarzenia. Broń wykorzystywaną w ostrzałach w szkołach jest w Szwecji łatwa do nabycia, a współcześni przestępcy mogą inspirować się tego typu wydarzeniami bądź naśladować je, czerpiąc wiedzę z internetu. Znaczące zakłócenia w nawigacji satelitarnej oraz awaria dostaw wody pitnej w wyniku zanieczyszczenia benzyną źródła w Sztokholmie są oceniane jako zdarzenia o bardzo małym prawdopodobieństwie. Na poziomie systemu nawigacja satelitarna ma zapewnioną odpowiednią odporność na zakłócenia, natomiast mogą one występować lokalnie, co jest dość powszechne. Dostawa wody pitnej w regionie Sztokholmu jest również solidna. W przypadku obu systemów musiałoby zawieść kilka zabezpieczeń, aby doszło do wymienionych zdarzeń. Prawdopodobieństwo wystąpienia obu zdarzeń zostało więc oszacowane jako bardzo niskie.

Jako scenariusze o największych możliwych skutkach wytypowano: duży pożar na statku rejsowym, niedobór paliwa prowadzący do zakłóceń w dostawie żywności, usterkę tamy na rzece. Wszystkie trzy scenariusze uznano za sytuacje prowadzące do najpoważniejszych skutków, ale każde ze zdarzeń występuje

w innej kategorii konsekwencji (człowiek, gospodarka/środowisko, polityczny/społeczny). Scenariusze: niedobór paliwa prowadzący do zakłóceń w dostawie żywności i usterka tamy na rzece niosą znaczące konsekwencje dla gospodarki/środowiska, natomiast poważny pożar na statku dla gospodarki/środowiska i człowieka. Scenariusz dotyczący usterki tamy może także prowadzić do poważnych skutków dla człowieka, ale ocena nosi duże znamiona niepewności, gdyż zależy to od sposobu zarządzania sytuacją. Długa fala upałów miałyby poważne konsekwencje w kategoriach człowiek i gospodarka/środowisko, ponieważ scenariusz prowadziłby do cierpienia wielu ludzi w grupach ryzyka oraz złożonych skutków pośrednich (pożarów, przerw w dostawie prądu). Za najmniej poważny w skutkach scenariusz uznano awarię dostaw wody pitnej w wyniku zanieczyszczenia benzyną źródła w Sztokholmie. Niesie ona najmniejsze konsekwencje w kategorii: polityczny/społeczny.

Oceny zakłóceń nawigacji satelitarnej i przedłużonej fali upałów zostały zakwalifikowane jako te o wysokiej niepewności oceny. Oznacza to, że oceny te są zaniżone albo zawyżone. Analiza długiej fali upałów wykazała, że zdarzenie to różni się w niepewności oceny. Istnieje znaczna liczba danych w resorcie zdrowia, która wskazywałaby na niską niepewność oceny. Jednakże w odniesieniu np. do wpływu fali upałów na elektryczność, systemy komunikacyjne i informatyczne, niepewność oceny jest bardzo wysoka. Osiągnęła taki wynik głównie ze względu na niepewność oceny wpływu fali upałów na te systemy całościowo. Mogłaby zostać zredukowana do średniej, gdyby przeprowadzona została bardziej szczegółowa analiza. W przypadku strzelaniny w szkole, niedoboru paliwa prowadzącego do zakłóceń w dostawie żywności, usterki tamy i dużego pożaru na statku rejsowym niepewność oceny oszacowano na średnią. Jedynym zdarzeniem o niskiej niepewności oceny jest awaria dostaw wody pitnej w wyniku zanieczyszczenia benzyną źródła w Sztokholmie.

Ogólna ocena ryzyka zdarzeń

Matryca ryzyka zapewnia przegląd prawdopodobieństwa, konsekwencji i niepewności oceny. W związku z tym jedno z trzech poniższych zdarzeń: niedobór paliwa prowadzący do zakłóceń w dostawie żywności, usterka tamy na rzece oraz długa fala upałów – powinno osiągnąć najwyższy poziom ryzyka. Jest tak, ponieważ wszystkie zostały ocenione jako zdarzenia o poważnych lub bardzo poważnych konsekwencjach oraz od średniej do wysokiej niepewności oceny. Istnieją jednak duże różnice między ocenami tych zdarzeń, których matryca nie bierze pod uwagę, ponieważ skala jest niedostatecznie szczegółowa i powinna zostać ulepszona. Te trzy zdarzenia zostały również ocenione od średniej do wysokiej niepewności oceny, co znaczy, że mogło zdarzyć się zawyżenie lub zaniżenie faktycznej sytuacji. Dotyczy to szczególnie długiej fali upałów, którą oszacowano na wysoką niepewność oceny. Pozostałe dwa wydarzenia mają niską niepewność oceny. Poważne zakłócenie nawigacji satelitarnej nie zostało wybrane jako zdarzenie o największym ryzyku. Jest ono również uważane za zdarzenie o wysokiej niepewności oceny, co oznacza, że

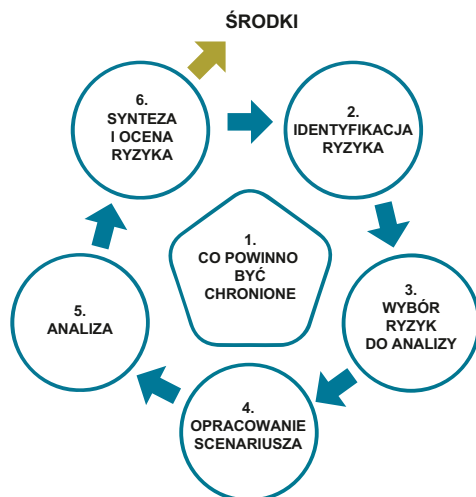
ocena prawdopodobieństwa i konsekwencji dla tego zdarzenia mogły zostać zaniżone lub zawyżone. W tym przypadku niepewność oceny, tak jak w przypadku długiej fali upałów, jest zależna od stanu wiedzy. Dogłębne analizy stanowią podstawę do przeprowadzenia ponownej oceny o mniejszej niepewności. Zakłócenie dostaw wody pitnej w związku z zanieczyszczeniem benzyną źródła w Sztokholmie zgodnie z przeprowadzoną oceną jest zdarzeniem o najniższym ryzyku spośród siedmiu analizowanych. Stwierdzono tak, ponieważ scenariusz ten ma najmniejsze prawdopodobieństwo oraz konsekwencje i charakteryzuje się najniższą niepewnością oceny.

Ogólny proces i metodyka

Praca nad *Narodową oceną ryzyka* wyłoniła sześć kroków prowadzących do osiągnięcia założonego wyniku:

- określenie, co powinno być chronione,
- identyfikacja ryzyka (zdarzeń niekorzystnych),
- wybór zdarzeń do analizy,
- opracowanie scenariuszy dla wybranych zdarzeń,
- analiza scenariuszy: konsekwencji, prawdopodobieństwa i niepewności oceny,
- synteza i ocena ryzyka.

Nietrudno zauważyć, że autorzy ze Szwecji również korzystali ze wzorów w postaci międzynarodowych norm, w tym ISO 31000 oraz wytycznych Komisji Europejskiej²⁷. Stąd wśród kroków *Narodowej oceny ryzyka* nie zabrakło głównych podprocesów stanowiących komponent procesu zarządzania ryzykiem, zgodnie ze wspomnianą normą.



Rys. 8. Sześć kroków oceny ryzyka

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Swedish...*, dz. cyt. s. 27.

²⁷ European Commission, Commission Staff Working Paper, Risk Assessment and Mapping Guidelines for Disaster Management, 2010, SEC(2010) 1626 wersja ostateczna (17899/10).

Zawarte w pierwszym kroku wartości narodowe podlegające ochronie to: życie i zdrowie człowieka, funkcjonowanie społeczne (funkcjonowanie i ciągłość tego, co znacząco wpływa na codzienne życie obywateli, przedsiębiorstw i innych organizacji – dotyczy to również wiedzy eksperckiej), demokracja, rządy prawa, prawa i wolności człowieka, mienie prywatne i publiczne, wartość produkcji dóbr i usług, niepodległość państwa.

Drugi krok obejmuje identyfikację zdarzeń, które mogą w pewien sposób zagrażać chronionym wartościom albo powodować negatywne dla nich skutki. Na tym etapie zdarzenia nie są określane jako ryzyko, ale jako zdarzenia ogólne. Stanowią one połączenie chronionej wartości, zagrożenia i sposobu jego oddziaływania na tę wartość. Aby dokonać wyboru zdarzenia, które będzie stanowiło podstawę do późniejszej analizy rozwoju scenariuszy, MSB sklasyfikowała i skatalogowała ponad 200 analiz ryzyka i podatności różnych zdarzeń, które przeprowadziły agencje rządowe w latach 2010–2011. Na podstawie tego materiału przeprowadzono warsztaty z 50 przedstawicielami ważnych instytucji i zarządów regionów. Na warsztatach dokonano przeglądu katalogów zdarzeń²⁸ w celu uzupełnienia ich innymi zdarzeniami i przeanalizowania sposobów, w których wartości mogłyby być zagrożone. Uczestnicy mieli także okazję przedstawić własne poglądy na temat zdarzeń, które uznali za cenną bazę do głębszej analizy. Przedstawiono 113 propozycji, kilka z nich powieliło te same kwestie przedstawione w różny sposób. Wybrano 40 zdarzeń, które uznano za istotne. Po warsztatach katalog dopracowano i ulepszono na podstawie propozycji uczestników.

Przeprowadzenie szczegółowej analizy 40 wybranych zdarzeń nie było ani możliwe, ani konieczne, dlatego też na podstawie obecnych warunków w Szwecji zdecydowano się w kolejnym kroku na przeprowadzenie analizy 5–10 zdarzeń rocznie. Zdarzenia zostały ocenione na podstawie wstępnych wymogów (pod względem spełnienia kryterium kryzysu społecznego, rozważenia jako zdarzenie o zasięgu narodowym, a także ze względu na dotkliwość), które pozwoliły na wybór 27 zdarzeń. W kolejnym etapie na podstawie przeglądu źródeł literaturowych nie wykluczono dalszej liczby zdarzeń, dlatego też przeanalizowano możliwość połączenia²⁹ tych o zbliżonej genezie. W wyniku takiego działania z 27 powstało 7 nowych zdarzeń oraz 11 wcześniej wytypowanych – w sumie 18. Po przeprowadzeniu ponownej oceny zredukowano liczbę zdarzeń do 13. Aby dostosować w przybliżeniu liczbę zdarzeń do założonej, wykluczono jeszcze dwa zdarzenia. Postanowiono o potrzebie szczegółowej analizy odrzuconych scenariuszy w kolejnych latach przeprowadzania oceny ryzyka. Tak ukształtowała się lista 11 scenariuszy:

- poważne zakłócenia nawigacji satelitarnej,
- ostrzał z broni na terenie szkoły,

²⁸ Katalog zdarzeń – uporządkowany wykaz lub spis zdarzeń. Źródło: opracowanie autorskie.

²⁹ Np. połączony scenariusz aktu terrorystycznego z rozproszeniem bomby chemicznej.

- zakłócenia dostaw wody pitnej w wyniku zanieczyszczenia paliwem źródła wody w Sztokholmie,
- zakłócenia dostaw żywności w wyniku niedoboru paliwa,
- duży pożar na statku rejsowym,
- awaria tamy na rzece,
- długa fala upałów,
- pandemia spowodowana wirusem grypy A/H5N1 (wirus ptasiej grypy),
- katastrofa nuklearna z emisją radioaktywną,
- atak terrorystyczny w Sztokholmie (bomby w Sergels i na dworcu centralnym),
- niepokoje społeczne i zamieszki polityczne).

Używając zdarzeń jako punktów wyjściowych, w dalszym kroku opracowywano analizy. Aby były przydatne i użyteczne na poziomie narodowym, musiały zostać skonstruowane w podobny sposób. W tym celu MSB opracowała i wdrożyła zmienne dla scenariuszy. Ważne jest, aby ciąg zdarzeń w nich zawarty był wiarygodny nie tylko dla osób zaangażowanych w analizę. Każdy powinien być opracowany jako czarny scenariusz. Aby scenariusz mógł zostać przeanalizowany, potrzebne jest wysokie prawdopodobieństwo jego wystąpienia, a jego przewidywane skutki muszą być poważne.

Na etapie analizy scenariusze zostają przeanalizowane pod kątem ich prawdopodobieństwa, konsekwencji (bezpośrednich i pośrednich), a także niepewności oceny. Ważnym elementem jest udział odpowiednio przygotowanych ekspertów, którzy zapewnią wysoki poziom tych analiz. Oceny konsekwencji są opracowywane z pomocą przewodnika. Konsekwencje oceniane są w odniesieniu do narodowych wartości, podlegających ochronie. Każda wartość chroniona oceniania jest na podstawie jednego lub większej liczby wskaźników.

Tabela 6. Wskaźniki dla wartości narodowych podlegających ochronie

Wartości chronione	Wskaźniki
funkcjonalność społeczeństwa	zakłócenia codzienności
życie i zdrowie ludzi	liczba ofiar śmiertelnych
	liczba ciężko rannych/chorych
	brak zapewnienia podstawowych potrzeb
	liczba osób, które muszą być ewakuowane
wartości ekonomiczne i środowisko	ogólne skutki ekonomiczne
	skutki dla natury i środowiska
demokracja, praworządność, prawa człowieka i wolność	niepokój społeczny wynikający z negatywnych zmian zachowania
	brak zaufania w instytucjach społecznych
	poważny wpływ na narodowe decyzje polityczne

Wartości chronione	Wskaźniki
demokracja, praworządność, prawa człowieka i wolność cd.	brak kontroli nad instytucjami publicznymi
	wpływ na międzynarodową reputację Szwecji
suwerenność narodowa	brak kontroli nad terytorium kraju

Źródło: Opracowanie własne na podstawie Swedish Civil Contingencies Agency, *Swedish...*, dz. cyt., s. 31.

Następnie oceniane jest prawdopodobieństwo, konsekwencje oraz niepewność oceny – co zostało opisane w *Przewodniku po analizie ryzyka i podatności*. W kroku piątym następuje porównanie z kryteriami i ewaluacja ryzyka. Celem tego działania jest porównanie wniosków uzyskanych z wyników analizy ryzyka. Rezultaty analiz zostają zebrane i zaprezentowane na wspólnej macyzy ryzyka, która pokazuje relatywne prawdopodobieństwo, konsekwencje oraz niepewność oceny na potrzeby ich porównania. Wnioski z ewaluacji ryzyka prowadzą do ustalenia priorytetów postępowania z ryzykiem i określenia niezbędnych środków do dalszych działań w perspektywie ogólnokrajowej.

W ostatnim kroku następuje zebranie zastosowanych metod i narzędzi identyfikacji, ewaluacja, ustalenie priorytetów i przedstawienie propozycji koniecznych środków na podstawie analizy i ewaluacji ryzyka. Propozycje są rozważane i porównywane z innymi zadaniami MSB w obszarze ochrony ludności oraz przygotowania na sytuacje kryzysowe.

5. ZARZĄDZANIE RYZYKIEM W WIELKIEJ BRYTANII

W rozdziale tym analizie poddano dokument *National Risk Register* (*Krajowy rejestr ryzyka*¹ – z lat 2010 i 2013), który obejmuje wiedzę z wielu departamentów i agencji odpowiedzialnych za zarządzanie kryzysowe w Wielkiej Brytanii. Dokument publikowany jest od 2008 r., według zapisów zawartych w *Strategii bezpieczeństwa narodowego (UK)* i zawiera opis głównych kategorii zagrożeń oraz sposobów zapobiegania im, a także ocenę ryzyka², której poświęcono więcej uwagi. Analiza dokonywana jest za pomocą oceny konsekwencji i prawdopodobieństwa wystąpienia głównych zagrożeń w perspektywie 5 lat, przy czym priorytetem są zagrożenia, które mogą mieć bezpośredni wpływ na działalność państwa. Każdego roku rząd przeprowadza ocenę ryzyka: *National Risk Assessment – NRA* (*Narodowa ocena ryzyka*). Na podstawie NRA publikowany jest *National Risk Register of Civil Emergencies – NRR* (*Krajowy rejestr ryzyka*).

W niniejszym rozdziale zaprezentowano brytyjskie doświadczenia z zakresu wypracowania i zastosowania elementów procesu zarządzania ryzykiem. Celem rozważań było wskazanie cennych praktyk tego kraju w omawianym zakresie oraz podkreślenie dobrych praktyk, możliwych do wykorzystania na potrzeby polskich rozwiązań.

5.1. Krajowy rejestr ryzyka

Zgodnie z informacją zawartą w edycji NRR z 2010 r., proces oceny ryzyka wykorzystuje historyczne i naukowe dane, modele numeryczne oraz opinie ekspertów. Każdy region i społeczność w państwie ma swój własny profil ryzyka³. Istnieją trzy

¹ Dokument zawiera zgodny z nomenklaturą normy ISO Guide 73:2009 wykaz informacji o zidentyfikowanych ryzykach oraz szeroki opis potencjalnych ryzyk, wraz z opisem działań państwa zmierzających do ich ograniczenia. Głównie stanowi jednak podstawę do planowania dla podmiotów i jednostek administracji publicznej.

² W normie ISO proces ten obejmuje identyfikację, analizę oraz ewaluację ryzyka, natomiast w dokumencie brytyjskim zawiera: identyfikację ryzyka, ocenę prawdopodobieństwa ryzyk i ich konsekwencji oraz porównanie ryzyk.

³ Profil ryzyka – opis zestawu ryzyk. Źródło: ISO Guide 73:2009 Risk Management – Vocabulary, definicja 3.8.2.5.

etapy analizy. Pierwszym jest identyfikacja ryzyka⁴ poprzez konsultacje eksperckie, co daje obraz potencjalnych zdarzeń, wypadków, zagrożeń naturalnych, a także ataków, które mogą spowodować znaczne szkody i zakłócenia w Wielkiej Brytanii.

W ramach procesu identyfikacji ryzyka do analizy wybierany jest czarny scenariusz, czyli scenariusz o wysokim ryzyku wystąpienia (duże prawdopodobieństwo i konsekwencje), co stanowi podstawę do opracowania scenariusza zdarzeń, a wysoce nieprawdopodobne scenariusze są wykluczane. W ramach konsultacji ekspertów z departamentów rządowych opracowano listę około 80 rodzajów zdarzeń, które spełniają definicję nagłych zgodnie z ustawą regulującą planowanie i zarządzanie kryzysowe (*Civil Contingencies Act 2004*). Dalsze 40 widnieje na liście rezerwowej, choć uznano, że nie wyczerpują definicji zdarzeń nagłych⁵. W związku z tym eksperci uważają, że mogą wziąć je pod uwagę w przyszłości i że powinny zostać poddane przeglądowi⁶.

Ustanawiając kontekst ryzyka⁷, rozważa się następujące kwestie:

- 1) jakie są cele w zarządzaniu ryzykiem?
- 2) jakie rodzaje ryzyka wymagają natychmiastowego działania? Które mogą zostać przyjęte?
- 3) jakie problemy pojawiły się w przeszłości – i jakie były tego konsekwencje?
- 4) w jaki sposób ograniczone zasoby należy rozmieścić, aby zminimalizować ryzyko?

Biorąc pod uwagę skutki, uwzględnia się:

- liczbę ofiar śmiertelnych,
- zranienia i urazy,
- zakłócenia społeczne, biorąc pod uwagę brak uzyskania dostępu do opieki zdrowotnej lub edukacji, przerwy w świadczeniu podstawowych usług (dostęp do wody i prądu), a także konieczność ewakuacji osób z danego obszaru,
- straty ekonomiczne.

Podjęto również próbę oszacowania, jakie konsekwencje psychologiczne dla społeczeństwa mogą mieć katastrofy.

Kolejnym etapem jest ocena prawdopodobieństwa i konsekwencji każdego ryzyka. Do oceny prawdopodobieństwa używane są dane statystyczne, naukowe i historyczne. Tam, gdzie to możliwe, w ocenie uwzględnia się rozwój znanych lub prawdopodobnych zagrożeń w perspektywie najbliższych 5 lat. Ryzyko definiowane jest według ustalonych kryteriów, a prawdopodobieństwo wystąpienia zdarzenia

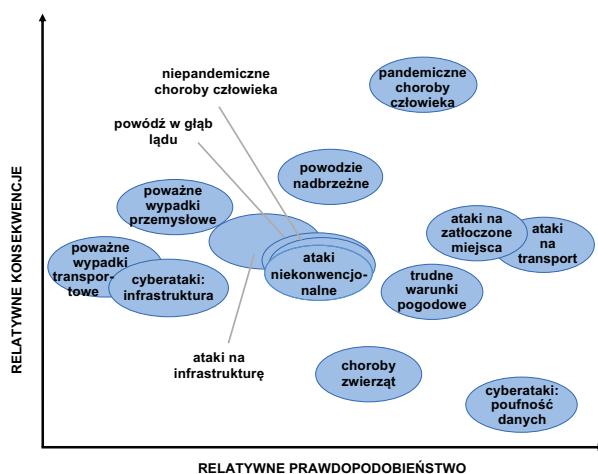
⁴ Patrz: definicja na s. 106.

⁵ Nagły wypadek (ang. emergency): a) zdarzenie lub sytuacja, która powoduje poważne zagrożenie dla ludzi w Wielkiej Brytanii, b) zdarzenie lub sytuacja, która powoduje poważne zagrożenie dla środowiska w Wielkiej Brytanii lub c) wojna lub terroryzm, który powoduje poważne zagrożenie dla bezpieczeństwa Wielkiej Brytanii. Źródło: *Civil Contingencies Act 2004*, art. 1, ust. 1.

⁶ Cabinet Office, The National Risk Register of Civil Emergencies (NRR), London 2010, s. 53. Przegląd – patrz: definicja na s. 113.

⁷ Patrz: definicja na s. 109.

określa się, biorąc także pod uwagę różne rodzaje ryzyka. Przyjmuje się skalę od 1 do 5. Kombinacja prawdopodobieństwa i konsekwencji wyznacza poziom ryzyka⁸, biorąc również pod uwagę ramy czasowe, w których działanie może być wymagane – wyższy wynik wskazywałby na potrzebę szybszego działania. Zagrożenia rozpatrywane są pod względem ich wystąpienia na terenie całego kraju w ciągu następnych 5 lat. Rys. 1 przedstawia relatywne⁹ prawdopodobieństwo i konsekwencje każdej z głównych grup ryzyka w odniesieniu do całego kraju. Analiza wskazuje epidemię grypy jako największe zagrożenie, jednak ryzyko może różnić się w zależności od lokalizacji.



Rys. 1. Zagrożenia umieszczone na wykresie w kontekście prawdopodobieństwa i wpływu

Źródło: Opracowanie własne na podstawie Cabinet Office, *The National...*, dz. cyt., s. 5.

Tam, gdzie to możliwe, ryzyka przedstawione są indywidualnie na matrycach. Ze względu na klasyfikację niektórych informacji zawartych w *National Risk Assessment* (NRA), zagrożenia zostały pogrupowane w kategorie¹⁰ (np. ataki na zatłoczone miejsca). Kategorie oraz ryzyka te przedstawiają matryce na rys. 2. Ponadto można zauważyć, że obie skale nie są bezpośrednio porównywalne ze sobą, na przykład zagrożenia „wysokie” niekoniecznie mają „większą niż 50 proc.” szansę wystąpienia. Zagrożenia w górnej prawej ćwiartce mają ten sam priorytet wystąpienia.

Prawa strona matrycy przedstawia prawdopodobieństwo wystąpienia ataku terrorystycznego, lewa zaś – innych zagrożeń możliwych. Dla obu prawdopodobieństwo zakładane jest w perspektywie najbliższych 5 lat.

⁸ Poziom ryzyka – patrz: definicja na s. 115.

⁹ Dotyczy prognozy prawdopodobieństwa na najbliższe 5 lat.

¹⁰ Kategoria – klasa obiektów mających określone cechy i powiązanych wzajemnymi relacjami. Źródło: <http://sjp.pl/kategoria> [dostęp: marzec 2015].

Krajowy rejestr ryzyka nie obejmuje:

- 1) długoterminowych globalnych zagrożeń – takich jak zmiany klimatu czy też konkurencja w dostawach energii,
- 2) ryzyka związanego z nagłymi wypadkami występującymi poza granicami kraju, chyba że mają one wpływ bezpośrednio na ludność lub środowisko w Wielkiej Brytanii,
- 3) codziennych zdarzeń, takich jak przestępstwa pospolite.

Relatywna względna ocena wpływu		katastrofalne ataki terrorystyczne			
		cyberataki: infrastruktura	ataki na infrastrukturę cyberataki na mniejszą skalę	ataki na zatłoczone miejsca	ataki na systemy transportu
					cyberataki: poufność danych
	niskie	średnio niskie	średnie	średnio wysokie	wysokie

Względne prawdopodobieństwo wystąpienia w kolejnych 5 latach

Relatywna względna ocena wpływu	5					pandemia grypy
	4			powodzie nadbrzeżne wylewny wybuch wulkanu		
	3	poważne wypadki transportowe	poważne wypadki przemysłowe	inne choroby zakaźne powodzie w głąb lądu	ciężka pogoda kosmiczna niskie temperatury i duże opady śniegu fale gorąca	
	2			choroby zwierząt susza zakłócanie porządku publicznego	eksplozywna erupcja wulkanu burze i wichury	
	1			poważne pożary	destrukcyjne działania przemysłowe	
	między 1 w 20000 i 1 w 2000	między 1 w 2000 i 1 w 200	między 1 w 200 i 1 w 20	między 1 w 20 i 1 w 2	większy niż 1 w 2	
	Względne prawdopodobieństwo wystąpienia w kolejnych 5 latach					

Rys. 2. Podstawowe zagrożenia, na jakie narażona jest Wielka Brytania

Źródło: Opracowanie własne na podstawie Cabinet Office, National..., dz. cyt., s. 10.

Wszystkie zagrożenia mające wpływ na bezpieczeństwo narodowe, łącznie z zagrożeniem katastrofami naturalnymi¹¹ oraz atakami terrorystycznymi, obejmuje dokument niejawni *National Security Risk Assessment* (NSRA). Wielka

¹¹ Katastrofa naturalna – zdarzenie związane z działaniem sił natury, w szczególności wyładowania atmosferyczne, wstrząsy sejsmiczne, silne wiatry, intensywne opady atmosferyczne, długotrwałe występowanie ekstremalnych temperatur, osuwiska ziemi, pożary, susze, powodzie, zjawiska lodowe na rzekach i morzu oraz jeziorach i zbiornikach wodnych, masowe występowanie szkodników, chorób roślin lub zwierząt albo chorób zakaźnych ludzi albo też działanie innego żywiołu. Źródło: art. 3 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2002 r. nr 62, poz. 558, z późn. zm.).

Brytania uważana jest na świecie za jednego z pionierów zarządzania ryzykiem w sytuacjach nadzwyczajnych¹².

5.2. Standard zarządzania ryzykiem FERMA

Specjaliści brytyjscy przyjmują dwoistą perspektywę postrzegania ryzyka – jako zagrożenia i szansy (ta perspektywa ma również swoje odzwierciedlenie w normie ISO 31000, dookreślając definicję ryzyka: niepewność powoduje pozytywne bądź negatywne odchylenie od oczekiwań), ale w obszarze bezpieczeństwa zajmują się przede wszystkim zagrożeniami, inaczej – zdarzeniami, które mogą mieć wyłącznie negatywne (niekorzystne) następstwa. Zarządzanie ryzykiem zostało ukierunkowane na zapobieganie szkodom¹³ i ich ograniczanie.

Punktem wyjścia dla zarządzania ryzykiem w obszarze bezpieczeństwa są zagrożenia dla funkcjonowania społeczności, wspólnot, rodzin, organizacji. Zagrożenia dla organizacji i jej działalności mogą wynikać zarówno z oddziaływania czynników wewnętrznych, jak i zewnętrznych w stosunku do organizacji. Może to dotyczyć każdego podmiotu, systemu, społeczności, wspólnoty, rodziny.

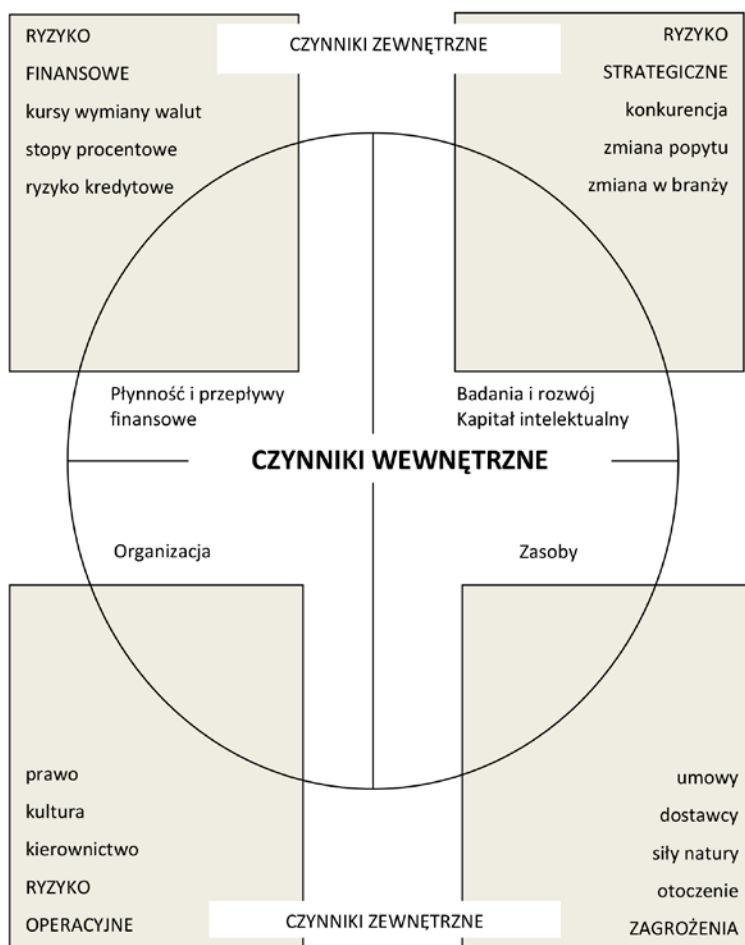
Rys. 3 prezentuje przykładowy zbiór czynników ryzyka¹⁴. Łatwo dostrzec, że nie wszystko jest tu jednoznaczne. Wiele czynników ma charakter zarówno wewnętrzny, jak i zewnętrzny, niektóre ryzyka mogą wynikać z przyczyn wewnętrznych i zewnętrznych – oba te obszary przenikają się lub nakładają na siebie. Każda klasyfikacja jest wynikiem przyjęcia jakiejś metody. W prezentowanym przykładzie (rys. 3) ryzyka te zestawiono w postaci czynników (strategiczne, finansowe, operacyjne, zagrożenia¹⁵ itd.).

¹² Sytuacja nadzwyczajna (ang. *emergency*) – nagle, gwałtowne, zazwyczaj niespodziewane zdarzenie (incydent) lub okoliczności, które z wysokim prawdopodobieństwem lub na pewno spowodują poważny uszczerbek na zdrowiu lub straty w mieniu i wymagają natychmiastowych działań zapobiegawczych lub naprawczych ze strony odpowiednich służb. Źródło: PN-EN 15975-1:2011 Bezpieczeństwo zaopatrzenia w wodę pitną. Przewodniki zarządzania kryzysowego i ryzyka. Część 1: Zarządzanie kryzysowe.

¹³ Szkoła (ang. *harm*) – uraz fizyczny lub uszczerbek na zdrowiu, uszkodzenie mienia lub degradacja środowiska, http://www.ciop.pl/CIOPPortalIWAR/appmanager/ciop/pl?_nfpb=true&_pageLabel=P20600158531378294224233&html_tresc_root_id=300001931&html_tresc_id=300001945&html_klucz=300001931&html_klucz_spis=, [dostęp: marzec 2015].

¹⁴ Czynniki ryzyka – okoliczność, stan prawny, stan faktyczny, które mogą, ale nie muszą wywołać ryzyko wystąpienia nieprawidłowości. Źródło: § 1 załącznika do zarządzenia nr 80 Wojewody Mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie. Zdarzenie, działanie lub zaniechanie, które może spowodować wystąpienie ryzyka lub też jego zwiększenie/zmniejszenie. Źródło: § 1 zarządzenia nr 3666/2012 Prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.

¹⁵ To m.in. możliwość poniesienia strat z tytułu niekorzystnych umów, niewywiązania się z umowy kontrahentów oraz inne zagrożenia, włącznie z możliwością odniesienia obrażeń lub śmierci w wyniku zdarzeń losowych lub działania sił natury.



Rys. 3. Przykładowy rozkład czynników ryzyka

Źródło: Opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, s. 4.

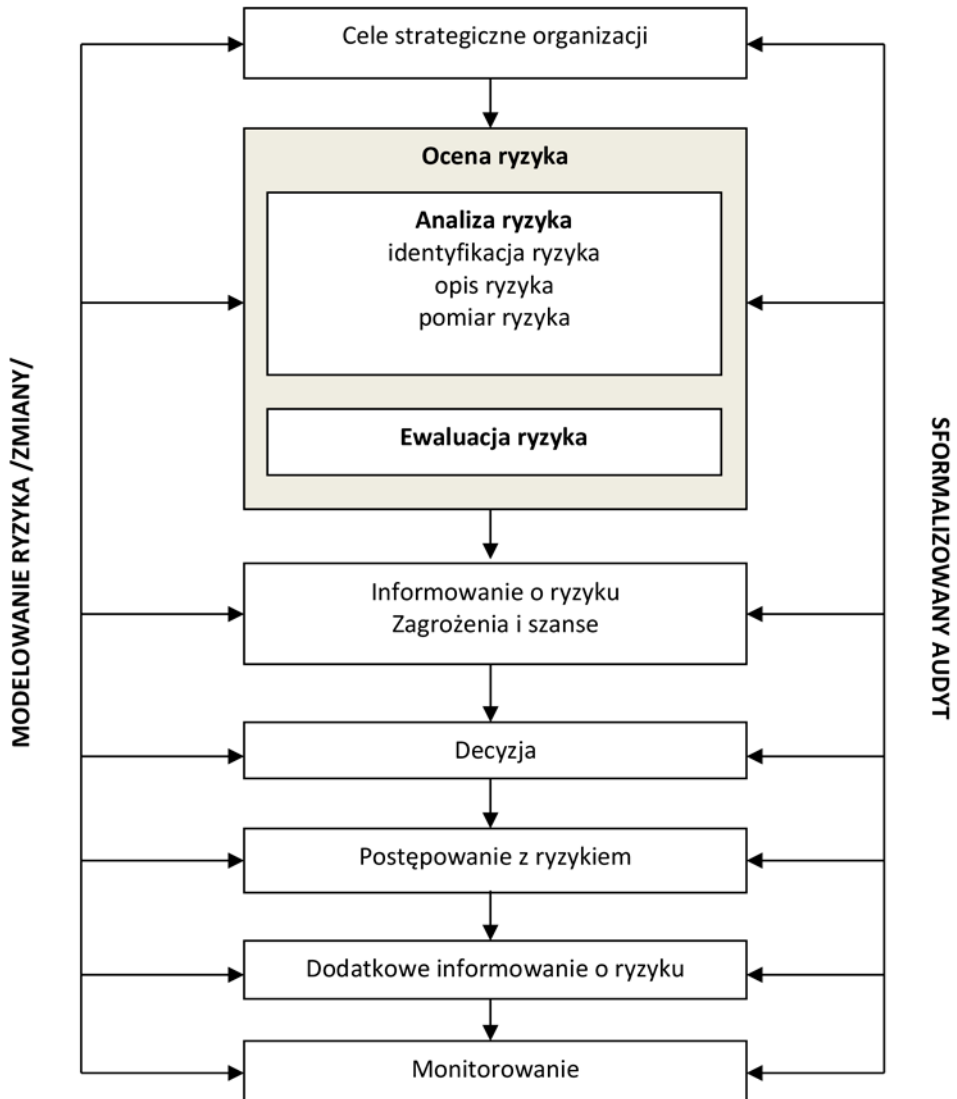
Zarządzanie ryzykiem stanowi o wartości organizacji systemu, przyczyniając się do realizacji celów organizacji poprzez¹⁶:

- 1) zapewnienie ram systemowych, dzięki którym działalność organizacji będzie prowadzona w sposób spójny i kontrolowany,
- 2) usprawnienie procesu podejmowania decyzji, planowania i określania rankingu priorytetów dzięki uzyskaniu kompleksowej wiedzy na temat działalności organizacji, stopnia niepewności oraz szans i zagrożeń,
- 3) przyczynienie się do efektywniejszego wykorzystania i alokacji zasobów, jakimi dysponuje organizacja,
- 4) zmniejszenie niepewności w innych obszarach działalności niż kluczowe,

¹⁶ *Standard zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 5.

- 5) ochronę oraz budowanie majątku i wizerunku organizacji (przedsiębiorstwa, systemu),
- 6) pomoc w rozwijaniu potencjału personalnego oraz bazy wiedzy organizacji,
- 7) poprawę efektywności działania.

Norma ISO 31000 stawia na uniwersalną definicję, wskazując, że w odniesieniu do ryzyka są to przede wszystkim skoordynowane działania obejmujące kierowanie organizacją i nadzorowanie jej.



Rys. 4. Proces zarządzania ryzykiem

Źródło: Opracowanie własne.

Ocena ryzyka¹⁷ jest procesem złożonym. Norma ISO Guide 73:2009 definiuje ocenę ryzyka jako całościowy proces złożony z identyfikacji, analizy ryzyka¹⁸ oraz ewaluacji ryzyka¹⁹. Analiza ryzyka jest z kolei procesem złożonym z identyfikacji ryzyka, opisu ryzyka i jego pomiaru. *Standard FERMA* pod pojęciem oceny ryzyka rozumie analizę ryzyka (w której skład wchodzi identyfikacja, opis i pomiar ryzyka) oraz ewaluację ryzyka.

Identyfikacja ryzyka jest określeniem stopnia niepewności, na jaką jest narażona organizacja – to zupełnie inne podejście niż w ramach omówionych metodyk czy międzynarodowych norm. Norma ISO 31000 rozumie ją wprost, jako proces poszukiwania, rozpoznawania i opisywania ryzyka. Proces ten wymaga szczególnej wiedzy na temat samej organizacji, uwarunkowań, w których działa oraz jej prawnego, społecznego, politycznego i kulturowego otoczenia, a także dogłębnego zrozumienia celów strategicznych i operacyjnych organizacji, w tym czynników zasadniczych dla osiągnięcia powodzenia oraz zagrożeń i szans związanych z realizacją tych celów. Identyfikacja ryzyka wymaga podejścia metodycznego, co powinno gwarantować uwzględnienie wszelkich istotnych obszarów aktywności organizacji, a także wszelkich związanych z tym ryzyk. Identyfikując ryzyko, określa się stopień niepewności w każdym obszarze działalności. Obszary działalności organizacji i podejmowane decyzje można podzielić na wiele sposobów, według różnych kryteriów²⁰, np.²¹:

1. Kwestie strategiczne – związane z długofalowymi celami strategicznymi²² organizacji. Mogą na nie wpływać takie okoliczności, jak dostępność zasobów, zagrożenia polityczne, zmiany w ustawodawstwie, wizerunek organizacji oraz zmiany w otoczeniu bezpieczeństwa.
2. Kwestie operacyjne – związane z rozwiązywaniem problemów bieżących organizacji w drodze do realizacji swoich celów strategicznych.
3. Kwestie alokacji i wykorzystania zasobów związane ze skutecznym zarządzaniem nimi. Wpływają na nie takie czynniki, jak dostępność zasobów, ich rotacja i wystarczalność.
4. Zarządzanie wiedzą – kwestie związane ze skutecznym zarządzaniem zasobami wiedzy i ich kontrolą, a także jej tworzeniem, ochroną i upowszechnianiem w ramach organizacji.
5. Przestrzeganie przepisów – kwestie związane z przestrzeganiem przepisów w zakresie BHP, ochrony środowiska, zasad obrotu gospodarczego, ochrony konsumentów, ochrony danych i warunków pracy, a także obowiązków nałożonych przez organy regulacyjne.

¹⁷ Patrz: definicja na s. 107.

¹⁸ Patrz: definicja na s. 109.

¹⁹ Patrz: definicja na s. 114.

²⁰ Patrz: definicja na s. 115.

²¹ *Standard zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 6.

²² Patrz: definicja na s. 105.

Identyfikację ryzyka można zlecić ekspertom zewnętrznym, jednak spójne, skoordynowane i wsparte właściwą komunikacją działania i instrumenty wewnętrzne mogą się okazać bardziej skuteczne. Sam proces zarządzania ryzykiem powinien być bezwzględnie realizowany w ramach organizacji.

Opis ryzyka²³ jest sporządzany w celu przedstawienia zidentyfikowanych ryzyk w czytelnej formie, np. w postaci tabeli, która ułatwia przejrzystą prezentację ich szacunkowych wartości. Użycie właściwie zaprojektowanej struktury opisu jest niezwykle ważnym elementem oceny w procesie kompleksowej identyfikacji, opisu i ewaluacji ryzyka. Rozważając konsekwencje i prawdopodobieństwo wystąpienia poszczególnych ryzyk (przedstawionych w tabeli 1), definiujemy priorytety, tzn. wybieramy kluczowe dla organizacji ryzyka, które wymagają bardziej szczegółowej analizy. Identyfikacja ryzyka związanego z działalnością gospodarczą i podejmowaniem decyzji obejmuje ryzyka strategiczne, taktyczne/projektowe i operacyjne²⁴. W obszarze bezpieczeństwa nic się nie zmienia. Zarządzanie ryzykiem to działalność, która rozpoczyna się na etapie projektowym już w fazie koncepcyjnej i jest prowadzona przez cały okres realizacji.

Tabela 1. Opis ryzyka (przykład)

Parametr ryzyka	Opis ryzyka
Nazwa ryzyka	
Zakres ryzyka	rodzaj, skala, zdarzenia pochodne
Charakter ryzyka	z czym jest związane: z wiedzą, prawem, umiejętnościami
Grupy nacisku	zdefiniowanie grup i ich oczekiwań
Ilościowy opis ryzyka	prawdopodobieństwo
Poziom akceptowany	potencjalne straty przy założonym poziomie nakładów
Mechanizmy kontroli	wystarczalność istniejących procedur kontroli
Możliwości poprawy	zalecenia w sprawie modelowania ryzyka

Źródło: Opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 7.

Pomiar ryzyka²⁵ to określenie jego prawdopodobieństwa oraz możliwych konsekwencji. Pomiar ten może być ilościowy, półilościowy lub jakościowy. Przykładowo: skutki (konsekwencje) – zarówno negatywne (zagrożenia), jak i pozytywne (szanse) – można podzielić na duże, średnie lub małe (tabela 2). Prawdopodobieństwo także można przyjąć jako duże, średnie lub małe. Podczas rozważania zarówno szans, jak i zagrożeń należy je definiować osobno (tabela 3). Podany sposób klasyfikacji (ujęty w metodyce) jest przykładowy, dlatego w przypadku różnych organizacji właściwe mogą się okazać odmienne schematy klasyfikowania skutków

²³ Por. profil ryzyka, s. 303.

²⁴ *Standard zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 5.

²⁵ Por. szacowanie ryzyka, s. 115.

i prawdopodobieństwa ryzyka (w dalszej części tego materiału). Przy zastosowaniu metody maczry skutków/prawdopodobieństwa (patrz część I, rozdział 2, podrozdział 2.15) rekomenduje się zastosowanie wartości liczbowych co najmniej w układzie 4x4 lub wyższym, natomiast w celu eliminacji uśredniania wyników pomiaru – maczry o liczbie parzystej.

Tabela 2. Pomiar skutków

Duże	Skutki katastrofy mogą przekroczyć zdolności systemu. Będzie to miało wpływ na strategię i działalność operacyjną organizacji. Możliwe jest niezadowolenie społeczeństwa
Średnie	Skutki katastrofy na poziomie zdolności operacyjnych systemu. Trzeba się liczyć z sięganiem po środki przeznaczone na inne cele
Małe	Skutki incydentu wystąpią, ale mogą się mieścić w granicach rezerw budżetowych państwa (województwa). Nie należy podejmować szczególnych działań

Źródło: Opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 8.

W podanych przykładach przyjęto trójstopniową klasyfikację prawdopodobieństwa i skutków. Można jednak spotkać np. klasyfikację pięciostopniową, daje ona dokładniejsze wyniki.

Tabela 3. Prawdopodobieństwo wystąpienia zagrożenia²⁶

Prawdopodobieństwo	Opis	Wskaźniki
Wysokie	zdarzenie cykliczne $P > 0,25$	zdarzenie występuje w cyklu rocznym, ostatnio wystąpiło 6 miesięcy temu
Średnie	zdarzenie cykliczne $P < 0,25$	zdarzenie występuje w cyklu 10-letnim, ostatnio wystąpiło 3 lata temu
Niskie	zdarzenie losowe $P < 0,02$	zdarza się bardzo rzadko, ostatnio wystąpiło 150 lat temu

Źródło: Opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 8.

W analizie ryzyka wykorzystuje się wiele metod, niektóre z nich nadają się do analizy ryzyka pozytywnego (szans), inne – do analizy zagrożeń, a jeszcze inne mogą być wykorzystane w obu przypadkach²⁷. Te ostatnie mają charakter uniwersalny. Wyniki analizy ryzyka służą opracowaniu profilu ryzyka²⁸. Do każdego ryzyka przypisana jest ocena opisująca jego znaczenie. Profil ryzyka porządkuje zidenty-

²⁶ Podobną tabelę sporządza się dla szans.

²⁷ Rekomendowane metody użyteczne do zastosowania w procesie oceny ryzyka opisano w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*.

²⁸ Patrz: definicja na s. 303.

fikowane ryzyka pod względem ważności dla organizacji i stanowi narzędzie do określenia priorytetów w zakresie postępowania względem ryzyka.

Sporządzenie profilu ryzyk pozwala przypisać poszczególne ryzyka do określonych dziedzin działalności (funkcji kryzysowych). Umożliwia również określenie głównych mechanizmów kontrolnych oraz dziedzin i obszarów, w jakich należy zwiększyć, zmniejszyć lub zreorganizować wydatki związane z kontrolowaniem ryzyka. Dzięki ścisłemu określeniu odpowiedzialności żadne ryzyka nie zostają pominięte. Każdemu ryzyku zostają przyporządkowane odpowiednie zasoby menedżerskie, a właścicielom – obszary zainteresowań ryzykiem²⁹.

Wynik analizy ryzyka umożliwia porównanie szacunków wartości ryzyka³⁰ z przyjętymi w organizacji (systemie) kryteriami, co stanowi podstawę do wydania ostatecznej oceny ryzyka, związanych z nim kosztów, korzyści, wymogów prawnych, organizacyjnych, szkoleniowych, ekonomicznych społecznych, a nawet politycznych. Pozwoli także sporządzić prognozy zachowań różnych grup społecznych. Ocena ryzyka stanowi podstawę do podejmowania decyzji co do rankingu priorytetów i przedsięwzięć w zakresie modelowania ryzyka, tak by nie przekraczało granicy akceptowalności. Trzeba zaplanować i wdrożyć działania, które sprowadzą ryzyko do poziomu akceptowanego. Te działania pozwolą określić koszty postępowania z ryzykiem i porównać je z niezbędnymi nakładami oraz podjąć decyzje w sprawach właściwych pakietów działań w zakresie każdego nieakceptowanego ryzyka.

Podejmowane działania względem ryzyka oznaczają wybór środków modyfikujących ryzyko i ich racjonalne wdrożenie. Podstawowym działaniem jest kontrolowanie i ograniczanie ryzyka³¹, przy czym zwraca się uwagę na jego unikanie i przenoszenie. Korzystniejsze jest modelowanie oparte na analizie koszt–efekt. W opracowaniach standardu podnosi się problem nie do końca zdefiniowanego finansowania ryzyka³², co wynika z podwójnego podejścia: 1) finansowania skutków (ubezpieczenia) czy 2) przeznaczenia środków na ograniczanie ryzyka.

Wszelkie podjęte działania względem ryzyka po jego ocenie powinny jako minimalny warunek gwarantować³³:

- skuteczne i sprawne funkcjonowanie organizacji,
- skuteczne mechanizmy kontroli wewnętrznej,
- zgodność działań z przepisami prawa i innymi obowiązującymi uregulowaniami.

²⁹ *Standard zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 9.

³⁰ Por. poziom ryzyka, s. 115.

³¹ Patrz: definicja na s. 238.

³² W standardzie termin „finansowanie ryzyka” odnosi się do mechanizmów, które służą finansowaniu skutków ryzyka (np. polisy ubezpieczeniowe). Nie oznacza natomiast generalnie przeznaczenia środków na realizację działań względem ryzyka (tak jak zdefiniowano to w zaleceniu ISO/IEC nr 73, s. 17, patrz: załącznik). Źródło: *Standard zarządzania ryzykiem FERMA 2003*, dz. cyt., s. 10.

³³ Tamże.

Reasumując, proces oceny ryzyka zapewnia skuteczne i sprawne funkcjonowanie organizacji, w porę identyfikując te ryzyka, które wymagają szczególnej uwagi kierownictwa, zarządu, rządu i menedżerów. To zarząd określa ciało stanowiące, przyjmuje, jakie działania w zakresie modelowania ryzyka są najważniejsze ze względu na potencjalne korzyści dla organizacji, samorządu, społeczności, wspólnoty, przedsiębiorstwa. Miarą skuteczności mechanizmów kontrolnych jest zapewnienie sprowadzenia ryzyka do poziomu akceptowanego w wyniku wprowadzenia proporcjonalnych działań i zasobów. Opłacalność mechanizmów kontrolnych odnosi się do porównania kosztów wdrożenia przedsięwzięć służących ograniczaniu ryzyka ze spodziewanymi korzyściami ze zmniejszenia tego ryzyka dożądanego poziomu.

Racjonalność proponowanych kosztów ocenia się na zasadzie porównań możliwych skutków ekonomicznych przy braku jakichkolwiek reakcji z kosztami proponowanych działań, co wymaga dysponowania odpowiednio wiarygodnymi informacjami i przyjęcia odpowiednio szczegółowych założeń. Na wstępie należy w miarę precyzyjnie określić prognozowane koszty wdrożenia adekwatnych rozwiązań, ponieważ stanowić to będzie bazę do określenia opłacalności tych rozwiązań. Z drugiej strony trzeba ocenić koszty strat wynikające z braku jakichkolwiek działań. Dysponując tymi danymi wyjściowymi, można podejmować decyzje o wdrażaniu konkretnych działań lub rezygnacji z nich. Należy wdrażać adekwatne do sytuacji mechanizmy kontrolne, które też wymagają nakładów.

Zarządzanie ryzykiem musi mieć podstawy prawa, a szczególnie wewnętrzne procesy kontrolne, które powinny zostać wdrożone i funkcjonować w jak najbardziej przejrzysty sposób. Bez kontroli trudno jest mówić o jakichkolwiek przedsięwzięciach postępowania z ryzykiem. W sytuacji, gdy koszty ograniczenia ryzyka są nieproporcjonalnie wysokie w stosunku do samego ryzyka, zaleca się elastyczność, jednak z wyłączeniem kwestii zdrowia i życia ludzkiego.

W codziennym życiu stosuje się metody ochrony finansowej przed potencjalnymi skutkami ryzyka, czego przykładem są ubezpieczenia (komunikacyjne, zdrowotne, działalności gospodarczej ochrony płodów rolnych itd.). W tym zakresie firmy ubezpieczeniowe stosują różne wyłączenia, np. nieubezpieczanie zdarzeń losowych lub spowodowanych przez tzw. siły wyższe. Wiele aktywności, np. sportów ekstremalnych, ma swoje zasady ubezpieczeń. Trzeba jednak zdecydowanie podkreślić, że ubezpieczenia to tylko pokrycie straty w razie braku możliwości uniknięcia konsekwencji konkretnego ryzyka.

Ważnym elementem zarządzania ryzykiem jest obieg i wykorzystanie informacji, co obejmuje wiele spraw związanych z działalnością codzienną. Oznacza to, że³⁴:

- 1) organizacja musi mieć pełną wiedzę o ryzykach, z jakimi ma do czynienia,
- 2) konieczna jest pełna świadomość potencjalnych skutków odchyień od zakładanych wskaźników dla wartości organizacji, przedsiębiorstwa,

³⁴ Tamże.

- 3) należy zapewnić odpowiedni poziom świadomości ryzyka wewnątrz organizacji,
- 4) organizacja musi wiedzieć, na ile jest gotowa sprostać wymogom sytuacji kryzysowej,
- 5) trzeba rozumieć wagę zaufania grup nacisku do organizacji,
- 6) koniecznością jest przestrzeganie transparentnych zasad komunikowania się ze środowiskiem (otoczeniem, społeczeństwem),
- 7) zapewnienie sprzężenia zwrotnego w zakresie otrzymywania informacji w zakresie tego, czy proces zarządzania ryzykiem funkcjonuje właściwie (normalnie),
- 8) konieczna jest czytelna strategia zarządzania ryzykiem, w tym koncepcja prowadzenia racjonalnych działań oraz podziału kompetencji i odpowiedzialności oraz obowiązków.

W kontekście powyższego najlepiej sens właściwego dysponowania informacją oddaje szósta zasada zarządzania ryzykiem normy ISO 31000, która wskazuje na kluczowe znaczenie dostępu do najlepszych, potwierdzonych informacji i ich efektywnego wykorzystywania.

Każdy podmiot, organizacja, instytucja, agencja powinna³⁵:

- 1) mieć świadomość zagrożeń towarzyszących jej działalności, potencjalnych skutków dla innych obszarów działalności, a także możliwych konsekwencji, jakie te zdarzenia mogą mieć w innych obszarach i w rezultacie ich własnej działalności,
- 2) dysponować wskaźnikami umożliwiającymi stałą kontrolę wyników prowadzonej działalności, postępów w realizacji założonych celów i identyfikację problemów wymagających korekt lub interwencji,
- 3) dysponować systemami detekcyjnymi, sygnalizującymi odchylenia od założeń lub prognoz w takim zakresie, aby możliwe było podjęcie odpowiednich działań,
- 4) zapewnić stałe informowanie organów decyzyjnych o wszelkich zmianach w rodzajach i skali zagrożeń lub braku skuteczności stosowanych przedsięwzięć.

Te i inne zasady reguluje w sposób kompleksowy i uniwersalny norma ISO 31000, opisana w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*.

Wszyscy członkowie organizacji, do poszczególnych jednostek włącznie, powinni³⁶:

- być świadomi odpowiedzialności za rodzaj ryzyka leżący w ich kompetencjach,
- znać metody postępowania w zakresie sprostania wymogom i stałego doskonalenia procesu zarządzania ryzykiem,

³⁵ Tamże.

³⁶ Tamże.

- mieć świadomość, w jaki sposób zarządzanie ryzykiem wynika z kultury organizacyjnej,
- być świadomymi uczestnikami procesów zarządzania ryzykiem.

Jest to podejście zgodne z zasadami normy ISO 31000 opisanymi w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, a także implementacją struktury ramowej zarządzania ryzykiem, dla której określone atrybuty nawiązują do: świadomej akceptacji odpowiedzialności za własne ryzyko, doskonalenia kontroli oraz strategii postępowania z ryzykiem czy identyfikacji właściwych osób i ich przygotowaniu w aspekcie odpowiedzialności za zarządzanie ryzykiem, którego są właścicielem.

PODSUMOWANIE I WNIOSKI

Różnorodność rozwiązań w metodykach oceny ryzyka przedstawionych w części III wynika przede wszystkim z podstaw, które służyły ich opracowaniu, a mianowicie wewnętrznych regulacji poszczególnych państw oraz instytucji. Niemniej jednak poddane analizie metodyki zawierają również elementy wspólne. Dostrzegamy to w tych dokumentach, które oparto również na wytycznych międzynarodowych norm i standardów w zakresie zarządzania ryzykiem.

Metodyka niemiecka, australijska, jak również w pewnej części szwedzka przygotowane zostały w zgodzie z normą ISO 31000:2009 *Risk Management – Principles and Guidelines* i ISO/IEC 31010:2009 *Risk Management – Risk Assessment Techniques*. Niewątpliwie wykorzystanie tych wytycznych należy uznać za mocną stronę wymienionych metodyk. Ich zastosowanie pozwala bowiem na wdrożenie dobrych praktyk m.in. w zakresie zasad i wytycznych z zakresu zarządzania ryzykiem potrzeby zarządzania kryzysowego (planowania cywilnego bądź ochrony ludności).

W przeważającej liczbie poddanych analizie metodyk (również tych, które bezpośrednio nie rekomendują wykorzystania norm ISO w tym zakresie, tj. Irlandii oraz Wielkiej Brytanii)³⁷ ocenę ryzyka postrzega się w kontekście całego procesu zarządzania ryzykiem.

Aby przystępnie przedstawić podejście poszczególnych państw do oceny ryzyka i wskazać ich mocne oraz słabe strony, dokonano porównania rozwiązań stosowanych w wybranych krajach. Za kryterium oceny przyjęto poszczególne etapy omawianych metodyk, w tym ich charakterystykę, wraz ze wskazaniem narzędzi i metod służących do oceny ryzyka.

Poszczególne etapy krajowych metodyk wyróżnia zarówno często odmienna liczebność, jak i terminologia – z ich nazwami włącznie. W poniższej części opracowania prześledzono je, kładąc szczególny nacisk na identyfikację ryzyka, analizę ryzyka oraz ewaluację ryzyka jako elementy wspólne dla wszystkich zaprezentowanych podejść, a rozważania te podsumowano tabelami ilustrującymi charakterystykę tych trzech etapów na potrzeby przeprowadzenia analizy porównawczej.

³⁷ Siłą rzeczy występują elementy podobne (między przeanalizowanymi metodykami a normą ISO 31000), jednak nie można uznać za pewnik, że są zbieżne albo jedne czerpią z drugich. Przykładowo standard FERMA powstał ok. 7 lat przed normą ISO 31000, a nawet przed poprzedniczką tej normy, która opublikowana została w 2004 r.

W metodyce szwedzkiej cały proces rozpoczyna się od określenia ról i odpowiedzialności podmiotów biorących udział w ocenie ryzyka. W metodyce irlandzkiej pierwszy etap stanowi ustalenie kontekstu organizacji. Pierwsza faza w metodyce irlandzkiej (ustanowienie kontekstu) oraz niemieckiej (opis zdefiniowanego obszaru) koncentruje się wokół charakterystyki obszaru objętego oceną ryzyka, zawierającej informację na temat geografii zidentyfikowanego terenu, klimatu, populacji, środowiska, zaopatrzenia czy też gospodarki.

Poniższa tabela przedstawia porównanie poszczególnych metodyk, z uwzględnieniem etapu identyfikacji ryzyka.

Tabela 1. Identyfikacja ryzyka (zagrożeń) w metodykach oceny ryzyka wybranych państw

Kraj/Etap oceny ryzyka	Identyfikacja ryzyka (zagrożeń)
Australia	Identyfikacja ryzyka opiera się na odpowiednio wysokiej jakości informacji, wiedzy i doświadczeniu kadr i personelu organizacji. Pod uwagę bierze się zarówno zagrożenia, jak i wrażliwość ekspozycji na konkretne ryzyko, które jest badane i opisywane. Rozważa się źródła ryzyka kontrolowane rutynowo oraz potencjalne zdarzenia i obszary ich możliwych wystąpień. Systematyczność i powszechność tych działań zapewnia wykluczenie znaczącego ryzyka lub jego poważne ograniczenie. Zwraca się uwagę na udział w tych działaniach wysokiej klasy ekspertów i tworzenie scenariuszy możliwych rozwojów sytuacji. Scenariusze wsparte zdarzeniami z przeszłości mogą wyraźnie wzbogacić wiedzę o możliwych fazach rozwoju sytuacji. Identyfikacja obejmuje wszystkie możliwe ryzyka, bez względu na to, czy są one pod kontrolą, czy nie, a także wszystkie problemy, istniejące i potencjalne, które wymagają wdrożenia rozwiązań w zakresie ograniczenia ryzyka.
Irlandia	Identyfikacja zagrożeń poprzedzona opisem zdefiniowanego obszaru, klasyfikacja zagrożeń w kategoriach: naturalne, transportowe, technologiczne i cywilne, wzięcie pod uwagę czarnych scenariuszy.
Niemcy	Identyfikacja zagrożeń poprzedzona opisem zdefiniowanego obszaru, opracowanie scenariuszy zdarzeń na podstawie wybranych zagrożeń, rozpatrywanie zdarzeń w skali narodowej w odniesieniu do najgorszego możliwego przypadku
Szwecja	Identyfikacja ryzyka jako element analizy ryzyka i podatności przeprowadzanej przez organy administracji rządowej i samorządowej. Etap rozpoczęty od opisu systemu (danej organizacji), biorąc pod uwagę model strukturalny, funkcjonalny i mieszany wraz z identyfikacją wewnętrznych i zewnętrznych czynników, które mogą zaburzyć system. Rozwinięte podejście scenariuszowe przy zastosowaniu wielu metod, np. MVA, ROSA. W krajowej ocenie ryzyka scenariusze opisane jako czarne scenariusze, o dużych skutkach, będących zagrożeniem dla co najmniej jednej wartości narodowej

Kraj/Etap oceny ryzyka	Identyfikacja ryzyka (zagrożeń)
Wielka Brytania	Identyfikacja ryzyka poprzez konsultacje eksperckie, wybranie zdarzeń stanowiących „możliwie najgorszy przypadek”, o wysokim ryzyku wystąpienia (duże prawdopodobieństwo i skutki). Selekcja scenariuszy wyczerpujących definicję zdarzenia nagłego oraz wykluczenie pozostałych poprzez umieszczenie ich na liście rezerwowej w celu późniejszego poddania ich przeglądowi.

Źródło: Opracowanie własne na podstawie poddanych analizie dokumentów opisujących metodyki oceny ryzyka stosowane w wybranych krajach.

Wspólnym etapem dla wszystkich omawianych metodyk jest identyfikacja potencjalnych zagrożeń wraz z określeniem scenariuszy zdarzeń niekorzystnych z nimi związanych. Stanowią one bowiem punkt wyjścia do analizy oraz ewaluacji ryzyka. Scenariusze są rozpatrywane w ramach poszczególnych elementów oceny ryzyka, tj. w ramach analizy, w tym szacowania prawdopodobieństwa oraz konsekwencji, jak również ewaluacji ryzyka. Stąd wynika konieczność ich jak najdokładniejszego opisanie. W poszczególnych metodykach oceny ryzyka wskazuje się niezbędne elementy składowe scenariusza, takie jak: zdarzenie bazowe (oraz inne zdarzenia powiązane z nim bezpośrednio lub pośrednio), ich charakterystyka – zawierająca przyczyny wystąpienia zdarzenia, konsekwencje danego zdarzenia oraz kontekst odnoszący się do okoliczności jego wystąpienia.

Szczegółowo problem opisu scenariuszy potraktowano w metodyce niemieckiej. Stanowi on odpowiedź na szereg pytań związanych z określeniem typu zdarzenia niebezpiecznego, jego wymiaru przestrzennego, natężenia oraz czasu trwania.

W omawianych metodykach wskazuje się na konieczność skupienia się na scenariuszach mających wpływ w skali krajowej, oddziałujących na wartości/żywotne interesy narodowe oraz będących czarnymi scenariuszami. Innowacyjnym rozwiązaniem jest opracowywanie scenariuszy zdarzeń w ramach cyklu seminariów, uwzględniających udział ludności w ocenie skutków scenariusza zdarzenia (wielowymiarowa analiza aktywności MVA w Szwecji).

Następnym etapem jest analiza ryzyka, dokonywana zwykle na podstawie danych historycznych, naukowych, statystycznych oraz szacowania eksperckiego, z uwzględnieniem wskazanych scenariuszy zdarzeń. Jej wynikiem są dane ilościowe i jakościowe. Analiza wybranych metodyk oceny ryzyka wskazuje na to, że jest ono szacowane na podstawie dwóch podstawowych czynników, tj. prawdopodobieństwa oraz konsekwencji. Jedynie w metodyce irlandzkiej ocena prawdopodobieństwa jest czynnością wtórną, po określeniu konsekwencji. Dodatkowo zwraca się uwagę na czynniki: niepewności szacowanego wyniku w odniesieniu do obu podstawowych parametrów oraz podatności (ocena), stanowiące część całego procesu zarządzania ryzykiem (Szwecja).

W poddanej analizie metodyce niemieckiej podkreśla się konieczność zagregowania wyników wpływu za pomocą obliczeń matematycznych. W przypadku

Niemiec całościowy wynik wpływu (konsekwencji) determinowany jest obliczeniowo. Poszczególne wyniki wartości wpływu dla poszczególnych parametrów wpływu w ramach danej kategorii są dodawane i dzielone przez liczbę parametrów (możliwe jest również określenie wagi dla poszczególnych parametrów wpływu).

Tabela 2 prezentuje porównanie poszczególnych metodyk, z uwzględnieniem etapu analizy ryzyka.

Tabela 2. Analiza ryzyka w metodykach oceny ryzyka wybranych państw

Kraj/Etap oceny ryzyka	Analiza ryzyka
Australia	<p>Prawdopodobieństwo: siedmiostopniowa skala ilościowo-jakościowa ze wskaźnikami częstości/średniego cyklu interwału/szansy wystąpienia</p> <p>Konsekwencje: pięciostopniowa skala jakościowa ze wskaźnikami konsekwencji</p>
Irlandia	<p>Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości</p> <p>Wpływ¹: ludzie (liczbowo), środowisko, infrastruktura (straty finansowe), społeczeństwo (pięciostopniowa skala jakościowa)</p>
Niemcy	<p>Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości</p> <p>Wpływ²: 20 parametrów wpływu w ramach kategorii: człowiek, środowisko, gospodarka, zaopatrzenie oraz niematerialne (np. polityczne, psychologiczne), rozpatrywane pod kątem ilościowym, tj. liczba, czas, kwota (oprócz kategorii niematerialne szacowanej w ujęciu jakościowym), przyjęcie metody agregacji wyników wpływu</p>
Szwecja	<p>Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości</p> <p>Konsekwencje: ludzie (liczba rannych, poszkodowanych), gospodarka/środowisko (kwota strat finansowych), polityka/społeczeństwo (jakościowo)</p>
Wielka Brytania	<p>Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości</p> <p>Konsekwencje: gospodarka, ludzie (ofiary i poszkodowani), wzburzenie społeczne, skutki psychologiczne</p>

Źródło: Opracowanie własne na podstawie poddanych analizie dokumentów opisujących metodyki oceny ryzyka stosowane w wybranych krajach.

Kolejny etap stanowi ocena ryzyka, obejmująca zarówno określenie wartości ryzyka na podstawie oszacowanych parametrów prawdopodobieństwa i konsekwencji, jak również jego wizualizację. Powszechnym narzędziem służącym do tego celu są matryce ryzyka. Umożliwiają one prezentację zidentyfikowanych ryzyk w formie porównawczej. W większości z omawianych metodyk przyjmuje się matrycę ryzyka 5×5 (Australia: 7×5), obejmującą pięciostopniowe skale: prawdopodobieństwa oraz konsekwencji (od 1 do 5). Zaznaczone punkty na matrycy wyznaczają szacowany wynik wartości ryzyka. W zależności od kraju przyjmuje się cztery (np. Niemcy)

lub pięć (np. Szwecja) parametrów wartości ryzyka. W niektórych krajach wartość ryzyka jest szacowana nie tylko na podstawie opisu jakościowego, ale również ilościowego, uwzględniającego częstość zdarzenia – np. raz na 100 lat w stosunku do liczby ofiar (Szwecja), jak również mieszanego (ilościowo-jakościowego), tj. parametru konsekwencji w skali jakościowej 1–5 oraz ilościowego, określającego częstość w odniesieniu do prawdopodobieństwa zdarzenia (Wielka Brytania). W niektórych krajach tworzy się oddzielne matryce ryzyka dla poszczególnych grup zagrożeń, tj. dla zagrożeń naturalnych, transportowych, technologicznych oraz cywilnych (Irlandia), jak również zagrożeń intencjonalnych (takich jak ataki terrorystyczne) i pozostałych (Wielka Brytania). W każdej z metodyk efektem finalnym jest jednak zbiorcza matryca ryzyka, na której prezentuje się łącznie wszystkie ryzyka poszczególnych zagrożeń (scenariuszy zdarzeń), co umożliwi ich porównanie. Oprócz parametru wartości ryzyka na matrycach (wykresie) zaznacza się poziom niepewności wyniku (Szwecja).

Tabela 3. Porównanie poszczególnych metodyk oceny ryzyka z uwzględnieniem etapu oceny ryzyka

Kraj/Etap oceny ryzyka	Ocena ryzyka
Australia	Wartość ryzyka: czterostopniowa skala jakościowa Wizualizacja ryzyka: matryce ryzyka 7×5 , ocena ryzyka zależy od wiarygodności informacji.
Irlandia	Wartość ryzyka: pięciostopniowa skala jakościowa Wizualizacja ryzyka: matryce ryzyka 5×5 dla każdej z czterech kategorii zagrożeń + zbiorcza matryca ryzyka
Niemcy	Wartość ryzyka: czterostopniowa skala jakościowa Wizualizacja ryzyka: matryca ryzyka 5×5 dla każdego scenariusza + zbiorcza matryca ryzyka
Szwecja	Wartość ryzyka: pięciostopniowa skala jakościowa Wizualizacja ryzyka: matryce ryzyka 5×5 uwzględniające parametry jakościowe oraz ilościowe, obejmujące częstość zdarzenia; matryca ryzyka 5×5 (ze wskaźnikiem oceny niepewności wyniku) w krajowej ocenie ryzyka
Wielka Brytania	Wartość ryzyka: pięciostopniowa skala Wizualizacja ryzyka: matryce ryzyka 5×5 , uwzględniające parametry jakościowe oraz ilościowe, obejmujące częstość zdarzenia, oddzielne dla zagrożeń intencjonalnych, w tym terrorystycznych, oraz dla pozostałych zagrożeń

Źródło: Opracowanie własne na podstawie poddanych analizie dokumentów opisujących metodyki oceny ryzyka stosowane w wybranych krajach.

W poddanych analizie dokumentach wskazuje się, że na podstawie wyników oceny ryzyka decydenci określają, które ryzyka wymagają postępowania z nimi oraz ustalają priorytety w reagowaniu. W metodyce szwedzkiej przeprowadza się

zaś dodatkowo tzw. ocenę podatności. Pozwala ona na uzyskanie odpowiedzi na pytanie, jakie są słabości w ramach dostępnych sił i środków niezbędnych do redukcji ryzyka i które z nich należy wzmocnić. Analiza ta stanowi więc doskonałe uzupełnienie oceny ryzyka przeprowadzonej we wcześniejszej fazie.

Wśród analizowanych metodyk zidentyfikowano szereg narzędzi stanowiących wsparcie dla osób prowadzących ocenę oraz analizę ryzyka. Szczególnie dużo narzędzi, w tym uznane m.in. przez normę ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, przedstawia przygotowany przez Szwedzką Agencję ds. Cywilnych Sytuacji Kryzysowych dokument *Guide to risk and vulnerability analyses*. Warto nadmienić, że spośród wskazanych w opracowaniu krajów wszystkie wypracowały własne analizy scenariuszowe: MVA, ROSA, IBERO (propozycje szwedzkie), dokumenty NRA (w ramach metodyki: irlandzkiej oraz brytyjskiej). Jeżeli spojrzymy na polecane narzędzia zawarte w normie ISO/IEC 31010, to na potrzeby planowania cywilnego warte polecenia są metody jakościowe: wstępna analiza ryzyka, analiza „co, jeśli?” oraz analiza drzewa błędów. Pierwsza z nich – wstępna analiza ryzyka ma raczej ograniczone zastosowanie. Pozwala jednak na zebranie ogólnego poglądu na temat wszystkich zidentyfikowanych zagrożeń i – po wzięciu pod uwagę odnotowanych przyczyn, skutków oraz prawdopodobieństwa – przeprowadzenie oceny i wskazanie propozycji rozwiązań. Z kolei metoda SWIFT umożliwia wnikliwą analizę wszystkich możliwych przyczyn oraz skutków dla szerokiej gamy scenariuszy, co wskazuje na jej uniwersalność. Analiza drzewa błędów w czytelny sposób wykazuje powiązanie ze sobą konkretnych skutków z ich przyczynami. Metoda ta pozwala również na przeprowadzenie w kolejnym kroku oszacowania prawdopodobieństwa lub częstotliwości wystąpienia w ramach wykorzystania metody ilościowej. Powstały obraz pomaga w zrozumieniu, jak dane zdarzenie powstaje poprzez następowanie po sobie poszczególnych czynników. Dzięki temu w dalszej perspektywie można podjąć odpowiednie działania zapobiegawcze. Narzędziem najpowszechniej wykorzystywanym na potrzeby ewaluacji ryzyka i prezentacji wyników są matryce ryzyka. Te najczęściej stosowane w krajowych metodykach obejmowały dwie pięciostopniowe skale prawdopodobieństwa i skutków (w Szwecji ujęto dodatkowo rozróżnienie trzech stopni niepewności oszacowanego wyniku).

Analiza metodyk oceny ryzyka stosowanych w wybranych krajach wykazała, że proces ten, podobnie jak w Polsce, stanowi podstawę planowania na potrzeby zarządzania kryzysowego (ochrony ludności). Zaprezentowane w ramach niniejszej części podejścia zawierają liczne przykłady rozwiązań odnoszących się do identyfikacji zagrożeń na szczeblu krajowym, szacowania ryzyka ich wystąpienia, jak również ewaluacji. Część z nich mogłaby zostać wykorzystana w warunkach polskich.

Analiza dokumentów z różnych krajów dowodzi, że postrzeganie oceny ryzyka w odniesieniu do całego procesu zarządzania ryzykiem jest dzisiaj powszechne. W tym ujęciu ów proces obejmuje takie elementy, jak: ustalenie kontekstu,

identyfikacja ryzyka, analiza ryzyka, ewaluacja ryzyka, jak również postępowanie z ryzykiem. Zasadne wydaje się również jego usankcjonowanie prawne w Polsce (dotychczas obejmuje on wybrane elementy, w tym ocenę ryzyka). Tym bardziej, że w poddanych analizie metodykach rekomenduje się wykorzystanie wytycznych wybranych standardów z zakresu zarządzania ryzykiem, zarówno rozwiązań właściwych dla danego kraju, jak i dyrektyw norm o charakterze międzynarodowym, np. ISO 31000 oraz ISO/IEC 31010. Mogłyby one zostać zastosowane w odniesieniu do terminologii, konstrukcji całego procesu zarządzania ryzykiem, jak również metod służących do szacowania ryzyka.

W kontekście wdrożenia w warunkach polskich rozwiązań stosowanych w wybranych krajach należałoby zastanowić się nad możliwością rozwinięcia podejścia scenariuszowego, zgodnie z którym scenariusze stanowią punkt wyjścia do analizy ryzyka, a w związku z tym główny nacisk kładzie się na ich precyzyjny opis, możliwość użycia wsparcia eksperckiego przy ich przygotowaniu oraz zastosowania metod i technik służących do opracowania scenariuszy zdarzeń, czy też ich selekcję poprzez wybór jedynie „najgorszych możliwych scenariuszy”, mających wpływ w skali narodowej.

W związku z powyżej wspomnianą koncepcją rozszerzenia oceny ryzyka do całego procesu zarządzania ryzykiem, wart przemyślenia jest pomysł uzupełnienia metody oceny ryzyka o element związany z ustaleniem kontekstu wewnętrznego oraz zewnętrznego organizacji (której dotyczy proces oceny ryzyka), z uwzględnieniem m.in. jej celów, struktury organizacyjnej, środowiska/otoczenia i prawa. Dzięki temu możliwe jest określenie jej podatności, mogącej skutkować zwiększeniem szacowanej wartości prawdopodobieństwa oraz skutków, a w konsekwencji zmianą prognozowanej wartości ryzyka. Co więcej, należałoby rozważyć możliwość przedstawienia na macierzy ryzyka sposobów postępowania z zidentyfikowanymi ryzykami.

Analiza metodyk stosowanych przez poszczególne państwa, przedstawionych w części III, pozwala wyodrębnić zalety każdej z nich:

1. Zaletą metodyki australijskiej jest kompleksowe podejście do zarządzania ryzykiem, przy jednoczesnym wprowadzaniu uniwersalnych i jednolitych zasad, ram (struktur) i procesów zarządzania ryzykiem, zgodnych z dokumentami krajowymi i międzynarodową normą ISO 31000:2009.
2. Zaletą metodyki irlandzkiej jest zwrócenie uwagi na wstępie analizy na konieczność ustalenia jej kontekstu, tj. opisanie terenu/obszaru, dla którego opracowuje się ocenę ryzyka, co pozwala na uzmysłowienie sobie wrażliwości i podatności danego obszaru w sytuacji zagrożenia.
3. Zaletę metodyki niemieckiej stanowi odniesienie procesu oceny ryzyka do precyzyjnie zdefiniowanego obszaru objętego analizą, tj. zdefiniowanych obiektów lub miejsc, co ułatwia późniejsze określenie wpływu, jak również rozwinięte podejście scenariuszowe (scenariusze stanowią punkt wyjścia

- do dalszej analizy). Uwagę zwraca opracowanie metody agregacji wyników wpływu (parametru określanego za pomocą szacunków ilościowych i jakościowych), przekonwertowanego po zsumowaniu do wyniku bliskiego skali jakościowej (dopuszczalnie z ułamkami dziesiętymi) w celu prezentacji wyników na matrycy ryzyka wraz z oszacowanym prawdopodobieństwem.
4. Zaletą metodyki szwedzkiej jest umiejscowienie poszczególnych grup sytuacji (zdarzenia codzienne, duże zdarzenia, kryzysy) na wykresie ryzyka, umożliwienie i opisanie wykorzystania wielu przydatnych narzędzi – metod wspomagających ocenę ryzyka oraz opracowywanie scenariuszy zdarzeń w ramach cyklu seminariów, uwzględniających udział ludności w ocenie skutków scenariusza zdarzenia.
 5. Zaletą metodyki brytyjskiej jest duża systematyzacja działań związanych z oceną ryzyka na potrzeby planowania kryzysowego (dokonywana jest ona w cyklu rocznym). Uwagę zwraca także wykorzystanie wsparcia eksperckiego na etapie identyfikacji zagrożeń, jak również wstępna selekcja scenariuszy zdarzeń w kierunku wykluczenia z dalszej analizy najbardziej nieprawdopodobnych z nich (wybór „najgorszego przypadku”, czyli zdarzeń o dużym ryzyku wystąpienia, tj. wiążących się z dużym prawdopodobieństwem i skutkami). Za mocną stroną metodyki stosowanej w Wielkiej Brytanii można uznać podjęcie próby oszacowania wpływu psychologicznego niekorzystnych zdarzeń na społeczeństwo. Ponadto jej zaletą jest rozpatrywanie zagrożeń pod względem ich wystąpienia w perspektywie następnych 5 lat.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

Boardman A., Greenberg D., Vining A., Weimer D., *Cost-Benefit Analysis: concepts and practice*, Prentice Hall 2010.

Gołębiewski J., *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, SA PSP, Kraków 2011.

Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005.

Akty prawne

Civil Contingencies Act 2004, UK.

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. nr 62, poz. 558, z późn. zm.).

Zarządzenie nr 3666/2012 Prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie

Zarządzenie nr 80 Wojewody Mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia Polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

European Commission, Commission Staff Working Paper, Risk Assessment and Mapping Guidelines for Disaster management, 2010, SEC(2010) 1626 final (17899/10).

Normy i standardy

ISO 31000:2009 Risk Management – Principles and Guidelines.

ISO Guide 73:2009 Risk Management – Vocabulary.

PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

PN-EN 15975-1:2011 Bezpieczeństwo zaopatrzenia w wodę pitną. Przewodniki zarządzania kryzysowego i ryzyka. Część 1: Zarządzanie kryzysowe.

PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.

Standard zarządzania ryzykiem FERMA 2003.

Dokumenty elektroniczne, strony internetowe i inne

A Framework for Major Emergency Management, A Guide to risk Assessment in Major Emergency Management, Dublin 2010, <http://mem.ie/wp-content/uploads/2015/05/A-Guide-to-Risk-Assessment.pdf>.

A National Risk Assessment for Ireland, Office of Emergency Planning, Dublin 2012, <https://emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf>.

- Cabinet Office, National Risk Register for Civil Emergencies 2013, London 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf.
- Cabinet Office, The National Risk Register of Civil Emergencies, London 2010, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211853/nationalriskregister-2010.pdf.
- Federal Office of Civil Protection and Disaster Assistance 2011 (Niemcy). *Method of Risk Analysis for Civil Protection 2011*, Bonn 2011, http://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/booklets_leaflets/Method_of_%20Risk_Analysis.pdf?__blob=publicationFile.
- <http://ciop.pl>.
- <http://sjp.pl>.
- <http://www.governica.com>.
- <http://www.ryzykozawodoweonline.pl>.
- State Emergency Service, *National Emergency Risk Assessment Guidelines*, Hobart 2010, <http://coastaladaptationresources.org/PDF-files/1438-National-Emergency-Risk-Assessment-Guidelines-Oct-2010.PDF>.
- Swedish Civil Contingencies Agency, *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, Karlstad 2012, <https://www.msb.se/RibData/Filer/pdf/26267.pdf>.
- Swedish Civil Contingencies Agency, *Swedish National Risk Assessment*, Karlstad 2012, <https://www.msb.se/RibData/Filer/pdf/26621.pdf>.

CZEŚĆ V

ZARZĄDZANIE RYZYKIEM
W POLSCE

WPROWADZENIE

Zarządzanie ryzykiem stało się nieodzownym elementem wielu gałęzi aktywności państwa. Dotyczy to w szczególności działalności związanych z bezpieczeństwem pojmowanym w szerokim (rozwiązania dla całego sektora) oraz wąskim zakresie (rozwiązania dla poszczególnych instytucji), ponieważ możemy mówić z jednej strony m.in. o bezpieczeństwie finansów publicznych, rozwoju gospodarczego czy resortów administracji rządowej i bezpieczeństwie powodziowym, natomiast z drugiej strony o bezpieczeństwie konkretnych jednostek terytorialnych i podmiotów.

W polskim systemie prawnym w sektorze finansów publicznych obowiązuje systemowe rozwiązanie zarządzania ryzykiem w Polsce, które swoim zakresem obejmuje kompleksowe podejście do ryzyka. Rozwiązania wzmacniające kontrolę nad wydatkowaniem środków publicznych wprowadziła ustawa o finansach publicznych¹ i zobligowała do ich stosowania szereg podmiotów, tj. ministerstwa, urzędy centralne, banki oraz inne jednostki i instytucje funkcjonujące w obszarze administracji publicznej.

W niniejszej części przedstawiono metodyki i rozwiązania wykorzystujące elementy zarządzania ryzykiem, które były wdrażane bądź obowiązują w różnych obszarach działalności w Polsce. Wszystkie opisane w kolejnych rozdziałach metodyki funkcjonują bezpośrednio lub pośrednio w sferze zainteresowań zarządzania kryzysowego i planowania cywilnego. Dla podanych przykładów rozwiązań wykazano powiązanie z wytycznymi uznanych norm w zakresie zarządzania ryzykiem bądź też określono potrzeby uwzględnienia zaproponowanych w nich rozwiązań.

W rozdziale pierwszym podjęto kwestie zastosowania elementów zarządzania ryzykiem w dokumentach opracowywanych na podstawie ustawy o zarządzaniu kryzysowym (plany zarządzania kryzysowego, raport o zagrożeniach bezpieczeństwa narodowego i plany ochrony infrastruktury krytycznej). Drugi rozdział nawiązuje do rozważań podjętych w rozdziale pierwszym, jak również w części II. Stanowi on próbę przybliżenia metody wdrażania do planowania cywilnego dobrych praktyk ujętych w normach. Kolejny rozdział porusza problematykę zarządzania ryzykiem powodziowym. Szczegółowej analizie poddano opracowaną na szczeblu unijnym metodykę oceny ryzyka dla zagrożeń powodziowych. Rozdział czwarty

¹ Ustawa wprowadzona na podstawie przepisów europejskich, podlegających harmonizacji z prawem polskim, m.in. jako delegacja Rozporządzenia Rady nr 1466/97/WE z dnia 7 lipca 1997 r. w sprawie wzmocnienia nadzoru pozycji budżetowych oraz nadzoru i koordynacji polityk gospodarczych.

rozszerza obszar badań nad zarządzaniem ryzykiem w kraju, koncentrując się na kontroli zarządczej. Stanowi ona wydzielony komponent, do którego stosowania zobligowane są m.in. jednostki administracji publicznej, których domeną jest także odpowiedzialność za planowanie cywilne. Daje to możliwość nowego spojrzenia na zagadnienie kontroli zarządczej – jako dodatkowe kompetencje pracowników jednostek administracji rządowej i samorządowej w zakresie zarządzania ryzykiem. Rozdział piąty przedstawia autorską metodykę PomRisc, umożliwiającą diagnozę stanu bezpieczeństwa i systemu ratownictwa, ze wskazaniem optymalnych kierunków działań doskonalących. Metodyka stanowi przykład wykorzystania metod i narzędzi oceny ryzyka oraz zarządzania ryzykiem. W rozdziale szóstym przywołany został praktyczny przykład zastosowania teleinformatycznych narzędzi wspomagających proces oceny ryzyka. Autorzy dokonali charakterystyki modułu oceny ryzyka oprogramowania RISK0, służącego do budowy planów zarządzania kryzysowego. Ostatni z rozdziałów części V podejmuje w sposób sygnalny kwestię zarządzania ryzykiem pożarowym w Polsce. Tematyka ta – bardzo ważna zarówno dla bezpieczeństwa narodowego, jak i społeczności lokalnych – została włączona w obszar zainteresowań projektu badawczo-rozwojowego na rzecz obronności i bezpieczeństwa państwa pt. „Opracowanie systemowych rozwiązań wspomagających prowadzenie dochodzeń popożarowych wykorzystujących nowoczesne technologie, w tym narzędzia techniczne i informatyczne”.

1. ZARZĄDZANIE RYZYKIEM W PLANOWANIU CYWILNYM

System zarządzania kryzysowego powstał w wyniku wieloletniej dyskusji, która toczyła się zarówno w przestrzeni publicznej, jak i instytucjonalnej. Potrzebę budowy systemu umożliwiającego skoordynowanie wszystkich działań państwa, bez względu na jego wymiar instytucjonalny, podnosili nie tylko decydenci czy ludzie nauki, ale również organizacje trzeciego sektora (organizacje pozarządowe). Pierwszym aktem prawnym wprowadzającym do polskiego porządku prawnego elementy struktury zarządzania kryzysowego było rozporządzenie z 3 grudnia 2002 r. w sprawie sposobu tworzenia gminnego zespołu reagowania, powiatowego i wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji Kryzysowej i ich funkcjonowania, realizujące delegację z art. 12 ustawy o stanie klęski żywiołowej. System ukonstytuował się 5 lat później, w chwili wejścia w życie ustawy o zarządzaniu kryzysowym.

Wskazane wyżej akty prawne, jak i rozporządzenia wydane na podstawie ustawy o zarządzaniu kryzysowym z 2007 r., nie podnosiły konieczności wykorzystywania w procesie zarządzania kryzysowego żadnego elementu zarządzania ryzykiem. Dopiero kolejne nowelizacje (szczególnie nowelizacja z 2009 r.) oraz rozporządzenia przygotowane na podstawie nowych delegacji ustawowych wprowadziły do porządku prawnego elementy zarządzania ryzykiem. Przepisy te określiły nie tylko pojęcie ryzyka, ale także mapy ryzyka i oceny ryzyka¹. Ponadto uzupełniły planowanie cywilne o dwa dokumenty strategiczne, w których w procesie przygotowywania 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 oraz posiadaczy samoistnych.

Od czasu wejścia w życie tych przepisów Rządowe Centrum Bezpieczeństwa przygotowało wytyczne określające sposób przygotowania obu dokumentów. Zarówno NPOIK, jak i *Procedura opracowania raportu cząstkowego na potrzeby RoZBN*

¹ Patrz: definicja na s. 107.

poruszają problematykę zarządzania ryzykiem. Niemniej jednak żadne z nich nie opiera się na normach ISO ani ich nie rekomenduje.

Analiza formalna wskazanych wyżej dokumentów² (charakteryzujących wykorzystywane metodyki) oraz opinie wytwórców dokumentów planistycznych wskazują, że zalecenia te nie są wystarczające i wciąż poszukiwane są nowe, bardziej komplementarne metody. Postulat ten był wielokrotnie podnoszony podczas procesu przygotowywania zarówno pierwszej, jak i drugiej edycji *Raportu o zagrożeniach bezpieczeństwa narodowego*.

Badania literaturowe zostały przeprowadzone w dwóch zasadniczych kierunkach. Pierwszy z nich to formalnie obowiązujące wymogi polskiego prawa w zakresie oceny ryzyka, drugi natomiast skoncentrował się na analizie, charakterystyce i wyodrębnieniu z norm ISO elementów możliwych do zastosowania przez system zarządzania kryzysowego i spełniających jego wymogi formalne.

Biorąc powyższe pod uwagę, można wskazać, że efektem pracy powinno być rozwiązanie głównego problemu badawczego, który można scharakteryzować poprzez postawienie pytania: czy narzędzie, jakim są normy ISO (w zakresie zarządzania ryzykiem), można efektywnie wykorzystać w procesie planowania cywilnego?

Odpowiedź na to pytanie pozwoli w dalszej kolejności określić, które z procesów, zasad czy wytycznych rekomendowanych przez ISO mogą przyczynić się do poprawy wykorzystywanych obecnie metod oceny ryzyka.

Wstępne badania literaturowe przeprowadzone przed przystąpieniem do zasadniczej części badań pozwalają na postawienie głównej hipotezy badawczej. Oparta ona została na spostrzeżeniu, że w dokumentach ISO mamy wskazane zalecenie dla ogólnych procesów postępowania z ryzykiem³, natomiast organizacja ISO nie podejmuje się wskazania szczegółowych zaleceń pozwalających na dokonanie samej oceny ryzyka. Hipoteza ta brzmi: normy ISO można wykorzystać w procesie planowania cywilnego w zakresie ujednoczenia nazewnictwa wykorzystywanego przez system zarządzania kryzysowego oraz przygotowania procesu oceny ryzyka.

Zarządzanie ryzykiem traktowane jako element ogólnych procesów zachodzących w organizacji nie jest zjawiskiem nowym. W organizacjach biznesowych od wielu lat stanowi podstawę efektywnego działania. Traktowanie czynnika ryzyka⁴ jako istotnej wytycznej dla planowania działań na poziomie strategicznym pozwala na uwiarygodnienie procesu decyzyjnego, a co za tym idzie – zmniejszenie prawdopodobieństwa podjęcia błędnych decyzji. Dlatego też, uznając skuteczność procesu zarządzania ryzykiem, polski ustawodawca wprowadził do porządku prawnego szereg rozwiązań odwołujących się właśnie do tego pojęcia.

² Pod tym pojęciem rozumie się technikę badawczą służącą do gromadzenia wstępnych, opisowych, także ilościowych informacji o badanej instytucji czy zjawisku, cyt. za: T. Pilch, *Zasady badań pedagogicznych*, wyd. Żak, Warszawa 1995, s. 76.

³ Patrz: definicja na s. 106.

⁴ Patrz: definicja na s. 119 (źródło ryzyka).

Pierwszym aktem prawnym podejmującym tę problematykę w obszarze bezpieczeństwa powszechnego były przepisy implementujące dyrektywę 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim do ustawy Prawo wodne. Ten szczególny przypadek zasługuje na uwagę nie tylko ze względu na szczegółowość rozwiązań, ale i ich powszechność. Kolejnym aktem prawnym, który odwołuje się do omawianej problematyki, jest ustawa o zarządzaniu kryzysowym. Nowelizacja ustawy w 2009 r. wprowadziła obowiązek uzupełnienia planowania cywilnego o nowy, ramowy w skali kraju dokument analityczny, którego podstawę stanowi proces oceny ryzyka – *Raport o zagrożeniach bezpieczeństwa narodowego*. Uzupełniono także o ten element uregulowania prawne dotyczące ochrony infrastruktury krytycznej.

W niniejszym rozdziale skoncentrowano się na wskazanych wyżej aktach prawnych. Ogólnym – regulującym w sposób kompleksowy kwestie bezpieczeństwa państwa (ustawa o zarządzaniu kryzysowym wraz z przepisami wykonawczymi) oraz szczególnym – podejmującym kwestie zagrożeń powodziowych. W trakcie badania poddano analizie przepisy prawne powszechnie obowiązujące, które podejmują kwestie zarządzania ryzykiem, oraz wskazano elementy mogące stanowić wytyczne metodyczne dla procesu oceny ryzyka.

1.1. Plany zarządzania kryzysowego

Zapisy odwołujące się do pojęcia ryzyka zostały włączone do porządku prawnego ustawą z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym. Nowelizacja ta uzupełniła wymogi dla planowania cywilnego w obszarze planów zarządzania kryzysowego. W odniesieniu do planów zarządzania kryzysowego ustawa została uzupełniona o⁵:

- art. 3 pkt 10 ustawy, który definiuje pojęcie mapy ryzyka – jako „mapę lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę”,
- art. 5 ust 2 pkt 1 ppkt a, który mówi, że charakterystyka zagrożeń (będąca elementem planu głównego PZK) powinna zawierać także ocenę ryzyka ich wystąpienia (w tym zagrożeń dotyczących infrastruktury krytycznej) oraz mapy ryzyka i mapy zagrożeń⁶,

⁵ Ustawa z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz. U. 2009 Nr 131, poz. 1076, z późn. zm.).

⁶ Zgodnie z art. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.) mapy ryzyka przedstawiają potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę (te mogą przyjąć również formę opisu), a mapy zagrożeń przedstawiają obszar geograficzny objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń.

- art. 5a ust 3 pkt 1, który określa jako jeden z elementów RoZBN charakterystykę zagrożeń bazującej na mapie ryzyka.

Należy zaznaczyć, że zapis ten odnosi się bezpośrednio do *Raportu o zagrożeniach bezpieczeństwa narodowego*, natomiast (poprzez zastosowanie ust. 5 art. 5a) pośrednio do planów zarządzania kryzysowego. Ustęp ten stwierdza, że kierunki działania wynikające z wniosków z *Raportu* stanowią element *Krajowego planu zarządzania kryzysowego* oraz są uwzględniane w planach zarządzania kryzysowego. Praktyczne wykorzystanie tego zapisu skutkuje prostym zabiegiem, polegającym na przeniesieniu map ryzyka do planów zarządzania kryzysowego.

Omawiając problematykę z zakresu zarządzania ryzykiem w ustawie o zarządzaniu kryzysowym, należy zaznaczyć, że określa ona organy właściwe w sprawach zarządzania kryzysowego, ich zadania i zasady działania oraz sposób finansowania w dziedzinie zarządzania kryzysowego⁷. W wymienionych definicjach omawianej ustawy na szczególną uwagę zasługują pojęcia:

- ochrony infrastruktury krytycznej, przez którą należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków, a także szybkiego odtworzenia tej infrastruktury na wypadek awarii⁸, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie⁹;
- zdefiniowanej wcześniej mapy ryzyka¹⁰.

Ustawa określa, że podstawowym zadaniem z zakresu planowania cywilnego jest przygotowanie planu zarządzania kryzysowego. Zgodnie z zapisami ustawy tworzy się *Krajowy plan zarządzania kryzysowego* oraz – odpowiednio do szczebli administracji – wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego. Plan zarządzania kryzysowego jest podstawowym dokumentem określającym zasady działania administracji rządowej oraz samorządowej, a także pozostałych uczestników procesu zarządzania i reagowania kryzysowego na danym terenie. Elementem składowym planu jest plan główny, zawierający charakterystykę zagrożeń oraz ocenę ryzyka. Obejmuje on również mapę ryzyka oraz zadania i obowiązki uczestników zarządzania kryzysowego (w tym siatkę bezpieczeństwa), a także zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych. Kolejną składową planu jest zespół przedsięwzięć na wypadek sytuacji kryzysowych. Składa się on z zadań obejmujących monitorowanie zagrożeń, trybu uruchamiania oraz współdziałania sił i środków uczestniczących w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowych. Ponadto zawiera szereg procedur

⁷ Art. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.).

⁸ Patrz: definicja na s. 135.

⁹ Art. 3 pkt 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.).

¹⁰ Tamże.

reagowania kryzysowego, dotyczących sposobu postępowania w sytuacjach kryzysowych. Kolejnymi składowymi planu są załączniki funkcjonalne planu głównego. Jest to zbiór dokumentów przedstawiających organizację łączności, organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania, zasad informowania ludności o zagrożeniach i sposobach postępowania z nimi. Zawiera on również informacje z zakresu organizacji ratownictwa, opieki medycznej, pomocy społecznej oraz psychologicznej, wykaz zawartych umów i porozumień, jak również zasady i tryb oceniania i dokumentowania szkód.

Ważnym zapisem omawianej ustawy jest fragment mówiący, że kierunki działania wynikające z wniosków z *Raportu* stanowią element *Krajowego planu zarządzania kryzysowego* oraz są uwzględniane w planach zarządzania kryzysowego¹¹.

1.2. Raport o zagrożeniach bezpieczeństwa narodowego

Na podstawie zmian noweli ustawy o zarządzaniu kryzysowym ustawodawca wydał także delegację dla rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego.

Rozporządzenie w sprawie raportu o zagrożeniach bezpieczeństwa narodowego nie wprowadziło nowych wymagań dla procesu zarządzania ryzykiem, niemniej jednak wskazało kategorie zagrożeń, które powinny zostać objęte procesem oceny ryzyka¹². Zdefiniowano je jako zagrożenia: mające wpływ na funkcjonowanie i rozwój państwa, w tym jego bezpieczeństwo, pozycję międzynarodową i potencjał ekonomiczno-obronny; skutkujące naruszeniem porządku konstytucyjnego; zagrażające życiu, zdrowiu, mieniu lub środowisku; obejmujące terytorium Polski i jej obywateli lub obywateli innych państw; wynikające z podpisanych porozumień i umów międzynarodowych; wyczerpujące cechy aktu terrorystycznego.

Ustawa o zarządzaniu kryzysowym w art. 5a określa, iż na potrzeby *Krajowego planu zarządzania kryzysowego* ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają *Raport o zagrożeniach bezpieczeństwa narodowego*. Pracami nad przygotowaniem *Raportu* kieruje dyrektor Rządowego Centrum Bezpieczeństwa. W dokumencie tym wskazuje się najważniejsze zagrożenia przedstawione na mapie ryzyka, określa cele strategiczne¹³ oraz priorytety w reagowaniu na wytypowane zagrożenia oraz siły i środki niezbędne do osiągnięcia celów strategicznych.

¹¹ Art. 5a pkt 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.).

¹² Ustawodawca nie przewidział zasadności włączenia innych elementów procesu zarządzania ryzykiem.

¹³ Patrz: definicja na s. 105.

*Rozporządzenie w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego*¹⁴ określa sposób, tryb i terminy jego opracowania. Na potrzeby *Raportu* przez właściwego ministra przygotowywane są raporty cząstkowe, w których skład wchodzi raporty cząstkowe wykonane przez podległego kierownika urzędu centralnego. Raporty cząstkowe zawierają informacje dotyczące wskazania najważniejszych zagrożeń i skutków ich wystąpienia zobrazowane na mapie ryzyka¹⁵. Charakter tych zagrożeń cechuje się istotnym wpływem na funkcjonowanie i możliwości rozwoju państwa, a ich skutki mogą godzić w bezpieczeństwo państwa, zagrażać życiu i zdrowiu dużej liczby osób oraz oddziaływać na sąsiednie kraje. *Raport* określa również cele strategiczne, które należy osiągnąć w dążeniu do zminimalizowania możliwości wystąpienia zagrożenia, a także wskazuje siły i środki niezbędne do ich osiągnięcia.

Mapę ryzyka, na której zobrazowane są zagrożenia i ich skutki, wykonuje się w formie mapy topograficznej i elektronicznej – wektorowej. Dane w niej zawarte przedstawiają zasięg geograficzny zagrożenia wraz z przypisanym prawdopodobieństwem jego wystąpienia i oceną skutków. Następnie opracowywaną mapę ryzyka przedstawia się za pomocą tabeli zawierającej parametry zagrożeń z prognozowanymi skutkami oraz w formie opisowej, gdy charakter zagrożenia uniemożliwia przedstawienie go na powyższych zasadach.

Raport cząstkowy jest systematycznie aktualizowany i przedkładany dyrektorowi Rządowego Centrum Bezpieczeństwa nie rzadziej niż raz na 2 lata. Dyrektor RCB dokonuje aktualizacji *Raportu* i przekazuje go Radzie Ministrów.

Rządowe Centrum Bezpieczeństwa opracowało metodykę na potrzeby *Raportu o zagrożeniach bezpieczeństwa narodowego*. Metodyka ta wykorzystywana jest w odniesieniu do zagrożeń¹⁶:

- 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;
- których skutki mogą:
 - godzić w bezpieczeństwo państwa, jego porządek konstytucyjny; a w szczególności w suwerenność, niepodległość i nienaruszalność terytorium;
 - zagrazić 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;

¹⁴ Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. Nr 83, poz. 540).

¹⁵ Mapy ryzyka nie można utożsamiać z matrycą ryzyka. Mapy ryzyka obrazują skutki i są przygotowywane dla zagrożeń o określonym już prawdopodobieństwie (np. wysokim).

¹⁶ Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, s. 4–5.

- 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,
- o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej.

Proces oceny ryzyka koncentruje się na czterech krokach:

- identyfikacji zagrożeń – zgodnie z działaniami administracji rządowej,
- opisanu scenariuszy – wskazanie potencjalnych miejsc wystąpienia zagrożenia oraz jego typu,
- analizie skutków¹⁷ – dla ludności, gospodarki, mienia, środowiska, infrastruktury krytycznej, wraz z danymi graficznymi i tabelarycznymi,
- ocenie ryzyka¹⁸ – określenie prawdopodobieństwa, skutków, wartości ryzyka¹⁹ oraz poziomu jego akceptacji.

Prawdopodobieństwo opisuje się według skali, którą prezentuje tabela 1:

Tabela 1. Skala prawdopodobieństwa na potrzeby *Raportu (...)*

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 udokumentowane lub częściowo przekazywane w formie ustnej i/lub bardzo mało zdarzeń i/lub jest pewna szansa, powód, czy też urządzenia powodujące, że zdarzenie może wystąpić. Może zdarzyć się raz na dwadzieścia lat.
4	prawdopodobne	Jest prawdopodobne, że wystąpi w większości okolicznościach 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.

¹⁷ Pod pojęciem skutków należy rozumieć konsekwencje, zgodnie z definicją normy ISO. Patrz: s. 108.

¹⁸ Pojęcie zastosowano w dokumencie błędnie, powinno być rozumiane jako analiza ryzyka. Patrz: definicja na s. 107.

¹⁹ Patrz: definicja na s. 115 (poziom ryzyka).

Skala	Prawdopodobieństwo	Opis
5	bardzo prawdopodobne	Oczekuje się, że zdarzy się w większości okolicznościach i/lub zdarzenia te są bardzo dobrze udokumentowane i/lub funkcjonują one wśród mieszkańców i przekazywane są w formie ustnej. Może wystąpić raz na rok lub częściej.

Źródło: Procedura opracowania raportu częściowego do *Raportu o zagrożeniach bezpieczeństwa narodowego*, s. 14.

Skutki opisywane są również w pięciostopniowej skali, ale rozpatruje się je ponadto w odniesieniu do: życia i zdrowia, mienia i środowiska (tabela 2).

Tabela 2. Skala konsekwencji na potrzeby *Raportu (...)*

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 finansowej 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.
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). Niewielkie straty finansowe. 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.

Skala	Skutki	Kat	Opis (Z – życie i zdrowie, M – mienie, S – środowisko)
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	Spółeczność 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*, s. 16.

Wyniki analizy prezentowane są na matrycy (5×5) (rys. 1):

PRAWDOPODOBIENSTWO	5					
	4					
	3					
	2					
	1					
		A	B	C	D	E
	SKUTKI					

Rys. 1. Matryca ryzyka na potrzeby *Raportu*...

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

Metody przedstawione w części I niniejszej publikacji wskazują, w jaki sposób za ich pomocą można/należy:

- identyfikować zagrożenia – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, drzewa zdarzeń, wpływu na działalność (BIA), przyczyn i skutków oraz przyczyn i efektów,
- określać ich prawdopodobieństwo – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, muchy (ang. *bow tie analysis*), wpływu na działalność (BIA) oraz przyczyn i efektów,
- określać ich konsekwencje – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, drzewa zdarzeń, muchy (ang. *bow tie analysis*), wpływu na działalność (BIA), przyczyn i skutków oraz przyczyn i efektów,
- określać poziom ryzyka – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, drzewa zdarzeń, muchy (ang. *bow tie analysis*), wpływu na działalność (BIA) oraz przyczyn i skutków,
- prezentować wyniki analizy – macierz ryzyka.

1.3. Ochrona infrastruktury krytycznej

Zgodnie ze wspomnianą już nowelizacją ustawy o zarządzaniu kryzysowym w odniesieniu do IK dokonano redefinicji pojęcia ochrony infrastruktury krytycznej (również w kwestiach zarządzania ryzykiem). Obecna treść art. 3 pkt 3 mówi, że: „są to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”.

Nowelizacja z 2010 r. wprowadziła natomiast zapis w art. 6c. pkt 1 ppkt 2, mówiący, że dyrektor Rządowego Centrum Bezpieczeństwa przekazuje Komisji Europejskiej co 2 lata sprawozdanie zawierające ogólne dane dotyczące rodzajów ryzyka oraz zagrożeń i słabych punktów stwierdzonych w każdym z systemów, w których została wyznaczona europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej.

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego programu ochrony infrastruktury krytycznej uszczegóławia ogólną ocenę ryzyka dla funkcjonowania opisywanego obszaru zadaniowego, poprzez uwzględnienie w niej podatności na zagrożenie oraz konsekwencje zakłócenia funkcjonowania infrastruktury krytycznej.

Trzecie z rozporządzeń wydanych na podstawie nowelizacji ustawy odnoszące się do planów ochrony IK rozszerza metodykę oceny ryzyka o scenariusze. Dokładny zapis rozporządzenia brzmi: „plan ochrony IK powinien zawierać między innymi

ocenę ryzyka wystąpienia zagrożenia wraz z przewidywanymi scenariuszami rozwoju zdarzeń”. W tym przypadku zdecydowano się więc na wskazanie nie tylko potrzeby wykorzystania metodyki oceny ryzyka, ale także przeznaczonego do tego procesu narzędzia, jakim jest metoda scenariuszowa.

Na podstawie *Narodowego programu ochrony infrastruktury krytycznej* tworzone są warunki do poprawy jej bezpieczeństwa. Oznacza to podejmowanie działań zmierzających do zapobiegania, przygotowania i reagowania w sytuacjach zakłócenia funkcjonowania infrastruktury krytycznej oraz na działaniach pozwalających na jej odtworzenie.

Program przygotowany jest przez dyrektora Rządowego Centrum Bezpieczeństwa przy współpracy z ministrami i kierownikami urzędów centralnych. Na jego podstawie dyrektor RCB przedstawia co 2 lata sprawozdanie określające dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów w europejskiej infrastrukturze krytycznej występującej na terytorium Rzeczypospolitej Polskiej.

Mimo przedstawiania pojęcia ryzyka w badanym akcie prawnym na etapie analizy dokumentu nie znaleziono metodyki zarządzania ryzykiem.

Rozporządzenie w sprawie Narodowego programu ochrony infrastruktury krytycznej zgodnie z § 1 określa sposób realizacji obowiązków i współpracy w zakresie NPOIK przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, zwanymi operatorami infrastruktury krytycznej. Zgodnie z rozporządzeniem dyrektor Rządowego Centrum Bezpieczeństwa opracowuje kryteria pozwalające na wyodrębnienie infrastruktury krytycznej. Założenia te przekazywane są ministrom i kierownikom urzędów centralnych, którzy składają propozycję wpisania infrastruktury krytycznej w wykazie. Dyrektor RCB weryfikuje zestawienie i sporządza wykaz, określając nazwę i lokalizację, podległość organizacyjną infrastruktury, dane operatora lub zarządzającego infrastrukturą krytyczną. Na podstawie tych danych ministrowie wraz z kierownikami urzędów centralnych przygotowują charakterystykę obszaru, propozycje wymagań i standardów pozwalających na zapewnienie ciągłości funkcjonowania IK, ogólną ocenę ich ryzyka, priorytety w zakresie odtwarzania IK, a także możliwe sposoby zapobiegania zakłóceniom działania oraz propozycję programów badawczych i rozwojowych mogących wpłynąć na zwiększenie bezpieczeństwa IK. Aktualizacja wykazu jest dokonywana według potrzeb.

Rozporządzenie w sprawie planów ochrony infrastruktury krytycznej określa sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej opracowywanych przez właścicieli obiektów, instalacji lub urządzeń infrastruktury krytycznej a także warunki i tryb spełnienia wymogów posiadania planu ochrony IK. Plan sporządza się w wersji papierowej i elektronicznej, zawiera on nazwę i lokalizację infrastruktury, dane pozwalające na identyfikację, takie jak Regon, NIP, KRS, dane osoby odpowiedzialnej za kontakty w zakresie ochrony

oraz sporządzającej plan. Dokumentacja IK do planu zawiera jej charakterystykę i parametry techniczne, plan z naniesioną lokalizacją (obiektów, instalacji, systemu) oraz funkcjonalne połączenie z innymi obiektami. Ponadto określana jest zarówno charakterystyka zagrożeń oraz ocena ryzyka ich wystąpienia z rzeczywistymi scenariuszami, zależność od pozostałych systemów, jak i możliwości zakłócenia jej funkcjonowania. Kolejne warunki, które muszą być spełnione, to przedstawienie wariantów działania IK w przypadku jej zagrożenia lub zakłócenia, zapewnienie ciągłości funkcjonowania, oraz jej odtworzenia, a także zasady współpracy z centrami zarządzania kryzysowego oraz organami administracji publicznej. Wykonanie planu wymaga uzgodnień z właściwym ministrem lub dyrektorem urzędu centralnego, wojewodą, komendantem wojewódzkim Państwowej Straży Pożarnej, Policji, dyrektorem regionalnego zarządu gospodarki wodnej, wojewódzkim inspektorem nadzoru budowlanego, lekarzom weterynarii, państwowym wojewódzkim inspektorom sanitarnym oraz dyrektorom urzędu morskiego. Uzgodniony plan przedkłada się dyrektorowi Rządowego Centrum Bezpieczeństwa. Aktualizację planów przeprowadza się według potrzeb, nie rzadziej jednak niż raz na 2 lata. Wykonany plan podlega przepisom o ochronie informacji niejawnych lub o ochronie tajemnicy przedsiębiorstwa.

2. METODA WDROŻENIA ZARZĄDZANIA RYZYKIEM W PROCESIE PLANOWANIA CYWILNEGO

Prowadzone w projekcie badania skłoniły autorów do analizy normy PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem. Terminologia* oraz normy PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne* również w kontekście procesu planowania cywilnego. Pierwszy dokument gromadzi wiedzę na temat definicji ogólnych terminów dotyczących zarządzania ryzykiem. Kolejny zawiera zasady i wytyczne dotyczące zarządzania ryzykiem. Ponadto systematyzuje cały proces zarządzania ryzykiem oraz pokazuje wzajemne zależności poszczególnych elementów tego procesu.

Bazując na ich zawartości, można stwierdzić, że na proces zarządzania ryzykiem składają się następujące działania:

- ustalanie kontekstu¹,
- ocena ryzyka²:
 - identyfikacja ryzyka³,
 - analiza ryzyka⁴,
 - ewaluacja ryzyka⁵;
- postępowanie z ryzykiem⁶.

Każde z tych działań powiązane jest również z komunikacją i konsultacjami⁷ oraz monitorowaniem⁸ i przeglądem⁹.

Przedstawione powyżej i zgodne z polską normą nazewnictwo działań zawiera pewną nieścisłość. Na przykład „identyfikacja ryzyka” może sugerować, że „szacowania ryzyka”¹⁰ już dokonano. W rzeczywistości o ryzyku możemy mówić dopiero po kroku ewaluacja. Wcześniejsze etapy dotyczą zagrożenia, jego cech i następstw. Dlatego

¹ Patrz: definicja na s. 109.

² Patrz: definicja na s. 107.

³ Patrz: definicja na s. 106.

⁴ Patrz: definicja na s. 109.

⁵ Patrz: definicja na s. 114.

⁶ Patrz: definicja na s. 106.

⁷ Patrz: definicja na s. 116.

⁸ Patrz: definicja na s. 113.

⁹ Patrz: definicja na s. 113.

¹⁰ Patrz: definicja na s. 115.

w dalszej części niniejszego rozdziału, w celu uniknięcia wątpliwości, będą używane następujące określenia: ocena ryzyka, identyfikacja, analiza, ewaluacja ryzyka.

Celem badań było opracowanie metody oceny ryzyka. Z tego względu zakres pracy został ograniczony do wyżej wymienionych działań.

2.1. Metoda wykorzystania norm ISO w zakresie zarządzania ryzykiem w planowaniu cywilnym

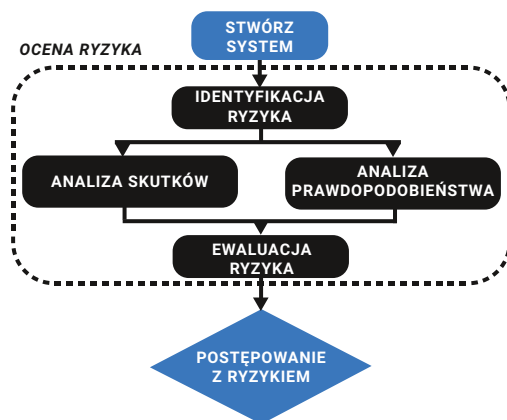
W wyniku analizy możliwości wykorzystania norm ISO w procesie planowania cywilnego wskazano, zgodnie z przepisami polskiego porządku prawnego, formalne potrzeby systemu zarządzania kryzysowego w zakresie planowania cywilnego. Zdefiniowano je jako ogólne postulaty:

- włączenia do planów zarządzania kryzysowego procedur oceny ryzyka oraz przygotowania na ich podstawie map ryzyka,
- wykorzystania przy ocenie ryzyka metody scenariuszowej¹¹.

Poddając generalizacji elementy pełnego procesu zarządzania ryzykiem (zgodnego z PN-ISO 31000:2012), wskazano także procesy, które mogą zostać wykorzystane przez system zarządzania kryzysowego w celu spełnienia tych postulatów. Procesy te zawierają się w ogólnej wytycznej dla oceny ryzyka i należą do nich:

- identyfikacja ryzyka,
- analiza ryzyka,
- ewaluacja ryzyka.

Procesy te uporządkowano w ramach schematu postępowania (rys. 1).

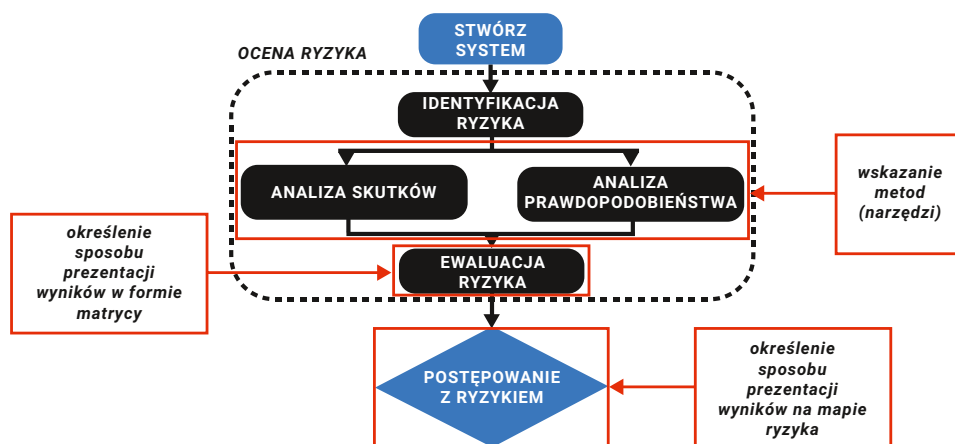


Rys. 1. Proces oceny ryzyka

Źródło: Opracowano na podstawie materiału szkoleniowego BSI, PN-ISO 31000:2012
Wytyczne w zakresie zarządzania ryzykiem korporacyjnym.

¹¹ Metoda ta jest formalnie wymagana jedynie przy analizie na potrzeby ochrony infrastruktury krytycznej.

Biorąc pod uwagę wymagania stawiane przez ustawę o zarządzaniu kryzysowym oraz konieczność przypisania poszczególnym krokom narzędzi badawczych, powyższą rycinę należało rozszerzyć. Uzupełnienie stanowi zakres koniecznych badań, które zostały zrealizowane w trakcie realizacji projektu nr DOBR/0016/R/ID2/003 (rys. 2).



Rys. 2. Prezentacja obszarów badawczych na podstawie wniosków z pierwszego etapu badań

Źródło: Opracowanie własne.

Biorąc pod uwagę powyższe założenia i ograniczenia procesu badawczego, efektem końcowym pracy będzie rozwiązanie głównego problemu badawczego, który można przedstawić w postaci pytania: jak powinien zostać zaplanowany proces oceny ryzyka by spełnił wymogi formalne systemu zarządzania kryzysowego przy jednoczesnym spełnieniu prakseologicznego celu badania?

Tak postawiony problem będzie wymagał odpowiedzi na zaprezentowane poniżej problemy cząstkowe:

- jakie metodyki są stosowane w innych krajach i na ile można dokonać ich implementacji do warunków polskich?
- jakie metody oceny ryzyka są obecnie wykorzystywane w Polsce?
- na ile spełniają one wymagania stawiane planom zarządzania kryzysowego?

Wstępne badania literaturowe przeprowadzone przed przystąpieniem do zasadniczej części badania wskazują, że:

1. Opublikowane i udostępnione metodyki innych krajów przedstawiają różny poziom szczegółowości prezentowanych treści. Jedne odwołują się przede wszystkim do ogólnego procesu postępowania przy ocenie ryzyka (Irlandia i Szwecja), inne (Niemcy) wskazują szczegółowe rozwiązania. W związku

z tym dokumenty te należy analizować w odniesieniu do ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*.

2. Nie wszystkie narzędzia oceny ryzyka zawarte w międzynarodowym standardzie ISO/IEC 31010 *Risk Management – Risk Assessment Techniques* można wykorzystać na potrzeby planowania cywilnego. Część narzędzi analitycznych (wszystkie metody ilościowe) są przeznaczone do analizy zdarzeń związanych z awariami¹² i nie można przetransponować ich na potrzeby systemu zarządzania kryzysowego. Dlatego też przygotowywana metoda będzie opierała się na metodach jakościowych.

Metodyka *Procedury opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego* nie jest dokumentem opracowanym z myślą o sporządzaniu planów zarządzania kryzysowego i jako taka nie jest w pełni wystarczająca, by została zaimplementowana na potrzeby projektu. Biorąc powyższe pod uwagę, zdecydowano się oprzeć dalsze rozważania dotyczące procesu zarządzania ryzykiem na normie PN-ISO 31000:2012 oraz ISO/IEC 31010.

Wybrana (powyższa) norma opisuje procesy i ogólne zasady. Odnosząc się do kwestii wyboru metodyki oceny ryzyka, zaleca ona aby: „organizacja stosowała narzędzia i techniki identyfikacji ryzyka odpowiednie do jej celów i zdolności oraz ryzyk, na które jest narażona”¹³. Możliwe do zastosowania metody i narzędzia zostały wskazane w normie ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*.

Mimo pozostawienia organizacji decyzji co do wyboru narzędzi i technik oceny ryzyka norma ta sugeruje, którymi narzędziami, na których etapach oceny ryzyka należy się posługiwać. Metody rekomendowane dla planowania cywilnego wskazuje tabela 1.

Tabela 1. Metody rekomendowane dla planowania cywilnego przy ocenie ryzyka

Metody oceny ryzyka	Procesy oceny ryzyka				
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka
		Skutki ¹⁴	Prawdopodobieństwo	Poziom ryzyka	
Analiza „co, jeśli?”	++	++	++	++	++
Analiza scenariuszy	++	++	+	+	+
Analiza drzewa błędów	+	-	++	+	+

¹² Patrz: definicja na s. 135.

¹³ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 49.

¹⁴ Konsekwencje – w rozumieniu normy ISO 31000.

Metody oceny ryzyka	Procesy oceny ryzyka				
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka
		Skutki ¹⁴	Prawdopodobieństwo	Poziom ryzyka	
Analiza drzewa zdarzeń	+	++	+	+	-
Analiza bow tie	-	+	++	++	-

Legenda:

++ – zdecydowanie dotyczy

+ – dotyczy

- – nie dotyczy

Źródło: ISO/IEC 31010 Risk Management – Risk Assessment Techniques (tłumaczenie własne).

2.2. Szczegółowy opis procesu z uwzględnieniem istniejących ograniczeń formalno-prawnych

Jak już wcześniej wspomniano, ocena ryzyka to proces, na który składają się:

- identyfikacja,
- analiza,
- ewaluacja ryzyka.

Celem procesu identyfikacji ryzyka jest stworzenie pełnej listy zagrożeń, wraz z ich źródłami, obszarami wpływów, zdarzeniami, przyczynami oraz następstwami. Najważniejszą kwestią dotyczącą tego etapu jest to, aby opracowana lista była wyczerpująca – ryzyka niezidentyfikowane nie są analizowane w dalszej części procesu. Do rozważań przyjęto listę zagrożeń i ich podział na grupy wypracowany w ramach projektu badawczego.

Celem analizy jest dostarczenie danych wejściowych do etapu ewaluacji, czyli określenia wartości ryzyka. W tym celu wyodrębnia się szereg aspektów składających się na proces powstawania, przebiegu i możliwych oddziaływań zjawiska (najczęściej niekorzystnego) poddawanego analizie. Następnie dokonuje się wartościowania każdego z nich. W zależności od stopnia szczegółowości prowadzonej oceny uwzględnia się szereg aspektów zarówno po stronie cech samego zjawiska, jak i jego oddziaływań. W dokumencie *All Hazards Risk Assessment – Methodology Guidelines 2012–2013*¹⁵ autorzy uwzględnili następujące aspekty: polityczny,

¹⁵ *All Hazards Risk Assessment – Methodology Guidelines 2012-2013* [dok. elektr.], <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ll-hzrds-sssmnt/ll-hzrds-sssmnt-eng.pdf> [dostęp: luty 2015].

ekonomiczny, społeczny, technologiczny oraz prawny i środowiskowy. W *National Security Programme – National Risk Assessment Method Guide 2008* wyszczególnia się zaś aspekt: terytorialny, materialny, ekonomiczny, ekologiczny, socjalny i polityczny. Podobne podejście prezentowane jest również w innych badanych metodykach oceny ryzyka.

Uogólniając różne podejścia do prowadzenia oceny ryzyka i jego następstw, można wyróżnić trzy etapy postępowania:

1. Określenie rodzaju zdarzenia (rozumianego jako wystąpienie lub zmiana konkretnego zestawu okoliczności). Na tym etapie określa się scenariusze prowadzące do powstania danego zjawiska.
2. Określenie sposobu postrzegania zdarzenia (okoliczności towarzyszących zagrożeniu). Na tym etapie należy rozważyć/określić, jakie czynniki naturalne, infrastrukturalne oraz społeczne powodują, że zdarzenie jest postrzegane jako zagrożenie. Analizie poddaje się każdy ze scenariuszy opracowanych w pierwszym etapie.
3. Określenie następstw (konsekwencji, rezultatów zdarzenia). Jest to etap, który pozwala ocenić, jakie konsekwencje wywołuje dane zdarzenie, uwzględniając poszczególne obszary oddziaływania: społeczeństwo (zdrowie i życie ludzkie), gospodarka, środowisko, utrata wizerunku.

Ostatnim etapem oceny ryzyka jest jego ewaluacja, czyli porównanie wyników analizy ryzyka z kryteriami pozwalającymi na jego wartościowanie. W wersji najprostszej jest to tabelaryczne przyporządkowanie prawdopodobieństwa zdarzenia i jego skutków, dające w rezultacie poziom ryzyka. Takie podejście zostało zastosowane w ramach opracowywania *Raportu o zagrożeniach bezpieczeństwa narodowego*. Oparcie szacowania poziomu ryzyka na jedynie dwóch parametrach nie pozwala na uwzględnienie różnorodności zjawisk i zdarzeń dotyczących społeczności lokalne. Jest to zatem zbyt duże uproszczenie, aby można było je zastosować na niższych poziomach administracji.

Przedstawiony powyżej proces oceny ryzyka różni się zasadniczo w zależności od tego, czy zdarzeniu da się przyporządkować prawdopodobieństwo jego wystąpienia, czy nie. Ta pierwsza grupa obejmuje zagrożenia naturalne i techniczne (infrastrukturalne). Dominującymi metodami stosowanymi w ocenie ryzyk związanych z tymi zagrożeniami są metody ilościowe, gdzie każdy z rozważanych elementów jest wartościowany w drodze obliczeń matematycznych lub przyporządkowania do pozycji tabelarycznej.

Zupełnie inaczej przedstawia się proces oceny ryzyka w odniesieniu do ryzyka związanego z procesami społecznymi. Zjawiska te mają charakter długotrwały i przebiegają z różnym nasileniem w kolejnych jednostkach czasowych. W tej sytuacji niezwykle trudno jest precyzyjnie określić okoliczności, czynniki (ang. *risk factors*) bądź moment, w którym proces dotychczas tolerowalny staje się zagrożeniem. Dla tej

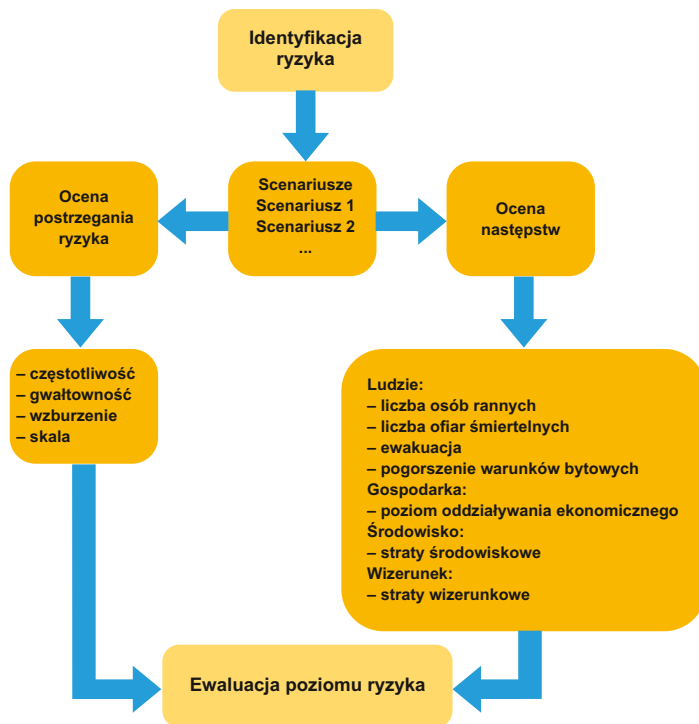
grupy zjawisk w celu przeprowadzenia oceny ryzyka stosuje się metody eksperckie. Polegają one na interpretacji przez specjalistów danych statystycznych, raportów, kwestionariuszy itp. Wykorzystując wiedzę i doświadczenie ekspertów, określa się spodziewane konsekwencje i szacuje poziom ryzyka. Wśród stosowanych metod wymienić można:

- burzę mózgow – konfrontowanie ze sobą ocen przygotowanych przez różnych ekspertów,
- grupowanie podobieństw (ang. *affinity grouping*) – metoda polegająca na przyporządkowaniu zagrożeniom o podobnych cechach podobnego poziomu ryzyka,
- listę kontrolną (ang. *checklist*) – poziom ryzyka określany jest na podstawie listy pewnych cech zagrożenia,
- analizę scenariuszy (ang. *scenario analysis*) – dla danego zagrożenia opracowuje się różne scenariusze, a ryzyko ustalane jest dla scenariusza najbardziej reprezentatywnego i skrajnego (tzw. czarnego scenariusza),
- analizę SWOT – gdzie dokonuje się oceny mocnych (ang. *strengths*) i słabych stron (ang. *weaknesses*) oraz szans (ang. *opportunities*) i zagrożeń (ang. *threats*) dla społeczności poddanej danemu zagrożeniu,
- analizę PEST – metoda pozwalająca na szacowanie wpływu oddziaływań zewnętrznych (otoczenia systemowego) na daną społeczność; w jej ramach poddaje się analizie czynniki polityczne, ekonomiczne, społeczne i technologiczne; istnieją modyfikacje tej metody, m.in. PESTLE – tam dodatkowo analizuje się czynniki prawne i środowiskowe,
- sondy i ankiety – poziom ryzyka określany jest na podstawie badań społecznych (przykładowo – badanie poczucia bezpieczeństwa wśród mieszkańców może dać wynik skrajnie różny od uzyskiwanego na podstawie badań statystycznych zgłaszanych przestępstw i wykrywalności ich sprawców).

Biorąc pod uwagę powyższe uwarunkowania, w dalszej części niniejszego rozdziału zastosowano zróżnicowane podejście do obu tych grup zagrożeń. Dla zagrożeń naturalnych i technicznych (infrastrukturalnych) opracowano metodykę opartą na analizie ilościowej, zaś dla zagrożeń społecznych metodykę opartą na analizie jakościowej.

Metodyka oceny ryzyka dla zagrożeń naturalnych i infrastrukturalnych

Kolejne kroki wykonywane w ramach metodyki zaprezentowane zostały na rys. 3.



Rys. 3. Schemat metody ilościowej

Źródło: Opracowanie własne.

Etap identyfikacji ryzyka

Bazując na źródłach danych o potencjalnych ryzykach, należy sporządzić wykaz zagrożeń charakterystycznych dla danego terenu, wyodrębniając z nich zagrożenia naturalne i infrastrukturalne (dla zagrożeń o charakterze społecznym opracowano odrębną metodykę postępowania). Identyfikacja potencjalnych ryzyk dokonywana jest na podstawie danych historycznych, wytycznych lub zaleceń wyższych szczebli, planów służb reagowania, danych literaturowych oraz obowiązku prawnego.

Etap analizy

Krok 1. Rodzaj ryzyka

Dla każdego zidentyfikowanego ryzyka należy opracować wszystkie możliwe scenariusze, tj. wskazać potencjalne drogi jego powstania oraz rozchodzenia się. Należy zwrócić uwagę na fakt, że ryzyko może mieć kilka różnych dróg powstawania i/lub rozchodzenia się. W przypadku ryzyka powodzi będzie to na przykład sześć potencjalnych dróg powstania: roztopy, zator, wezbranie, sztorm, nawalny deszcz czy katastrofa budowli piętrzącej.

Dla każdego scenariusza przeprowadza się ocenę postrzegania ryzyka oraz ocenę jego następstw.

Krok 2. Ocena postrzegania ryzyka

Na ocenę postrzegania ryzyka składają się następujące wskaźniki:

1. Częstotliwość – zależność wpływu ryzyka od tego, jak często dane zagrożenie występuje na danym poziomie administracji.

Tabela 2. Częstotliwość

Wpływ	Częstotliwość występowania (co najmniej raz na [lat])
1	500 lub rzadziej
2	100
3	20
4	5
5	1

Źródło: Procedura opracowania raportu cząstkowego do *Raportu o zagrożeniach bezpieczeństwa narodowego*.

2. Gwałtowność – zależność wpływu ryzyka od tego, jak szybko dane zjawisko się pojawia, czy możliwe jest jego monitorowanie oraz ostrzeżenie społeczeństwa.

Tabela 3. Gwałtowność

Wpływ	Gwałtowność
1	zagrożenie pojawiające się powoli, możliwe do monitorowania, istnieje możliwość ostrzeżenia społeczeństwa z dużym wyprzedzeniem czasowym
2	zagrożenie pojawiające się powoli, możliwe do monitorowania, istnieje możliwość ostrzeżenia społeczeństwa z małym wyprzedzeniem czasowym
3	zagrożenie pojawiające się szybko, możliwe do monitorowania, istnieje możliwość ostrzeżenia społeczeństwa z małym wyprzedzeniem czasowym, pozwalającym na podjęcie działań tylko przez społeczność do tego przygotowaną
4	zagrożenie pojawiające się gwałtownie, trudne do monitorowania, istnieje możliwość ostrzeżenia społeczeństwa z małym wyprzedzeniem czasowym pozwalającym na przeprowadzenie ewakuacji wyłącznie samodzielnej
5	zagrożenie pojawiające się gwałtownie, niemożliwe do monitorowania, brak możliwości ostrzeżenia społeczeństwa ¹⁷

Źródło: Opracowanie własne.

¹⁶ Przykładem takiego zdarzenia jest upadek samolotu na budynki mieszkalne. Zagrożenie takie jest standardowo rozważane na trasach dołotowych do lotnisk.

3. Wzburzenie – zależność wpływu ryzyka od tego jak jest ono postrzegane przez społeczeństwo nim dotknięte.

Tabela 4. Wzburzenie

Wpływ	Wzburzenie
1	zagrożenie o znanym charakterze, mieszkańcy znają wzorce prawidłowych zachowań i posiadają zasoby własne pozwalające na łagodzenie jego skutków ¹⁸ lub nie ma potrzeby reagowania na zagrożenie i łagodzenia jego skutków
2	zagrożenie o znanym charakterze, mieszkańcy znają wzorce prawidłowych zachowań, ale nie posiadają zasobów własnych pozwalających na łagodzenie jego skutków (wymagana interwencja służb ratowniczych i/lub administracji) ¹⁹
3	zagrożenie o częściowo znanym charakterze, wymagane jest podanie mieszkańcom wzorców prawidłowych zachowań oraz interwencja służb ratowniczych i/lub administracji ²⁰
4	zagrożenie o częściowo znanym charakterze, wymagane jest podanie mieszkańcom wzorców prawidłowych zachowań, nie ma możliwości zwalczania jego skutków w krótkim okresie ²¹
5	zagrożenie o niespotykanym charakterze, mieszkańcy nie znają wzorców prawidłowych zachowań, brak możliwości zwalczania jego skutków w krótkim czasie ²²

Źródło: Opracowanie własne.

4. Skala – zależność wpływu zagrożenia od poziomu administracyjnego, który jest odpowiedzialny za zwalczanie zagrożenia bądź jego skutków.

Tabela 5. Skala

Wpływ	Poziom administracji
1	gmina
2	powiat
3	województwo
4	kraj
5	międzynarodowy ²³

Źródło: Opracowanie własne.

¹⁷ Przykładem jest grypa sezonowa.

¹⁸ Przykładem jest pożar wielkoobszarowy.

¹⁹ Przykładem są zagrożenia w pobliżu zakładów stwarzających ryzyko awarii przemysłowej.

²⁰ Przykładem są zagrożenia radiologiczne.

²¹ Przykładem takiego zdarzenia jest wystąpienie pandemii nowej, nieznannej choroby, jak np. wirus AH1N1.

²² Dotyczy to zagrożeń, dla których konieczna jest współpraca o charakterze ponadnarodowym, np. migracji spowodowanych konfliktami polityczno-militarnymi.

Krok 3. Ocena następstw

Rozpatrywana jest w czterech kategoriach – ludzie, gospodarka, środowisko i wizerunek.

Kategoria – oddziaływanie na ludzi

Ocena oddziaływania na społeczeństwo jest uszczegółowiona przez następujące podkategorie:

1. Ranni – zależność wpływu zagrożenia od liczby rannych.

Tabela 6. Ranni

Wpływ	Liczba rannych
1	< 10
2	< 100
3	< 500
4	< 1000
5	> 1000

Źródło: Opracowanie własne.

2. Ofiary śmiertelne – zależność wpływu zagrożenia od liczby ofiar śmiertelnych.

Tabela 7. Ofiary śmiertelne

Wpływ	Liczba ofiar śmiertelnych
1	< 5
2	< 10
3	< 100
4	< 500
5	> 500

Źródło: Opracowanie własne.

3. Ewakuacja – zależność wpływu zagrożenia od liczby ewakuowanych osób oraz czasu jej trwania. Jeżeli możliwe jest wystąpienie różnego czasu ewakuacji dla różnych grup poszkodowanych, do oceny skutków zagrożenia bierze się pod uwagę grupę o najdłuższym czasie ewakuacji. Uwzględniając spodziewaną liczbę osób do ewakuacji i czas jej trwania, należy z tabeli odczytać liczbę obrazującą poziom wpływu.

Tabela 8. Ewakuacja

Liczba osób ewakuowanych	Okres ewakuacji				
	< 3 dni	< tydzień	< miesiąc	< rok	> rok
< 10	1	2	2	3	3
< 100	2	2	3	3	3
< 500	2	3	3	3	4
< 1000	3	3	3	4	4
> 1000	3	3	4	4	5

Źródło: Opracowanie własne.

4. Pogorszenie warunków bytowych – zależność wpływu zagrożenia od liczby osób, których warunki bytowe uległy pogorszeniu oraz czasu trwania tego stanu; przez pogorszone warunki bytowe należy rozumieć utrudniony dostęp (lub jego brak) do tak podstawowych usług, jak jedzenie, woda, prąd, posiadane środki finansowe, opieka medyczna, ogrzewanie, obiekty użyteczności publicznej, droga, transport publiczny itp.

Tabela 9. Pogorszenie warunków bytowych

Liczba osób	Okres pogorszonych warunków bytowych				
	< 2 dni	< tydzień	< miesiąc	< rok	> rok
< 10	1	2	2	3	3
< 100	2	2	3	3	3
< 500	2	3	3	3	4
< 1000	3	3	3	4	4
> 1000	3	3	4	4	5

Źródło: Opracowanie własne.

Kategoria – oddziaływanie na gospodarkę

Z uwagi na odmienny sposób kształtowania budżetu, wpływ zagrożenia na gospodarkę należy rozpatrywać odrębnie w odniesieniu do jednostek samorządu terytorialnego i administracji rządowej. Jednostki samorządu terytorialnego dysponują budżetem własnym zatwierdzanym w drodze uchwały przez organ stanowiący (radę gminy, radę powiatu, sejmik wojewódzki). Dlatego też wpływ zagrożenia na gospodarkę rozpatrywany jest na podstawie tego, jaki procent budżetu danej jednostki administracyjnej stanowi kwota wydana na realizację zadań własnych jednostki administracyjnej związanych z wystąpieniem danego zagrożenia, zgodnie z tabelą 10.

Tabela 10. Poziom oddziaływania ekonomicznego dla jednostek dysponujących budżetem własnym (samorząd terytorialny)

Wpływ	Koszty
1	< 0,5% wydatków budżetu ²⁴
2	< 5% wydatków budżetu
3	< 15% wydatków budżetu
4	> 15% wydatków budżetu
5	brak możliwości uchwalenia budżetu na kolejny rok – przekroczony indywidualny wskaźnik zadłużenia ²⁵

Źródło: Opracowanie własne.

UWAGA: Zgodnie z wytycznymi ministra administracji i cyfryzacji w sprawie zasad i trybu uruchamiania środków budżetu państwa dla jednostek samorządu terytorialnego na zadania związane z przeciwdziałaniem zdarzeniom noszącym znamiona klęsk żywiołowych i usuwaniem ich skutków, jeżeli straty wywołane klęską żywiołową są nie mniejsze niż 5% planowanych dochodów własnych jednostki na rok bezpośrednio poprzedzający rok wystąpienia klęski żywiołowej, możliwe jest otrzymanie dotacji celowej z budżetu państwa na dofinansowanie zadań własnych związanych z remontem i odbudową zniszczonych lub uszkodzonych obiektów budowlanych. Dotacja ta może sięgać 80% kosztów realizacji danego zadania. Otrzymanie takiej dotacji zmniejsza koszty ponoszone przez jednostkę samorządu terytorialnego i należy ten fakt uwzględnić przy szacowaniu oddziaływania ekonomicznego.

Budżet administracji rządowej regulowany jest ustawą budżetową przyjmowaną przez Sejm. Administracja rządowa corocznie planuje swoje wydatki, opierając się na wydatkach roku poprzedniego. Na poziomie poszczególnych resortów i poziomie wojewódzkim nie uwzględnia się natomiast zdarzeń o charakterze nadzwyczajnym. Rezerwami takimi na potrzeby całej administracji dysponuje natomiast Biuro Usuwania Skutków Klęsk Żywiołowych. Biuro wspiera działania związane z przeciwdziałaniem klęskom żywiołowym i usuwaniem ich skutków w dwóch obszarach:

- pomoc jednostkom samorządu terytorialnego w zakresie odbudowy infrastruktury,

²³ Kwota 0,5% wydatków budżetu stanowi minimalną wartość rezerwy celowej przeznaczonej na realizację zadań własnych z zakresu zarządzania kryzysowego. Rezerwę tę tworzy się zgodnie z art. 26 par. 4 ustawy o zarządzaniu kryzysowym z 2007 r. (Dz. U. Nr 89, poz. 590 z późn. zm.).

²⁴ Od 1 stycznia 2014 r. jednostka samorządu terytorialnego nie będzie mogła uchwalić budżetu, jeśli nie będzie spełniona relacja zwana „indywidualnym wskaźnikiem zagrożenia” opisana w art. 243 ustawy o finansach publicznych z 2009 r. (Dz. U. Nr 157, poz. 1240). Jeśli poniesione koszty sprawiają, że ten współczynnik jest przekroczony, to zagrożeniu należy przypisać wartość „5”, niezależnie od wartości ilorazu kosztów do wysokości wydatków budżetowych.

- przyznawanie i wypłacanie zasiłków celowych na pokrycie wydatków związanych z klęską żywiołową lub ekologiczną (jest to zadanie zlecone z zakresu administracji rządowej realizowane przez samorząd gminny).

Dodatkowo corocznie w budżecie państwa przewiduje się rezerwę ogólną przeznaczoną na sytuacje nadzwyczajne. Rezerwę tę może uruchomić na wniosek odpowiedniego dysponenta odpowiednio: minister finansów (do kwoty 1 mln zł), prezes Rady Ministrów (do 5 mln zł), Rada Ministrów (całość rezerwy). W razie wyczerpania się rezerwy konieczna jest nowelizacja ustawy budżetowej i związane z tym zwiększenie zadłużenia państwa lub pozyskanie środków zewnętrznych, np. pomocy Banku Światowego, Funduszu Solidarności Unii Europejskiej itp. Wpływ zdarzenia na gospodarkę w odniesieniu do jednostek administracji rządowej zawiera tabela 11.

Tabela 11. Poziom oddziaływania ekonomicznego dla jednostek administracji rządowej (objętych regulacjami ustawy budżetowej)

Wpływ	Koszty
1	środki zaplanowane na dany rok budżetowy wystarczają na pokrycie kosztów prowadzenia działań i łagodzenia skutków zdarzenia
2	zaplanowane środki zwiększone o rezerwy będące w dyspozycji Biura Usuwania Klęsk Żywiołowych pozwalają na pokrycie kosztów, a ewentualne uruchomienie rezerwy ogólnej budżetu państwa dotyczy kwoty nieprzekraczającej 5 mln zł
3	wymagane jest uruchomienie rezerwy ogólnej budżetu państwa w wysokości powyżej 5 mln zł (decyzją Rady Ministrów)
4	wysokość kosztów przekracza rezerwę ogólną – wymagana jest nowelizacja budżetu państwa
5	wysokość nakładów wymaga skorzystania z pomocy Banku Światowego lub innych środków międzynarodowych (np. Funduszu Solidarności Unii Europejskiej)

Źródło: Opracowanie własne.

Kategoria – oddziaływanie na środowisko

Ocena wpływu skutków zagrożenia na środowisko rozpatrywana jest przez opis strat środowiskowych.

Tabela 12. Straty środowiskowe

Wpływ	Wpływ na środowisko
1	mała powierzchnia (kilka hektarów) skażonego terenu, brak innych oddziaływań
2	powierzchnia skażonego terenu powyżej 10 ha, brak innych oddziaływań

Wpływ	Wpływ na środowisko
3	utrata rzadkich i/lub zagrożonych gatunków lub zdarzenie ma negatywny wpływ na obszar chroniony, niezależnie od wielkości skażonego terenu (np. park narodowy, obszar Natura 2000 itp.)
4	długotrwałe zanieczyszczenie wód lądowych, podziemnych, terenów rolniczych itp.
5	nieodwracalne zniszczenia środowiska (utrata różnorodności gatunkowej, nieodwracalne zmiany krajobrazu, utrata bogactw naturalnych)

Źródło: Opracowanie własne.

Kategoria – oddziaływanie na wizerunek

Wpływ zagrożenia na wizerunek danej społeczności określany jest na podstawie opisu strat wizerunkowych wywołanych przez zagrożenie.

Tabela 13. Straty wizerunkowe

Wpływ	Wpływ na wizerunek
1	krótkotrwały, dotyczący do małej grupy ludzi, nie ma wpływu na gospodarkę danej jednostki terytorialnej, nie wywołuje napięć i niepokojów społecznych, nie wymaga podejmowania specjalnych działań naprawczych
2	krótkotrwały, mogący wywołać stan napięcia i niezadowolenia lub dotyczący, wielu grup odbiorców, nie ma wpływu na gospodarkę danej jednostki terytorialnej, nie wymaga podejmowania specjalnych działań naprawczych
3	krótkotrwały, dotyczący wielu grup odbiorców, wywołuje stan napięcia i niezadowolenia; ma wpływ na gospodarkę danej jednostki terytorialnej, wymaga podjęcia specjalnych działań naprawczych
4	długoterminowy, dotyczący wielu grup odbiorców, wywołuje długotrwały stan napięcia i niezadowolenia; ma wpływ na gospodarkę danej jednostki terytorialnej, wymaga podjęcia specjalnych działań naprawczych
5	długoterminowy, dotyczący jednocześnie dużej liczby odbiorców, może doprowadzić do wybuchu społecznego niezadowolenia lub ma negatywny wpływ na gospodarkę danej jednostki terytorialnej, wymaga długotrwałych działań naprawczych

Źródło: Opracowanie własne.

Etap ewaluacji ryzyka

Ewaluacja – określenie poziomu ryzyka poprzez:

- zsumowanie wartości wskaźników dla postrzegania zagrożenia (suma liczb obrazujących wpływ z tabel 3 do 6),

- zsumowanie wartości wskaźników dla następstw zagrożenia (suma liczb obrazujących wpływ z tabel 7 do 13, przy czym w zależności od rodzaju jednostki stosuje się jedną z tabel obrazujących wpływ na ekonomię – tabelę 10 albo 11),
- odczyt poziomu ryzyka z tabeli.

Uzyskiwane wartości ryzyka²⁵:

- minimalne (kolor niebieski – 1),
- małe (kolor zielony – 2),
- średnie (kolor żółty – 3),
- duże (kolor czerwony – 4),
- ekstremalne (kolor brązowy – 5).

Tabela 14. Szacowanie wartości poziomu ryzyka

		NASTĘPSTWA ZAGROŻENIA				
		< 8	< 12	< 18	< 25	> 25
POSTRZEGANIE ZAGROŻENIA	< 5	1	2	2	3	3
	< 8	2	2	3	3	3
	< 11	2	3	3	3	4
	< 15	3	3	3	4	4
	> 15	3	3	4	4	5

Źródło: Opracowanie własne.

Metodyka oceny ryzyka dla zagrożeń społecznych

Dla zagrożeń społecznych, ze względu na brak możliwości zastosowania wyżej wymienionych wskaźników, opracowana została metoda jakościowa. Na jej podstawie właściwy organ zarządzania kryzysowego może przeprowadzić badania eksperckie i określić wartość ryzyka związanego z danym zagrożeniem. Grupa zagrożeń społecznych obejmuje patologie, zmiany demograficzne oraz migracje ludności.

Etap identyfikacji ryzyka

Identyfikacja potencjalnego ryzyka dokonywana jest na podstawie danych historycznych, wytycznych lub zaleceń wyższych szczebli, planów służb reagowania, danych literaturowych oraz obowiązku prawnego.

Etap analizy ryzyka

Informacje o tym, które instytucje/organy są zobowiązane do zbierania danych o poszczególnych zagrożeniach społecznych, przedstawia tabela 15.

²⁵ Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego.

Tabela 15. Wykaz instytucji dysponującymi danymi wyjściowymi

Zagrożenie	Organ odpowiedzialny
migracje	urząd statystyczny
protesty społeczne	policja lub organ wydający pozwolenie na zgromadzenia publiczne
alkoholizm	ośrodek pomocy społecznej
bezrobocie strukturalne	urząd pracy
narkomania	ośrodek pomocy społecznej
ubóstwo	ośrodek pomocy społecznej
czyny o charakterze chuligańskim	policja
przestępczość nieletnich	policja
walczące o dominację ruchy nieformalne i subkulturowe	policja
niż/wyż demograficzny	urząd statystyczny
starzenie się społeczeństwa	urząd statystyczny

Źródło: Opracowanie własne.

Ze względu na charakter tych zagrożeń niemożliwe jest opracowanie metod ilościowych służących oszacowania poziomu ryzyka. Należy zatem korzystać z zespołu (zespołów) ekspertów powoływanych z ww. instytucji. Dane niezbędne do pracy zespołu można pozyskać z następujących źródeł:

- komisji bezpieczeństwa i porządku – której zadaniem jest ocena zagrożeń porządku publicznego i bezpieczeństwa obywateli na terenie powiatu²⁶;
- spisów powszechnych – pozwalających na określenie wielkości migracji;
- wykazu dzieci objętych obowiązkiem szkolnym – pozwalających z dużą dokładnością oszacować zmianę liczby mieszkańców w perspektywie pokolenia, a także przewidzieć konieczność budowania/zamykania szkół, co przekłada się na wzrost zatrudnienia/bezrobocia; obowiązek informowania dyrektorów szkół o zmianach w ewidencji dzieci jest nałożony przez ustawę o systemie oświaty²⁷;
- gminnego programu profilaktyki i rozwiązywania problemów alkoholowych – jego powstanie zakłada ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi²⁸; na jego podstawie można określić skalę problemu alkoholowego na danym terenie, tzn. oszacować liczbę osób z problemem

²⁶ Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. Nr 91, poz. 578 z późn. zm.).

²⁷ Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. Nr 95, poz. 425 z późn. zm.).

²⁸ Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. Nr 35, poz. 230 z późn. zm.).

alkoholowym, liczbę osób żyjących w otoczeniu takiej osoby oraz skalę przemocy domowej spowodowanej tym nałogiem,

- gminnego programu przeciwdziałania narkomanii – jego powstanie zakłada ustawa o przeciwdziałaniu narkomanii²⁹; na jego podstawie można określić skalę problemu narkomanii na danym terenie, tzn. oszacować liczbę uzależnionych od narkotyków.

Zespół, bazując na tych danych, powinien przeprowadzić analizę SWOT, którą przedstawiono w tabeli 16.

Tabela 16. Analiza SWOT

	Pozytywne (pomocne w zwalczeniu zagrożenia)	Negatywne (utrudniające zwalczenie zagrożenia)
Elementy związane z działaniami własnymi prowadzonymi przez daną jednostkę (gminę, powiat, województwo)	<p>Mocne strony:</p> <ul style="list-style-type: none"> • skuteczny monitoring zagrożenia, • dobra współpraca instytucjonalna, • posiadanie narzędzi lub programów redukujących dane zagrożenie, • wystarczające środki finansowe, • malejący trend zjawiska. 	<p>Słabe strony:</p> <ul style="list-style-type: none"> • ograniczony monitoring zjawiska bądź jego brak, • brak współpracy między instytucjami zajmującymi się danym zagrożeniem, • brak narzędzi i środków finansowych niezbędnym do ograniczenia zjawiska, • zagrożenie o charakterze narastającym.
Czynniki związane z otoczeniem zewnętrznym	<p>Szanse:</p> <ul style="list-style-type: none"> • korzystny stan prawny lub spodziewane zmiany prawne sprzyjające zwalczaniu zagrożenia, • możliwość wsparcia instytucjonalnego ze strony wyższych szczebli administracji, • możliwość uzyskania środków pomocowych lub opracowania projektów finansowanych przez instytucje zewnętrzne. 	<p>Zagrożenia:</p> <ul style="list-style-type: none"> • stan prawny nie pozwala na aktywne zwalczanie zagrożenia, • nie należy oczekiwać wsparcia ze strony administracji wyższych szczebli, • brak możliwości uzyskania zewnętrznych środków finansowych na realizację projektów redukujących dane zagrożenie.

Źródło: Opracowanie własne.

²⁹ Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. Nr 179, poz. 1485 z późn. zm.).

Po przeanalizowaniu wszystkich powyższych aspektów należy przyporządkować danemu zagrożeniu poziom ryzyka, korzystając z poniższej tabeli.

Tabela 17. Szacowanie wartości poziomu ryzyka

Ryzyko	
1 (minimalne)	pojedyncze przypadki monitorowane
2 (małe)	zjawisko narastające, niewymagające pomocy od wyższych szczebli
3 (średnie)	zjawisko narastające, wymagające zaangażowania dodatkowych osób i środków finansowych
4 (duże)	zjawisko narastające, wymagające wsparcia finansowego i organizacyjnego wyższych szczebli
5 (ekstremalne)	zjawisko narastające, powodujące nieodwracalne negatywne zmiany społeczne w ciągu najbliższych 25 lat

Źródło: Opracowanie własne.

3. ZARZĄDZANIE RYZYKIEM POWODZIOWYM

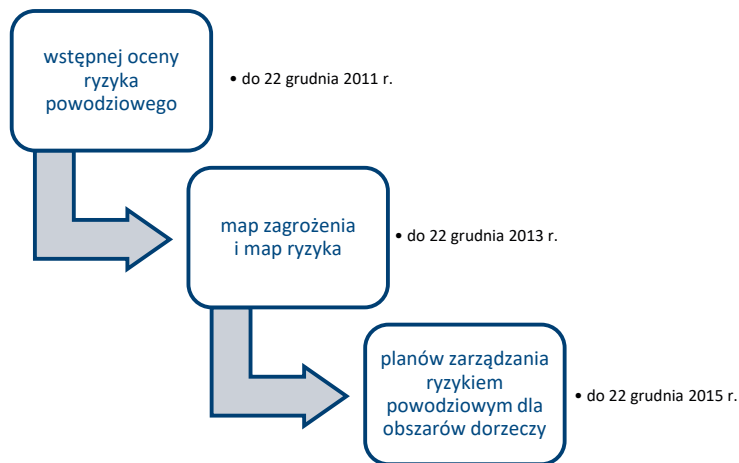
W Polsce dyskusja nad zarządzaniem ryzykiem powodziowym została podjęta wraz z rozpoczęciem prac nad tzw. dyrektywą powodziową, kiedy w połowie 2004 r. Komisja Europejska zaprezentowała Radzie ds. Środowiska projekt programu działań dotyczący zarządzania ryzykiem występowania powodzi na skalę europejską. Projekt zakładał, że państwa UE powinny współpracować przy opracowywaniu map zagrożenia i map ryzyka oraz wdrażaniu planów zarządzania ryzykiem powodziowym. W tym samym roku w październiku, podczas spotkania Rady Unii Europejskiej ds. Środowiska, uzgodniono, że osiągnięcie tego celu wymaga opracowania dyrektywy poświęconej kwestiom powodzi. W kolejnym roku grupa ekspertów Europejskiego Programu Działań w sprawie zarządzania ryzykiem występowania powodzi doprowadziła do opracowania projektu dyrektywy powodziowej. Prace nad dyrektywą zakończono w 2007 r. W kwietniu tego roku Parlament Europejski przyjął dyrektywę, która została zatwierdzona w październiku. Dyrektywa została zaimplementowana do polskiego prawa nowelizacją Prawa wodnego z dnia 5 stycznia 2011 r.

Celem niniejszego rozdziału jest wskazanie zasad zarządzania ryzykiem powodziowym opartych o rozwiązania przyjęte w dyrektywie powodziowej. W poszczególnych jego częściach zostaną zaprezentowane główne założenia dyrektywy oraz proces jej wdrażania, polityka zarządzania ryzykiem powodziowym oraz metodyka sporządzania planów w tym zakresie. Taka prezentacja treści pozwala na wskazanie we właściwym świetle zasad zarządzania ryzykiem powodziowym na tle ogólnych założeń kształtowania strategii przeciwpowodziowych. Struktura rozdziału została oparta na kolejnych etapach realizacji tej strategii, a więc przygotowaniu: wstępnej oceny ryzyka, map zagrożeń i map ryzyka oraz planów zarządzania ryzykiem powodziowym.

3.1. Implementacja dyrektywy do polskiego systemu prawnego

Ustawa – Prawo wodne reguluje kwestie związane z gospodarowaniem wodami zgodnie z zasadą zrównoważonego rozwoju, a w szczególności kształtowanie i ochronę zasobów wodnych, korzystanie z wód oraz zarządzanie ich zasobami. Gospodarowanie wodami uwzględnia zasadę wspólnych interesów i jest realizowane przez współpracę administracji publicznej, użytkowników wód i przedstawicieli lokalnych społeczności, tak aby uzyskać maksymalne korzyści społeczne.

Przepisy tej ustawy odnoszące się do kwestii zarządzania ryzykiem powodziowym zostały wprowadzone w trakcie koniecznej implementacji dyrektywy powodziowej. Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim wymagała sporządzenia:



Rys. 1. Proces wprowadzania wymogów dyrektywy powodziowej

Źródło: Opracowanie własne na podstawie dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r.

Omawiana ustawa zawiera szereg definicji związanych z prawem wodnym. W termin ryzyka powodziowego wpisują się następujące definicje:

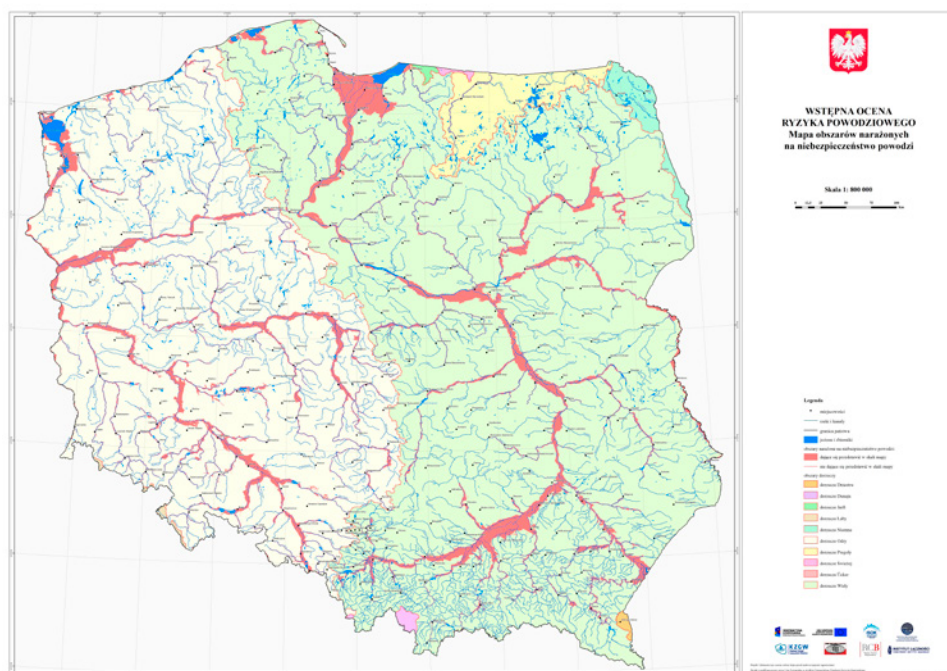
- **cele zarządzania ryzykiem powodziowym** – rozumiane jako ograniczenie potencjalnych negatywnych skutków powodzi dla życia i zdrowia ludzi, środowiska oraz dziedzictwa kulturowego, jak i działalności gospodarczej¹;
- **obszary narażone na niebezpieczeństwo powodzi** – rozumie się przez to określenie we wstępnej ocenie ryzyka powodziowego obszarów, na których istnieje znaczące ryzyko powodzi² lub jest prawdopodobne wystąpienie znaczącego ryzyka powodzi³;

¹ Tamże, art. 16 pkt 4.

² Znaczące ryzyko powodziowe – określane jest w wyniku oceny ryzyka powodziowego prowadzonej dla obszarów potencjalnie zagrożonych powodzią, pod kątem następujących kryteriów (wskaźników): (i) bezpośredni wpływ powodzi na życie i zdrowie ludzi, (ii) wpływ powodzi na obszary działalności gospodarczej wraz z infrastrukturą, (iii) skuteczność istniejących budowli przeciwpowodziowych, (iv) wpływ rozwoju zagospodarowania przestrzennego na wzrost ryzyka powodziowego. Źródło: Krajowy Zarząd Gospodarki Wodnej, *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, Warszawa 2013, s. 6.

³ Art. 16 pkt. 33 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2017 r., poz. 1566); Obszary, na których wystąpienie powodzi jest prawdopodobne – obszary z zasięgami powodzi prawdopodobnych – są to obszary wyznaczone głównie na podstawie studiów ochrony przeciwpowodziowej opracowanych przez

- **cele główne planów zarządzania ryzykiem** – cele odwołujące się do kolejnych faz zarządzania ryzykiem powodziowym: prewencji, ochrony, przygotowania, odbudowy i analiz⁴. Dodatkowym celem głównym jest rozwój instrumentów prawnych, finansowych i informacyjnych wspomagających wdrażanie działań. Proponowany jako piąty cel główny, ze względu na braki w zakresie wspomagania działań poprzez dostosowywanie odpowiednich instrumentów. Cele główne obowiązują we wszystkich obszarach dorzeczy oraz wszystkich regionach wodnych⁵;



Rys. 2. Wstępna ocena ryzyka powodziowego. Mapa obszarów narażonych na niebezpieczeństwo powodzi

Źródło: http://www.kzgw.gov.pl/files/file/Materialy_i_Informacje/WORP/Polska/1.jpg [dostęp: styczeń 2015].

- **wrażliwość** – odporność infrastruktury zlokalizowanej w terenach zagrożonych na podtopienia i zalanie, charakteryzuje stopień przygotowania zagrożonych

regionalne zarządy gospodarki wodnej. Ponieważ zostały wyznaczone na podstawie modelowania hydraulicznego dla przepływów o określonym prawdopodobieństwie wystąpienia, traktowane są jako powódzie mogące wystąpić w przyszłości, o których mowa w art. 167 ust. 2 pkt 3 ustawy – Prawo wodne oraz w art. 4.2d dyrektywy powodziowej. Źródło: Krajowy Zarząd Gospodarki Wodnej, *Metodyka...*, dz. cyt., s. 6.

⁴ Wprowadzenie faz zarządzania ryzykiem powodziowym można zinterpretować jako przyjęcie w pewnym zakresie struktury ramowej niezbędnej do celów realizacji tego procesu.

⁵ Krajowy Zarząd Gospodarki Wodnej, *Metodyka...*, dz. cyt., s. 8.

ludzi i obiektów do powodzi, np. zabezpieczenia indywidualnych obiektów infrastrukturalnych, stosowanie materiałów budowlanych odpornych na działanie wody i filtracji itp. Wrażliwością jest także zdolność reagowania społeczności na zagrożenie, np. korzystanie lub niekorzystanie z systemu ostrzegania⁶;

- **ryzyko powodzi** – to kombinacja prawdopodobieństwa wystąpienia powodzi i potencjalnych negatywnych skutków⁷ powodzi dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej⁸.

3.2. Proces wdrażania polityki zarządzania ryzykiem

Zgodnie z zapisami ustawy, ochrona przed powodzią leży w kompetencji zadań organów administracji rządowej i samorządowej na podległym terenie. Realizuje się ją przy wykorzystaniu map zagrożenia powodziowego⁹, map ryzyka powodziowego¹⁰, a także planów zarządzania ryzykiem powodziowym. Zgodnie z art. 167 przywołanej ustawy na początku dla obszarów dorzeczy przygotowuje się **wstępną ocenę ryzyka powodziowego** (rys. 2). „Opracowanie wstępnej oceny ryzyka powodziowego (WORP) ma na celu oszacowanie skali zagrożenia powodziowego dla obszarów dorzeczy oraz identyfikację znaczącego ryzyka powodziowego na tych obszarach. Informacje te posłużyły do wskazania odcinków rzek, dla których zostaną opracowane mapy zagrożenia powodziowego i mapy ryzyka powodziowego”¹¹. Do sporządzenia oceny konieczne było przyjęcie poniższego procesu¹²:

- zebranie i zestawienie materiałów do wykonania WORP,
- utworzenie wejściowej bazy danych WORP,
- zlokalizowanie znaczących powodzi (historycznych i prawdopodobnych),
- zlokalizowanie i zidentyfikowanie obszarów potencjalnie zagrożonych powodzią,
- wydzielenie obszarów narażonych na niebezpieczeństwo powodzi,
- utworzenie wynikowej bazy danych WORP,
- opracowanie map wstępnej oceny ryzyka powodziowego.

WORP stanowi jedynie materiał poglądowy, niewymagający danych o wysokiej dokładności, dlatego też do jego przygotowania wykorzystano dane powszechnie

⁶ Tamże.

⁷ Pod pojęciem skutków należy rozumieć konsekwencje, zgodnie z definicją normy ISO na s. 108.

⁸ Art. 16 pkt. 48 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2017 r., poz. 1566).

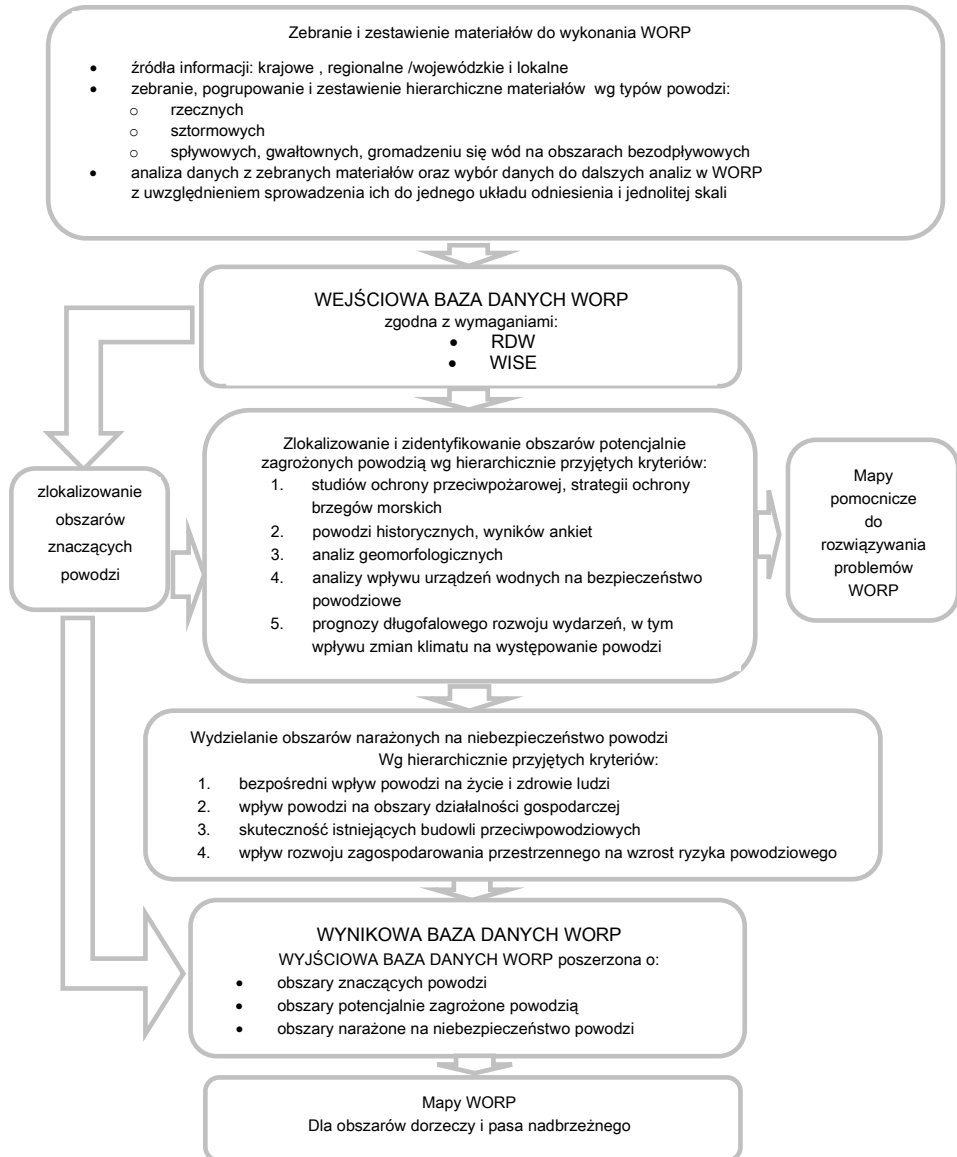
⁹ Mapy zagrożenia powodziowego – mapy przedstawiające obszary narażone na niebezpieczeństwo powodzi. Źródło: art. 6 ust. 3 dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim.

¹⁰ Mapy ryzyka powodziowego – mapy przedstawiające potencjalne negatywne skutki powodzi. Źródło: art. 6 ust. 5 dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim.

¹¹ Krajowy Zarząd Gospodarki Wodnej, *Raport z wykonania wstępnej oceny ryzyka powodziowego*, Warszawa 2011, s. 4.

¹² Tamże, s. 8.

dostępne. W trakcie tego etapu dokonano analizy ponad 250 rzek o łącznej długości ponad 15 tys. km. Na mapie kolorem czerwonym zaznaczono obszary narażone na niebezpieczeństwo powodzi. Wyłonienie powyższych procesów pozwoliło na przygotowanie algorytmu dla wstępnej oceny (patrz rys. 3).



Rys. 3. Algorytm opracowania wstępnej oceny ryzyka powodziowego
Źródło: Krajowy Zarząd Gospodarki Wodnej, *Raport z wykonania wstępnej oceny ryzyka powodziowego*, Warszawa 2011, s. 9.

Obszary dorzeczy definiuje się jako tereny, z których wody powierzchniowe spływają do określonej rzeki lub jej dopływów. W Polsce występują dorzecza Wisły, Odry oraz rzek na terytorium Polski będących częścią międzynarodowych dorzeczy¹³. I właśnie dla obszarów dorzeczy Państwowe Gospodarstwo Wodne Wody Polskie, zgodnie z art. 168¹⁴, opracowuje wstępną ocenę ryzyka powodziowego, która zawiera mapy obszarów dorzeczy¹⁵, opis powodzi historycznych i ocenę potencjalnych negatywnych skutków powodzi mogących wystąpić w przyszłości. Ponadto prognozuje się wpływ zmian klimatu na potencjalne występowanie powodzi oraz określa obszary narażone na niebezpieczeństwo ich wystąpienia. W opracowywaniu dokumentu w zakresie wstępnej oceny ryzyka powodziowego od strony morza, w tym morskich wód wewnętrznych, uczestniczy również minister właściwy do spraw gospodarki morskiej. Gotowy projekt wstępnej oceny ryzyka powodziowego przekazywany jest, zgodnie z obowiązującym porządkiem prawnym, do uzgodnienia w zakresie śródlądowych dróg wodnych ministrowi właściwemu do spraw żeglugi śródlądowej oraz do zaopiniowania właściwym wojewodom oraz marszałkom województw. W przypadku obszarów dorzeczy, których części znajdują się na terytorium innych państw członkowskich Unii Europejskiej, przed opracowaniem projektu dokonuje się wymiany niezbędnych informacji z właściwymi organami tych państw. Wstępną ocenę ryzyka powodziowego Wody Polskie przedkłada do zatwierdzenia ministrowi właściwemu do spraw gospodarki morskiej. Zatwierdzony dokument minister przekazuje dyrektorowi Rządowego Centrum Bezpieczeństwa. Omawiany dokument podlega przeglądowi co 6 lat, a także w razie potrzeby aktualizacji¹⁶.

Celem wstępnej oceny jest wskazanie obszarów potencjalnie narażonych na powódź, dla których prowadzone są dalsze prace związane z procesem zarządzania ryzykiem. Proces identyfikacji przedstawia rys. 4.

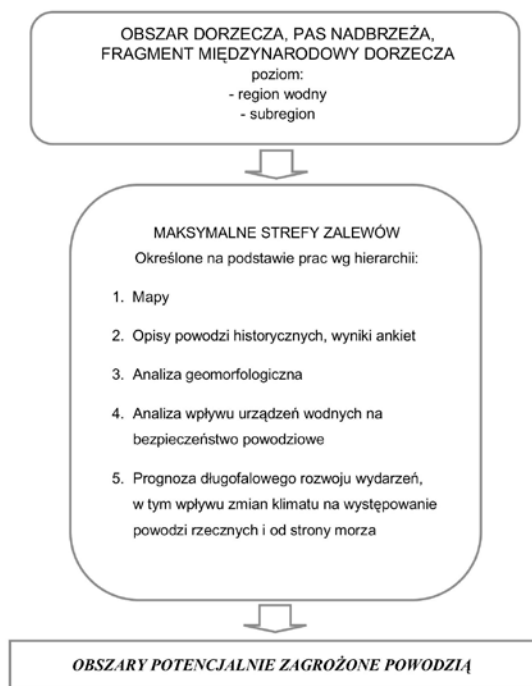
W przypadku obszarów narażonych na niebezpieczeństwo wystąpienia powodzi wymienionych we wstępnej ocenie ryzyka powodziowego konieczne jest sporządzenie mapy zagrożenia powodziowego (zob. rys. 5), zgodnie z art. 169 ustawy z dnia 20 lipca 2017 r. – Prawo wodne.

¹³ Art. 13 ust. 1 i 2 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2017 r., poz. 1566).

¹⁴ Zgodnie z art. 88c ustawy z dnia 18 lipca 2001 r. – Prawo wodne (Dz. U. 2001 nr 115 poz. 1229 z późn. zm.) za opracowanie wstępnej oceny ryzyka powodziowego do 31.12.2017 r. odpowiada prezes Krajowego Zarządu Gospodarki Wodnej.

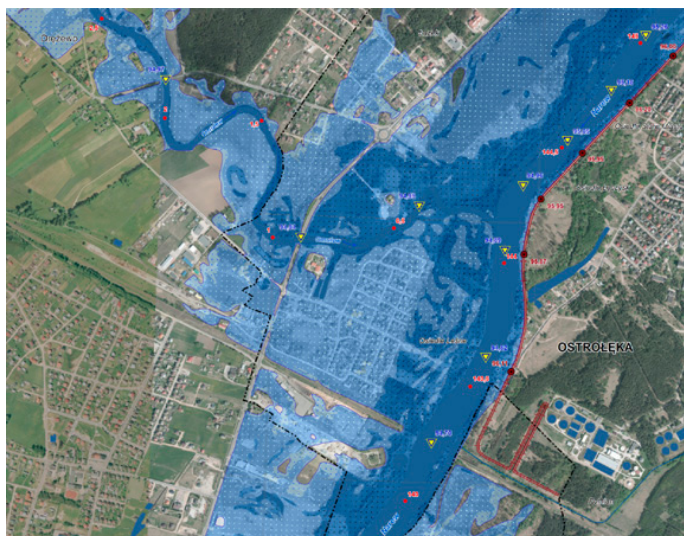
¹⁵ Mapy obszarów dorzeczy przedstawiają granice dorzeczy, granice zlewni, granice pasa nadbrzeżnego oraz topografię terenu wraz z jego zagospodarowaniem.

¹⁶ Art. 168 ust. 8–10 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2017 r., poz. 1566).



Rys. 4. Schemat blokowy lokalizacji i identyfikacji obszarów potencjalnie zagrożonych powodzią

Źródło: Krajowy Zarząd Gospodarki Wodnej, *Raport z wykonania...*, dz. cyt. s. 13.



Rys. 5. Fragment mapy zagrożenia powodziowego wraz z głębokością wody (Ostrołęka)

Źródło: <http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego> [dostęp: styczeń 2015].

Zamieszczone w mapie informacje dotyczą obszarów, na których prawdopodobieństwo wystąpienia powodzi jest niskie (raz na 500 lat), obszarów szczególnego zagrożenia powodzią, terenów narażonych na zalanie w razie przelania się wód przez koronę wału przeciwpowodziowego, a także jego zniszczenia lub uszkodzenia, zniszczenia lub uszkodzenia budowli piętrzących oraz budowli ochronnych pasa technicznego. Na omawianej mapie zamieszcza się ponadto zasięg powodzi, głębokość wody lub poziom zwierciadła wody, a w uzasadnionych przypadkach – prędkość przepływu wody lub jej natężenie¹⁷. Kolorem niebieskim zaznaczono tereny bezpośredniego zagrożenia powodzią, natomiast fioletowym zalania potencjalnego. Obszary te, zgodnie z art. 169 ustawy – Prawo wodne, uwzględnia się przy sporządzaniu planu zagospodarowania przestrzennego województwa, studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy, miejscowego planu zagospodarowania przestrzennego oraz decyzji o lokalizacji inwestycji celu publicznego oraz decyzji o warunkach zabudowy.

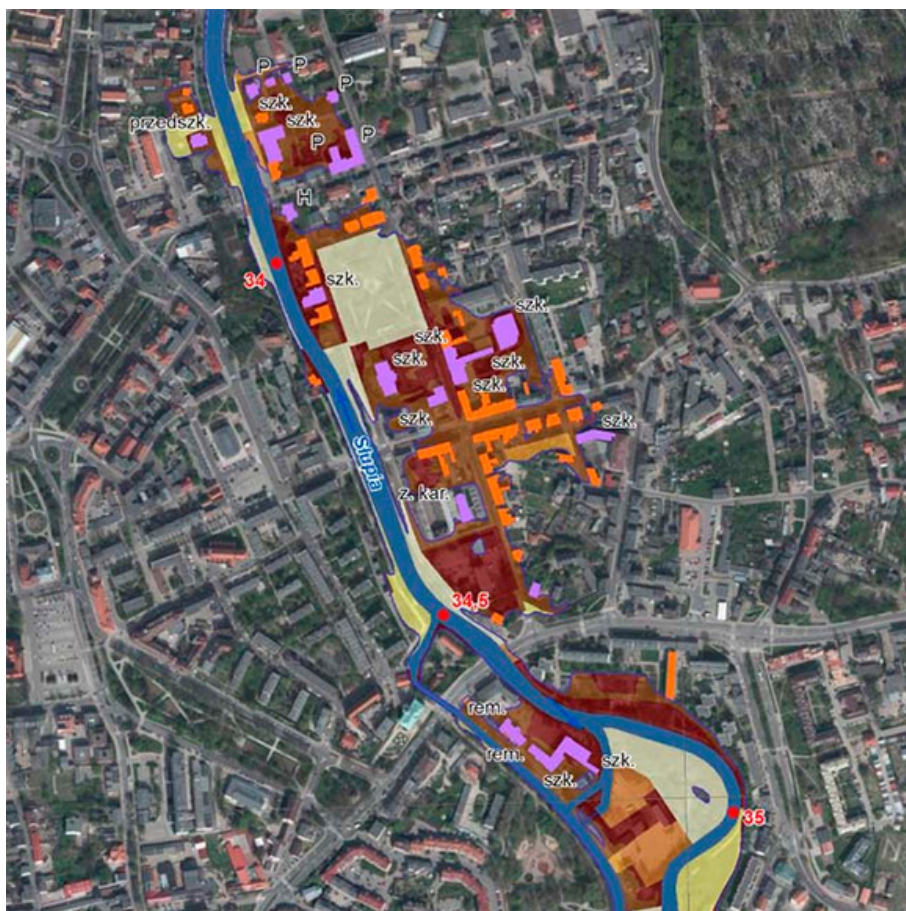
Dla obszarów szczególnie zagrożonych powodzią dodatkowo sporządza się **mapę ryzyka powodziowego**, z danymi zawierającymi m.in. szacunkową liczbę mieszkańców oraz rodzaje działalności gospodarczej¹⁸. Dane te gromadzi się przede wszystkim na potrzeby ewakuacji (rys. 6).

„Jako granicę terenów zurbanizowanych przyjęto granice działek usługowych, produkcyjnych i zabudowy mieszkaniowej oraz zasięg zabudowy dla zabudowy zagrodowej. Liczbę osób w tak zdelimitowanych jednostkach można uzyskać w podziale na: a) mieszkańców z gminnej ewidencji ludności, b) pracowników z REGON, c) użytkowników indywidualnie, w zależności od rodzaju usług (liczba łóżek w szpitalu, liczba miejsc w kinie, liczba miejsc parkingowych dla wielkopowierzchniowych obiektów handlowych itd.). W sposób uproszczony liczbę mieszkańców można oszacować: a) dla zabudowy jednorodzinnej, mnożąc liczbę budynków mieszkaniowych przez średnią wielkość rodziny w gminie, b) dla zabudowy wielorodzinnej, dzieląc powierzchnię całkowitą zabudowy przez średnią powierzchnię mieszkania przypadającą na jednego mieszkańca (średnia dla Polski 24m²/osobę)”¹⁹. Na mapie zaznacza się również budynki o znaczeniu społecznym: żłb. – żłobek, przedszk. – przedszkole, szk. – szkoła, P – policja, rem. – straż pożarna, SG – jednostka Straży Granicznej, szpit. – szpital, san. – sanatorium, d. op. – dom opieki społecznej, c. han. – centrum handlowe, H – hotel, d. wyp. – dom wypoczynkowy, d. wych. – dom wychowawczy oraz z. kar. – zakład karny.

¹⁷ Tamże, art. 169 ust. 3.

¹⁸ Tamże, art. 170 ust. 2.

¹⁹ T. Majda, P. Wałdykowski, J. Adamczyk, M. Grygoruk, *Typologia terenów narażonych na niebezpieczeństwo powodzi*, TUP, Warszawa 2012, s. 49.

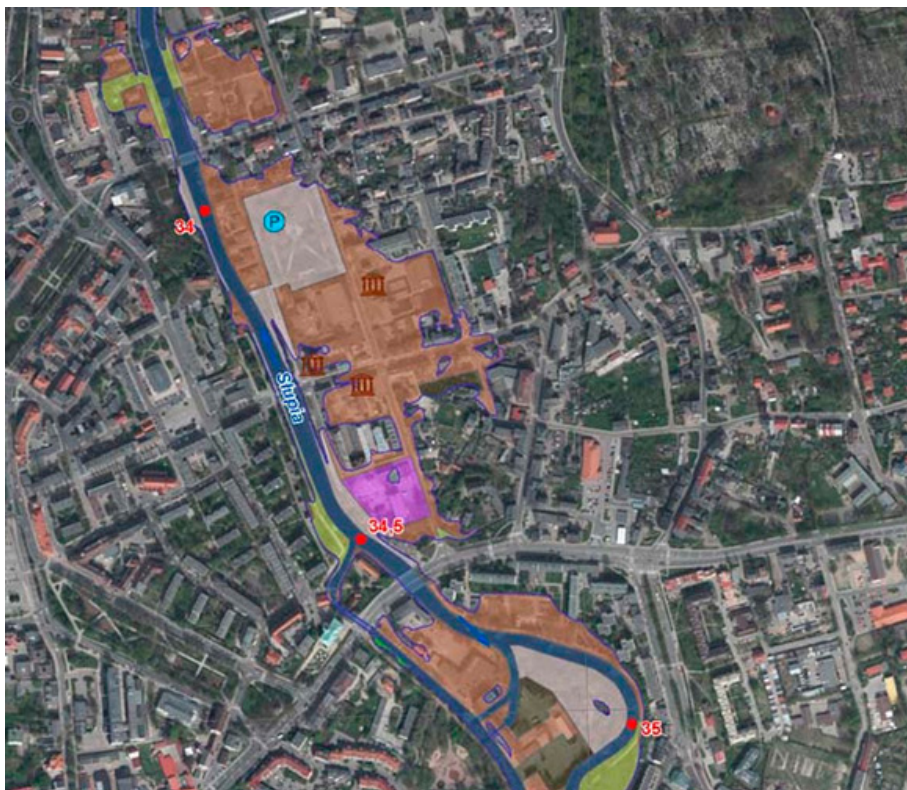


Rys. 6. Fragment mapy ryzyka powodziowego – negatywne konsekwencje dla ludności i wartość potencjalnych strat powodziowych

Źródło: <http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego> [dostęp: styczeń 2015].

Mapy ryzyka powodziowego prezentują także negatywne konsekwencje, jakie może mieć powódź dla środowiska, dziedzictwa kulturowego i działalności gospodarczej (rys. 7). Oznacza się na nich klasy użytkowania terenu (zabudowa mieszkaniowa, przemysłowa, las, grunty orne itp.), ujęcia wody (podziemnej, powierzchniowej, kąpieliska itp.), obszary i obiekty dziedzictwa kulturowego (zabytki, pomniki, skanseny, biblioteki), formy ochrony przyrody (parki narodowe, rezerваты, obszary Natura 2000) oraz potencjalne ogniska zanieczyszczeń (m.in. zakłady o dużym i zwiększonym ryzyku wystąpienia poważnej awarii, obiekty przemysłu: chemicznego, energetycznego, gospodarki odpadami, składowiska odpadów)²⁰.

²⁰ Art. 170 ust. 2 ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2017 r., poz. 1566).



Rys. 7. Fragment mapy ryzyka powodziowego – negatywne konsekwencje dla środowiska, dziedzictwa kulturowego i działalności gospodarczej

Źródło: <http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego> [dostęp: styczeń 2015].

Przedstawione powyżej mapy sporządzają Wody Polskie, natomiast część opracowania, w zakresie map od strony morza, w tym morskich wód wewnętrznych, zleca się do opracowania dyrektorom urzędów morskich. Gotowe mapy zagrożenia powodziowego i ryzyka powodziowego minister właściwy do spraw gospodarki wodnej przekazuje zgodnie z art. 171 ust. 4 Wodom Polskim, Głównemu Geodecie Kraju, Głównemu Inspektorowi Ochrony Środowiska, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz Komendantowi Głównemu Państwowej Straży Pożarnej. Opracowane mapy przekazywane są ponadto właściwym wojewodom, marszałkom, starostom, wójtom (burmistrzom, prezydentom miast) oraz komendantom wojewódzkim i powiatowym (miejskim) PSP, a także dyrektorom urzędów żeglugi śródlądowej, dyrektorom urzędów morskich, zarządcom infrastruktury kolejowej oraz zarządcom dróg publicznych. Mapy zagrożenia powodziowego oraz ryzyka powodziowego mogą być wykorzystywane na potrzeby zagospodarowania przestrzennego.

Wymienione w podrozdziale 3.2. dokumenty, zgodnie z procesem wskazanym we wstępie podrozdziału, zostały już przygotowane, wciąż trwa natomiast proces sporządzania planów zarządzania ryzykiem powodziowym. Wykonuje się go na podstawie map zagrożenia powodziowego oraz map ryzyka powodziowego. Plany te zawierają mapę obszaru dorzecza, mapy zagrożenia powodziowego oraz mapy ryzyka powodziowego wraz z opisem wniosków z analizy tych map, opis celów zarządzania ryzykiem powodziowym, a także katalog działań służących osiągnięciu celów zarządzania ryzykiem powodziowym, z uwzględnieniem ich priorytetu²¹. W przypadku planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy dokumenty te przygotowywane są przez Wody Polskie w uzgodnieniu z ministrem do spraw transportu w zakresie infrastruktury transportowej, z właściwymi wojewodami oraz po zasięgnięciu opinii marszałków województw, a w zakresie śródlądowych dróg wodnych z ministrem właściwym do spraw żeglugi śródlądowej. Minister właściwy do spraw gospodarki morskiej przygotowuje projekty planów zarządzania ryzykiem powodziowym od strony morza, w tym morskich wód wewnętrznych. Przedstawione plany podlegają przeglądowi w celu aktualizacji co 6 lat.

Metodyka zakłada, że strukturę planu powinny tworzyć następujące elementy:

- streszczenie w języku nietechnicznym,
- wprowadzenie – cele i zakres planu, podstawy prawne, relacje PZRP z innymi dokumentami,
- opis obszaru planowania – topografia, hydrografia, gleby, geologia, hydrologia, charakter zagrożenia powodziowego w zlewni, użytkowanie terenu,
- partnerzy procesu planowania i zasady udziału społecznego – analiza interesariuszy, zarządzanie procesem planowania, zasady udziału społecznego,
- podsumowanie wstępnej oceny ryzyka powodziowego,
- ocena zagrożenia powodziowego – wnioski z analiz map zagrożenia powodziowego, dodatkowe analizy, podsumowanie,
- ocena ryzyka powodziowego – wnioski z analiz map ryzyka powodziowego, dodatkowe analizy, podsumowanie,
- uwzględnienie wpływu zmian klimatu na ryzyko powodziowe,
- analiza obecnego systemu zarządzania ryzykiem powodziowym,
- cele zarządzania ryzykiem powodziowym – analiza problemów zarządzania ryzykiem powodziowym i wnioski, cele zarządzania ryzykiem powodziowym,
- podsumowanie działań i ich priorytety – opis metodyki budowy i oceny wariantów, strategia zarządzania ryzykiem powodziowym (opis wybranego rozwiązania, priorytety w realizacji działań, harmonogram, jednostki realizujące i źródła finansowania),
- opis zakresu i sposobu koordynacji z ramową dyrektywą wodną,

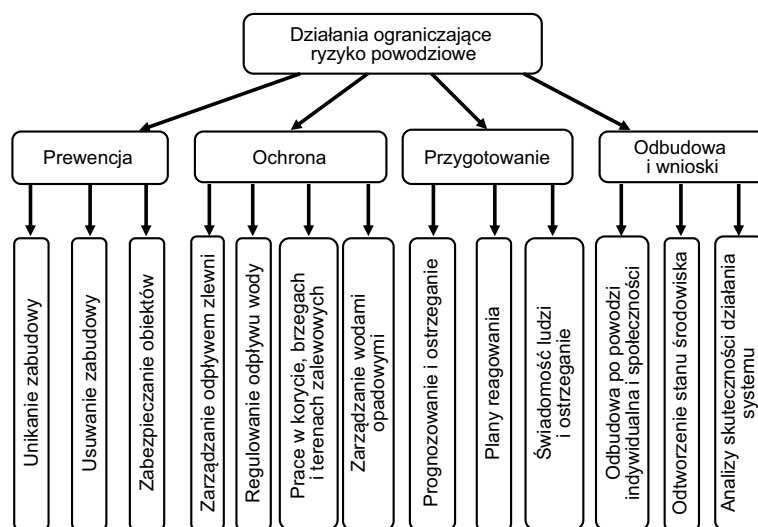
²¹ Tamże, art. 172 ust. 3.

- podsumowanie strategicznej oceny oddziaływania na środowisko,
- podsumowanie procesu konsultacji społecznych i informowania społeczeństwa – konsultacje społeczne, informowanie ogółu społeczeństwa,
- opis zakresu i sposobu współpracy międzynarodowej,
- sposób monitorowania postępów realizacji planu zarządzania ryzykiem powodziowym,
- literatura/źródła.

Plan powinien także zawierać załączniki:

- listę skrótów,
- słownik pojęć,
- listę interesariuszy,
- katalog celów,
- katalog działań,
- wstępną ocenę ryzyka powodziowego,
- mapy zagrożenia powodziowego,
- mapy ryzyka powodziowego,
- materiały dokumentujące proces konsultacji i udziału społecznego,
- program działań dla planu zarządzania ryzykiem powodziowym.

Plan jest elementem podprocesu „postępowanie z ryzykiem”, dlatego też powinien odwoływać się do działań ograniczających ryzyko powodziowe. Metodyka, jako narzędzia pozwalające na określenie katalogu planowanych działań, definiuje te działania następująco:



Rys. 9. Struktura działań ograniczających ryzyko powodziowe

Źródło: Krajowy Zarząd Gospodarki Wodnej, *Metodyka...*, dz. cyt., s. 40.

„Według tej klasyfikacji sporządzony został katalog działań podstawowych, czyli takich, które bezpośrednio wpływają na wielkość ryzyka powodziowego”²².

W związku z tym, że zarządzanie ryzykiem powodziowym nie dotyczy działalności prowadzonej przez konkretną organizację i jej otoczenie, a wynika z prawa europejskiego²³ oraz wewnętrznie stanowionego w poszczególnych krajach Unii Europejskiej, obligując szereg instytucji do podjęcia odpowiednich działań w tym zakresie, nie znalazły tu zastosowania wytyczne ani elementy normy ISO 31000. Odnosząc się do normy ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, dyrektywa powodziowa narzuca natomiast w ramach przygotowania planów zarządzania ryzykiem powodziowym jedynie przygotowanie analizy kosztów i korzyści z podjętych działań na rzecz osiągnięcia celów.

Analizując użyteczność zaprezentowanych w niniejszym rozdziale rozważań, należy zwrócić uwagę na ich szczególny charakter, determinowany przez branżowy i strategiczny wymiar rozwiązań. Wskazana metoda nie znajduje zastosowania w innych obszarach zarządzania ryzykiem właśnie dlatego, że została przygotowana dla jednego charakterystycznego zagrożenia. W związku z powyższym nie może być wykorzystana do pomiaru ryzyk innych zagrożeń. Dane będące wynikiem oceny ryzyka powodziowego należy jednak wziąć pod uwagę, badając np. ryzyko dla bezpieczeństwa narodowego.

²² Krajowy Zarząd Gospodarki Wodnej, *Metodyka...*, dz. cyt., s. 40.

²³ Komisja Europejska przygotowała w latach 2000–2007 w postaci projektu dyrektywy własną metodykę zarządzania ryzykiem powodziowym, nie odwołując się do zasad obowiązujących wówczas i dość w ograniczonym stopniu rozpowszechnionych norm.

4. ZARZĄDZANIE RYZYKIEM W KONTROLI ZARZĄDCZEJ

Kontrola zarządcza została wprowadzona w Polsce przez ustawę o finansach publicznych, jako wymóg harmonizacji prawa krajowego z prawem europejskim, a także przede wszystkim z potrzeby przyjęcia rozwiązań wzmacniających kontrolę nad wydatkami środków publicznych. Należy przy tym podkreślić, że wydatkowanie środków publicznych przez jednostki finansów publicznych ma bezpośredni związek z: misją, celami i zadaniami danej jednostki¹. Tym bardziej nie powinna dziwić tak szeroka kwalifikacja kontroli zarządczej w rozdziale 6 działu I ustawy². W rozdziale tym zdefiniowano kontrolę zarządczą oraz sprecyzowano cele, które ma ona spełniać. A należą do nich:

- 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,
- **zarządzanie ryzykiem**³.

Załącznik do komunikatu nr 6 Ministra Finansów z dnia 18 grudnia 2012 r. tylko potwierdza powyższy sposób postępowania, rozszerzając zapisy ustawy: „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”⁴. Przywołana definicja

¹ D. Wróblewski, B. Połeć, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, D. Majchrzak (red.), AON, Warszawa 2014, s. 197.

² D. Wróblewski (red.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 95.

³ Art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870 z późn. zm.).

⁴ Komunikat nr 6 Ministra Finansów z dnia 18 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (Dz. Urz. MF poz. 56).

nie jest niczym innym, jak rozwinięciem zarządzania ryzykiem na potrzeby kontroli zarządczej. Proces ten zgodnie z normą ISO 31000 określono właśnie jako „skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka, które stanowi wpływ niepewności na cele”⁵.

Zarządzanie ryzykiem jako element kontroli zarządczej istotnie przyczynia się do realizacji wyznaczonych celów jednostki. Obowiązek ten stanowi jednak świadomy kompromis pomiędzy ponoszonymi kosztami zabezpieczenia jednostki przed potencjalnym ryzykiem a tolerowaniem poziomu ryzyka, jaki kierownicy są w stanie zaakceptować⁶. Co istotne, z punktu widzenia niniejszej publikacji oraz przedstawianych w rozdziale rozważań, podmiotami odpowiedzialnymi za sprawne wdrożenie i funkcjonowanie kontroli zarządczej są: wójt, burmistrz, prezydent miasta, przewodniczący zarządu jednostki samorządu terytorialnego⁷, jak również ministrowie i kierownicy jednostek i urzędów centralnych – organy wiodące bądź pełniące znaczące funkcje w systemie zarządzania kryzysowego. Ponadto osoby te jako organizatorzy kontroli zarządczej w swoich jednostkach, przekazują w tym zakresie uprawnienia do swoich pracowników. Należy więc domniemywać, że w jednostkach tych istnieją kompetencje w zakresie zarządzania ryzykiem, które są scedowane na pracowników⁸, ponieważ dokonują oni identyfikacji i analizy ryzyka⁹, podejmują zaplanowane działania względem ryzyka oraz wdrażają do stosowania mechanizmy kontroli ryzyka.

W rozdziale scharakteryzowano metodyki oceny ryzyka wdrożone przez wybrane podmioty centralne oraz jednostki administracyjne na szczeblu województwa, powiatu i gminy. Wskazano również potrzebę zmian i udoskonaleń w prowadzonych procesach zarządzania ryzykiem.

4.1. Zarządzanie ryzykiem na szczeblu centralnym

Głównym celem niniejszego rozdziału jest analiza metodyk na podstawie dokumentów prawa resortowego w zakresie zarządzania ryzykiem. Według podręcznika „Zarządzanie ryzykiem w sektorze publicznym”, sporządzonego w ramach środków projektu UE *Transition Facility*, „zarządzanie ryzykiem to logiczna i systematyczna metoda ustanawiania kontekstu¹⁰, identyfikacji¹¹, analizy¹², oceny¹³, działania,

⁵ PN-EN ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne, s. 17.

⁶ Komunikat nr 6 Ministra Finansów z dnia 18 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem (Dz. Urz. MF poz. 56).

⁷ Art. 69 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870 z późn. zm.).

⁸ Patrz szerzej: D. Wróblewski (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego*, CNBOP-PIB, Józefów 2014, s. 25–29.

⁹ W jednostkach opisanych w niniejszym rozdziale pracownicy prowadzą nawet pełny proces oceny ryzyka oraz w ograniczonym zakresie inne etapy procesu zarządzania ryzykiem.

¹⁰ Patrz: definicja na s. 109.

¹¹ Patrz: definicja na s. 106.

¹² Patrz: definicja na s. 109.

¹³ Patrz: definicja na s. 114 (ewaluacja ryzyka).

nadzoru oraz informowania o ryzyku w sposób, który umożliwi organizacji minimalizację strat i maksymalizację możliwości¹⁴. W praktyce przekłada się to na:

- możliwie najszybszą identyfikację ryzyka związanego z działaniem operacyjnym, ocenę stopnia wpływu ryzyka na wyniki lub cele organizacji oraz zastosowanie odpowiednich środków kontroli ryzyka;
- upewnienie się, że środki kontroli stosowane przez organizację do zarządzania ryzykiem będą skuteczne¹⁵.

Mimo że na świecie tematyka związana z zarządzaniem ryzykiem jest bardzo dobrze rozwinięta, w Polsce zagadnienie to znajduje się dopiero w fazie wprowadzania. Przepis nakazujący realizowanie zadań dotyczących zarządzania ryzykiem wprowadzony został w ustawie o finansach publicznych z dnia 27 sierpnia 2009 r.¹⁶ Przepisy te nie precyzują, w jaki sposób ocena ryzyka¹⁷ powinna być prowadzona ani jaki powinien być jej zakres. Dlatego też resorty wprowadziły tę praktykę na własnych zasadach.

Spośród przeanalizowanych zarządzeń wprowadzających zarządzanie ryzykiem w ministerstwach i urzędach centralnych najdokładniej przygotowane zostały dokumenty w Ministerstwie Spraw Wewnętrznych i Administracji, Ministerstwie Spraw Zagranicznych oraz w Wyższym Urzędzie Górniczym i to właśnie na nich w głównym stopniu oparto analizę metodyk oceny ryzyka.

Zasadniczym celem badań jest analiza zarządzeń wraz z dokumentami uzupełniającymi w wyżej wymienionych jednostkach: przykładowym urzędzie centralnym (WUG) i ministerstwach w zakresie wprowadzenia zasad oraz kontroli zarządzania ryzykiem w działach administracji rządowej.

Analizie poddano:

- zarządzenie nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65);
- zarządzenie nr 27 Ministra Spraw Zagranicznych z dnia 27 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych;
- zarządzenie nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

¹⁴ Norma AS/NZS 4360:1999 Risk Management.

¹⁵ Ministerstwo Finansów, *Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce*, wyd. Bentley Dennison, Warszawa 2007, s. 8.

¹⁶ Rozdział 6 ustawy o finansach publicznych z dnia 27 sierpnia 2009 r. (Dz. U. z 2016 r. poz. 1870 z późn. zm.) – Kontrola zarządcza oraz koordynacja kontroli zarządczej w jednostkach sektora finansów publicznych.

¹⁷ Patrz: definicja na s. 107.

Celem zarządzania ryzykiem w ministerstwach jest zwiększenie prawdopodobieństwa realizacji założonych celów i zadań (w tym poprawa jakości ich realizacji), zwiększenie efektywności wykorzystania istniejących zasobów oraz podniesienie świadomości podejmowanych decyzji i związanego z tym ryzyka. Wyższy Urząd Górniczy ze względu na specyfikę swojego działania ma zbliżone, nieznacznie różniące się cele. Należą do nich: osiąganie celów strategicznych, poprawa jakości zarządzania na wszystkich poziomach kierowania oraz doskonalenie procesów pracy poprzez optymalne wykorzystanie posiadanych zasobów¹⁸.

Odpowiedzialność za prawidłowe funkcjonowanie zarządzania ryzykiem w podanych analizie jednostkach ponosi najwyższe kierownictwo. We wszystkich powołano jednak właściciela ryzyka¹⁹, który odpowiada na danym poziomie za monitorowanie ryzyka²⁰. Ponownie osobliwym przypadkiem w całej grupie jednostek jest WUG, w którym dodatkowo powołano funkcję decydenta ryzyka, w postaci osoby podejmującej ostateczną decyzję, uwzględniającą dane zdarzenie jako ryzyko oraz przeprowadzenie dla niego oceny i postępowania z ryzykiem²¹. Szerszy zakres odpowiedzialności posiadają właściciele ryzyka w MSWiA oraz MSZ. Odpowiadają oni praktycznie za cały proces zarządzania ryzykiem w resorcie, począwszy od identyfikacji ryzyka po przygotowanie planów postępowania z ryzykiem włącznie, ale za wyjątkiem prowadzenia rejestru ryzyka.

W MSZ powołano został ponadto Komitet ds. Zarządzania Ryzykiem, w skład którego wchodzi:

- 1) przewodniczący komitetu – dyrektor komórki organizacyjnej właściwej w sprawach obsługi dyrektora generalnego,
- 2) pełnomocnik ministra spraw zagranicznych do spraw reformy kontroli wewnętrznej, przeciwdziałania nadużyciom i procedur antykorupcyjnych,
- 3) dyrektorzy albo zastępcy dyrektorów, komórki organizacyjnej właściwej w przedmiotowych sprawach.

Do zadań Komitetu należy dokonywanie analizy i akceptacji wykazu ryzyk²² w zakresie zgodności z zasadami wynikającymi z przepisów zarządzenia, adekwatności działań zapobiegawczych do zidentyfikowanych ryzyk i zadań realizowanych przez właścicieli ryzyka, adekwatności i kompletności rejestru ryzyk z najważniejszymi celami i zadaniami ministra spraw zagranicznych oraz przypisania właścicieli

¹⁸ § 1 ust. 3 zarządzenia nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65).

¹⁹ Patrz: definicja na s. 109.

²⁰ Patrz: definicja na s. 113.

²¹ Patrz: definicja na s. 106; § 2 zarządzenia nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65).

²² Należy rozumieć jako rejestr ryzyk zgodnie z normą ISO 31000.

ryzyka do poszczególnych ryzyk. Komitet dokonuje także przeglądu monitoringu z realizacji działań zapobiegawczych, inicjuje prace nad rejestrem ryzyk na rok kolejny, przygotowuje informacje na temat procesu zarządzania ryzykiem w ministerstwie i placówkach zagranicznych²³.

Dyrektor generalny, na wniosek przewodniczącego komitetu, powołuje w drodze decyzji skład osobowy Komitetu spośród pracowników komórek organizacyjnych ministerstwa²⁴, a właścicielem ryzyka, który odpowiada za zarządzanie ryzykiem, jest kierujący komórką organizacyjną lub kierownik placówki zagranicznej.

Każdy pracownik komórki organizacyjnej lub placówki zagranicznej ma obowiązek zgłaszać ryzyka, które mogą negatywnie wpłynąć na realizację celów, zadań bądź wizerunek ministerstwa lub placówek zagranicznych. W przypadku zgłaszania przez kierowników komórek organizacyjnych zmian w rejestrze ryzyk po akceptacji Komitetu ryzyka podlegają procedurze określonej w zarządzeniu²⁵.

W zidentyfikowanych zarządzeniach, wynikających z obowiązku uregulowania w jednostkach zasad prowadzenia kontroli zarządczej, nigdzie nie odnaleziono etapu procesu zarządzania ryzykiem „ustalenie kontekstu”, który inicjuje ten proces zgodnie z normą ISO 31000. Można jednak domniemywać, że jest on realizowany w ramach zadań wynikających z przygotowywania innej dokumentacji związanej z funkcjonowaniem jednostek, np. planów realizacji celów. Wyodrębnione są natomiast etapy identyfikacji, analizy, ewaluacji i postępowania z ryzykiem oraz dokonywania monitorowania i przeglądu²⁶. Zostały one zawarte w trzech opracowanych zarządzeniach (MSWiA, MSZ i WUG) dotyczących zarządzania ryzykiem bądź są przez te podmioty wybiórczo realizowane.

Identyfikacja ryzyka

W zarządzaniu ryzykiem nie została opracowana jedna, uniwersalna metoda identyfikacji ryzyka. Każda organizacja powinna opracować własną metodę, biorąc pod uwagę własne doświadczenie, wielkość i charakter organizacji. Wobec tego najczęściej korzysta się z kombinacji kilku metod (kwestionariuszy i burzy mózgów).

W MSZ brakuje szczegółowo opisanej procedury identyfikacji ryzyka. W zarządzeniu wskazano natomiast, co należy brać pod uwagę podczas tego procesu:

- ryzyka związane ze zmianami w ministerstwie lub w jego otoczeniu,

²³ § 5 ust. 1 zarządzenia nr 27 Ministra Spraw Zagranicznych z dnia 27 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych.

²⁴ Tamże, § 6.

²⁵ Tamże, § 17.

²⁶ Patrz: definicja na s. 113.

- ryzyka związane z obowiązkiem zapewnienia efektywnego i skutecznego nadzoru nad jednostkami podległymi ministrowi, w szczególności placówkami zagranicznymi,
- zagrożenia zidentyfikowane w dokumentach planistycznych i sprawozdawczych komórek organizacyjnych i placówek zagranicznych,
- ustalenia audytu, kontroli wewnętrznych i zewnętrznych w ministerstwie,
- ryzyka zasygnalizowane przez Komitet Audytu (...),
- wyniki samooceny kontroli zarządczej przeprowadzanej na potrzeby oświadczenia ministra o stanie kontroli zarządczej za dany rok²⁷.

W MSWiA wyniki przeprowadzonej identyfikacji ryzyka odnotowuje się w zbiorczym arkuszu całej analizy ryzyka (załącznik nr 3 do zarządzenia) w odniesieniu do konkretnego celu i zadania jednostki.

Tabela 1. Arkusz analizy ryzyka

Cel	Zadanie	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka (7)	Postępowanie z ryzykiem (8)
		zdarzenie (1)	następstwo ²⁸ (2) (N)	prawdopodobieństwo (3) (P)	ocen* (N) (4)	ocena** (P) (5)	poziom ryzyka = N x P (6)		

* W kolumnie wprowadza się punktową ocenę dla konsekwencji.

** W kolumnie wprowadza się punktową ocenę dla prawdopodobieństwa.

Źródło: Załącznik nr 3 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

W WUG identyfikacja ryzyka realizowana jest w kontekście przyjętych celów i zadań na podstawie: aktualnego planu strategicznego, zadań operacyjnych jednostki na dany rok i planu pracy – w zależności od poziomu planowania²⁸.

²⁷ § 10 zarządzenia nr 27 Ministra Spraw Zagranicznych z dnia 27 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych.

²⁸ § 10 zarządzenia nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65).

Analiza ryzyka

Konieczność analizy ryzyka wynika z potrzeby lepszego zrozumienia charakteru zidentyfikowanego ryzyka, na które narażona jest organizacja. Aby identyfikacja ryzyka przyniosła odpowiednie rezultaty i umożliwiła określenie przyszłej metody zarządzania nim, należy określić przyczynę każdego zidentyfikowanego ryzyka oraz jego późniejsze oddziaływanie. W tym przypadku wykorzystuje się matryce prawdopodobieństwa oraz matryce oddziaływania. W pierwszej kolejności szereguje się prawdopodobieństwa wystąpienia zagrożenia, a następnie każdemu zagrożeniu przypisuje się odpowiednią wartość. W WUG matryca składa się z czterech poziomów prawdopodobieństwa i czterech poziomów wpływu²⁹, natomiast w MSZ prawdopodobieństwo oraz wpływ składają z pięciu poziomów. Przy ocenie wpływu brane są pod uwagę zarówno skutki materialne, jak i niematerialne. Poziom ryzyka³⁰ mierzy się, mnożąc wartości prawdopodobieństwa wystąpienia zdarzenia oraz jego ewentualnego skutku³¹.

Tabela 2. Matryca określania istotności ryzyka

Prawdopodobieństwo	Wpływ			
	bardzo mały (1)	mały (2)	duży (3)	bardzo duży (4)
nikłe prawdopodobieństwo (1)	2	3	4	5
raczej nie wystąpi (2)	3	4	5	6
raczej wystąpi (3)	4	5	6	7
prawie pewne	5	6	7	8

Źródło: Załącznik nr 4 do zarządzenia nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65).

W MSWiA wsparciem dla urzędnika w merytorycznym uzupełnieniu arkusza analizy ryzyka (przedstawionego w tabeli 1) jest zestaw pomocniczych tabel, opisujących wartości: następstw, prawdopodobieństwa, poziomu ryzyka, czyli wielkości ryzyka (również ewaluacji i postępowania z ryzykiem, co zostało opisane w dalszej części podrozdziału) wraz ze wskazaniem sposobu liczenia wartości.

²⁹ Rozumianego jako określenie konsekwencji dla realizowanych celów i zadań.

³⁰ Patrz: definicja na s. 115.

³¹ § 11 zarządzenia nr 27 Ministra Spraw Zagranicznych z dnia 27 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych.

§ 11 ust. 5 zarządzenia nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65).

Arkusze analizy ryzyka określa³²:

1. Zdarzenie – wystąpienie lub zmiana konkretnego zestawu okoliczności.
2. Następstwo – konsekwencje, rezultat zdarzenia mający wpływ na cele.

Oceniając prawdopodobieństwo należy przeanalizować:

- skalę potencjalnych strat finansowych, zobowiązań finansowych;
- wartość majątku narażonego na utratę bądź uszkodzenie;
- odpowiedzialność prawną wynikającą z niezgodności z przepisami prawa, z postanowieniami umów, istnienia (bądź nie) procedur regulujących dany proces;
- skalę zakłóceń organizacyjnych - wpływ na możliwość realizacji celów i zadań;
- wpływ na wizerunek;
- stosowane (bądź nie) mechanizmy kontroli oraz ich skuteczność.

Następstwo powinno zostać ocenione w skali od 1 do 5 (tabela 3)³³.

Tabela 3. Ocena następstw ryzyka

Poziom	Ocena (N)	Opis
1	nieznaczne	Zdarzenie objęte ryzykiem powoduje nieznaczną stratę finansową lub krótkotrwałe zakłócenia lub opóźnienie w wykonywaniu zadań. Nie wpływa na wizerunek. Skutki zdarzenia można łatwo usunąć.
2	małe	Zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, niewielkie zakłócenia lub opóźnienie w wykonywaniu zadań. Nie wpływa na reputację. Skutki zdarzenia można łatwo usunąć.
3	średnie	Zdarzenie objęte ryzykiem powoduje znaczną stratę posiadanych zasobów, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, reputację. Z wystąpieniem zdarzenia objętego ryzykiem może się wiązać trudny proces przywracania stanu poprzedniego.
4	poważne	Zdarzenie objęte ryzykiem powoduje brak realizacji kluczowego zadania lub osiągnięcia konkretnego założonego celu, poważną stratę finansową i reputacji, ciężki uszczerbek na zdrowiu osób. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się długotrwały i trudny proces przywracania stanu poprzedniego.

³² Załącznik nr 3 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

³³ Tamże.

Poziom	Ocena (N)	Opis
5	katastrofalne	Zdarzenie objęte ryzykiem powoduje brak realizacji kluczowych zadań albo osiągnięcia założonych celów - poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa albo na reputacji, utratę życia osób. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się długotrwały i trudny proces przywracania stanu poprzedniego.

Źródło: Załącznik nr 3 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

1. Prawdopodobieństwo – możliwość, szansa wystąpienia zdarzenia.

Oceniając prawdopodobieństwo należy przeanalizować:

- dotychczasowe doświadczenia - częstość występowania danego zdarzenia,
- liczbę i intensywność działań podejmowanych w ramach procesu,
- liczbę komórek organizacyjnych i innych podmiotów zaangażowanych w realizację zadań w danym obszarze - potrzebę współdziałania, współpracy przy przepływie informacji,
- zmiany technologiczne, organizacyjne, kadrowe w danym obszarze (ich częstość, zakres, istotność), wchodzące zmiany przepisów prawnych,
- poziom uregulowania prawnego danego obszaru regulacjami o różnym charakterze³⁴.

Prawdopodobieństwo powinno zostać ocenione w skali od 1 do 5 (tabela 4).

Tabela 4. Ocena prawdopodobieństwa ryzyka

Poziom	Ocena (P)	Opis
1	Znikome	Zdarzenie objęte ryzykiem może wystąpić jedynie w wyjątkowych okolicznościach.
2	Mało prawdopodobne	Istnieje niewielkie prawdopodobieństwo wystąpienia zdarzenia objętego ryzykiem.
3	Prawdopodobne	Zdarzenie objęte ryzykiem może wystąpić w określonych przypadkach.
4	Bardzo prawdopodobne	Wystąpienie zdarzenia objętego ryzykiem jest bardzo prawdopodobne.
5	Prawie pewne	Oczekuje się, że zdarzenie objęte ryzykiem wystąpi.

Źródło: Tamże.

³⁴ Tamże.

Poziom ryzyka – wielkość ryzyka lub kombinacji ryzyk. Poziom ryzyka wyrażony jest w postaci kombinacji następstw oraz ich prawdopodobieństwa.

Poziom ryzyka to iloczyn oceny następstw (N) i prawdopodobieństwa (P)³⁵ (tabela 5).

Tabela 5. Poziom ryzyka

Następstwo (N) Prawdopodobieństwo (P)	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Źródło: Tamże.

1. Ewaluacja ryzyka (istotność ryzyka – wg załącznika ministerstwa).
2. Postępowanie z ryzykiem.

Ewaluacja ryzyka

Punktowa ocena ryzyka umożliwia uporządkowanie rodzajów ryzyka według ich wagi lub kryteriów matrycy punktowej oceny ryzyka. Dla różnych wartości iloczynu prawdopodobieństwa i wpływu określa się odpowiednie reakcje. Ryzyka o dużym prawdopodobieństwie wystąpienia i dużym oddziaływaniu (wysokie) wymagają pilnej uwagi organizacji. Ryzyka o małym prawdopodobieństwie i dużym oddziaływaniu oraz małym oddziaływaniu i dużym prawdopodobieństwie wystąpienia (średnie, znajdujące się w środku matrycy oceny ryzyka) należy omawiać i monitorować. W pewnych wypadkach organizacja może podjąć dalsze działania. Ryzyka o małym oddziaływaniu i małym prawdopodobieństwie (niskie) stanowią najmniejsze zagrożenie dla organizacji. O tym, do jakiej kategorii należy zaliczyć dane ryzyko Ministerstwo Spraw Zagranicznych oraz Wyższy Urząd Górniczy decydują we własnym zakresie, według sporządzonych analiz ryzyka³⁶.

Rezultatem sporządzenia hierarchizacji³⁷ jest rejestr ryzyk, który był brany pod uwagę podczas aktualizacji czy też tworzenia nowych planów. Obecnie jest

³⁵ Tamże.

³⁶ § 12 zarządzenia nr 27 Ministra Spraw Zagranicznych z dnia 27 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych.

§ 11 ust. 5 zarządzenia nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65).

³⁷ Patrz: definicja na s. 154.

on tworzony również niezależnie dla planów: strategicznych, operacyjnych i planów pracy.

Analogiczne podejście przyjęto w MSWiA. Kryteria ustalone w tej jednostce prezentuje poniższa tabela.

Tabela 6. Ewaluacja ryzyka

Kryteria	
Poziom	Ryzyko
1–5	małe
6–9	średnie
10–16 oraz gdzie P = 1, N = 5	duże
20–25	bardzo duże

Źródło: Załącznik nr 3 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

Postępowanie z ryzykiem

Po dokonanej ocenie ryzyka organizacja musi rozważyć wszystkie możliwe działania służące kontroli tego ryzyka. W MSZ stosuje się następujące sposoby postępowania z ryzykiem: tolerowanie ryzyka, transfer ryzyka, przeciwdziałanie oraz przesunięcie w czasie. Ryzyko jest akceptowalne jedynie w przypadku oszacowania niskiego poziomu. Dla Wyższego Urzędu Górniczego stosuje się działania polegające na: eliminacji, redukcji, wdrożeniu planu rezerwowego, przeniesieniu oraz akceptacji ryzyka.

MSWiA w zakresie postępowania z ryzykiem przyjmuje analogiczne podejście, jak w pozostałych jednostkach, stosując jednak własne kryteria, które zostały przedstawione w poniższej tabeli.

Tabela 7. Postępowanie z ryzykiem

Poziom	Ryzyko	Postępowanie z ryzykiem według kolejności rozważanych do podjęcia działań
1–5	małe	1. tolerowanie
6–9	średnie	1. tolerowanie 2. zapobieganie
10–16 (gdzie P = 1, N = 5)	duże	1. zapobieganie 2. przeniesienie 3. tolerowanie (wraz z pisemnym uzasadnieniem) 4. unikanie

Poziom	Ryzyko	Postępowanie z ryzykiem według kolejności rozważanych do podjęcia działań
20–25	bardzo duże	1. unikanie 2. przeniesienie 3. zapobieganie 4. tolerowanie (wraz z pisemnym uzasadnieniem)

Źródło: Załącznik nr 3 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

Decyzję dotyczącą postępowania z ryzykiem podejmuje właściciel ryzyka. Właściciel ryzyka monitoruje i nadzoruje realizację planu postępowania z ryzykiem, a w przypadku modyfikacji postępowania z ryzykiem podejmuje odpowiednie działania zapobiegawcze. Plan postępowania z ryzykiem sporządza się zgodnie ze wzorem określonym w załączniku nr 4 do zarządzenia³⁸.

Tabela 8. Plan postępowania z ryzykiem

Cel	Zadanie	Zdanie	Poziom ryzyka	Postępowania z ryzykiem	Działania	Terminy	Odpowiedzialni	Informacje o realizacji

Źródło: Załącznik nr 4 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

Właściciel ryzyka monitoruje ryzyko i o wszelkich nowych zdarzeniach, zmianach prawdopodobieństwa i możliwych następstwach informuje koordynatora celu, który odnotowuje zmiany w rejestrze ryzyk. Wzór rejestru ryzyk stanowi załącznik nr 5 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r.³⁹ Koordynator celu przekazuje ocenę ryzyka i plan postępowania z ryzykiem do biura ministra, a w razie zaistnienia ryzyka (które zagraża realizacji celów określonych w planie działalności ministra) informacja jest przekazywana także do nadzorującego członka kierownictwa ministerstwa,

³⁸ § 13 zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

³⁹ Tamże, § 14.

z jednoczesną informacją o podjętych działaniach mających ograniczyć skutki zmaterializowania się ryzyka⁴⁰.

Tabela 9. Rejestr ryzyk

Cel	Zadanie	Zdarzenie (należy wskazać wszystkie zidentyfikowane zdarzenia)	Informacje o zmaterializowaniu się ryzyka i podjętych działaniach

Źródło: Załącznik nr 5 do zarządzenia nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

Monitorowanie i przegląd

W zarządzaniu ryzykiem bardzo ważnym elementem jest monitoring, który powinien obejmować:

- dokonanie przeglądu w celu określenia, czy ryzyko uległo zmianie,
- sprawdzenie, czy punktowa ocena ryzyka jest wciąż odpowiednia,
- zapewnienie skuteczności dotychczasowych mechanizmów kontrolnych,
- weryfikację czy działania zapobiegawcze są realizowane.

W przypadku resortu MSZ i WUG monitoring oraz raportowanie prowadzone są regularnie. W Wyższym Urzędzie Górniczym dokonuje się przeglądu planów dwa razy do roku, natomiast w Ministerstwie Spraw Zagranicznych do 31 marca każdego roku⁴¹.

W resorcie spraw wewnętrznych corocznie kierownicy komórek organizacyjnych oraz kierownicy jednostek składają do nadzorującego ich członka kierownictwa ministerstwa oświadczenie częściowe o stanie kontroli zarządczej w swoich działach, który następnie przedkłada zbiorcze oświadczenie do zatwierdzenia ministra⁴².

W przypadku analizowanych jednostek szczebla centralnego dokumenty dotyczące oceny ryzyka zostały częściowo oparte na strukturze ramowej zaproponowanej w normie ISO 31000 bądź są z nią tożsame. Ponieważ norma ta zawiera ramy,

⁴⁰ Tamże, § 15.

⁴¹ § 16 i § 19 zarządzenia nr 27 Ministra Spraw Zagranicznych z dnia 27 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych.

§ 19 i § 20 zarządzenia nr 13 Prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2015 r. poz. 65).

⁴² Tamże, § 16.

procesy i zasady dotyczące procesu oceny ryzyka mające pomóc w ujednoczeniu procesów zarządzania ryzykiem, zarówno MSWiA, MSZ, jak i WUG mogły właśnie na niej oprzeć swoje systemy zarządzania ryzykiem.

Pierwszym charakterystycznym elementem normy ISO 31000 wykorzystanym w systemach zarządzania ryzykiem jest struktura ramowa. Zawiera ona pięć niezbędnych atrybutów opisanych w części pierwszej, została skutecznie zaimplementowana do tych jednostek. Zarówno w MSWiA, MSZ, jak i WUG wyżej wymienione atrybuty są opisane szczegółowo w kontekście działalności resortów.

Kolejnym elementem normy ISO 31000, który pojawia się w dokumentach dotyczących zarządzania ryzykiem w resortach, jest zbliżony proces zarządzania ryzykiem. Składa się on z identyfikacji, analizy, ewaluacji, podejmowania decyzji, postępowania z ryzykiem, monitorowania i przeglądu. Przedstawione jednostki prawie każdemu etapowi procesu zarządzania ryzykiem poświęcają jeden paragraf z informacją, co na danym etapie należy wykonać oraz jaki powinien być przewidywany skutek tych działań.

4.2. Zarządzanie ryzykiem w województwie, powiecie i gminie

Jednostki samorządu terytorialnego wprowadziły w obszarach swojej działalności dokumenty wdrażające procesy zarządzania ryzykiem. Akty prawne o charakterze zarządzeń w przeważającej części zawierają elementy zarządzania ryzykiem funkcjonujące w ramach kontroli zarządczej⁴³, a stosowane dla nich nazewnictwo obejmuje między innymi tzw. polityki, zasady, wytyczne i procedury.

W niniejszym podrozdziale przedstawiono metodyki z zakresu zarządzania ryzykiem, które wdrożono w jednostkach samorządu terytorialnego województwa mazowieckiego – wytypowanego do przeprowadzenia badań oraz analiz w projekcie „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”⁴⁴. W związku z powyższym na szczelbu wojewódzkim przeanalizowanym dokumentem było zarządzenie nr 587 wojewody mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie. Na szczelbu powiatowym analizie poddano zarządzenie nr 828/2015 Prezydenta Miasta Stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie. Spośród mazowieckich gmin wybrano Karczew, gdzie metodykę ujęto w zarządzeniu Nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 roku w sprawie wprowadzenia polityki zarządzania ryzykiem.

⁴³ Patrz: D. Wróblewski (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego*, CNBOP-PIB, Józefów 2014, s. 24.

⁴⁴ D. Wróblewski (red.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 108.

Celem prowadzonych w ramach projektu analiz wybranych dokumentów źródłowych z zakresu zarządzania ryzykiem było wyselekcjonowanie użytecznej wiedzy oraz diagnoza stanu, obejmująca uregulowania związane z zarządzaniem ryzykiem w samorządzie terytorialnym⁴⁵, w tym zawarte w nich metodyki.

Nawiązując przy opisie prawa miejscowego do normy ISO 31000, należy zwrócić uwagę na znaczne rozbieżności i ograniczenia w stosowaniu zarządzania ryzykiem. W aktach prawa miejscowego dostrzegamy mnogość terminologii. Żaden z dokumentów nie uwzględnia wszystkich aspektów w celu kompleksowego wdrożenia zarządzania ryzykiem. Norma ISO 31000 określa meritum danej definicji, którą można elastycznie wykorzystać dla każdej sfery działalności organizacji.

Norma ISO prezentuje dokładnie sprecyzowany cel, na podstawie którego można ocenić skuteczność realizowanych działań. Do podstawowych celów zarządzania ryzykiem zaliczono działania organizacyjne oraz działania doskonalące, szerzej przedstawione w części II *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdziale 1 *Zarządzanie ryzykiem według normy ISO 31000*, podrozdziale 1.1 *Norma ISO 31000:2009 – zakres i przeznaczenie*. Poprzez właściwe ukierunkowanie na cele⁴⁶ organizacja będzie w stanie, bez względu na charakter oraz zakres działalności, wytyczyć szczeble swojego rozwoju.

Scharakteryzowane w podrozdziale zarządzenia administracji wojewódzkiej i terenowej uwidaczniają znaczące różnice we wprowadzanych regulacjach w odniesieniu do procesu zarządzania ryzykiem ujętego w normie ISO 31000. Akty prawa miejscowego, które przygotowano na podstawie standardów kontroli zarządczej, wprowadziły takie elementy jak: identyfikacja ryzyka, analiza ryzyka⁴⁷, odpowiedź bądź reakcja na ryzyko oraz raportowanie o ryzyku i jego monitorowanie⁴⁸. Ostatnie zmiany dokumentów przeanalizowanych jednostek ujednoliciły tryb raportowania na: roczne i niezwłoczne⁴⁹. Jedynym całkowicie zbieżnym zaleceniem zgodnym z normą jest w jednostkach administracyjnych częstotliwość monitorowania ryzyka w okresie przed, w trakcie oraz po przeprowadzeniu procesu zarządzania ryzykiem.

⁴⁵ Tamże.

⁴⁶ Tu rekomenduje się na potrzeby definiowania celów m.in. wykorzystanie metodyki SMART (*Simple, Measurable, Achievable, Relevant, Timely*): prosty (zrozumienie nie powinno stanowić kłopotu, sformułowanie powinno być jednoznaczne i niepozostawiające miejsca na luźną interpretację), mierzalny (sformułowany tak, by można było liczbowo wyrazić stopień realizacji celu lub przynajmniej umożliwić jednoznaczną „sprawdzalność” jego realizacji), osiągalny (realistyczny), istotny (cel powinien być ważnym krokiem naprzód, jednocześnie musi stanowić określoną wartość dla tego, kto będzie go realizował), określony w czasie (cel powinien mieć dokładnie określony horyzont czasowy, w jakim zamierzamy go osiągnąć).

⁴⁷ Zarządzenie prezydenta m.st. Warszawy zastępuje analizę ryzyka oceną ryzyka, podczas której wyznaczany jest poziom ryzyka.

⁴⁸ D. Wróblewski, B. Poleć, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, D. Majchrzak (red.), AON, Warszawa 2014, s. 210.

⁴⁹ Raportowanie bieżące w razie zaistniałych incydentów.

Szczelbel wojewódzki

Zarządzenie⁵⁰ wprowadza do stosowania przez uczestników wdrożonego systemu zarządzania ryzykiem podstawową terminologię w tym zakresie. Autorzy dokumentu zdefiniowali podmioty uczestniczące w procesie zarządzania ryzykiem, a także takie pojęcia jak: ryzyko, zarządzanie ryzykiem, czynniki ryzyka, istotność ryzyka czy akceptowany poziom ryzyka⁵¹.

Zarządzanie ryzykiem ustalone przez wojewodę wiąże się ściśle z planem działalności urzędu wojewódzkiego i realizacją celów, zadań oraz mierników w nim ujętych. Zarządzanie ryzykiem odbywa się poprzez:

- identyfikację ryzyka,
- ocenę ryzyka (w tym analizę i ewaluację ryzyka),
- reakcję na ryzyko⁵²,
- monitorowanie.

Identyfikacja i ocena ryzyka obejmuje rozpoznanie oraz analizę czynników ryzyka poprzez przypisanie im odpowiedniego parametru wpływu na działanie i prawdopodobieństwa wystąpienia⁵³. Zidentyfikowane ryzyka podlegają kategoryzacji na ryzyko operacyjne (krótkookresowe) i ryzyko strategiczne (długookresowe), a następnie podlegają one ocenie pod kątem istotności dla realizacji celów. Do oszacowania prawdopodobieństwa i skutków potencjalnych zdarzeń stosowana jest skala ocen w przedziałach punktowych od 1 do 3.

Ewaluacja ryzyka jest oparta na trzech poziomach istotności ryzyka, do których zostaną przyporządkowane ryzyka po ich identyfikacji i analizie⁵⁴. Do poziomu ryzyka nieznacznego zakwalifikowano ryzyko akceptowalne, które nie wymaga podjęcia działań przeciwdziałających. Dla ryzyka umiarkowanego oraz poważnego kierownicy jednostek są zobligowani do podjęcia stosownych działań przeciwdziałających oraz zaplanowaniu reakcji na ryzyko.

W zarządzaniu ryzykiem w urzędzie wojewódzkim przewidziano następujące sposoby postępowania z ryzykiem: ograniczanie, tolerowanie, unikanie, a także dzielenie się ryzykiem⁵⁵. Można zauważyć, że działania te są niemalże tożsame z opcjami przywołanymi przez normę ISO 31000 (kolejno jw.: dzielenie się ryzykiem, podjęcie ryzyka na podstawie świadomej decyzji, zmiana prawdopodobieństwa lub następstw oraz usunięcie źródła ryzyka, unikanie ryzyka). Ponadto dla ryzyk przekraczających akceptowalny poziom należy planować i wdrażać odpowiednie

⁵⁰ Zarządzenie nr 587 wojewody mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

⁵¹ Tamże, § 2.

⁵² Należy rozumieć jako postępowanie z ryzykiem według normy ISO 31000.

⁵³ § 16 zarządzenia nr 587 wojewody mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

⁵⁴ Tamże, § 17.

⁵⁵ Tamże, § 20.

mechanizmy przeciwdziałające ryzyku w postaci monitoringu okresowego lub ciągłego⁵⁶. Monitorowanie oraz raportowanie o zidentyfikowanych zagrożeniach odbywa się na każdym szczeblu zarządzania. Arkusze identyfikacji i oceny ryzyka oraz raporty z zarządzania ryzykiem stanowią narzędzia wykorzystywane do przygotowania corocznych planów audytu⁵⁷.

W województwach na potrzeby analizy ryzyka wykorzystywane są m.in. arkusze identyfikacji bądź identyfikacji i oceny ryzyka – przykład wskazano poniżej. Innymi stosowanymi dokumentami ramach kontroli zarządczej są także rejestry ryzyka.

Tabela 10. Arkusz identyfikacji i oceny ryzyka

Lp.	Cel	Nazwa miernika	Wartość miernika		Zadania służące realizacji celu	Nr identyfikacyjny ryzyka	Obszar ryzyka	Czynnik ryzyka	Opis ryzyka (przyczyna i skutek)	Wpływ	Prawdopodobieństwo	Poziom istotności	Ryzyko (wraz z podaniem kategorii)	Reakcja na ryzyko	Przeciwdziałanie ryzyku
			bazowa	docelowa											
1		2	3	4	5	6	7	8	9	10	11	12	13	14	15

Źródło: Załącznik Nr 6 do zarządzenia Nr 587 Wojewody Mazowieckiego z dnia 14 grudnia 2016 r.

Szczebel powiatowy

Ramy działania systemu zarządzania ryzykiem w Warszawie prezydent ustanowił zarządzeniem⁵⁸, które przedstawia przede wszystkim terminologię, zakres zadań i obowiązków uczestników systemu⁵⁹, zasady identyfikowania ryzyka oraz dokonywania jego oceny, zasady określania reakcji na ryzyko, zasady identyfikowania i raportowania incydentów, zakres i sposób monitorowania oraz raportowania ryzyka⁶⁰.

⁵⁶ Tamże, § 19.

⁵⁷ Tamże, § 13 ust. 7.

⁵⁸ Zarządzenie nr 828/2015 Prezydenta miasta stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.

⁵⁹ Uczestnikami systemu zarządzania ryzykiem miasta stołecznego Warszawy są wszyscy pracownicy jednostek, biur, dzielnic i urzędów. Za poziom koordynowania systemem odpowiedzialny jest Pełnomocnik ds. ryzyka i właściciele procesów przekrojowych, za poziom zarządzania strategicznego – Prezydent m.st. Warszawy, jego zastępcy, Sekretarz i Skarbnik przy współpracy Pełnomocnika ds. ryzyka, za poziom zarządzania operacyjnego – dyrektorzy biur, burmistrzowie i kierownicy jednostek.

⁶⁰ D. Wróblewski (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego*, CNBOP-PIB, Józefów 2014, s. 26.

Pierwszym etapem procesu zarządzania ryzykiem jest identyfikacja ryzyka w odniesieniu do celów i zadań wyznaczonych przez jednostkę. Wykorzystuje się tu wyniki monitorowania realizacji zadań, sposób organizacji i zarządzania jednostką oraz jej komórkami, jakość wewnętrznych i zewnętrznych regulacji prawnych, uwarunkowania makroekonomiczne, uwarunkowania społeczno-polityczne, informacje o incydentach czy też ustalenia z przeprowadzonych audytów i kontroli⁶¹. Wśród analizowanych czynników potencjalnych ryzyk pod uwagę brane są zarówno te o charakterze wewnętrznym, jak i zewnętrznym.

Każde zidentyfikowane ryzyko podlega ocenie w pięciostopniowej skali w odniesieniu do prawdopodobieństwa jego wystąpienia oraz siły oddziaływania. Iloczyn tych czynników stanowi o poziomie danego ryzyka, uzyskane wyniki po uwzględnieniu hierarchizacji odnotowuje się w rejestrze ryzyka⁶².

Tabela 11. Rejestr ryzyka

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
L.p.	Cele/procesy	Rodzaj celu (zadaniowy, pozostały)	Symbol procesu z SZJ	Miernik realizacji celu	Planowany poziom miernika	Wykonany poziom miernika	Opis ryzyka	Mechanizmy kontrolne	Właściciel ryzyka	Prawdopodobieństwo wystąpienia ryzyka ⁶⁶	Siła oddziaływania ryzyka ⁶⁷	Poziom ryzyka	Reakcja na ryzyko	Opis reakcji na ryzyko

Źródło: Załącznik nr 4 do zarządzenia nr 828/2015 Prezydenta miasta stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.

Właściciele ryzyk po ich przeanalizowaniu są zobowiązani określić sposób reakcji na dane ryzyko. Przewidziano następujące działania: akceptację, dzielenie

⁶¹ § 14 zarządzenia nr 828/2015 Prezydenta miasta stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.

⁶² Tamże, § 16.

się, unikanie bądź ograniczanie ryzyka. Wyżej wskazane działania w istocie niczym nie różnią się (mimo zastosowania zbliżonych pojęć) od wymienionych w przykładzie szczebla wojewódzkiego i odpowiadają tym określonym przez normę ISO 31000, jak również komunikat nr 6 ministra finansów – stanowiący wytyczne w zakresie zarządzania ryzykiem dla sektora finansów publicznych. Decyzja o wyborze jednego ze sposobów reakcji powinna być umotywowana analizą kosztów podjęcia lub ograniczenia ryzyka⁶³. Należy w tym celu wykorzystać także matrycę ryzyka (rys. 1), która prezentuje akceptowalny oraz nieakceptowalny poziom ryzyka.

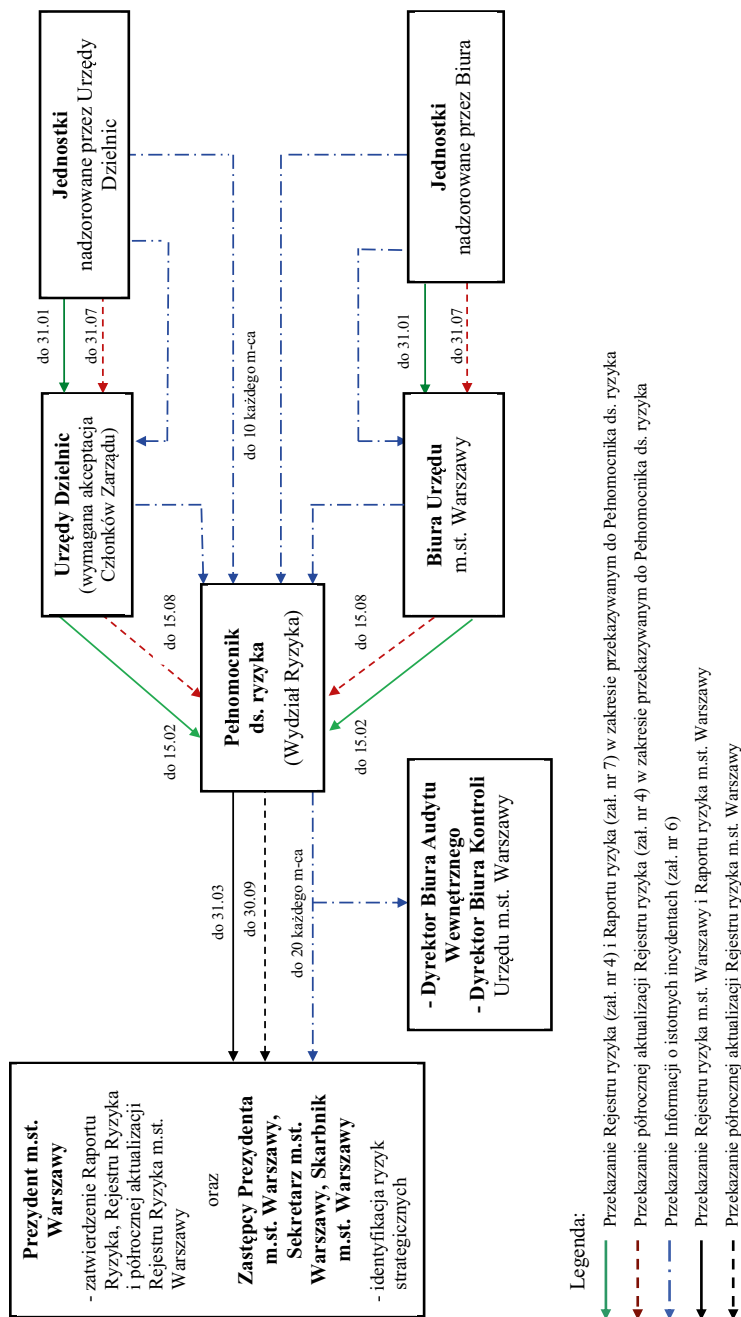
SILA ODDZIAŁYWANIA							
KATASTROFALNE POWAŻNE ŚREDNIE MAŁE NIEZNACZNE		5	10	15	20	25	
		4	8	12	16	20	
		3	6	9	12	15	
		2	4	6	8	10	
		1	2	3	4	5	
		ZNIKO- ME	NISKIE	ŚRED- NIE	WYSO- KIE	BARDZO WYSO- KIE	PRAWDOPODO- BIENSTWO WYSTĄPIENIA
LEGENDA:	zielony	żółty	pomarańczowy	czerwony			
kolor:							
poziom ryzyka:	niski	średni	wysoki	bardzo wysoki (nieakceptowalny)			

Rys. 1. Matryca ryzyka

Źródło: Załącznik nr 3 do zarządzenia nr 828/2015 Prezydenta miasta stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.

⁶³ § 19 zarządzenia nr 828/2015 Prezydenta miasta stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.

**SCHEMAT PRZEPLYWU INFORMACJI
W SYSTEMIE ZARZĄDZANIA RYZYKIEM W M.ST. WARSZAWIE**



Rys. 2. Schemat przepływu informacji w systemie zarządzania ryzykiem w m.st. Warszawie

Źródło: Załącznik nr 9 do zarządzenia nr 828/2015 Prezydenta miasta stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m.st. Warszawie.

Czterostopniowa skala oznaczona na mapie kolorami wskazuje działania do podjęcia dla każdego z poziomów ryzyka. W przypadku ryzyka oszacowanego na poziomie bardzo wysokim uznano za niezbędne przeprowadzenie szczegółowej analizy i sporządzenie planu postępowania z ryzykiem w celu podjęcia dalszych działań, stosując listę wyboru decyzji jn.:

- rezygnacja z realizacji celu;
- przesunięcie w czasie realizacji celu;
- realizacja celu w ograniczonym zakresie;
- wdrożenie działań sprowadzających ryzyko do akceptowalnego poziomu wraz z ustanowieniem osoby odpowiedzialnej za realizację działań;
- realizacja celu przy akceptacji ryzyka o poziomie bardzo wysokim bez uruchamiania dodatkowych działań zmniejszających ryzyko⁶⁴.

System zarządzania ryzykiem w Warszawie podlega bieżącemu monitorowaniu, corocznym przeglądom oraz doskonaleniu. Raportowanie ryzyk sprzężone jest ściśle ze strukturą urzędu miasta i odbywa się poprzez przekazywanie w ściśle określonych terminach rejestrów i raportów ryzyk. Od kierownictwa jednostek do dyrektorów biur i burmistrzów, następnie do Pełnomocnika ds. ryzyka, który przedkłada raport ryzyka za rok ubiegły i rejestr ryzyka za rok bieżący do zatwierdzenia: Prezydentowi m.st. Warszawy, jego zastępcom, Sekretarzowi i Skarbnikowi.

Szczebel gminny

W gminie Karczew zarządzeniem⁶⁵ burmistrza wprowadzona została polityka zarządzania ryzykiem. Odpowiedzialność za właściwą realizację postanowień dokumentu ponoszą wszyscy pracownicy urzędu miejskiego oraz jednostek organizacyjnych. W dokumencie objaśnione zostały podstawowe pojęcia niezbędne do prawidłowego stosowania metodyki zarządzania ryzykiem. Za realizację systemu zarządzania ryzykiem odpowiadają odpowiednio: Burmistrz Karczewa – na poziomie strategicznym, kierownicy jednostek oraz inne osoby na stanowiskach kierowniczych – na poziomie operacyjnym, koordynator ds. kontroli zarządczej i właściciele ryzyk – na poziomie koordynacji systemem⁶⁶.

To właśnie na najniższym poziomie właściciele ryzyk, nadzorując prowadzone przez siebie procesy, odpowiadają za:

- dentyfikację⁶⁷ i ocenę ryzyka (w odniesieniu do celów i procesów),

⁶⁴ Tamże.

⁶⁵ Zarządzenie nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 r. w sprawie wprowadzenia polityki zarządzania ryzykiem.

⁶⁶ § 3 załącznika do zarządzenia nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 r. w sprawie wprowadzenia polityki zarządzania ryzykiem.

⁶⁷ Dokument jako etap zarządzania ryzykiem wyodrębnia identyfikację ryzyka, jednakże nie występuje ona w wykazie pojęć przywołanych w zarządzeniu – gdzie zdefiniowano natomiast analizę ryzyka jako identyfikowanie i opisywanie ryzyka oraz oszacowanie wielkości jego oddziaływania i prawdopodobieństwa przy uwzględnieniu skuteczności istniejących mechanizmów kontroli. Faktycznie etap ten obejmuje zgodnie z rozumieniem normy ISO 31000: identyfikację i analizę ryzyka.

- określenie reakcji na ryzyko⁶⁸,
- wdrażanie działań zaradczych,
- bieżącą współpracę z koordynatorem ds. kontroli zarządczej
- gromadzenie, analizę i raportowanie informacji o ryzykach⁶⁹.

Identyfikacja ryzyka dokonywana jest w odniesieniu do wszystkich zadań na dany rok budżetowy przy rozważeniu wewnętrznych oraz zewnętrznych czynników ryzyka. Do zidentyfikowanego ryzyka przyporządkowywany jest obszar ryzyka⁷⁰, np. utrzymanie dróg i transport zbiorowy dla zadania: transport i komunikacja. Każde ryzyko wprowadzane zostaje do rejestru ryzyka – przykład poniżej.

Tabela 12. Rejestr ryzyka

Kod	Zadania/ obszary działalności	Obszar ryzyka	Cel	Ryzyko	Ocena ryzyka (punktowa)	Reakcja na ryzyko	Właściciel ryzyka
1							
2							
...							

Źródło: Załącznik nr 2 do Polityki zarządzania ryzykiem – zarządzenie nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 r. w sprawie wprowadzenia polityki zarządzania ryzykiem.

Właściciele ryzyk niezwłocznie po identyfikacji ryzyk dokonują punktowej oceny w skali od 1 do 3 w kontekście skutków oraz prawdopodobieństwa wystąpienia każdego z nich.

Tabela 13. Prawdopodobieństwo wystąpienia ryzyka

Prawdopodobieństwo	Opis	Wartość prawdopodobieństwa w skali punktowej
wysokie	Zdarza się częściej niż raz na rok	3
średnie	Zdarza się raz na rok lub rzadziej	2
niskie	Nie zdarzyło się	1

Źródło: Załącznik nr 3 do Polityki zarządzania ryzykiem – zarządzenie nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 r. w sprawie wprowadzenia polityki zarządzania ryzykiem.

⁶⁸ Należy rozumieć jako postępowanie z ryzykiem według normy ISO 31000.

⁶⁹ § 5 załącznika do zarządzenia nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 r. w sprawie wprowadzenia polityki zarządzania ryzykiem.

⁷⁰ Tamże, § 6.

Tabela 14. Skutki wystąpienia ryzyka

Skutek	Opis	Wartość prawdopodobieństwa w skali punktowej	Proponowane działania naprawcze
wysoki	Duża istotność. Prawdopodobieństwo poważnych konsekwencji ⁷⁴ , w tym także finansowych. Wymaga natychmiastowych działań naprawczych ze strony kierownictwa	3	polityka, strategia zarządzania ryzykiem, analiza ryzyka w obszarach narażonych na wystąpienie ryzyka, organizacja szkoleń, samoocena ryzyka, działalność audytu.
średni	Średnia istotność. Oczekuje się przeciwdziałania ze strony kierownictwa i personelu pracowniczego.	2	monitorowanie ryzyka poprzez wdrożone kontrole, funkcja kontrolna głównego księgowego, procedury, instrukcje, działalność audytu.
niski	Mała istotność. Przeciwdziałanie zależy od decyzji kierownictwa. Monitorowanie ryzyka wskazane. Racjonalny dobór mechanizmów kontroli - uwzględnia się koszty na wprowadzenie dodatkowych kontroli	1	samoocena kontrole wewnętrzne, funkcja kontrolna głównego księgowego, bieżące przeglądy kierownictwa,

Źródło: Tamże.

Na tym etapie określony zostaje poziom ryzyka w wyniku iloczynu punktowej oceny prawdopodobieństwa i skutków.

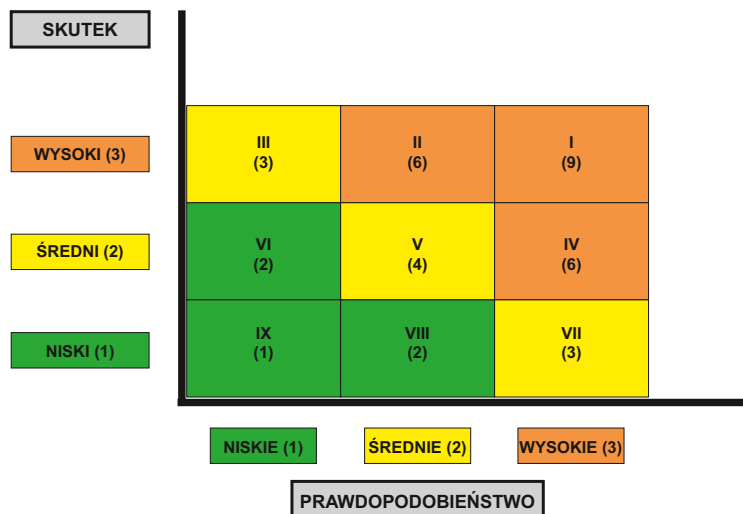
Tabela 15. Poziom istotności ryzyka

Ryzyko wysokie (6–9)	Zdarza się częściej niż raz na rok
Ryzyko średnie (3–5)	Zdarza się raz na rok lub rzadziej
Ryzyko niskie (1–2)	Nie zdarzyło się

Źródło: Tamże.

⁷¹ Dokument tworzy nowe pojęcia: prawdopodobieństwo wystąpienia/prawdopodobieństwo konsekwencji – niezgodnie ze sztuką, terminy te powinny zostać ujęte jako prawdopodobieństwo i skutki (konsekwencje), gdyż takie znaczenie wnoszą w proces oceny ryzyka.

Po przeprowadzonej ocenie ryzyk, dokonywana jest ich hierarchizacja od najwyższego poziomu do najniższego i tak zostaje wprowadzona do rejestru ryzyk⁷². W kolejnym etapie „reakcja na ryzyko” właściciel ryzyka przypisuje do poszczególnych ryzyk jedno z następujących działań: akceptację, dzielenie się, unikanie lub ograniczanie. Wybór decyzji powinien wiązać się z rozważeniem zarówno potencjalnych kosztów, jak i korzyści z podjęcia ryzyka oraz akceptowalny poziom ryzyka, który przedstawiany jest na mapie ryzyka⁷³.



Rys. 3. Mapa ryzyka

Legenda⁷⁴:

- 1) poziom niski – kolor zielony – akceptowalny poziom ryzyka, zaplanowanie i wdrożenie działań zaradczych zależy od decyzji właściciela ryzyka;
- 2) poziom średni – kolor żółty – akceptowalny poziom ryzyka, konieczność stałego monitorowania poziomu ryzyka;
- 3) poziom wysoki – kolor pomarańczowy – akceptowalny poziom ryzyka, wymóg stałego monitorowania poziomu ryzyka oraz konieczność zaplanowania działań zaradczych do ewentualnego wdrożenia.

Źródło: Tamże.

W ramach raportowania ryzyk kierownicy jednostek, osoby zatrudnione na stanowiskach kierowniczych, właściciele procesów w wyznaczonym w roku terminie są zobowiązani przedłożyć koordynatorowi ds. kontroli zarządczej rejestry ryzyk oraz raporty z przeglądu ryzyk. Koordynator na podstawie zebranych informacji przygotowuje zbiorczy rejestr ryzyk gminy Karczew oraz zbiorczy raport z przeglądu ryzyk.

⁷² § 7 załącznika do zarządzenia nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 r. w sprawie wprowadzenia polityki zarządzania ryzykiem.

⁷³ Tamże, § 8.

⁷⁴ Tamże.

5. METODYKA DIAGNOZOWANIA SYSTEMÓW REAGOWANIA POMRISC – ELEMENTY ZARZĄDZANIA RYZYKIEM

W latach 2008–2009 na zlecenie władz Samorządu Województwa Pomorskiego CNBOP podjęło się realizacji zadania badawczego pt. „Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego” na podstawie strategii województwa pomorskiego zawartej w regionalnym programie operacyjnym dla tego województwa na lata 2007–2013¹.

Celem głównym realizacji tematu była ocena funkcjonującego systemu ratownictwa oraz przedstawienie podstaw funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa na terenie województwa pomorskiego, które pozwoliłyby na kompleksową diagnozę stanu bezpieczeństwa oraz podniesienie jego poziomu, zwłaszcza w tych elementach, ocenionych jako najbardziej narażone na ryzyko.

Niepewność i ryzyko to zjawiska właściwe zarówno dla samej organizacji ukierunkowanej na osiągnięcie założonych celów związanych z prowadzoną działalnością, jak i jej otoczenia zewnętrznego. W zależności od środowiska, w jakim działa oraz od jego podmiotów, organizacja prowadzi procesy planowania, kierowania i kontroli działalności, mające na celu zmniejszenie wpływu ryzyka na jej wyniki. Ze względu na niebывалą dynamikę czynników, od których zależy efektywność działania organizacji, we współczesnym świecie wzrasta zainteresowanie teoriami działania w warunkach kryzysu, wskazującymi sposoby ograniczania niepewności i redukcji ryzyka.

Nowatorskie podejście zespołu projektowego² do realizacji zadania polegało na badaniu ankietowym wszystkich podmiotów deklarujących chęć uczestnictwa w systemie: administracji, służb oraz ekspertów. Identyfikacji, analizie i ocenie (pod kątem rekomendacji zmian – przyp. autora) poddano obszary ludzkiej działalności i potencjalne zdarzenia mające wpływ na bezpieczeństwo. Badania okazały się polem do wykorzystania specjalistycznej wiedzy zespołu projektowego w zakresie zarządzania ryzykiem, w wyniku czego powstała unikatowa w Polsce metodyka

¹ D. Wróblewski (red.), *Koncepcja regionalnego zintegrowanego systemu ratownictwa województwa pomorskiego*, s. 23.

² Zespół autorski w składzie: kierownik projektu – D. Wróblewski, zespół – E.W. Roguski, A. Kłodziej-Saramak, D. Kwiatkowski, J. Prasula, T. Sowa, T. Wilczyński, R. Zakrzewski.

oceny ryzyk i ich interpretacji: PomRisc³. Metodyka ta okazała się kompletnym i systemowym podejściem do diagnozowania systemu ratownictwa, jako elementu zarządzania ryzykiem na terenie województwa pomorskiego.

Głównym problemem poruszonym w niniejszym rozdziale jest diagnoza rzeczywistego stanu bezpieczeństwa poprzez analizę ryzyka, która posłużyła do monitorowania zmian i uzyskanych efektów poprzez wyniki opracowane w ramach realizacji badań z tematu badawczego nr 4092/DB/2008⁴.

5.1. Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego (RZSR WP)

W utrzymaniu prawidłowego i zrównoważonego rozwoju każdego regionu bardzo ważne są kwestie bezpieczeństwa, minimalizacji potencjalnych zagrożeń oraz sprawne i skuteczne działanie w przypadku ich wystąpienia. Opracowano wiele metod wykorzystywanych podczas oceny ryzyka⁵, jednakże brakowało takiej, która byłaby odpowiednio dopasowana do potrzeb zdiagnozowania stanu elementów systemu ratownictwa województwa pomorskiego. Narzędziem, które wspomogło identyfikację obszarów ryzyka⁶ – zarówno zagrożeń, jak i szans, była wypracowana w ramach realizacji projektu, relatywnie obiektywna metodyka PomRisc⁷. Warunkiem realizacji projektu „Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego” było objęcie systemu analizą wszystkich podmiotów w nim uczestniczących oraz aspektów jego funkcjonowania.

Przedmiot badań zespołu projektowego stanowiły następujące zagadnienia:

- analiza ryzyka⁸, przeprowadzona według odpowiedniej metodologii badawczej;
- diagnoza obecnego stanu elementów w systemie ratownictwa (np. zasoby, infrastruktura, wyposażenie, lokalizacja placówek);
- analiza słabych ogniw systemu (brakujące lokalizacje, deficyty infrastruktury i wyposażenia, wyposażenie, zasady integracji) – w świetle analizy ryzyka oraz diagnozy;

³ Rozwinięcie skrótu PomRisc – Pomorska Regionalna Integracja Systemów Cywilnych, RZSR WP.

⁴ Umowa z dn. 05.05.2008 r. na wykonanie projektu pt. „Koncepcja Funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego”.

⁵ Patrz: definicja na s. 107.

⁶ Patrz: definicja na s. 119.

⁷ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda oceny ryzyk i systemów reagowania PomRisc jako narzędzie programowania zmian doskonalących systemy bezpieczeństwa i ich monitorowania*, BiTP Vol. 12 Issue 4, 2008, 3.

⁸ Patrz: definicja na s. 109.

- docelowa (całościowa) wizja zintegrowanego systemu ratownictwa w województwie pomorskim – sieć placówek, standardy wyposażenia, narzędzia, zasady integracji itp.;
- rekomendacje w sprawie priorytetowych potrzeb inwestycyjnych wskazanych do współfinansowania z Regionalnego Programu Operacyjnego Województwa Pomorskiego (RPO WP), uporządkowanych rankingowo według takich kryteriów, jak np.:
 - stopień pilności przedsięwzięcia,
 - kluczowe znaczenie dla funkcjonowania systemu jako całości,
 - waga finansowa (koszty przekraczające bieżące możliwości zainteresowanej jednostki organizacyjnej),
 - brak możliwości finansowania z innych źródeł niż RPO (uwzględnienie uwarunkowań wynikających z demarkacji pomiędzy różnymi mechanizmami finansowymi).

W ramach realizacji zadania przygotowano pakiet formularzy skierowanych do podmiotów mających funkcjonować w ramach systemu. Ich zasadniczym celem było zebranie i przetworzenie informacji w kontekście istotnych potrzeb i problemów, z jakimi się borykają oraz nadanie im priorytetów realizacji. Ankiety objęły trzy obszary kluczowe dla funkcjonowania RZSR WP. Ocenie kwalifikacyjnej poddano: gotowość do realizacji inwestycji oraz całkowitego wykorzystania środków (ocena wykonalności), celowość inwestycji w kontekście RZSR WP oraz zdolność do obniżania potencjalnych ryzyk na danym terenie (ocena strategiczna)⁹.

5.2. Metody badawcze wykorzystane na potrzeby analizy oceny ryzyka PomRisc¹⁰

Podstawą do opracowania eksperckiej metodyki PomRisc była szeroka analiza literatury krajowej i zagranicznej oraz norm i metod, w tym między innymi:

- Australian/New Zealand Standard *Risk Management* AS/NZS 4360:2004¹¹,
- Handbook *Risk Management Guidelines* HB 436:2004,
- *Governance, Risk Management and Control Assurance* HB 254-2005,
- J. Wolanin, *Zarys teorii bezpieczeństwa obywateli. Ochrona ludności na czas pokoju*, Warszawa 2005,
- *Schutz kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden*, Bundesministerium des Innern, Berlin,

⁹ D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 23.

¹⁰ Patrz szerzej: PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.

¹¹ Patrz: AS/NZS 4360 Zarządzanie ryzykiem (ostatnie zmiany dokonane w 2004 r.), po raz pierwszy opublikowana w 1995 r.

- *Protection of Critical Infrastructures – Baseline Protection Concept Recommendation for Companies*, Federal Ministry of the Interior, Berlin.

Podstawę stanowiła także ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. nr 89, poz. 590) oraz projekt normy *Standard zarządzania ryzykiem*¹² – ISO 31000¹³.

Realizacja zadania oparta została na zbiorze ankiet, zawierających pytania dotyczące elementów technicznych, funkcjonalnych, powiązań między podmiotami i ich zakresu odpowiedzialności, z możliwością wskazania kluczowych ogniw i podstawowych błędów systemu na tle występujących i potencjalnych zagrożeń. Ankiety skierowane były do terenowych organów administracji samorządowej i ekspertów oraz podmiotów deklarujących uczestnictwo w Regionalnym Zintegrowanym Systemie Ratownictwa Województwa Pomorskiego¹⁴.

Ocenę oparto na metodyce PomRisc w odniesieniu do kryterium adekwatności systemu do potencjalnych i kinetycznych ryzyk występujących na konkretnym rozpatrywanym obszarze administracyjnym. Dotyczyła ona w szczególności:

- gotowości do realizacji inwestycji oraz wykorzystania w pełni środków (ocena wykonalności);
- celowości inwestycji w kontekście RZSR WP;
- zdolności do obniżania potencjalnie istniejących ryzyk na danym terenie (ocena strategiczna)¹⁵;
- oceny systemów reagowania;
- szacowania ryzyka¹⁶ poprzez tworzenie aktualnych matryc ryzyka i powiązania informacji zarówno z procedurami w powiązaniu z bazami infrastrukturalno-sprzętowymi oraz kapitałem ludzkim;
- procedur operacyjno-logistycznych podmiotów;
- instytucji świadczących usługi w zakresie ratownictwa i ochrony ludności, jak również określenia sposobu postępowania w sytuacjach zagrożenia na obszarze.

Na podstawie wyżej wymienionych dokumentów sporządzono matryce ryzyk, w których wskazano 10 wybranych ryzyk – najistotniejszych dla bezpieczeństwa mieszkańców, niezakłóconego funkcjonowania i rozwoju gminy, powiatu, województwa, występujących na terenach własnych i sąsiadujących. Następnie uszeregowano je od najważniejszych do mniej ważnych z punktu widzenia własnego podmiotu, polityki gminy, powiatu, województwa. Podczas kwalifikowania ryzyka zespół projektowy w dużej mierze korzystał z własnej wiedzy (w tym własnych

¹² ISO 31000:2009 Risk Management – Principles and Guidelines zastępuje AS/NZS 4360:2004.

¹³ Międzynarodowy Komitet Normalizacyjny (International Organization for Standardization) 13 listopada 2009 r. opublikował standard ISO 31000:2009 Risk Management – Principles and Guidelines.

¹⁴ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 2.

¹⁵ D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 23.

¹⁶ Patrz: definicja na s. 115.

baz danych) i wiedzy pozyskanej od podmiotów. Wskazane ryzyka ograniczono do zdarzeń destrukcyjnych wywołujących straty i uszeregowano według rodzaju:

- wypadki i katastrofy w komunikacji i transporcie,
- awarie infrastruktury technicznej (wodno-kanalizacyjnej, energetycznej, gazowej itd.);
- pożary według rodzajów;
- klęski i zagrożenia naturalne (powodzie, pożary lasów, gradobicia, silne wiatry, nadmierne opady atmosferyczne, oblodzenia, silne mrozy i susze itp.);
- awarie i katastrofy budowlane, w tym dotyczące budowli hydrotechnicznych;
- awarie i katastrofy chemiczne;
- awarie i katastrofy ekologiczne oraz radiacyjne;
- zagrożenia biologiczne (epidemie, epizootie, epifitozy);
- utonięcia itp.

Po zidentyfikowaniu ryzyk oszacowano dwa parametry ryzyka, tj. prawdopodobieństwo lub częstość występowania oraz wielkość strat powodowanych przez określone ryzyko. Następnie wypełnione przez podmioty matryce ryzyk poddano analizie i segregacji w rozbiciu na powiaty, tworząc jedną zbiorczą matrycę dla danego powiatu. Matryca zbiorcza uwzględniła najbardziej niekorzystne zdarzenie i wszystkie kategorie (zdrowie i bezpieczeństwo, straty materialne, środowisko naturalne, społeczne/dziedzictwo kulturowe, społeczeństwo/rząd/reputacja/mass media, kategoria cywilnoprawna)¹⁷.

Wykonawcy badań zidentyfikowali 17 rodzajów zagrożeń. Brali przy tym pod uwagę miejsce danego zagrożenia w hierarchii, liczbę wskazań (dot. danego zagrożenia w powiecie) oraz wartość punktową wielkości strat i częstości zdarzenia z matrycy¹⁸.

Projekt „Regionalne zarządzanie bezpieczeństwem – narzędzia wspomagające zarządzanie – PomRisc” został wdrożony na terenie województwa pomorskiego w 2009 r. i był jednym z narzędzi wykorzystywanych do oceny stopnia zaawansowania integracji systemu ratownictwa na szczeblu wojewódzkim, powiatowym i gminnym.

5.2.1. Zarys systemu bezpieczeństwa w województwie pomorskim

Zdaniem zespołu projektowego jedną z najlepszych metod oceny stanu bezpieczeństwa jest identyfikacja¹⁹, analiza i ewaluacja ryzyka²⁰. Przed przystąpieniem do wykonania procedury oceny ryzyka należy zebrać informacje dotyczące omawianego terenu, czyli dokonać identyfikacji zagrożeń, a następnie identyfikacji ryzyka²¹.

¹⁷ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 5.

¹⁸ Patrz szerzej: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 25.

¹⁹ Patrz: definicja na s. 106.

²⁰ Patrz: definicja na s. 114.

²¹ D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 1.

Skuteczność w zapewnieniu bezpieczeństwa mieszkańcom uzależniona jest w dużym stopniu od sposobu zarządzania bezpieczeństwem poprzez zarządzanie ryzykiem i ratownictwem. Ocena funkcjonującego systemu ratownictwa w województwie pomorskim oparta została na kryterium zgodności systemu w odniesieniu do kinetycznych i potencjalnych zagrożeń występujących na konkretnie rozpatrywanym obszarze administracyjnym²².

Na terenie województwa funkcjonuje wiele podmiotów świadczących usługi ratownicze dla mieszkańców i osób przebywających na jego terenie. Każdy z podmiotów działa we własnym otoczeniu prawnym, najczęściej na podstawie ustaw, rozporządzeń, zarządzeń lub innych regulacji formalnoprawnych. Stan otoczenia prawnego podmiotów ratowniczych oraz praktyka prowadzą do zjawiska zwanego hermetyzacją. Oznacza to, że każdy z podmiotów w naturalnym procesie dostrzega wyłącznie swoje potrzeby, służące realizacji jego zadań, w celu zaspokajania swoich potrzeb. Takie podejście jest sprzeczne z teorią zarządzania i pojęciem kontekstu – otoczenia. W wyniku tego podmioty nie odczuwają potrzeby współdziałania i zespolenia²³.

Głównym zadaniem w tworzeniu i rozwijaniu RZSR WP było stworzenie mechanizmów umożliwiających i wspierających tworzenie i rozwijanie funkcjonalnych relacji pomiędzy podmiotami w celu uzyskania zjawiska synergii w świadczeniu usług ratowniczych dla poszkodowanych.

Wszystkie działania zmierzały do tego, aby system charakteryzował się otwartością, kontekstowością, dynamicznością, drożnością, elastycznością, sterowalnością i synergicznością. Wyżej wymienione cechy systemu, stanowiące efekt analiz przedmiotowego opracowania, zdefiniowały tworzony RZSR WP²⁴.

Zakres prac obejmował:

- 1) analizę ryzyka, przeprowadzoną według odpowiedniej metodologii badawczej;
- 2) diagnozę obecnego stanu elementów systemu ratownictwa, a w szczególności:
 - a) zasobów,
 - b) infrastruktury,
 - c) wyposażenia,
 - d) lokalizacji placówek;
- 3) analizę słabych ogniw systemu – w świetle analizy ryzyka i diagnozy, a w szczególności:
 - a) brakujących lokalizacji,
 - b) deficytów infrastruktury i wyposażenia,
 - c) poziomu wyszkolenia;
- 4) ocenę propozycji (przedstawionych przez podmioty) zasad funkcjonowania każdego z podmiotów ratowniczych w Regionalnym Zintegrowanym Systemie Ratownictwa Województwa Pomorskiego (RZSR WP) wraz z uzasadnieniem,

²² Tamże.

²³ Tamże, s. 6.

²⁴ Patrz szerzej: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 7.

- przy założeniu realizacji wymagań formalnych i funkcjonalnych, zdolnych do osiągnięcia wskaźników określonych w kierunku wsparcia 7.2 Regionalnego Programu Operacyjnego Województwa Pomorskiego 2007–2013;
5. określenie schematów funkcjonalnych każdego z podmiotów ratowniczych zdefiniowanych w RZSR WP;
 6. docelową (całościową) wizją RZSR WP, w szczególności na podstawie wniosków i propozycji w zakresie:
 - a) sieci placówek,
 - b) standardów wyposażenia,
 - c) narzędzi i zasad integracji,
 - d) poziomu wyszkolenia, itp.;
 7. opracowanie zintegrowanego schematu funkcjonowania wszystkich podmiotów ratowniczych w RZSR WP;
 8. oszacowanie kosztów uczestnictwa każdego z podmiotów ratowniczych w RZSR WP na podstawie docelowej wizji tego systemu;
 9. rekomendacje w kwestii priorytetowych potrzeb inwestycyjnych uporządkowanych rankingowo w ujęciu przestrzennym i przedmiotowym na tle obszarów szczególnie zagrożonych w relacji do zdiagnozowanych deficytów (m.in. obiektowych, organizacyjnych, sprzętowych), według takich kryteriów jak np.:
 - a) stopień pilności przedsięwzięcia,
 - b) kluczowe znaczenie dla funkcjonowania systemu jako całości,
 - c) waga finansowa (koszty przekraczające bieżące możliwości zainteresowanego podmiotu)²⁵.

5.2.2. Diagnoza stanu bezpieczeństwa w województwie pomorskim²⁶

Wiedza uzyskana w toku oceny funkcjonującego systemu, poprzedzonej szczegółową identyfikacją zagrożeń, pozwoliła na opracowanie strategii zmniejszenia prawdopodobieństwa ich wystąpienia, łagodzenia ich przebiegu po uaktywnieniu oraz usuwania skutków. Dzięki uzyskanym informacjom możliwe było także opracowanie procedur zarządzania bezpieczeństwem podmiotu i optymalizacji jego procesów informacyjno-decyzyjnych²⁷.

Zespół projektowy wykorzystał dane historyczne, czyli dane o awariach, wypadkach i innych zdarzeniach destrukcyjnych, które miały miejsce na omawianym terenie²⁸. Zakres tych danych obejmował zagadnienia dotyczące ogólnej wiedzy na temat omawianego obszaru (charakterystyka terenu, charakterystyka aktualnej

²⁵ Patrz szerzej: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 23–24.

²⁶ Opracowanie na podstawie: E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 3–8.

²⁷ Patrz szerzej: D. Wróblewski (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego: analiza wybranych przepisów*, CNBOP-PIB, Józefów 2014, s. 20–24.

²⁸ Patrz: PN-ISO 31000. Identyfikacja ryzyka może obejmować dane historyczne, analizy teoretyczne, pozyskane opinie, opinie ekspertów oraz potrzeby interesariuszy.

sytuacji, substancji niebezpiecznych, warunków hydrologiczno-meteorologicznych, struktury społecznej i demograficznej, zagospodarowania przestrzennego, podmiotów tworzących system bezpieczeństwa itp.).

Otrzymane informacje umożliwiły przegląd dotychczas zaistniałych sytuacji – **ryzyk kinetycznych**²⁹. Dane historyczne stanowią istotne źródło wiedzy o zagrożeniach, negatywnych skutkach i ewentualnych przyczynach niekorzystnych zdarzeń. Inne z tych danych pozwalają na identyfikację i wyodrębnienie źródeł i miejsc najbardziej narażonych na zagrożenia – **ryzyk potencjalnych**³⁰.

Informacje dotyczące identyfikacji i analizy ryzyk, oszacowanie ich wielkości i hierarchizacja³¹ mogą mieć wpływ na podejmowanie wszelkich decyzji związanych z ochroną ludności oraz tworzenie lokalnej polityki bezpieczeństwa³². Aby zapewnić prawidłowość oceny ryzyk, poza działaniami analitycznymi i probabilistycznymi, prowadzono dialog między społeczeństwem a władzami różnych szczebli podziału administracyjnego, służbami i podmiotami świadczącymi usługi dla ludności w zakresie ratownictwa oraz środowiskami ekspertów. Takie podejście do problemu pozwoliło na wybór optymalnej drogi poprawy bezpieczeństwa mieszkańców poprzez określenie kierunku działań w zakresie ograniczenia liczby zdarzeń niekorzystnych (działania czysto profilaktyczne) oraz negatywnych skutków zdarzeń niekorzystnych (działania głównie operacyjne, ale i prewencyjne).

Identyfikacja i ocena wielkości ryzyka³³ są częścią procedury zarządzania bezpieczeństwem. Na ich podstawie można przystąpić do tworzenia planów ratowniczych, procedur informowania, ostrzegania, alarmowania, wyboru dróg do przewożenia substancji niebezpiecznych, doskonalenia powiązań organizacyjnych, planowania inwestycji i zakupów inwestycyjnych dla elementów systemu bezpieczeństwa oraz planowania szkoleń doskonalących. Po zakończeniu procesu identyfikacji ryzyk należy dokonać ich wstępnej hierarchizacji i zdecydować o kierunku działań skierowanych na każde z nich³⁴.

Szacowanie ryzyka³⁵ polega na określeniu wielkości ryzyka, z uwzględnieniem prawdopodobieństwa jego wystąpienia, strat i innych konsekwencji przez nie wywołanych oraz skutków socjologicznych, społeczno-ekonomicznych

²⁹ Ryzyko kinetyczne – źródło bądź miejsce uwolnienia zagrożenia o określonych skutkach. Źródło: E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 4.

³⁰ Ryzyko potencjalne – źródło bądź miejsce najbardziej narażone na zagrożenie o określonych skutkach. Źródło: E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 4.

³¹ Patrz: definicja na s. 154.

³² D. Wróblewski, *Zarządzanie ryzykiem jako element kształtowania bezpieczeństwa lokalnego*, Szkolenie podstawowe dla: starostów, wójtów, burmistrzów i prezydentów miast województwa dolnośląskiego z zakresu ochrony ludności i obrony cywilnej „Zarządzanie w stanach zagrożeń i doskonalenie systemu ochrony ludności”, Józefów 2011.

³³ Patrz: definicja na s. 115 (poziom ryzyka).

³⁴ Patrz szerzej: D. Wróblewski (red.), *Zagadnienia ogólne...*, dz. cyt., s. 20–24.

³⁵ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 3.

i środowiskowych³⁶. W praktyce stosowane są dwie metody szacowania ryzyka: jakościowa i ilościowa.

Umiejętność szacowania ryzyka stanowi ważne narzędzie, niezbędne do prawidłowego zarządzania ryzykiem. W praktyce daje możliwość przewidywania rozwoju sytuacji i wpływu niekorzystnych zdarzeń na stan bezpieczeństwa społeczności.

5.3. Identyfikacja i ocena wielkości ryzyka

Celem tego etapu było stworzenie wyczerpującej listy ryzyk, opartej na tych zdarzeniach, które mogą tworzyć, stymulować, zapobiegać, przeszkadzać, przyspieszać lub opóźniać osiągnięcie celów. Badaniu poddano źródła ryzyka, obszary wpływów, zdarzenia (łącznie ze zmianami okoliczności) oraz ich przyczyny i potencjalne następstwa. Wykorzystanie danych dotyczących omawianego obszaru (charakterystyka terenu, charakterystyka aktualnej sytuacji, substancji niebezpiecznych, warunków hydrologiczno-meteorologicznych, struktury społecznej i demograficznej, zagospodarowania przestrzennego, podmiotów tworzących system bezpieczeństwa itp.) dało wyczerpujący obraz identyfikacji ryzyk i oceny wielkości ryzyka.

Wnioski płynące z identyfikacji ryzyk i oceny wielkości ryzyka są nieodzowną częścią procedury zarządzania bezpieczeństwem oraz są niezbędne do przeprowadzenia kolejnych kroków:

- tworzenia planów ratowniczych,
- wyboru dróg do przewożenia substancji niebezpiecznych,
- tworzenia procedur informowania, ostrzegania i alarmowania,
- tworzenia planów obrony cywilnej i zarządzania kryzysowego,
- doskonalenia powiązań organizacyjnych,
- planowania inwestycji i zakupów inwestycyjnych dla elementów systemu bezpieczeństwa,
- planowania szkoleń doskonalących³⁷.

Korzystając z metodyki PomRisc, zidentyfikowano 17 ryzyk istotnych w kontekście powiatów:

- ataki terrorystyczne,
- skażenia radiacyjne,
- gradobicia,
- niewypały,
- mrozy, śnieżyce, oblodzenia,
- susze,
- naruszenia porządku publicznego,
- utonięcia,
- wichury,

³⁶ Patrz szerzej: D. Wróblewski (red.), *Zarządzanie ryzykiem. Przegląd wybranych metodyk*, CNBOP-PIB, Józefów 2015, s. 37–41.

³⁷ Na podstawie: E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 8.

- powodzie i podtopienia,
- skażenia chemiczne,
- katastrofy ekologiczne,
- awarie,
- katastrofy budowlane,
- pożary,
- zakażenia masowe,
- wypadki komunikacyjne.

Hierarchiczny rozkład wielkości wymienionych ryzyk w każdym z 20 analizowanych powiatów przedstawiał się inaczej, co było ściśle związane z lokalnymi specyfikami zagrożeń. Zgodnie z teorią analizy ryzyka na potrzeby projektu przyjęto założenie, że wielkość poszczególnych ryzyk jest ekwiwalentem punktowym zależności częstości (prawdopodobieństwa) występowania danego ryzyka na rozpatrywanym terenie i przewidywanych skutków uwolnionego (kinetycznego) ryzyka. W wyniku takiego podejścia stworzono zespół map terytorialnego rozkładu cząstkowych ryzyk obszarowych (dla każdego ryzyka oddzielna mapa). Poziomy ryzyka są oznaczone kolorami, które – uszeregowane malejąco – oznaczają: kolor czerwony – ryzyko nieakceptowane, kolor żółty – ryzyko tolerowalne, kolor zielony – ryzyko akceptowalne, kolor biały – ryzyko pomijalne. Mapy te tworzone z wykorzystaniem danych z poziomu powiatowego. Z racji sposobu ich tworzenia obrazują one ryzyka postrzegane w perspektywie powiatowej. Standardowe podejście do analizy ryzyka terenu województwa oraz mapowania ryzyka okazały się w ujęciu województwa niewystarczające. Aby lepiej zobrazować poziom ryzyk na terenie województwa i tym samym trafniej sformułować rekomendację działań zapobiegawczych, korygujących lub doskonalących system reagowania, autorzy stworzyli zespół matryc zbiorczych, które podlegały przekształceniom³⁸.

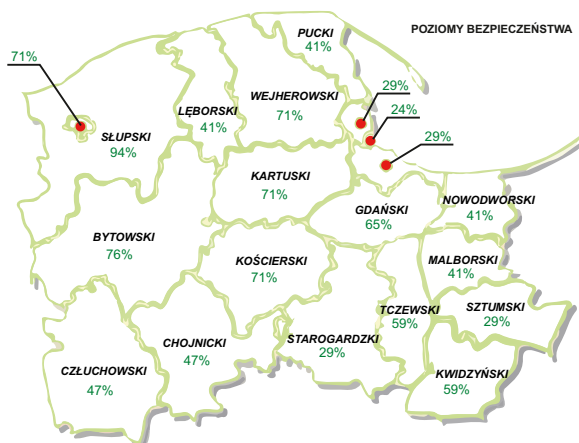
Do sformułowania rekomendacji niezbędna była wizualizacja względna wielkości ryzyk w kontekście powiatów i województwa, które budowały relacyjną przestrzeń ryzyka. Przekształcenia te miały umożliwić opracowanie matryc rekomendacji działań z perspektywy powiatów oraz województw. Warto dodać, że w metodyce wielkość ryzyka zobrazowana za pomocą koloru jest podczas przekształceń niezmienna i stanowi stały poziom odniesienia. Ostateczna analiza matryc rekomendacji działań w powiązaniu z wnioskami z diagnozy systemu reagowania prowadzi do sformułowania kierunków strategicznych poprawy bezpieczeństwa na rozpatrywanym terenie. W zależności od szczegółowości prowadzonych analiz wnioski mogą dotyczyć działań o charakterze strategicznym albo operacyjnym³⁹.

Mapę administracyjną ryzyk województwa wykonano na podstawie analizy matryc wypełnionych przez podmioty deklarujące udział w RZSR WP. Uzupełnieniem

³⁸ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 24.

³⁹ Tamże, s. 24–25.

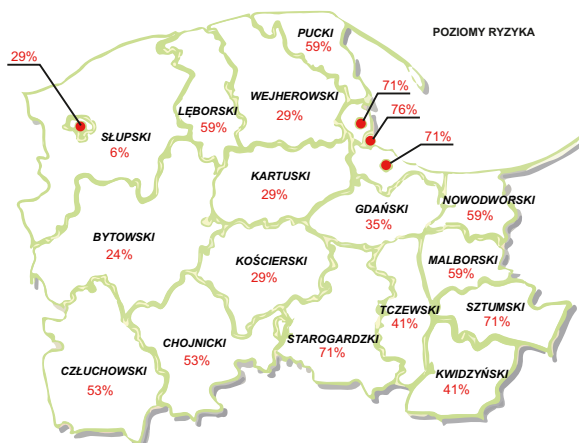
mapy administracyjnej ryzyk województwa pomorskiego są graficzne wizualizacje w postaci „poziomów bezpieczeństwa”.



Rys. 1. Mapa terytorialnego rozkładu poziomu bezpieczeństwa województwa pomorskiego

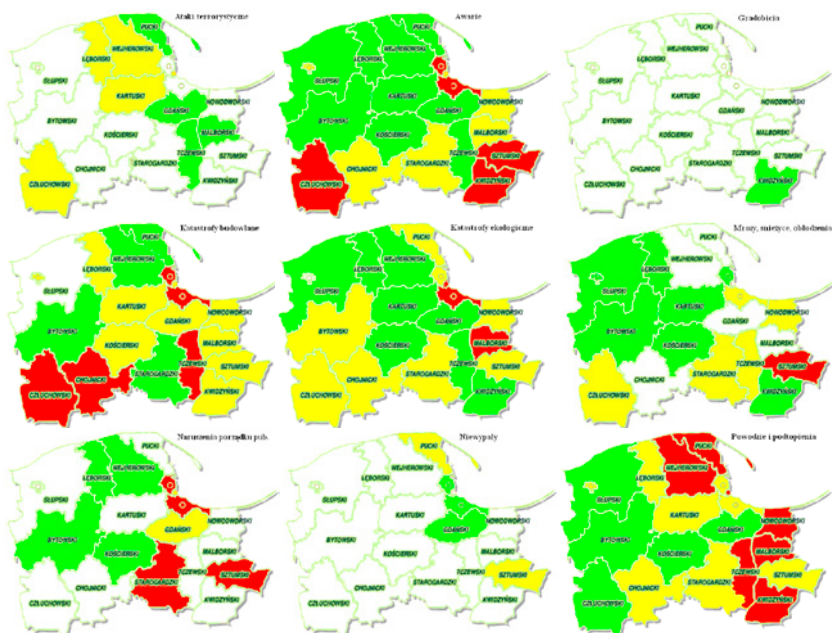
Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 53.

W celu uzyskania porównywalności ryzyk w powiatach z perspektywy województwa stworzono mapę terytorialnego rozkładu ryzyk obszarowych, którą przedstawia rys. 2.



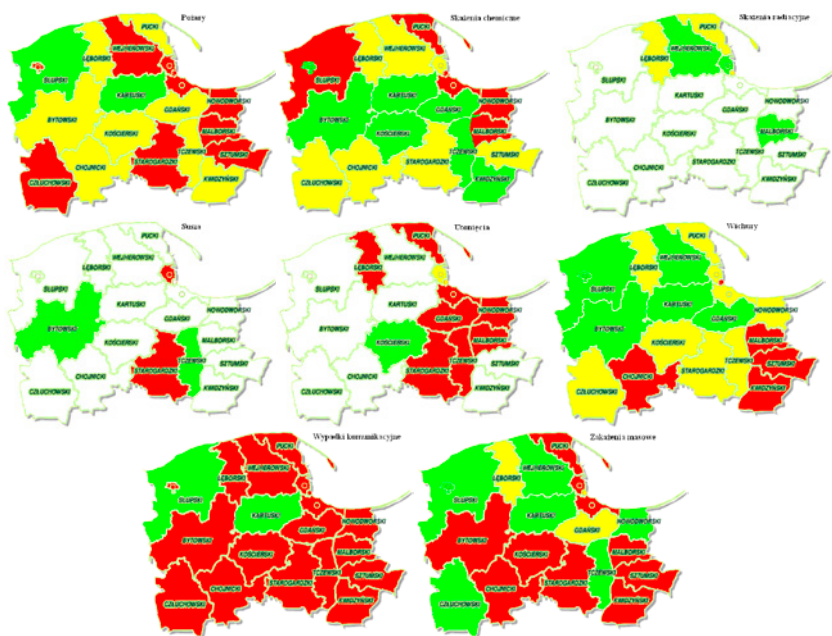
Rys. 2. Mapa terytorialnego rozkładu ryzyk obszarowych województwa pomorskiego

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 54.



Rys. 3a. Mapy terytorialnego rozkładu ryzyk cząstkowych województwa pomorskiego – cz. 1/2

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 5.



Rys. 3b. Mapy terytorialnego rozkładu ryzyk cząstkowych województwa pomorskiego – cz. 2/2

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 5.

Poniżej w celach poglądowych przedstawiono matryce ryzyk powiatu kwidzyńskiego.

Tabela 1. Matryca ryzyk – pow. kwidzyński (przykład)

Wielkość strat Częstość		1	2	3	4	5
		nie-istotne	ograniczone	poważne	bardzo poważne	katastrofalne
A	sporadyczne					
B	rzadkie		mrozy, śnieżyce, oblodzenia gradobicia		katastrofy budowlane	
C	częste		skażenia chemiczne katastrofy ekologiczne		powodzie i podtopienia wichury wypadki komunikacyjne zakażenia masowe	
D	bardzo częste		pożary	awarie		
E	ustawiczne (permanentne)					

	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 66.

Kolejnym etapem było sporządzenie mapy administracyjnej ryzyk województwa⁴⁰ pomorskiego. Na mapie tej zaznaczono procentowe poziomy ryzyka i bezpieczeństwa w danym powiecie.

W skład poziomu bezpieczeństwa wchodziły ryzyka pomijalne (kolor biały) i akceptowalne (kolor zielony), a w skład poziomu ryzyka – ryzyka tolerowalne (kolor żółty) i ryzyka nietolerowane (kolor czerwony).

⁴⁰ Mapa administracyjna ryzyk województwa – graficzne zobrazowanie na podstawie matryc bazujących na danych z poziomu powiatowego, przedstawiające procentowy poziom ryzyka i bezpieczeństwa. Źródło: na podstawie D. Wróblewski (red.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 30.

te posłużyły jako instrument pomocniczy podczas wyboru rekomendowanych inwestycji⁴³.

Matryce ryzyk w rozbiciu na powiaty

Hierarchizacji zagrożeń dokonano na podstawie analizy matryc wypełnionych przez podmioty, biorąc pod uwagę liczbę wskazań (dotyczących danego zagrożenia w powiecie) oraz wartość punktową – iloczyn (miejsce przecięcia wielkości strat i częstości zdarzenia) z matrycy. Poniżej zamieszczono trzy przykładowe matryce ryzyk dla powiatu bytowskiego i miasta Sopotu na prawach powiatu⁴⁴.

Tabela 2. Matryca ryzyk – powiat bytowski (przykład)

Wielkość strat Częstość		1	2	3	4	5
		nieistotne	ograniczone	poważne	bardzo poważne	katastrofalne
A	sporadyczne		naruszenie porządku pub.			katastrofy ekologiczne
B	rzadkie		mrozy, śnieżyce, oblodzenia susze	katastrofy budowlane		
C	częste	awarie	powodzie i podtopienia wichury skażenia chemiczne	pożary		zakażenia masowe
D	bardzo częste					
E	ustawiczne (permanenne)			wypadki komunikacyjne		

	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 60.

Hierarchizacja zagrożeń pod względem częstotliwości wskazania:

- zakażenia masowe,
- pożary,
- wypadki komunikacyjne,

⁴³ Patrz szerzej: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 393.

⁴⁴ D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 60.

- katastrofy ekologiczne,
- powódzie i podtopienia,
- wichury,
- katastrofy budowlane,
- skażenia chemiczne,
- awarie,
- mrozy, śnieżyce, oblodzenia,
- susze,
- naruszenia porządku publicznego.

Tabela 3. Matryca ryzyk – Sopot, miasto na prawach powiatu (przykład)

Wielkość strat		1	2	3	4	5
		nie-istotne	ograniczone	poważne	bardzo poważne	katastrofalne
A	sporadyczne					skażenia radiacyjne, ataki terrorystyczne
B	rzadkie				katastrofy budowlane, utonięcia	wichury, skażenia chemiczne, katastrofy ekologiczne
C	częste			awarie, zakażenia masowe, naruszenia porządku pub	powódzie i podtopienia, pożary, wypadki komunikacyjne	
D	bardzo częste					
E	ustawiczne (permanentne)					

	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

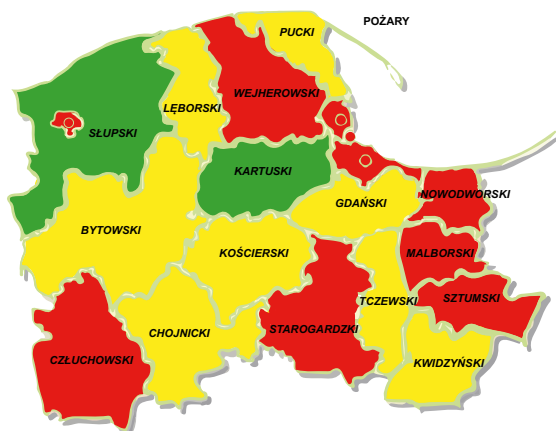
Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 79.

Hierarchizacja zagrożeń pod względem częstotliwości wskazania:

- powódzie i podtopienia,
- pożary,
- wypadki komunikacyjne,
- awarie,
- wichury,
- katastrofy budowlane,
- katastrofy ekologiczne,
- skażenia chemiczne,
- zakażenia masowe,
- naruszenie porządku publicznego,
- utonięcia,
- skażenia radiacyjne,
- ataki terrorystyczne.

Mapy ryzyk⁴⁵

Na podstawie matryc ryzyk realizatorzy projektu opracowali mapy ryzyk. Poniżej przedstawiono dwie przykładowe mapy zagrożeń dla pożarów oraz wypadków komunikacyjnych.

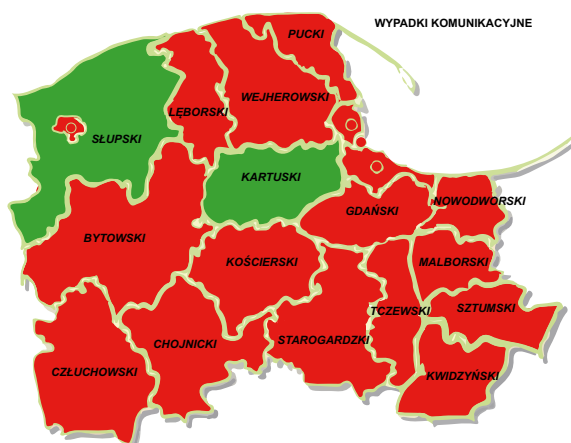


	ryzyko pomijalne
	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

Rys. 8. Mapa terytorialnego rozkładu ryzyk części województwa pomorskiego – pożary

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 90.

⁴⁵ D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 81–90.



	ryzyko pomijalne
	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

Rys. 9. Mapa terytorialnego rozkładu ryzyk częściowych województwa pomorskiego – wypadki komunikacyjne

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 96.

5.4. Diagnoza systemu reagowania jako komponentu zarządzania ryzykiem

Ryzyko w uproszczonym podejściu obejmuje skutki i prawdopodobieństwo lub częstość zdarzenia. Diagnoza stanu elementów systemu ratownictwa województwa pomorskiego pozwoliła na szczegółowe określenie słabych i silnych elementów systemu zarówno w skali województwa, jak i poszczególnych powiatów.

Dla osiągnięcia głównego celu osi priorytetowej Regionalnego Programu Operacyjnego dla województwa pomorskiego w zakresie zintegrowanego systemu ratownictwa kluczowe znaczenie mają następujące podmioty:

- Państwowa Straż Pożarna,
- ochotnicze straże pożarne,
- policja,
- Morska Służba Poszukiwania i Ratownictwa SAR,
- pogotowie ratunkowe, szpitale oraz SOR,
- straże miejskie oraz gminne,
- Straż Graniczna,
- inspektoraty ochrony środowiska,

- inspektoraty nadzoru budowlanego,
- inspektoraty weterynarii,
- stacje sanitarno-epidemiologiczne,
- Wodne Ochotnicze Pogotowie Ratunkowe,
- centra zarządzania kryzysowego.

Każdy z wymienionych podmiotów działa we własnym otoczeniu prawnym, tj. najczęściej na podstawie ustaw, rozporządzeń, zarządzeń lub innych regulacji formalnoprawnych.

W związku z szybkim rozwojem naszego kraju regulacje te były i są tworzone na różnych etapach, dlatego często mamy do czynienia z nakładaniem się kompetencji lub niewypełnieniem pełnego obszaru potrzeb. Ponadto na terenie województwa istnieją podsystemy reagowania, takie jak krajowy system ratowniczo-gaśniczy województwa pomorskiego. Podsystemy te jednak nie gwarantują pełnego zespolenia i integracji i obejmują ograniczoną liczbę wyżej określonych podmiotów⁴⁶.

Głównym zadaniem w tworzeniu i rozwijaniu Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego było wytworzenie mechanizmów umożliwiających i wspierających tworzenie oraz rozwijanie skutecznych relacji pomiędzy podmiotami w celu uzyskania zjawiska synergii w świadczeniu usług ratowniczych dla potrzebujących.

Podejście do diagnozy zwykle ograniczane jest do indywidualnej analizy podsystemów, ma charakter doraźny i wycinkowy, a nie systemowy i kompleksowy. Podejmowane próby diagnozowania wybranych elementów wspólnego działania, ograniczały się do wspólnych ćwiczeń i manewrów doskonalących współdziałanie i koordynację. Niedoskonałości współdziałania i koordynacji podczas reagowania były łagodzone przez podmioty w ramach działalności informacyjno-prasowej. W projekcie rozwiązano ten problem poprzez stworzenie matrycy zgodności⁴⁷.

W skali województwa zaobserwowano, że do silnych elementów zaliczają się: liczba jednostek interwencyjnych, rozlokowanie jednostek interwencyjnych, czas dojazdu, współdziałanie, koordynacja i wyszkolenie służb ratowniczych. Słabymi elementami systemu są natomiast: stan kadrowy, system powiadamiania ludności oraz świadomość społeczna. Pozostałe elementy systemu można sklasyfikować jako akceptowalne. Diagnoza ta wskazuje, które elementy systemu należy przede wszystkim wzmocnić⁴⁸.

Należy podjąć działania zmierzające do minimalizacji ryzyka w rozumieniu systemu bezpieczeństwa funkcjonującego na danym terenie, doskonaląc zabezpieczenia techniczne i nietechniczne zmniejszające prawdopodobieństwo wystąpienia

⁴⁶ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda oceny ryzyk i systemów reagowania PomRisc jako narzędzie programowania zmian doskonalących systemy bezpieczeństwa i ich monitorowania*, BiTP Issue 4, 2008, s. 10–11.

⁴⁷ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 13–14.

⁴⁸ Tamże, s. 17.

zdarzenia oraz reagowanie, pozwalające na ograniczenie rozmiaru strat spowodowanych uwolnionym zagrożeniem.

Działania z obszaru doskonalenia reagowania powinny być realizowane w fazach zapobiegania, przeciwdziałania i odbudowy (w rozumieniu faz zarządzania kryzysowego), ale weryfikacja przyjętych rozwiązań technicznych, organizacyjnych, prawnych i finansowych dokonywana jest w fazie reagowania i powinna być mierzona. Wśród przykładowych wskaźników można wymienić wskaźniki czasowe, jakościowe i efektywnościowe⁴⁹.

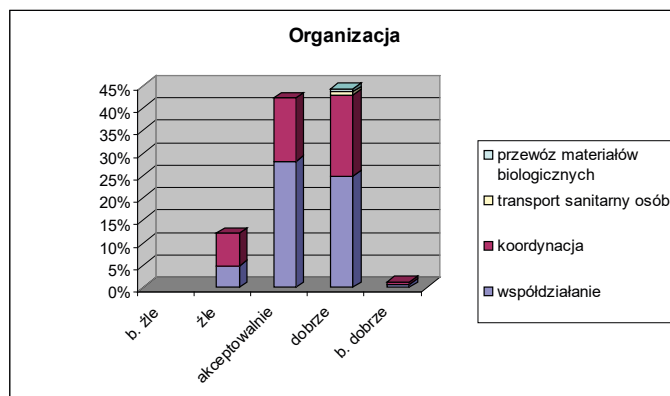
5.4.1. Diagnoza kluczowych elementów systemu RZSR WP

Badania dotyczyły czterech kluczowych kategorii, nazwanych kapitałem: świadomości strategicznej, technicznym, nietechnicznym i ludzkim. Podział na cztery rodzaje kapitału ułatwił formułowanie zadań służących doskonaleniu systemu reagowania w kontekście strategicznym, zaś zidentyfikowanie kluczowych elementów w ramach grup ułatwiło analizę danych i na ich podstawie formułowanie wniosków w kontekście słabych i silnych stron oraz kierunków doskonalenia systemu reagowania.

W ramach tych kategorii badaniu poddano elementy uporządkowane tematycznie w takich grupach jak np.: organizacja, zasoby ludzkie i informacyjne, infrastruktura, wyposażenie, lokalizacja placówek, szkolenie i edukacja⁵⁰.

Organizacja

Rys. 10 przedstawia sumaryczny rozkład takich elementów organizacji jak przewóz materiałów biologicznych, transport sanitarny, koordynacja i współdziałanie.



Rys. 10. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – organizacja

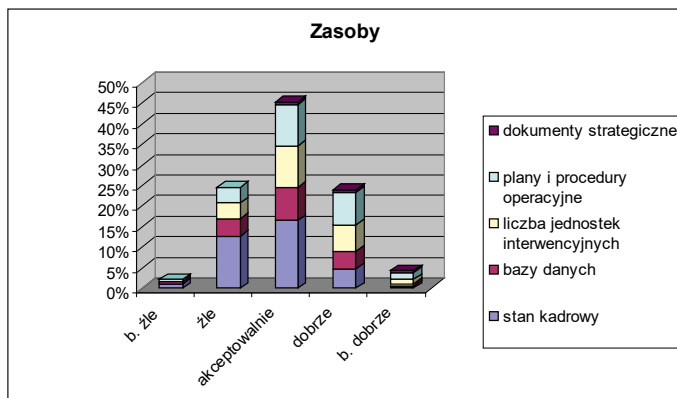
Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 13.

⁴⁹ Tamże, s. 13.

⁵⁰ Tamże, s. 17.

Zasoby

Rys. 11 obrazuje sumaryczny rozkład zasobów, takich jak dokumenty strategiczne, plany i procedury operacyjne, liczba jednostek interwencyjnych, bazy danych oraz stan kadrowy.

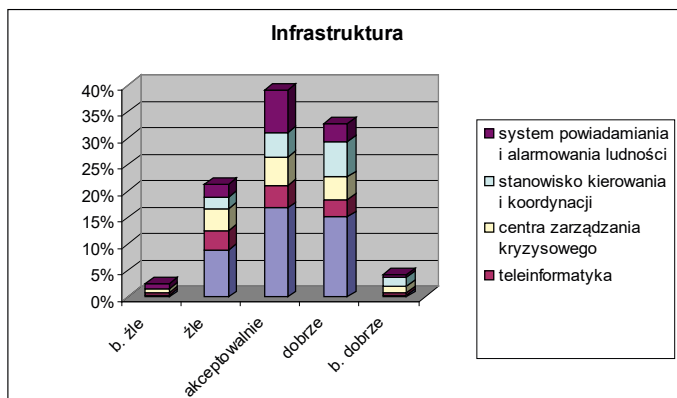


Rys. 11. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – zasoby

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 8.

Infrastruktura

Na rys. 12 przedstawiono sumaryczny rozkład elementów infrastruktury, takich jak system powiadamiania i alarmowania ludności, stanowiska kierowania i koordynacji, centra zarządzania kryzysowego, teleinformatyka oraz zintegrowana łączność.

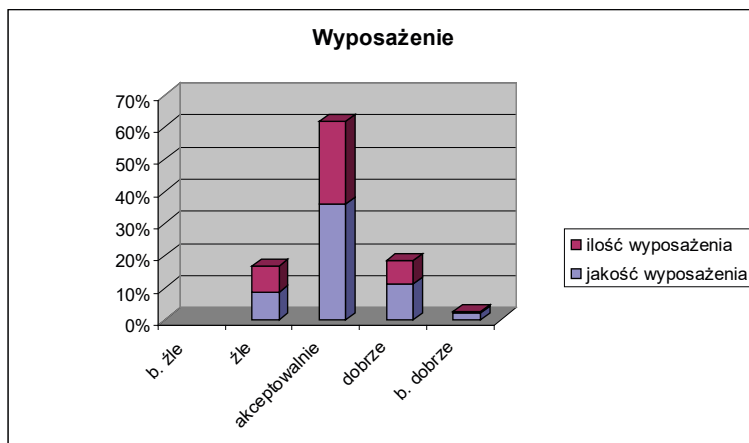


Rys. 12. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – infrastruktura

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 9.

Wyposażenie

Rys. 13 przedstawia sumaryczny rozkład cech wyposażenia: jego ilości i jakości.

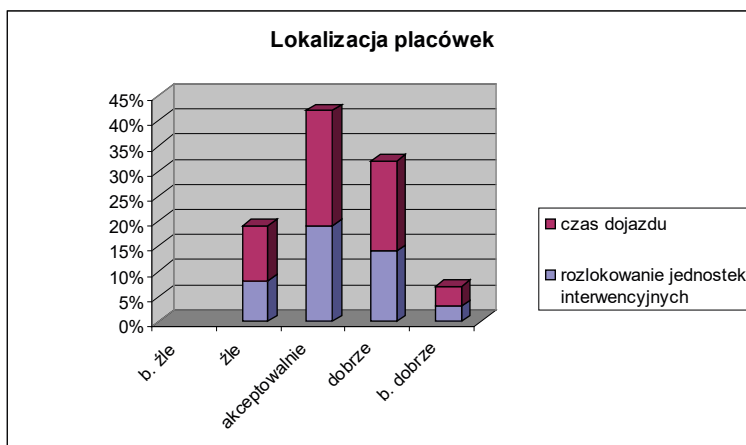


Rys. 13. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – wyposażenie

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 11.

Lokalizacja placówek

Na rys. 14 zobrazowany został sumaryczny rozkład elementów systemu określających lokalizację, czas dojazdu i rozlokowanie jednostek interwencyjnych.

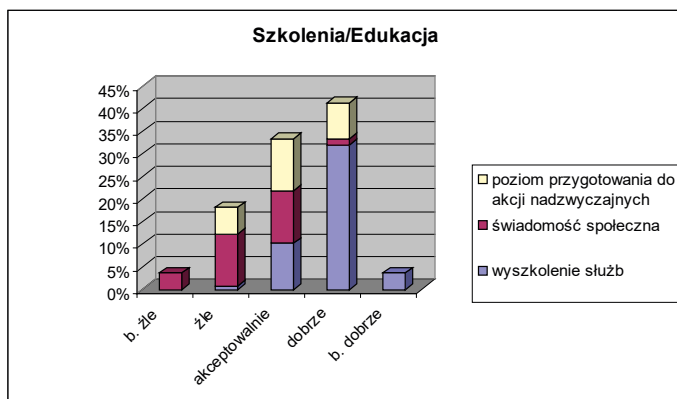


Rys. 14. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – lokalizacja placówek

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 12.

Szkolenie i edukacja

Rys. 15 pokazuje sumaryczny rozkład kolejnych elementów systemu, czyli cech szkolenia/edukacji.



Rys. 15. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – szkolenia/edukacja

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 14.

5.4.2. Analiza systemu

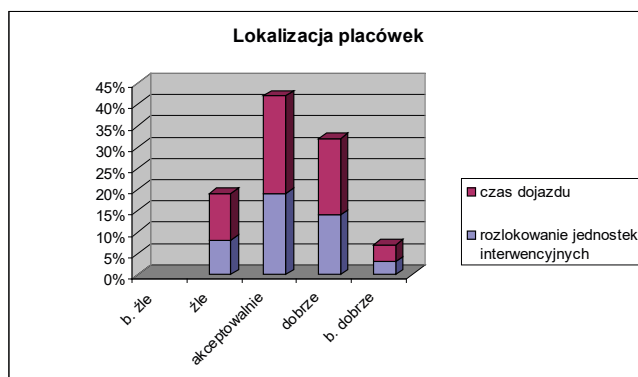
Zespół projektowy dokonał analizy w oparciu o materiały (formularze) nadesłane przez wybrane podmioty zaangażowane w tworzenie RZSR WP.

Na podstawie wypełnionych formularzy wraz z uzasadnieniem wyszczególnionych wcześniej potrzeb i określonych priorytetów dokonano zestawienia danych tabelarycznych w zależności od terytorialnego zasięgu działania danego podmiotu, według poniższej kolejności:

- podmioty prowadzące działalność w skali województwa,
- podmioty prowadzące działalność w skali powiatów,
- podmioty prowadzące działalność w skali miast na prawach powiatu.

Z analizy wynika, że do słabych ogniw systemu należy zaliczyć brak dodatkowych lokalizacji dla jednostek interwencyjnych. Najwięcej potrzeb w tym zakresie zgłosiły podmioty zajmujące się ratownictwem medycznym, Państwowa Straż Pożarna, ochotnicze straże pożarne oraz policja. Deficyt obejmujący potrzeby infrastrukturalne poszczególnych podmiotów dotyczył głównie prac remontowych i modernizacyjnych i innych działań mających na celu poprawę sytuacji w tym dużych potrzeb w zakresie wyposażenia. Podobnie przedstawia się sytuacja, jeżeli chodzi o potrzeby szkoleniowe w zakresie specjalistycznych kursów i szkoleń. Z punktu widzenia prawidłowego funkcjonowania RZSR WP potrzeby te zdaniem autorów są w pełni racjonalne⁵¹.

⁵¹ Tamże, s. 135–165.



Rys. 16. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – lokalizacja placówek

Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 107.

Bez względu na charakter systemu ważna jest świadomość wzorów, na jakich opiera się rozpatrywany system reagowania. Jest to szczególnie ważne w strukturach wielopodmiotowych, w odniesieniu do celu nadrzędnego, czyli misji i wizji, a więc docelowego obrazu systemu reagowania. Brak jednoznacznej misji i wizji oraz priorytetów systemu może prowadzić do rozpraszania energii podmiotów, a w skrajnych sytuacjach do działania niezgodnie z założonymi priorytetami systemu reagowania oraz potrzebami użytkownika końcowego. Warto dodać, że promowanie zorganizowanego i systemowego myślenia o bezpieczeństwie może prowadzić do wytworzenia się kultury bezpieczeństwa⁵², definiowanej w organizacji i zarządzaniu jako zestaw wartości i norm, które wytyczają określony sposób myślenia, mówienia i działania związanego z bezpieczeństwem⁵³.

W ramach badań dotyczących kapitału technicznego badaniu poddano elementy mające wpływ na:

- sprawne zarządzanie informacją oraz siłami i środkami systemu reagowania (stanowiska kierowania i koordynacji, centra zarządzania kryzysowego, teleinformatyka i zintegrowana łączność),
- poziom i jakość nasycenia systemu siłami i środkami (liczba jednostek ratowniczych oraz prawidłowość ich rozlokowania, ilość i jakość wyposażenia),
- system powiadamiania i alarmowania ludności.

Elementy nietechniczne podzielono na dwie zasadnicze grupy. Do pierwszej zaliczono elementy związane z prawidłowym działaniem własnym i współpracą z innymi podmiotami, np. dokumenty strategiczne, plany i procedury operacyjne,

⁵² Patrz: definicja na s. 111.

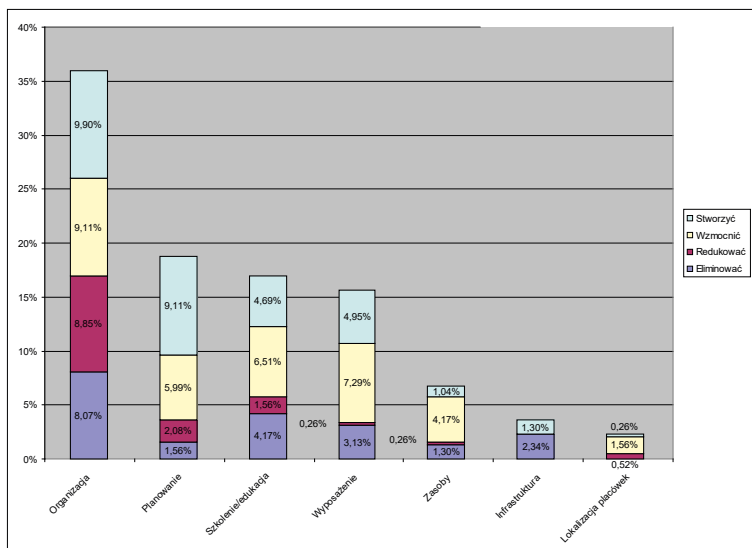
⁵³ E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt., s. 17.

bazy danych. Drugą grupę stanowiły elementy związane ze wspólnym działaniem, do których zaliczono koordynację i współdziałanie. Ostatnią zaś grupę tworzyły takie elementy jak czas dojazdu jednostek oraz poziom przygotowania do akcji.

W odniesieniu do kapitału ludzkiego analizowane były dokumenty dotyczące stanu kadrowego, wykszolenia służb i świadomości społecznej. Największe znaczenie w ocenie partnerstwa i komplementarności miały podmioty wchodzące w skład powiatów oraz funkcje, jakie mogą pełnić w razie wystąpienia określonych zagrożeń, a także podział tych podmiotów na komórki organizacyjne i wykonywane przez nie zadania. Rozpatrując poszczególne zagrożenia, można określić, jakie porozumienia należy zawrzeć, jakie podmioty w razie jakiego zdarzenia pełnią funkcję wiodącą i wspomagającą oraz jakie uzgodnienia pomiędzy poszczególnymi podmiotami na terenie powiatu zostały już zawarte lub jaka jest potrzeba ich wprowadzenia⁵⁴.

5.4.3. Docelowa (całościowa) wizja RZSR WP na podstawie dotychczasowych wniosków

Z badań jasno wynika, że elementem, który w ramach docelowej wizji systemu wymaga wprowadzenia najwięcej zmian, jest organizacja. Na następnych pozycjach, jeżeli chodzi o zakres koniecznych zmian, sklasyfikowane zostało planowanie, szkolenie/edukacja, wyposażenie, zasoby, infrastruktura i lokalizacja placówek. Graficzne przedstawienie zmian sugerowanych przez podmioty systemu przedstawia rys. 17⁵⁵.



Rys. 17. Wskaźnik oczekiwanej potrzeby zmian sugerowanych przez podmioty systemu
Źródło: D. Wróblewski (red.), *Koncepcja...*, dz. cyt., s. 273.

⁵⁴ D. Wróblewski (red.), *Koncepcja Funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 188–190.

⁵⁵ Tamże, s. 273.

Rekomendacje w kontekście potrzeb zarządzania ryzykiem na rozpatrywanym terenie⁵⁶

Rekomendacje w kontekście potrzeb zarządzania ryzykiem można sformułować na podstawie wniosków z diagnozy systemu reagowania oraz wniosków z badania kierunków i siły oczekiwanych zmian. Proces formułowania rekomendacji został podzielony na: sformułowanie rekomendacji podmiotowych, przedmiotowych, technicznych, nietechnicznych, kapitał ludzki oraz świadomości strategicznej.

Rekomendacje podmiotowe

Rekomendacje podmiotowe obejmują wytypowane podmioty tworzące i mogące tworzyć (rozbudowywać) system reagowania, jak np.:

- administracja rządowa,
- administracja samorządowa,
- organizacje pozarządowe,
- jednostki sektora finansów publicznych,
- przedsiębiorcy,
- związki i stowarzyszenia,
- Państwowa Straż Pożarna,
- ochotnicze straże pożarne,
- policja,
- Morska Służba Poszukiwania i Ratownictwa SAR,
- pogotowie ratunkowe, szpitale oraz SOR;
- straże miejskie i gminne,
- Straż Graniczna,
- inspektoraty ochrony środowiska,
- inspektoraty nadzoru budowlanego,
- inspektoraty weterynarii,
- stacje sanitarno-epidemiologiczne,
- Wodne Ochotnicze Pogotowie Ratunkowe,
- centra zarządzania kryzysowego.

Rekomendacje przedmiotowe

Rekomendacje przedmiotowe obejmują rozwiązania służące poprawie systemu reagowania, do których można zaliczyć:

1. Wyposażenie:
 - a) pojazdy i kontenery specjalistyczne,
 - b) statki powietrzne i pływające,
 - c) sprzęt/urządzenia, w tym pływające,
 - d) materiały,
 - e) środki;

⁵⁶ Patrz szerzej: E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda...*, dz. cyt.

2. Lokalizacja placówek:
 - a) nowe inwestycje,
 - b) adaptacja istniejących;
3. Infrastruktura:
 - a) remonty i modernizacja,
 - b) termomodernizacja,
 - c) teleinformatyka,
 - d) systemy powiadamiania i alarmowania ludności,
 - e) zintegrowana łączność;
4. Szkolenia/edukacja:
 - a) kursy i szkolenia specjalistyczne,
 - b) programy edukacyjne.

Rekomendacje działań technicznych i nietechnicznych

Wymienione rekomendacje techniczne i nietechniczne służą powiązaniu zidentyfikowanych i zhierarchizowanych ryzyk oraz wniosków z diagnozy systemu reagowania z konkretnymi działaniami zapobiegawczymi, korygującymi i doskonalącymi. Najczęściej działania techniczne wiążą się ze zwiększonymi nakładami finansowymi w porównaniu do nietechnicznych, opartych na rozwiązaniach i usprawnieniach organizacyjnych, które mogą mieć niższe koszty. Do rekomendacji działań nietechnicznych można zaliczyć kapitał ludzki oraz budowanie świadomości strategicznej⁵⁷.

Podział na rekomendacje techniczne i nietechniczne powstał z uwagi na fakt, że z rekomendowanymi działaniami wiążą się wymierne koszty finansowe.

„Aby dokonać wyboru odpowiedniego sposobu postępowania z ryzykiem, należy wziąć pod uwagę potencjalne koszty w kontekście uzyskiwanych użyteczności. Nie jest to jednak warunek konieczny. Norma zaleca wzięcie pod uwagę również tych ryzyk, które trudno jest uzasadnić, biorąc pod uwagę jedynie ekonomiczność wyboru. Należy rozpatrywać również tzw. ryzyka dotkliwe (o dużych, negatywnych następstwach, ale o niskim prawdopodobieństwie)”⁵⁸.

System monitorowania skuteczności zmian

Kolejnym etapem po wdrożeniu rekomendacji działań powinno być monitorowanie efektów działań i porównywanie ich z wcześniej przyjętymi założeniami. Zarówno monitorowanie⁵⁹, jak i przegląd⁶⁰ powinny być planowaną częścią procesu zarządzania ryzykiem w organizacji i obejmować regularne weryfikowanie lub nadzór wszystkich aspektów procesu zarządzania ryzykiem. Rezultaty monitoro-

⁵⁷ Patrz szerzej: tamże, s. 110.

⁵⁸ Patrz: część I, *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 1 *Zarządzanie ryzykiem według normy ISO 31000*, podrozdział 1.4. *Proces zarządzania ryzykiem*.

⁵⁹ Patrz: definicja na s. 113.

⁶⁰ Patrz: definicja na s. 113.

wania i przeglądu powinny być dokumentowane oraz raportowane na zewnątrz i wewnątrz, jeśli jest to uzasadnione. Zalecane jest także, aby były używane również jako dane wejściowe do przeglądu struktury ramowej zarządzania ryzykiem⁶¹.

Z tego względu warto ustalić zestaw wskaźników w kontekście sformułowanych celów i oczekiwanych efektów oraz rozważyć, kto będzie monitorował, co i kiedy będzie podlegało monitorowaniu oraz o jakie wskaźniki: dotychczasowe, nowe i wcześniej niemonitorowane. Najczęściej każdy z podmiotów uczestniczących w systemie ma własny system zbierania i analizowania danych, konstruowany dla zaspokajania własnych wewnętrznych potrzeb organizacyjnych, a nie służący monitorowaniu i diagnozowaniu systemu reagowania w kontekście potrzeb zarządzającego bezpieczeństwem na szczeblu powiatu czy województwa⁶².

Jeżeli przyjmiemy założenie, że systemy reagowania oraz systemy bezpieczeństwa powszechnego pełnią funkcję usługową, należy rozważyć wykorzystanie do wdrożenia strategii poprawy bezpieczeństwa narzędzia zwanego strategiczną kartą wyników. Strategiczna karta wyników służy do przekształcenia wizji i strategii organizacji w zestaw indywidualnych celów i wskaźników, zrozumiałych dla pracowników na wszystkich szczeblach organizacji oraz do monitorowania etapów realizacji rozpisanej w ten sposób strategii. Narzędzie to wykorzystywane jest głównie w biznesie i za jego pomocą m.in. monitoruje się wyniki w perspektywach: finansowej, klienta, procesów wewnętrznych oraz rozwoju. Warto dodać, że na świecie są przykłady zastosowania strategicznej karty wyników na potrzeby administracji publicznej⁶³.

Realizując temat badawczy pt. „Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego”, zespół autorski za pośrednictwem ankietowej formy wywiadu zgromadził materiał, którego największą wartością jest eksperckie podejście do problemu, uzyskane dzięki bezpośredniej współpracy z zaangażowanymi podmiotami i służbami. Materiał ten jest niezwykle cenny ze względu na wielopłaszczyznowe podejście do problemu, uzyskane poprzez zebranie opinii różnych służb i instytucji będących ekspertami w dziedzinie ratownictwa. Metodyka PomRisc jako narzędzie do oceny ryzyka, zawierające elementy przydatne w wytyczaniu kierunków rozwoju bezpieczeństwa, może być wykorzystywana w pracach zespołów zarządzania kryzysowego, budowania planów oraz zespołów zarówno badawczych, jak i praktyków.

⁶¹ Patrz: definicja na s. 105.

⁶² Patrz szerzej: E.W. Roguski, D. Wróblewski, *Diagnostyczna metoda oceny ryzyk i systemów reagowania PomRisc jako narzędzie programowania zmian doskonalących systemy bezpieczeństwa i ich monitorowania*, BiTP Issue 4, 2008, s. 25.

⁶³ Tamże.

6. NARZĘDZIA TELEINFORMATYCZNE WSPOMAGAJĄCE OCENĘ RYZYKA NA PRZYKŁADZIE OPROGRAMOWANIA RYSKO

Głównym efektem projektu badawczo-rozwojowego pt. „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne” finansowanego przez Narodowe Centrum Badań i Rozwoju (umowa nr DOBR/0016/R/ID2/2012/03), realizowanego w latach 2012–2015 jest oprogramowanie „RYSKO – wspomaganie tworzenia planów zarządzania kryzysowego”.

Oprogramowanie RYSKO jest samodzielnym oprogramowaniem wspomagającym tworzenie planów zarządzania kryzysowego dla gmin, powiatów i województw, umożliwiającym gromadzenie i zarządzanie informacjami niezbędnymi do sprawnego zarządzania zasobami, także podczas sytuacji kryzysowej. Uzyskane wyniki badań zostały zaimplementowane do modelu laboratoryjnego oprogramowania RYSKO, wykonanego w metodyce wytwarzania oprogramowania SCRUM. Zastosowana metoda unifikuje proces tworzenia planów, ułatwia wymianę informacji pomiędzy jednostkami administracyjnymi opracowującymi Plany Zarządzania Kryzysowego (PZK). Centralizacja rozwiązania (serwerowa wersja aplikacji dostępna dla użytkownika przez internet) unifikuje formę i treść generowanych w nim PZK.

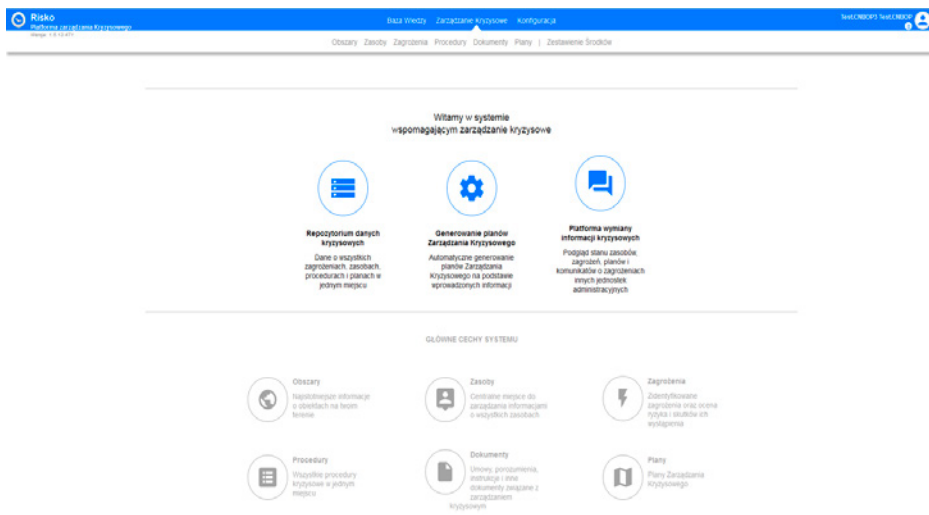
6.1. Oprogramowanie RYSKO

Za zasadnicze elementy architektury oprogramowania należy wskazać¹: system główny jako zbiór katalogów danych, w tym planów zarządzania kryzysowego; moduł mapowy służący do geolokalizacji informacji wprowadzonych w katalogach danych, będący również wspólną platformą do tworzenia przez użytkownika map zagrożeń i ryzyka; moduł plany będący centralnym miejscem tworzenia PZK,

¹ D. Wróblewski, M. Kędzierska, B. Poleć, *Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne*, w: *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, D. Majchrzak (red.), wyd. AON, Warszawa 2014, s. 373.

wykorzystując dane ze wszystkich katalogów systemu; moduł wydruków umożliwiający generowanie dokumentów PDF z dostępnych danych zebranych w katalogach; moduł administracyjny do zarządzania systemem oraz jego użytkownikami, słownikami referencyjnych danych i szablonami; moduł komunikacyjny pozwalający na generowanie komunikatów kryzysowych; moduł baza wiedzy stanowiący dodatkowe źródło aktualnych informacji na temat zarządzania kryzysowego w postaci ujednoliconego słownika pojęć oraz wykazu aktów prawnych. Ponadto w systemie zdefiniowano trzy główne role użytkowników:

1. Administratora – posiadającego uprawnienia umożliwiające konfigurację systemu oraz zarządzanie słownikami i użytkownikami na poziomie centralnym (przewidziano również rolę administratora regionalnego, który zarządzałby słownikami i użytkownikami na swoim obszarze odpowiedzialności).
2. Planisty – posiadającego uprawnienia do funkcjonalności systemu umożliwiających przygotowanie planu zarządzania kryzysowego dla obszaru, do którego jest przypisany dany użytkownik (dodatkowo możliwość podglądu planów zarządzania kryzysowego oraz podstawowych danych z innych jednostek administracyjnych).
3. Czytelnika – posiadającego uprawnienia do przeglądania planów zarządzania kryzysowego oraz podstawowych danych jednostek administracyjnych (rola umożliwiająca w wygodny i prosty sposób udostępniania planów zarządzania kryzysowego użytkownikom odpowiedzialnym za ich uzgadnianie)².



Rys. 1. Ekran startowy interfejsu użytkownika oprogramowania RISKO

Źródło: Zrzut ekranu z oprogramowania RISKO.

² D. Wróblewski, B. Połec, J. Maciak, *Informacyjne wspomaganie zarządzania kryzysowego – oprogramowanie „RISKO”*, w: *Organy administracji publicznej i instytucje w zarządzaniu kryzysowym*, G. Sobolewski, D. Majchrzak, Z. Sobejko (red.), wyd. AON, Warszawa 2016, s. 486–487.

Po zalogowaniu się do systemu ukazuje się ekran startowy oprogramowania RISKÓ z krótkim wprowadzeniem prezentującym przeznaczenie systemu, opisem jego głównych funkcjonalności oraz zawartości katalogów – głównych elementów pracy z aplikacją. Z tego miejsca można przejść do wszystkich komponentów oprogramowania: komunikatora (narzędzia do wysyłania i odbierania komunikatów), bazy wiedzy (zawierającej słownik pojęć i wykaz aktów prawnych), zarządzania kryzysowego (centralnego elementu systemu, w którym planista gromadzi w katalogach niezbędne dane o jednostce administracyjnej, jej zasobach, zidentyfikowanych zagrożeniach, procedurach i załącznikach) oraz konfiguracji (miejsca do administracji systemem)³.

6.2. KATALOG ZAGROŻENIA – MODUŁ OCENY RYZYKA „SKROJONY NA MIARĘ”

Katalog zagrożenia stanowi jeden z najbardziej rozbudowanych modułów aplikacji. Udostępnia funkcjonalność analizy zagrożeń występujących w obrębie danej jednostki administracyjnej kraju⁴. Moduł ten wspiera analityka w ocenie zagrożeń i ryzyka występujących na jego obszarze. Bazując na wspólnym słowniku zagrożeń, analityk może w systemie stworzyć jego ogólną charakterystykę. Pozwala to jednocześnie na definiowanie siatek bezpieczeństwa, czy określanie zadań związanych z monitorowaniem danego zagrożenia, z wykorzystaniem podmiotów znajdujących się w katalogu zasobów. Wszystkie te informacje można też zobrazować i zobaczyć na podkładzie mapowym w uniwersalnym module mapowym⁵.

Podstawą analizy zagrożeń w systemie są zdefiniowane scenariusze. Scenariusze zagrożeń posiadają wbudowaną ocenę ryzyka zawierającą informacje na temat prawdopodobieństwa wystąpienia zagrożenia oraz przewidywanych skutków. Poza informacją tekstową, udostępniona jest zagregowana informacja geograficzna w postaci przewidywanych stref zagrożeń wystąpienia zdarzenia. Poszczególne mapy mogą zostać wyeksportowane do formatu plików graficznych, a następnie załączone do planu zarządzania kryzysowego⁶.

Moduł posiada widok zdefiniowanych zagrożeń w postaci drzewa według jednostki administracyjnej, typu zagrożenia i scenariusza lub poziomu ryzyka. W zakresie katalogu zagrożeń, występuje również widok siatki bezpieczeństwa

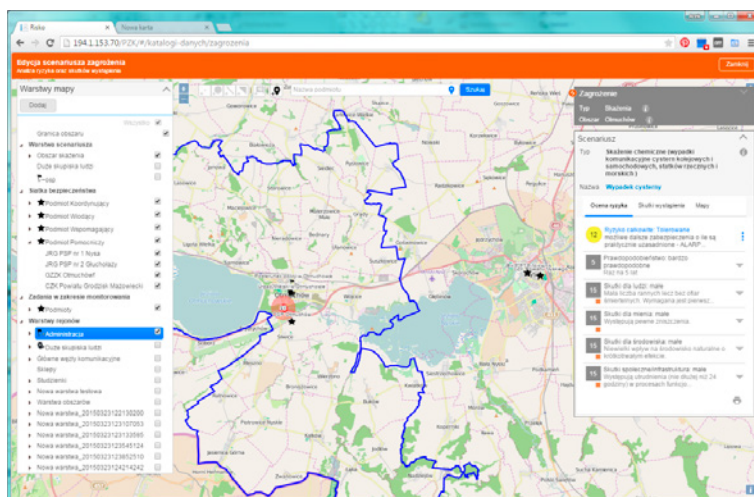
³ D. Wróblewski, B. Połeć, J. Maciak, *Informatyczne wspomaganie...*, dz. cyt., s. 490.

⁴ Tamże, s. 492.

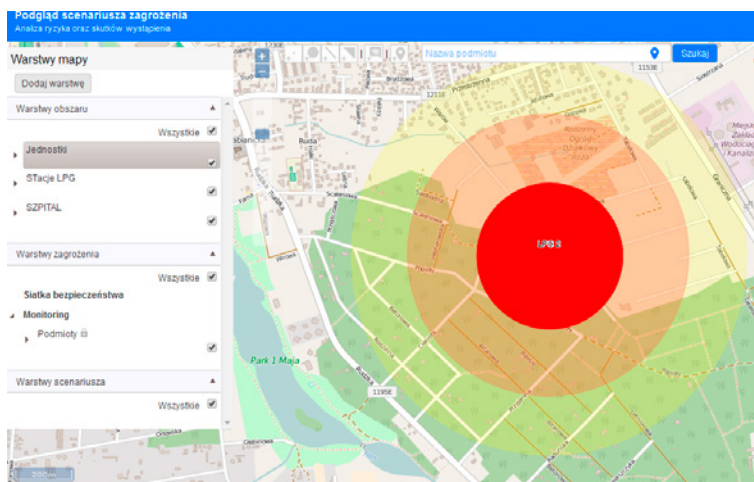
⁵ A. Olszewski, B. Krzywicki, *Budowa systemu informatycznego wspierającego przygotowywanie planów zarządzania kryzysowego RISKÓ*, w: *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, D. Wróblewski (red.), wyd. CNBOP-PIB, Józefów 2015, s. 90.

⁶ Zadanie VI.5 Opracowanie metodyk analizy i oceny dla zagrożeń i ryzyka. Projekt badawczo-rozwojowy pt. „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne” – koordynator: Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy.

definiującej podział ról podmiotów lub grup podmiotów reagujących na dane zagrożenie. Możliwe jest również definiowanie oraz przeglądanie zadań i obowiązków podmiotu w ramach monitorowania zagrożenia. Dodatkowym elementem jest matryca funkcjonalna tworzona automatycznie na podstawie Procedur Reagowania Kryzysowego, wykazująca role podmiotów podczas poszczególnych kroków procedury dla danego zagrożenia⁷.

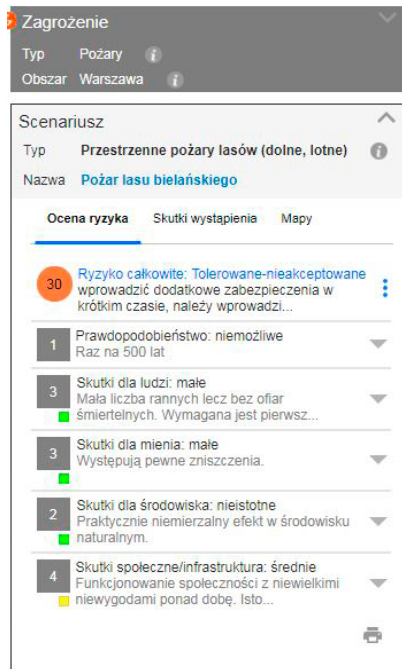


Rys. 2. Moduł Zagrożeń – ocena ryzyka
Źródło: Zrzut ekranu z oprogramowania RYSKO.



Rys. 3. Moduł Zagrożeń – wizualizacja ryzyka
Źródło: Zrzut ekranu z oprogramowania RYSKO.

⁷ D. Wróblewski, B. Połęć, J. Maciak, *Informatyczne wspomaganie...*, dz. cyt., s. 493.



Rys. 4. Ekran oceny ryzyka scenariusza
Źródło: Zrzut ekranu z oprogramowania RYSKO.

Następstwem opisu zagrożenia jest ocena ryzyka wystąpienia jednego lub wielu scenariuszy z nim związanych. Ocenę ryzyka dla scenariusza zagrożenia może z powodzeniem wykonać użytkownik na każdym poziomie administracyjnym. System RYSKO wspiera użytkownika w takiej ocenie, wykorzystując jednolitą macierz ryzyka. Wystarczy kliknąć na jeden z wierszy z opisami prawdopodobieństwa i skutków. Aby wyliczyć ryzyko całkowite należy wypełnić prawdopodobieństwo i wszystkie kategorie skutków (dla ludzi, mienia, środowiska oraz infrastruktury/ społeczne). Po kliknięciu pojawia się okno do oceny ich wartości w sześciostopniowej skali. Aby ustalić poziom ryzyka należy wypełnić wszystkie elementy. System nie szacuje automatycznie poziomów skutków. Niemniej każdy wskazywany poziom skutków ma swoją opisową definicję pozwalającą różnym użytkownikom przygotowującym plany zachować wspólny punkt odniesienia i ustalać poziom skutków, będący w zgodności do wszystkich planów. Przyjęto w projekcie, że gdy poziom ryzyka w kategorii „zagrożeni ludzie” jest nieakceptowalny to ryzyko całkowite także powinno być nieakceptowalne. Po określeniu ryzyka całkowitego dla scenariusza zagrożenia istnieje możliwość ręcznej zmiany poziomu ryzyka za pomocą suwaka do ręcznego ustawienia poziomu ryzyka całkowitego. Jest to zasadne na przykład, gdy dany użytkownik dokonał we własnym zakresie eksperckiej oceny ryzyka⁸.

⁸ D. Wróblewski, B. Połec, J. Maciak, *Informatyczne wspomaganie...*, dz. cyt., s. 493–494.

Tabela 1. Jakościowy opis kategorii prawdopodobieństwa

Charakterystyka	Opis	Częstotliwość
1 Zdarzenia prawie pewne	Oczekuje się, że wystąpią w większości okoliczności i/lub są bardzo dobrze udokumentowane i/lub funkcjonują wśród mieszkańców i przekazywane są w formie ustnej. Mogą wystąpić raz na rok lub częściej.	Raz na 1 rok
2 Zdarzenia bardzo prawdopodobne	Oczekuje się, że wystąpią w pewnych znanych okolicznościach i/lub występują systematycznie oraz są dobrze udokumentowane, przekazywane w formie ustnej i/lub występuje znaczna szansa ich wystąpienia ze względu na znaną przyczynę, istniejące urządzenia lub procesy. Mogą wystąpić raz na pięć lat.	Raz na 5 lat
3 Prawdopodobne	Oczekuje się, że mogą wystąpić w niektórych okolicznościach znanych lub nieznanach. Nie mają dobrego udokumentowania. Funkcjonują w pamięci społecznej i są przekazywane w formie ustnej. Ich występowanie związane może być z awarią urządzeń lub/i procesów. Mogą wystąpić raz na dwadzieścia lat.	Raz na 20 lat
4 Zdarzenia mało prawdopodobne	Oczekuje się, że mogą wystąpić w określonym czasie na ogół losowo, są udokumentowane lub/i funkcjonujące w pamięci społecznej, szczątkowo przekazywane w formie ustnej i/lub występuje ich mała liczba i/lub znane są przyczyny istnienia szansy ich wystąpienia, czy też zidentyfikowane są urządzenia procesy powodujące, że zdarzenia te w ogóle mogą wystąpić. Zdarzenia mogą wystąpić raz na pięćdziesiąt lat.	Raz na 50 lat
5 Zdarzenia bardzo rzadkie	Nie oczekuje się, że mogą wystąpić i/lub nie istnieje dokumentacja z nimi związana; nie funkcjonują w przekazach ludzi i/lub zdarzenia te nie wystąpiły w podobnych społecznościach, organizacjach, urządzeniach, procesach i/lub istnieje mała szansa, przyczyna, czy też inne okoliczności, aby zdarzenia mogły wystąpić. Mogą one wystąpić raz na sto lat.	Raz na 100 lat
6 Zdarzenia niemożliwe	Nie oczekuje się, że zdarzenia te mogą wystąpić. Ich wystąpienie może mieć miejsce tylko w wyjątkowych okolicznościach (np. scenariusz najgorszego przypadku). Mogą one wystąpić raz na pięćset lub więcej lat.	Raz na 500 lat

Źródło: Opracowanie zespołu SGSP w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

Tabela 2. Jakościowa ocena skutków – zagrożeni ludzie

Charakterystyka skutków	Opis
A Zaniedbywalne	Dyskomfort. Brak przemieszczeń ludzi
B Niestotne	Brak ofiar śmiertelnych i rannych. Mała liczba ludzi przemieszczonych na krótki okres. Brak lub niewielka liczba osób wymagających pomocy (nie dotyczy pomocy finansowej lub materialnej)
C Małe	Mała liczba rannych, bez ofiar śmiertelnych. Wymagana pierwsza pomoc. Mają miejsce pewne przemieszczenia ludzi (na mniej niż 24 godziny). Część ludzi potrzebuje pomocy
D Średnie	Potrzebna pomoc medyczna ofiarom, bez ofiar śmiertelnych. Niektóre ofiary wymagają hospitalizacji. Ewakuacja ludzi do wyznaczonych miejsc z możliwością powrotu w ciągu 24 godzin. Udzielanie pomocy ludziom w miejscu zbiórki ewakuowanych
E Duże	Ofiary śmiertelne lub/i poważne obrażenia dużej liczby osób, dużo osób hospitalizowanych, duża liczba osób przemieszczonych (na więcej niż 24 godziny). Występuje potrzeba szczególnych zasobów do pomocy ludziom i usuwania zniszczeń
F Katastrofalne	Duża liczba ofiar śmiertelnych. Duża liczba poważnie rannych. Duża liczba hospitalizowanych. Ogólne i długotrwałe przemieszczenie ludności

Źródło: Tamże.

Tabela 3. Jakościowa ocena skutków – zagrożone środowisko

Charakterystyka skutków	Opis
A Zaniedbywalne	Brak wpływu na środowisko
B Nieistotne	Praktycznie niemierzalny efekt w środowisku naturalnym
C Małe	Niewielki wpływ na środowisko naturalne o krótkotrwałym efekcie
D Średnie	Większe skutki w środowisku naturalnym lecz krótkotrwałe lub małe skutki o długotrwałym efekcie
E Duże	Długotrwałe efekty w środowisku naturalnym
F Katastrofalne	Duży wpływ na środowisko naturalne i /lub stałe zniszczenia

Źródło: Tamże.

Tabela 4. Jakościowa ocena skutków – zagrożone mienie

Charakterystyka skutków	Opis
A Zaniedbywalne	Brak jakichkolwiek zniszczeń
B Nieistotne	Niewielkie praktycznie bez znaczenia zniszczenia
C Małe	Występują pewne zniszczenia
D Średnie	Zidentyfikowanie zniszczeń, które wymagają rutynowej naprawy
E Duże	Występuje potrzeba szczególnych zasobów do pomocy ludziom i do usuwania zniszczeń
F Katastrofalne	Rozległe zniszczenia. Niemożność funkcjonowania społeczności bez istotnej zewnętrznej pomocy

Źródło: Tamże.

Tabela 5. Jakościowa ocena skutków – skutki społeczne, w tym infrastruktura

Charakterystyka skutków	Opis
A Zaniedbywalne	Niezakłócone funkcjonowanie ludzi lub tylko w niewielkim stopniu. Niezakłócone procesy
B Nieistotne	Brak wpływu lub bardzo niewielki wpływ na funkcjonowanie społeczności lokalnej. Niewielkie straty finansowe
C Małe	Występują utrudnienia (nie dłużej niż 24 godziny) w procesach funkcjonowania. Niewielkie straty finansowe
D Średnie	Funkcjonowanie społeczności z niewielkimi niewygodami ponad dobę. Istotnie odczuwalne straty finansowe bez pomocy zewnętrznej
E Duże	Społeczność częściowo niefunkcjonująca, niektóre służby są nieosiągalne. Duże straty finansowe – potrzebna pomoc z zewnątrz
F Katastrofalne	Niemożliwość funkcjonowania społeczności bez istotnej zewnętrznej pomocy. Potrzebna zewnętrzna pomoc finansowa w znacznych rozmiarach

Źródło: Tamże.

Tabela 6. Matryca ryzyka

Skutki Prawdopodobieństwo	1	2	3	4	5	6
	Zaniedbywalne	Nieistotne	Małe	Średnie	Duże	Katastrofalne
6 Zdarzenia prawie pewne	6	12	18	24	30	36
5 Zdarzenia bardzo prawdopodobne	5	10	15	20	25	30
4 Prawdopodobne	4	8	12	16	20	24
3 Zdarzenia mało prawdopodobne	3	6	9	12	15	18
2 Zdarzenia bardzo rzadkie	2	4	6	8	10	12
1 Zdarzenia niemożliwe	1	2	3	4	5	6

Źródło: Tamże.

7. MOŻLIWOŚCI WYKORZYSTANIA BADAŃ PRZYCZYN POŻARÓW W ZARZĄDZANIU RYZYKIEM POŻAROWYM W POLSCE

W Polsce kwestie związane z niską jakością dochodzeń popożarowych oraz niewykorzystaniem możliwości prewencyjnych (m.in. rezerwy w zakresie udoskonalenia standardu ustalania przyczyn pożarów) były podnoszone wielokrotnie, m.in. podczas poznańskich konferencji „Research into the causes of fire”. Były również prezentowane na posiedzeniu komisji sejmowej MSWiA, jednak nie przyniosły oczekiwanych rezultatów.

To właśnie powyżej wskazana przyczyna oraz szerzej wymienione w rozdziale problemy były głównym powodem rozpoczęcia prac nad projektem pt. „Opracowanie systemowych rozwiązań wspomagających prowadzenie dochodzeń popożarowych wykorzystujących nowoczesne technologie, w tym narzędzia techniczne i informatyczne” finansowanego przez NCBR, którego celem było rozpoznanie przyczyn problemów występujących w obszarze postępowań prowadzonych w sprawach o pożary, a także opracowanie innowacyjnego systemu organizacji dochodzeń popożarowych i narzędzi technicznych oraz informatycznych zwiększających ich efektywność. Gestorem projektu była Komenda Główna Państwowej Straży Pożarnej. Główne zadania zaplanowane do realizacji i wykonane w ramach projektu to:

1. Analiza ekonomiczno-funkcjonalna dochodzeń popożarowych w Polsce obejmująca:
 - a) charakterystykę obecnego systemu dochodzeń popożarowych oraz ustalania przyczyn pożarów, ich rozprzestrzeniania się oraz sprawców pożarów (podmioty oraz zakres realizowanych zadań),
 - b) analizę sprawności (skuteczności) systemu dochodzeń popożarowych oraz ustalania przyczyn pożarów, ich rozprzestrzeniania się oraz sprawców pożarów poprzez badanie organizacji dochodzeń prowadzonych w sprawach o pożary, badanie skuteczności ujawniania sprawców pożarów oraz ich karania,
 - c) analizę jakości wstępnego ustalania przyczyn pożarów przez państwową straż pożarną i zakresu wykorzystania informacji o wstępnie ustalonej

- przyczynie pożaru w postępowaniu wyjaśniającym i przygotowawczym prowadzonym przez uprawniony organ procesowy,
- d) analizę kosztów postępowań prowadzonych w sprawach o pożary.
2. Rozpoznanie głównych problemów występujących w obszarze dochodzeń popożarowych w Polsce (przygotowanie merytoryczne, zaplecze organizacyjno-techniczne, skuteczność prowadzonych postępowań etc.), w szczególności:
 - a) zbadanie przygotowania organów procesowych pod względem merytorycznym do prowadzenia czynności związanych z ustaleniem przyczyny pożaru,
 - b) analiza środków i zaplecza technicznego służącego organom procesowym do ustalania przyczyn pożarów (zidentyfikowanie braków),
 - c) analiza dochodzeń pożarowych pod kątem skuteczności oraz sprawności funkcjonowania (współpraca podmiotów, formy pracy, czas od powstania zdarzenia do przeprowadzenia procesowych oględzin z udziałem technika kryminalistyki oraz biegłego z listy SO etc.),
 - d) rozpoznanie systemu przygotowywania osób prowadzących dochodzenia w sprawach o pożary oraz ustalających przyczyny ich powstania i rozprzestrzenienia się.
 3. Rozpoznanie rozwiązań w zakresie dochodzeń popożarowych funkcjonujących w wybranych państwach UE (Niemcy, Czechy, Słowacja, Bułgaria, Szwecja, Wielka Brytania, Holandia, Włochy).
 4. Przygotowanie publikacji pt. *Czerwona księga pożarów*, ukazującej społeczno-ekonomiczne koszty pożarów.
 5. Opracowanie innowacyjnych narzędzi podnoszących efektywność dochodzeń pożarowych, w tym w szczególności:
 - a) stworzenie prostej w obsłudze aplikacji na urządzenia przenośne usprawniające odwzorowanie pogorzeliska, aplikacja powinna dawać możliwość wykorzystania nowoczesnych narzędzi multimedialnych takich jak wbudowany aparat cyfrowy, notatka głosowa itp.,
 - b) rozpoczęcie budowy ogólnodostępnej bazy z danymi wejściowymi niezbędnymi do prowadzenia symulacji pożarowych (właściwości materiałów palnych),
 - c) opracowanie kodu numerycznego w technologii CFD (ang. *Computational Fluid Dynamics*) do symulacji rozwoju pożarów w pomieszczeniach przy standardowych założeniach przewidzianych w programie.
 6. Opracowanie koncepcji poligonowego stanowiska do szkolenia osób zaangażowanych w proces ustalania przyczyn pożarów wraz z wykonaniem wybranych stanowisk, w tym:
 - a) rozpoznanie funkcjonalności i efektywności istniejących na świecie rozwiązań służących do szkolenia osób zaangażowanych w proces ustalania przyczyn pożarów;

- b) opracowanie własnej koncepcji stanowiska poligonowego, określenie celów przewidzianych do realizacji;
 - c) opracowanie propozycji programów oraz scenariuszy do zajęć praktycznych na stanowisku poligonowym pozwalających na zapoznanie osób uczestniczących w szkoleniu z metodyką prowadzenia oględzin miejsca pożaru pod kątem:
 - analizy śladów rozwoju pożaru,
 - ustalenia miejsca źródła pożaru,
 - określenia przyczyny powstania pożaru,
 - ustalenia przyczyny rozprzestrzenienia się pożaru,
 - metod prowadzenia oględzin, z uwzględnieniem ochrony śladów i dowodów przed przypadkowym zniszczeniem,
 - sposobów zabezpieczenia dowodów z miejsca pożaru,
 - podstaw dokumentowania miejsca pożaru,
 - zarządzania pracą na pogorzeli (organizacja oględzin, współpraca zaangażowanych podmiotów, bezpieczeństwo podczas oględzin etc.);
 - d) wykonanie wybranego stanowiska poligonowego.
7. Przygotowanie poradnika z zakresu dochodzeń pożarowych dla biegłych i ekspertów.
 8. Opracowanie koncepcji rozwiązania systemowego opartego na partnerskim podejściu w procesie ustalania przyczyn pożarów oraz ujawniania ich sprawców.

Projekt realizowany był w okresie od grudnia 2013 r. do grudnia 2016 r. przez konsorcjum w składzie:

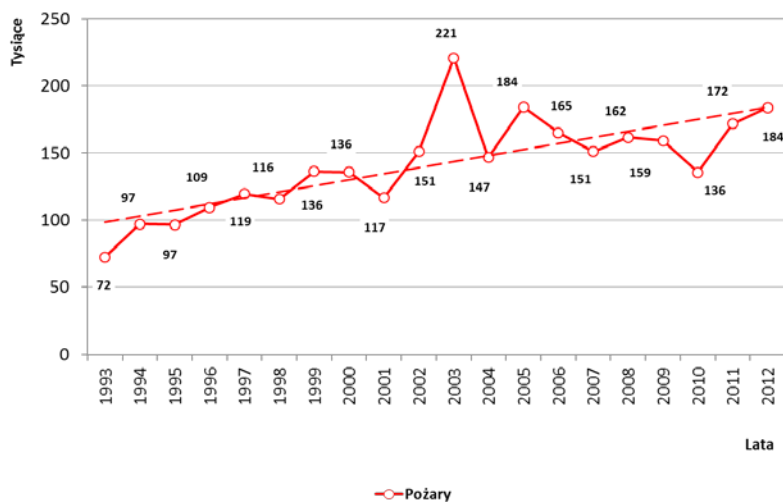
- Szkoła Główna Służby Pożarniczej,
- Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy,
- Centralne Laboratorium Kryminalistyczne Policji – Instytut Badawczy,
- Szkoła Aspirantów Państwowej Straży Pożarnej w Poznaniu,
- Przedsiębiorstwo CYBID Sp. j. w Krakowie.

7.1. Społeczno-ekonomiczne koszty pożarów jako bodziec rozwoju zarządzania ryzykiem pożarowym

Pożary – mimo niekwestionowanych osiągnięć nauki i techniki na przestrzeni ostatnich dwóch wieków – nadal znajdują się w grupie czterech nieopanowanych przez człowieka żywiołów. Szacuje się, że każdego roku na świecie powstaje ok. 7 mln pożarów, w których ginie przeciętnie 60–70 tys. ludzi, a kolejnych 300–500 tys. odnosi różnego rodzaju obrażenia. Z danych opublikowanych przez Centre of World Fire Statistics (CWFS) wynika, że w ubiegłym stuleciu koszt pożarów w grupie 63

objętych badaniem państw świata (46% ludności Ziemi) wyniósł przeciętnie 0,3% PKB, a kolejne 0,7% PKB pochłaniały wydatki na utrzymanie jednostek straży pożarnej, techniczne środki zabezpieczeń przeciwpożarowych, ubezpieczenia oraz edukację i szkolenia, rozwój badań naukowych w tym obszarze. Według prognoz CWFS w XXI wieku koszt pożarów osiągnie poziom ok. 0,4-0,45% PKB, a całkowity koszt ponoszony w związku z pożarami oraz utrzymaniem ochrony przeciwpożarowej może dojść nawet do ok. 1,5-1,7% PKB. Główne problemy związane z zagrożeniami pożarowymi dzięki osiągnięciom nauki będą mogły być skutecznie rozwiązane dopiero w kolejnych stuleciach.

W Polsce w latach w 2003–2012 rejestrowano około 150–180 tys. pożarów rocznie (rys. 1). Z tego przeciętnie 92–94% to pożary małe, o powierzchni nieprzekraczającej 70 m², 5–7% – pożary średnie, o powierzchni w przedziale 71–300 m² i ok. 0,5% – pożary duże (301 do 1000 m²) i bardzo duże (pow. 1000 m²) liczone razem. Blisko połowa wszystkich pożarów powstawała w grupie tzw. innych obiektów, ok. 20% pożarów – w obiektach mieszkalnych, kolejne 20% – w rolnictwie i uprawach, na terenach leśnych oraz w środkach transportu – po ok. 5% pożarów, w obiektach produkcyjnych i magazynowych – ok. 3% i obiektach użyteczności publicznej – ok. 2% pożarów.

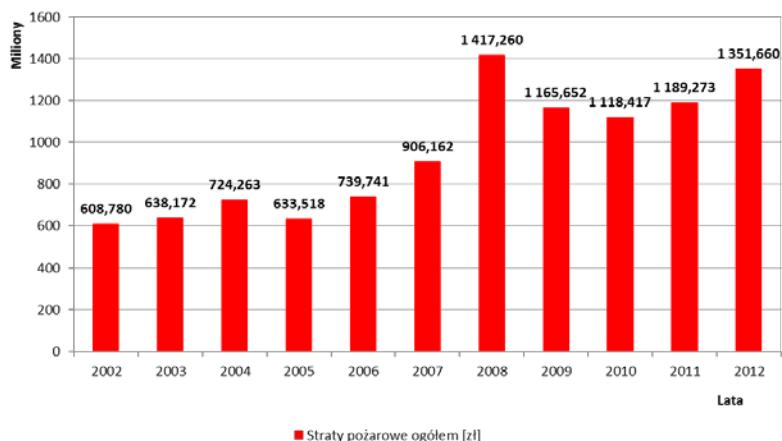


Rys. 1. Pożary w Polsce ogółem w latach 1993–2012

Źródło: Opracowanie własne na podstawie: Komenda Główna Państwowej Straży Pożarnej, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 1993–2012*, Warszawa 1994–2013.

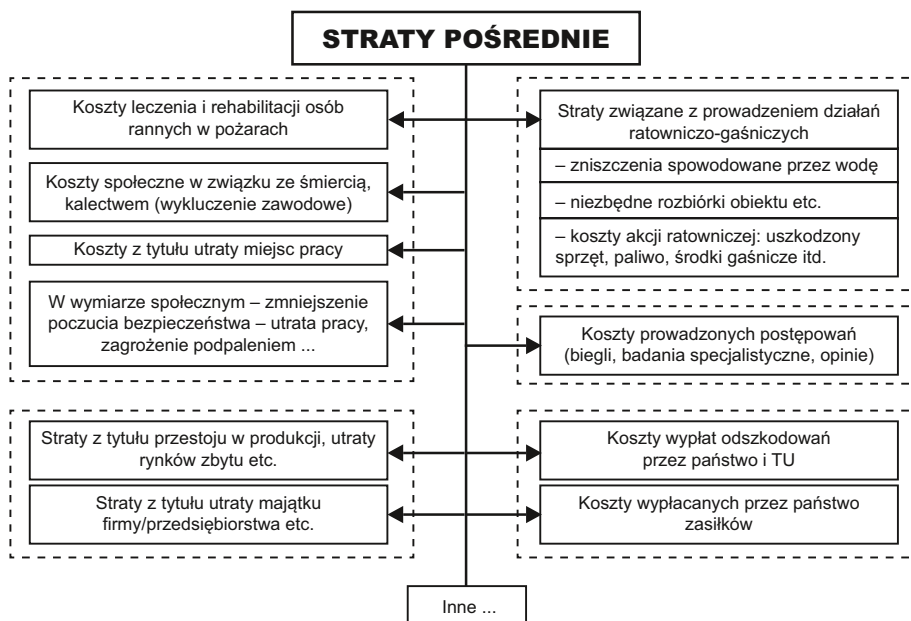
Wartość mienia, które ulegało spaleniowi w pożarach w tym samym okresie (tzw. straty bezpośrednie), mieściła się w przedziale od ok. 1 do 1,4 mld zł rocznie (rys. 2), ze średnią stratą przypadającą na jeden pożar wynoszącą ok. 6 tys. zł.

Straty pośrednie (rys. 3), nieobjęte ewidencją, nie są znane. Ocenia się, że mogą one stanowić wielokrotność strat bezpośrednich, zwłaszcza w grupie pożarów średnich, dużych i bardzo dużych.



Rys. 2. Straty bezpośrednie w pożarach w latach 2002–2012

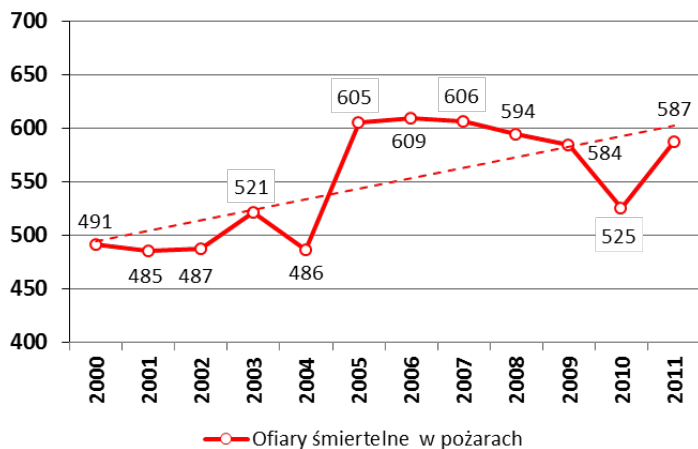
Źródło: Opracowanie własne na podstawie: Komenda Główna Państwowej Straży Pożarnej, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2002–2012*, dz. cyt.



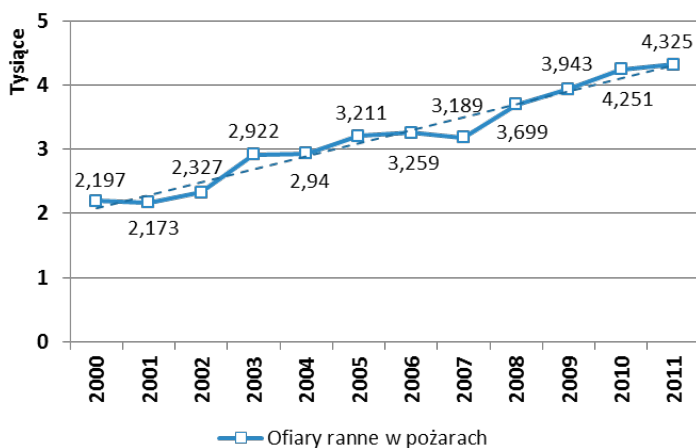
Rys. 3. Straty pośrednie w pożarach

Źródło: Opracowanie własne.

W Polsce w ostatnich latach w pożarach ginie każdego roku przeciętnie 540–580 osób (rys. 4), a ok. 4,0–4,3 tys. odnosi obrażenia (rys. 5). Koszty ponoszone przez państwo w związku ze śmiercią człowieka oszacowano na kwotę ok. 1 mln euro. Koszty leczenia osób rannych w pożarach nie zostały jak do tej pory oszacowane z uwagi na brak odrębnych zestawień w odniesieniu do ofiar pożarów. Z danych Centrum Leczenia Oparzeń w Siemianowicach Śląskich, gdzie hospitalizowane są ofiary z najcięższymi urazami termicznymi, wynika, że średni koszt leczenia pacjentów oparzonych to ok. 31 tys. zł, natomiast rzeczywiste koszty oscylują w przedziale od 4 do 100 tys. zł.



Rys. 4. Liczba ofiar śmiertelnych w pożarach w latach 2000–2011 (w tym ratownicy)
 Źródło: Opracowanie własne na podstawie: Komenda Główna Państwowej Straży Pożarnej, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2000–2011*, dz. cyt.



Rys. 5. Liczba ofiar rannych w pożarach w latach 2000–2011 (w tym ratownicy)
 Źródło: Opracowanie własne na podstawie: Komenda Główna Państwowej Straży Pożarnej, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2000–2011*, dz. cyt.

W Polsce w pożarach ginie ok. 15 osób w przeliczeniu na 1 mln mieszkańców, ok. 112 osób na 1 mln odnosi obrażenia (dane za lata 2010–2012). Wskaźnik ofiar śmiertelnych jest jednym z najwyższych w grupie 63 państw analizowanych przez Centre of Fire Statistics w okresie 1993–2002 oraz w 2006 r. grupie 30 analizowanych państwach świata. Podobnie wygląda sytuacja w odniesieniu do ofiar rannych.

7.2. Zarządzanie ryzykiem pożarowym w aspekcie teoretycznym i praktycznym

Ryzyko pożarowe można zdefiniować jako kombinację prawdopodobieństwa wystąpienia pożaru oraz jego skutków. Ryzyko jest codziennym elementem życia człowieka i podejmowanych przez niego wyborów. Identyfikacja ryzyka pożarowego, analiza prawdopodobieństwa jego wystąpienia, ewaluacja ryzyka stanowią podstawowe kroki w procesie zarządzania ryzykiem, którego efektem jest planowanie przedsięwzięć ukierunkowanych na obniżenie ryzyka do akceptowalnego poziomu (rys. 6).



Rys. 6. Zarządzanie ryzykiem pożarowym

Źródło: Opracowanie własne.

Zarządzanie ryzykiem pożarowym odbywa się na każdym poziomie funkcjonowania państwa i jego obywateli. W przemyśle w ramach ogólnej oceny ryzyka związanego z realizowanymi procesami technologicznymi jednym z ważniejszych ryzyk uwzględnianych przez specjalistów ds. bezpieczeństwa jest właśnie ryzyko wystąpienia zdarzenia krytycznego, w którym pożar rozpatrywany jest jako zdarzenie pierwotne lub wtórne (rys. 7). Scenariusze zdarzeń pożarowych oraz ich wpływ na funkcjonowanie firmy uwzględniane są w planach zapewnienia ciągłości funkcjonowania firmy – Business Continuity Planning (BCP) oraz analizach wpływu na efekt finansowy – Business Impact Analysis (BIA).

OCENA RYZYKA POŻAROWEGO

OBIEKT	PROCESY	CZŁOWIEK	UWARUNKOWANIA ZEWN.
<ul style="list-style-type: none"> - Czy obiekt spełnia wymogi aktualnych przepisów związanych z bezpieczeństwem? - Czy konstrukcja obiektu odpowiada funkcjom w nim realizowanym? - Czy obiekt posiada systemy wczesnego wykrywania zagrożeń i alarmowania o zagrożeniach? - Czy obiekt przygotowany jest do samoobrony do czasu interwencji specjalistycznych służb? - Czy obiekt wyposażony jest w podręczny sprzęt gaśniczy? - ... 	<ul style="list-style-type: none"> - Jakie materiały niebezpiecz. pożarowo stosowane są w procesach? - W jaki sposób są przemieszczane, składowane? - Jakie ilości materiałów niebezpiecznych pożarowo znajdują się na stanowiskach pracy? - Czy realizowane procesy były źródłem zagrożeń pożarowych? - Jeśli tak, to jaką mamy wiedzę o tych zdarzeniach i zapobieganiu ich wystąpieniu - ... 	<ul style="list-style-type: none"> - Czy wszyscy pracownicy są przeszkoleni z ogólnych zasad bezpieczeństwa pożarowego w zakładzie/obiekcie oraz na stanowiskach pracy? - Czy pracownicy przestrzegają ustanowionych norm związanych z bezpieczeństwem pożarowym? - Czy jak często sprawdzane są warunki przestrzegania ustanowionych norm bezpieczeństwa pożarowego? - ... 	<ul style="list-style-type: none"> - Czy w zakładzie/obiekcie odbywa się ruch ludzi nie związanych z zakładem? - Gdzie mają dostęp kontrahenci, dostawcy, klienci? - Czy osoby z zewnątrz znają zagrożenia pożarowe w zakładzie oraz czy je przestrzegają? - Czy wdrożony jest system monitorowania ruchu klientów? - Czy opracowane są warunki przyjmowania materiałów stwarzających szczególne zagrożenia pożarowe - ...

Rys. 7. Obszary oceny ryzyka pożarowego

Źródło: Opracowanie własne.

Zarządzanie ryzykiem pożarowym odbywa się także w obszarze działalności organów Państwowej Straży Pożarnej, które na bieżąco analizują sytuację pożarową na szczeblu powiatów, województw i kraju. Nadzorują one przestrzeganie ustanowionych aktów prawnych w zakresie ochrony przed pożarami oraz analizują przyczyny pożarów i wdrażają działania ukierunkowane na obniżenie liczby pożarów oraz ograniczenia ich skutków.

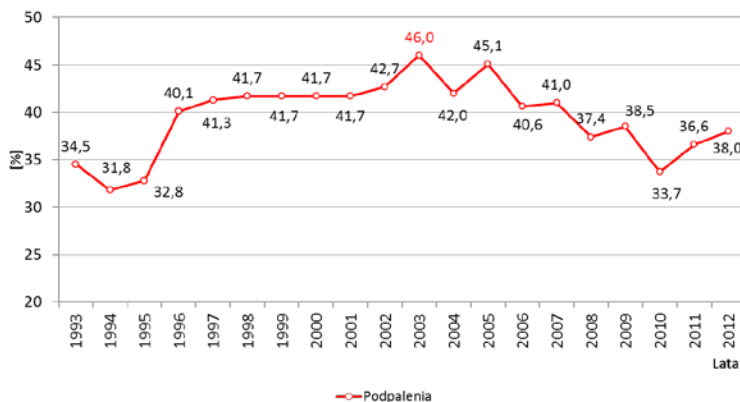
Elementem zarządzania ryzykiem pożarowym w społecznościach lokalnych są realizowane w coraz szerszym zakresie przedsięwzięcia w obszarze tzw. prewencji społecznej, która skupia się na budowaniu świadomości zagrożeń pożarowych w społecznościach lokalnych oraz wczesnym reagowaniu na zjawiska mogące doprowadzić do powstania pożaru. Zorganizowane działania organów administracji rządowej i samorządowej w tym obszarze przyczyniają się do istotnego obniżenia poziomu ryzyka pożarowego w tych społecznościach.

Analiza ryzyka pożarowego jest przedmiotem szczególnego zainteresowania towarzystw ubezpieczeniowych, które przed zawarciem umowy ubezpieczenia obliczają prawdopodobieństwo wystąpienia szkody pożarowej, opierając się na analizie realizowanych procesów technologicznych, stosowanych zabezpieczeń, konstrukcji obiektów, zagrożeń, których źródłem są pracownicy i kontrahenci

itd. Służy to bezpośrednio zarządzaniu ryzykiem ubezpieczeniowym obiektu od wystąpienia szkody całkowitej.

W wymiarze indywidualnym każdy człowiek na co dzień „zarządza” ryzykiem pożarowym w swoim najbliższym otoczeniu, dokonując stosownych ocen i wyborów w zakresie np. eksploatacji urządzeń i instalacji elektrycznych, grzewczych, stosowanych materiałów budowlanych, stosowania zasad bezpiecznego postępowania z materiałami niebezpiecznymi (cieczkami łatwopalnymi, gazem w instalacjach stałych i z butli przenośnych itp.) czy też podczas posługiwania się otwartym ogniem w innych okolicznościach (palenie papierosów, wypalenie traw, spalanie śmieci itd.).

Przez wiele lat jednym z niedocenionych obszarów w zarządzaniu ryzykiem pożarowym, zarówno na poziomie lokalnym, jak i w skali ogólnopaństwowej, było badanie przyczyn pożarów oraz ujawnianie i karanie ich sprawców. Na możliwości prewencyjne tkwiące w kryminalistycznym badaniu pożarów uwagę zwracał już w latach 50. ubiegłego wieku w swoich pracach Brunon Hołyst. Mimo że instytucje państwowe odpowiedzialne za bezpieczeństwo mają świadomość znaczenia i roli ustalania przyczyn pożarów w budowaniu bezpieczeństwa pożarowego, do chwili obecnej tym zagadnieniom nie poświęcono należytej uwagi. Problem niskiej jakości ustalania przyczyn pożarów oraz niskich wskaźników wykrywalności i karania ich sprawców obserwowany jest nie tylko w Polsce, ale również w wielu państwach UE i świata. Dotyczy on zarówno państw słabo rozwiniętych, jak i wysoko rozwiniętych. Źródła problemów w tym obszarze tkwią w szczególnej trudności przeprowadzania badań miejsc objętych pożarem. Pogorzelnisko z punktu widzenia badań pożarowych i kryminalistycznych przysparza organom prowadzącym postępowanie w sprawie pożarów wielu problemów – zarówno w zakresie ujawniania miejsca źródła pożaru oraz jego przyczyny, jak i śladów działalności sprawcy oraz śladów i dowodów wskazujących na sprawcę. Główną przyczyną tych trudności jest natura ognia, który niszczy większość śladów i dowodów. W dalszej kolejności ślady i dowody niszczone są podczas działań ratowniczo-gaśniczych oraz podczas niewłaściwie prowadzonych przez uprawnione podmioty czynności procesowych związanych z zabezpieczeniem miejsca zdarzenia i kryminalistycznych oględzin. Wynika to głównie z braku organizacji dochodzeń popożarowych, braku szkoleń i wielu innych przyczyn. Niska sprawność ustaleń dotyczących przyczyn pożarów ma wpływ na kształtowanie się przestępczości z użyciem ognia. Analiza wieloletnich danych publikowanych przez Komendę Główną Państwowej Straży Pożarnej pokazuje, że dominującą przyczyną pożarów na przestrzeni wielu lat są podpalenia (rys. 8).



Rys. 8. Podpalenia w latach 1993–2012

Źródło: Opracowanie własne na podstawie: Komenda Główna Państwowej Straży Pożarnej, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 1993–2012*, dz. cyt.

Powyższe problemy coraz częściej stają się przedmiotem badań i analiz, których następstwem jest wdrożenie nowych zasad prowadzenia postępowań w sprawach o pożary, nowej struktury organizacyjnej itd.

W większości państw na świecie ustalanie przyczyn pożarów oraz ujawnianie ich sprawców to domena działalności policji oraz prokuratury. Służby te jednak nie są właściwie przygotowane do działań w tym obszarze, głównie z powodu jego wyjątkowej specyfiki oraz niewielkiej liczby przestępstw pożarowych w porównaniu do innych przestępstw będących przedmiotem zainteresowania tych podmiotów. Organy Państwowej Straży Pożarnej, choć najlepiej przygotowane do analiz pożarowych i badań w tym zakresie, nie są zobligowane do szczegółowego badania przyczyn pożarów.

Właściwe i sprawne ustalanie przyczyn pożarów oraz ich sprawców, oparte na podstawach naukowych oraz sprawnej organizacji, to z pewnością ważny i niedoceniany obszar oddziaływania na ryzyko pożarowe. Pozytywnym przykładem zmian wprowadzonych w organizacji dochodzeń w sprawach o pożary, które przyczyniły się do istotnej poprawy bezpieczeństwa pożarowego, jest Wielka Brytania. W latach 90. ubiegłego wieku 47% wszystkich pożarów (w niektórych hrabstwach nawet ponad 50%), powstawało w wyniku zamierzonego działania człowieka. Przyczyniały się one do powstawania wielomiliardowych strat dla gospodarki narodowej Wielkiej Brytanii. W związku z powyższym przeprowadzono badania i analizę przyczyn tak dużego odsetka podpalenia, a następnie opracowano i wdrożono nowe zasady ustalania przyczyn pożarów, oparte na współpracy dwóch wiodących podmiotów: policji i straży pożarnej. Po 20 latach prowadzenia dochodzeń w sprawach o pożary według nowych zasad udało się obniżyć odsetek pożarów spowodowanych podpaleniami z około 47% w roku 1997

do 18% w roku 2011. W tym okresie odnotowano również zmniejszenie liczby pożarów oraz strat pożarowych. Koszty wdrożenia i utrzymania programów okazały się wielokrotnie niższe od strat, które wcześniej były generowane przez podpalenia. Udało się osiągnąć sukces w wymiarze nie tylko finansowym, ale także społecznym – uzyskując poprawę bezpieczeństwa ludności na poziomie lokalnych społeczności. Istotne zmiany w organizacji dochodzeń popożarowych w ostatnim 20-leciu dokonano również w Szwecji, we Włoszech oraz w Republice Czeskiej. We wszystkich tych państwach wdrożone zmiany oparte były na zwiększeniu znaczenia straży pożarnej w ustalaniu okoliczności powstawania pożarów. Z uwagi na doświadczenia tych państw zasadne wydaje się wdrożenie podobnych rozwiązań w Polsce.

PODSUMOWANIE I WNIOSKI

Dla zarządzania kryzysowego potrzeby związane z systemowym podejściem do zarządzania ryzykiem są dziś bardziej aktualne niż kiedykolwiek. Od momentu wprowadzenia elementów zarządzania ryzykiem w 2009 r. jego znaczenie stale wzrasta. Stąd też rekomenduje się wykorzystanie uznanych wytycznych w zakresie zarządzania ryzykiem, które ujednolicają terminologię, wnoszą uniwersalne zasady, elastyczną strukturę ramową i właściwie dopasowane procesy, w tym narzędzia wspomagające ocenę ryzyka i dokumentowanie zarządzania ryzykiem. Obowiązujący stan prawny nie wspiera obecnie w takim zakresie możliwości wdrażania do zarządzania kryzysowego najlepszych praktyk dotyczących zarządzania ryzykiem, dlatego też istotną do podjęcia kwestią jest nowelizacja przepisów.

W 2002 r. Donald Rumsfeld wygłosił przemówienie, którego jeden z fragmentów jest często cytowany. Wyróżnił w nim trzy kategorie wiedzy, odwołując się do pojęcia zagrożenia. Wskazał, że są to sytuacje, w których:

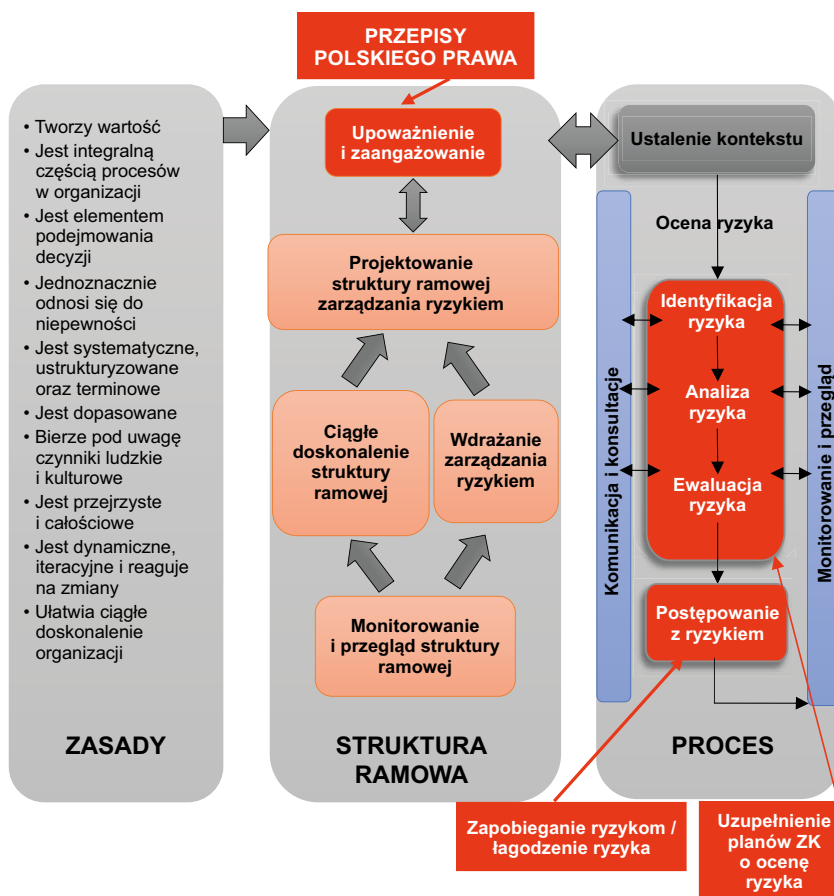
- wiemy, że wiemy (ang. *known knowns*),
- wiemy, że nie wiemy (ang. *known unknowns*),
- nie wiemy, że nie wiemy (ang. *unknown unknowns*).

„Dwie pierwsze kategorie dotyczą sytuacji, gdy mamy kontrolę poznawczą. W przypadku trzeciej kategorii zagrożenia nie są wzięte pod uwagę w określonym momencie. Może być bowiem tak, że w ogóle nie zdajemy sobie sprawy z tego, że czegoś nie wiemy. Rumsfeld nie wspominał jednak o jeszcze jednej kategorii, niezbędnej dla kombinatorycznej kompletności – kiedy udajemy, że nie wiemy, świadomie ignorując wiedzę (*unknown knowns*)”.

O ile ignorancja jest kategorią, której nie można poddać racjonalnemu dyskursowi, o tyle pozostałe kategorie (wskazane jako trzy pierwsze) zakładają racjonalność zachowań, w których analizie, chcąc uzyskać jak największą użyteczność, należy brać pod uwagę takie pojęcia, jak **niepewność**, **konsekwencje** czy **ryzyko**. To właśnie ocena ryzyka pozwala organizacji identyfikować i opisywać zagrożenia oraz zarządzać bezpieczeństwem bez względu na to, czy potrafi ona, czy też nie potrafi na początku tego procesu, przejmować nad nimi kontrolę. Można więc wskazać, że zarządzanie ryzykiem to proces, w wyniku którego organizacja (a więc i państwo) zdobywa zdolność łagodzenia ryzyka, a w konsekwencji ograniczania skutków zagrożeń. Refleksja nad tymi możliwościami (a także obowiązkiem państwa) w rezultacie prowadzi do sformalizowania wymagań w postaci dedykowanych rozwiązań prawnych.

Biorąc pod uwagę analizę przepisów ustawy o zarządzaniu kryzysowym wraz towarzyszącymi jej rozporządzeniami, poprzez ich uogólnienie, można określić generalne obszary wymagań w zakresie zarządzania ryzykiem, które dla systemu zarządzania kryzysowego wskazał ustawodawca. Wymagania te to:

- rozszerzenie planów zarządzania kryzysowego o **ocenę ryzyka** oraz **mapy ryzyka**,
- **zapobieganie ryzykom** (łagodzenie ryzyka) funkcjonalności i ciągłości działań oraz integralności infrastruktury krytycznej,
- uwzględnienie w ocenie ryzyka **podatności** obiektów IK,
- wykorzystanie przy ocenie ryzyka **metody scenariuszowej**.



Rys. 1. Proces zarządzaniem ryzykiem a potrzeby systemu zarządzania kryzysowego

Źródło: Opracowanie własne na podstawie PN-ISO 31000:2012.

Biorąc pod uwagę powyższe warunki oraz wskazane propozycje organizacji ISO, można skazać graficznie (rys. 1) obszary zaleceń ISO, które mogą zostać

wykorzystane (przy obecnie obowiązujących normach prawnych) przez system zarządzania kryzysowego.

Ujęte na rys. 1 wymagania ze strony systemu zarządzania kryzysowego są wymaganiami bezpośrednimi i wynikają literalnie z przepisów prawa. Niemniej jednak należy zwrócić uwagę na fakt, że istnieją również inne pośrednie zapisy prawa, które pośrednio odwołują się do reguł norm ISO.

Dokonując porównania **zasad** zarządzania ryzykiem z wymaganiami przepisów ustawy i delegowanymi dla niej rozporządzeniami, można wskazać, że:

1. W wyniku wprowadzenia do procesu planowania cywilnego wymogu oceny ryzyka spełniono by zasadę **integralności zarządzania ryzykiem z procesami właściwymi dla organizacji**.
2. Biorąc pod uwagę proces sporządzania, zatwierdzania i strukturę raportów częściowych i *Raportu o zagrożeniach bezpieczeństwa narodowego* (obowiązki organów administracji publicznej, konieczność uwzględnienia wniosków z raportów w planach zarządzania kryzysowego czy przyjmowanie *Raportu* przez Radę Ministrów), można wskazać, że proces zarządzania ryzykiem jest **elementem podejmowania decyzji wpływającym na ciągle doskonalenie organizacji i ułatwia proces doskonalenia organizacji**¹.
3. Zarządzanie ryzykiem **jest usystematyzowane, ustrukturalizowane i terminowe**, ponieważ przepisy prawa określają strukturę nie tylko dokumentów, ale i procesu oraz terminy kolejnych aktualizacji dokumentów. Jednocześnie to właśnie obowiązek dwuletniej aktualizacji sprawia, że jest ono **dynamiczne, iteracyjne i reaguje na zmiany**².
4. Poprzez swoje cele zarządzanie ryzykiem **tworzy, ale przede wszystkim chroni wartości** (życie ludzkie, środowisko, interesy państwa) a w procesie, w wyniku udziału wszystkich istotnych podmiotów (ministrów, kierowników urzędów centralnych i wojewodów), **wykorzystuje najlepsze dostępne informacje**³.

Dyskusyjne jest oczywiście, na ile samo nałożenie obowiązków na organy władzy, a więc strukturę państwa, zadań planowania cywilnego (w tym także w zakresie oceny ryzyka) można opisać jako wypełnienie zalecenia dotyczącego przygotowania struktury ramowej. Z pewnością niektóre jej elementy zostają wypełnione przez ogólne zasady systemu ZK. Wymóg **zrozumienia kontekstu** z pewnością wypełniany jest poprzez konieczność ujmowania w procesie planowania zagrożeń wraz z ich charakterystyką. Działanie to odnosi się do szeroko rozumianego zewnętrza

¹ Zapewnia również zaangażowanie w proces zarządzania ryzykiem decydentów (wymóg procesu projektowania struktury ramowej)

² Kolejne aktualizacje uzupełniają dokument o nowe zagrożenia/ryzyka i wskazują sposoby postępowania z nimi.

³ Wymienione zasady (wskazane w dalszej części rozdziału poprzez zastosowanie *kursywy*) wskazuje norma PN-ISO 31000:2012 w części: Zasady, s. 27–29.

systemu (sytuacje kryzysowe czy zagrożenia polityczno-militarne), ale i ukazania własnego potencjału (czyli wnętrza).

Ponadto należy zauważyć, że niektóre elementy struktury ramowej, tj.: **ustalenie komunikacji wewnętrznej i zewnętrznej oraz raportowanie** są w posiadaniu (istnieją narzędzia mogące służyć realizacji tej funkcji) systemu zarządzania kryzysowego, niemniej nie są wykorzystywane w literalnie odczytywanym procesie zarządzania ryzykiem. Funkcjonujące centra zarządzania kryzysowego, które można by było umownie uznać za podmioty wypełniające te zalecenia, nie są angażowane w opisywany proces. Podobnie można odnieść się do problemu **ciągłego doskonalenia, monitorowania i przeglądu struktury ramowej, komunikacji czy konsultacji**.

Biorąc pod uwagę złożoność systemu i różnorodne procesy, które są w nim realizowane, można byłoby zbudować teoretyczny model systemu zarządzania kryzysowego, w którym każdy element wskazany w normach można by przypisać już istniejącym organom, osobom lub instytucjom. Tego typu rozważania pozostałyby jednak czysto postulatywne z co najmniej dwóch powodów:

1. System oparty jest na formalnych rozwiązaniach prawnych, więc w konsekwencji, aby jego poszczególne elementy mogły realizować przypisane im role w procesie zarządzania ryzykiem, niezbędna jest zmiana obowiązującego prawa.
2. Nowelizacja ustawy o zarządzaniu kryzysowym z 2009 r. oraz towarzysząca jej rozporządzenia wprowadziły do systemu zarządzania kryzysowego jedynie elementy procesu zarządzania ryzykiem. Elementem, na który położono główny nacisk, była ocena ryzyka, nie wdrożono pełnego procesu zarządzania nim. Stan taki jest dysfunkcjonalny, ponieważ nawet przy poprawnie ocenionym ryzyku nie ma prawnego obowiązku zarządzania nim we właściwy sposób.

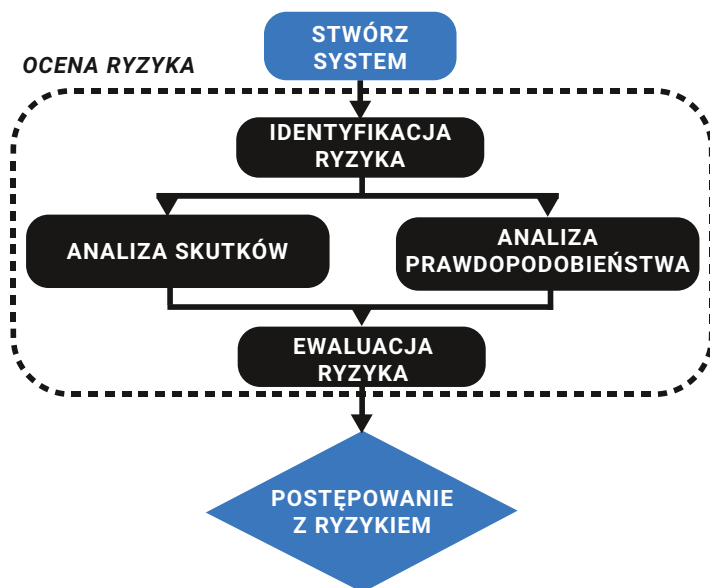
W tych warunkach mamy do czynienia z sytuacją, w której to brak odpowiednich przepisów prawa utrudnia wdrożenie i wykorzystanie pełni norm ISO.

Porównanie norm z przepisami prawa wykazało jeszcze jeden problem uniemożliwiający pełną ich implementację. Ocena ryzyka na potrzeby zarządzania kryzysowego inicjowana jest od oceny wystąpienia zagrożeń (w tym dla zdrowia, życia, mienia i środowiska). W tej sytuacji to zagrożenie staje się podstawową kategorią i to jego właściwe zdefiniowanie jest punktem wyjścia dla całego procesu. Dla zarządzania ryzykiem opisanego w normach główną kategorią jest natomiast proces. W tym przypadku ryzyko określa się dla procesów służących realizacji określonych celów w organizacji i to one są podstawową kategorią, do której odnosi się całość dalszych działań.

Wskazane powyżej rozbieżności determinują więc sposób rozwiązania problemu badawczego. Na obecnym etapie rozważań konieczne jest odniesienie się do wskazanych na rys. 1 obszarów:

- upoważnienia i zaangażowania,
- oceny ryzyka,
- postępowania z ryzykiem.

Ponieważ upoważnienie i zaangażowanie są wypadkową przepisów prawnych z zakresu zarządzania kryzysowego i ogólnych norm prawa konstytuujących sposób funkcjonowania administracji publicznej w Polsce, nie odniesiono się do nich szerzej w rozważaniach podjętych w części V. Przy dokonywaniu oceny ryzyka i określaniu sposobów postępowania z nim można zastosować rozwiązania wykorzystywane w standardzie BSI. Sposób ten przedstawia rys. 2.



Rys. 2. Proces oceny ryzyka

Źródło: Opracowanie własne na podstawie materiału szkoleniowego BSI:
PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym.

Jak wynika z rys. 2, do oceny ryzyka niezbędne jest dokonanie identyfikacji ryzyka, analizy skutków i prawdopodobieństwa.

Po dokonaniu analizy metod wskazanych w tabeli 3 oraz potrzeb projektu, na rzecz którego realizowane były badania, można wykazać, że w celu dokonania oceny ryzyka (pomijając problem identyfikacji ryzyka) można wykorzystać poniższe metody⁴:

- 1) SWIFT – „co, jeśli?”,
- 2) metodę scenariuszową,
- 3) metodę drzewa błędów,

⁴ K. Gawęcki, PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym, materiał szkoleniowy BSI, Warszawa 2012.

- 4) metodę drzewa zdarzeń,
- 5) metodę *bow tie*.

Bez względu na wybór metody w celu określenia kolejnego elementu pożądane jest przedstawienie wyników powyższych analiz na macierzy ryzyka.

Tabela 1. Przykładowa macierz ryzyka 6×6

X	Prawdopodobieństwo					
Skutki						

Źródło: Opracowanie własne na podstawie ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*.

Matryce stosowane obecnie przez system zarządzania kryzysowego są macierzami nieparzystymi 5×5⁵. W opinii autorów (po dokonaniu analizy raportów częściowych) należy wskazać, że w projektowanej metodzie powinno się zastosować matryce o liczbie parzystej (np. 4×4 lub 6×6). Rozwiązanie to wyeliminuje powszechnie stosowany zabieg uśredniania wyników zarówno prawdopodobieństwa, jak i skutków.

Celem opracowania matrycy jest określenie kontekstu dla ustalenia dalszego postępowania z ryzykiem, które powinno zostać w dalszej kolejności ujęte w planach zarządzania kryzysowego⁶. Zanim jednak organizacja przystąpi do sporządzenia procedur (właściwych dla procesu planowania cywilnego), normy wskazują jej ogólne kierunki kolejnych działań. Zgodnie z przyjętą pragmatyką postępowania z ryzykiem⁷ do wypełnionej matrycy można zastosować poniżej przedstawiony zabieg. Matryce dzielimy na cztery części, tak by stworzone w ten sposób pola determinowały dalsze sposoby postępowania.

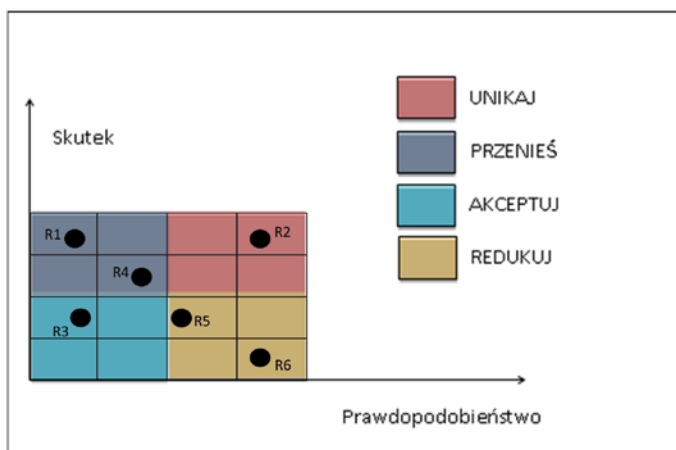
Problem oceny ryzyka został ujęty w polskim porządku prawnym ponad 5 lat temu. W tym czasie system zarządzania kryzysowego wdrożył te zasady i obecnie możemy wskazać, na ile zaproponowane prawem podejście spełniło swoje zadanie. Na podstawie doświadczenia, o które wzbogacił się system w tym okresie, można wysunąć generalny postulat: **ze względu na ograniczony zakres wykorzystywanych**

⁵ Takie matryce 5×5 stosuje się między innymi podczas sporządzania raportów częściowych i Raportu o zagrożeniach bezpieczeństwach narodowego.

⁶ Dyrektywy wskazują jako nazwę dokumentu przypisanego do tego działania: *Plan postępowania z ryzykiem*.

⁷ K. Gawecki, PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym, materiał szkoleniowy BSI, Warszawa 2012.

przez system zarządzania kryzysowego metod zarządzania ryzykiem należy dążyć do jego rozszerzenia.



Rys. 3. Zasady wyboru opcji postępowania na przykładzie matrycy ryzyka

Źródło: Opracowanie własne na podstawie

ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*.

Analiza przedstawiona w niniejszej części wskazuje, że postulat ten może zostać spełniony z wykorzystaniem norm ISO. Potwierdza ona również postawioną w części V hipotezę, że: **zalecenia i dyrektywy ISO można wykorzystać w procesie planowania cywilnego w zakresie ujednolicenia nazewnictwa wykorzystywanego przez system ZK oraz przygotowania procesu oceny ryzyka i procedur postępowania z ryzykiem.**

Tak więc pozytywna odpowiedź na problem badawczy⁸ pozwoliła określić, które z procesów, wytycznych oraz metod rekomendowanych przez ISO można wykorzystać do wypełnienia obecnie obowiązującego prawa w zakresie zarządzania kryzysowego (rozdział VI ustawy).

W części V przedstawiono diagnozę obecnego stanu (obowiązującego prawa, wykorzystywanych metodyk), która pozwoliła na wskazanie pożądanych i skutecznych rozwiązań zmierzających do usprawnienia procesu planowania cywilnego w zakresie, w którym posługuje się ono pojęciem ryzyka.

Biorąc pod uwagę powyższe, należy sformułować następujące wnioski:

1. Obecnie wdrożone przez system zarządzania kryzysowego metody w zakresie zarządzania ryzykiem (determinowane przez porządek prawny) są niewystarczające dla pełnego zastosowania norm ISO.
2. Wdrożenie pełnego procesu zarządzania ryzykiem w systemie zarządzania kryzysowego jest możliwe, jednak dopiero po zmianie obowiązującego prawa.

⁸ Który brzmiał: czy narzędzie, jakim są normy ISO (w zakresie zarządzania ryzykiem), można efektywnie wykorzystać w procesie planowania cywilnego?

3. Wiele norm podejmuje problematykę zarządzania czy oceny ryzyka, niemniej jednak na potrzeby planowania cywilnego wystarczające jest oparcie się na następujących: PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia* oraz ISO/IEC 31010 *Risk Management — Risk Assessment Techniques*.
4. Wskazane w punkcie trzecim normy można wykorzystać w zakresie:
 - a) PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia* – ujednoczenia słownictwa,
 - b) PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne* – określenia procesów,
 - c) ISO/IEC 31010 *Risk Management — Risk Assessment Techniques* – wykorzystania wskazanych w niej metod i narzędzi badawczych.
5. Przedstawione wyniki badań wskazują, że normy (mimo innego podejścia do ryzyka) należy brać pod uwagę przy przygotowywaniu metodyki oceny ryzyka.
6. Zarządzanie ryzykiem powodziowym determinowane jest przez branżowy oraz strategiczny wymiar tego rozwiązania i ma na celu zwalczenie tego wciąż nieujarzmionego przez człowieka żywiołu. Wskazana metoda nie znajduje zastosowania w innych obszarach zarządzania ryzykiem. W jej strukturze można natomiast odnaleźć miejsca możliwe do doskonalenia w świetle założeń międzynarodowych norm ISO w obszarze zarządzania ryzykiem.
7. Wszystkie zebrane metodyki oceny ryzyka w przepisach krajowego prawa resortowego zawierają elementy wspólne, jakimi są podstawowe etapy zarządzania ryzykiem, m.in.: identyfikacja ryzyka, analiza ryzyka, ewaluacja ryzyka, postępowanie z ryzykiem czy monitorowanie podjętych działań. Do szacowania ryzyka stosowane są nieskomplikowane opisy jakościowe. Wykorzystuje się również matryce ryzyka oraz proste zilustrowania graficzne w postaci map ryzyka. W większości przypadków dokumentem odniesienia są informacje zawarte w komunikatach ministra finansów, dotyczące szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem.
8. Istniejące dokumenty dotyczące zarządzania ryzykiem w prawie resortowym są w zadowalającym stopniu spójne z wytycznymi normy ISO 31000:2009. Istotny jest jednak fakt, że analiza opierała się jedynie na tych resortach i urzędach centralnych, które przygotowały pełne dokumenty dotyczące oceny ryzyka. W tym wypadku niezbędne wydaje się stworzenie jednolitych wytycznych (np. na podstawie normy ISO 31000), według których resorty opracowałyby swoje metody zarządzania ryzykiem.
9. Z analizowanych dokumentów administracji rządowej wynika, że zarządzanie ryzykiem powinno być ciągłym, aktywnym i systematycznym procesem,

mającym na celu zrozumienie ryzyka, zarządzanie nim i informowanie o nim. Zarządzanie ryzykiem na szczeblu centralnym powinno ułatwiać podejmowanie strategicznych decyzji, które przyczynią się do osiągnięcia celów.

10. Zarządzanie ryzykiem w krajowym prawie miejscowym występuje w ograniczonym zakresie. Metodyki oceny ryzyka są stosowane głównie na potrzeby kontroli zarządczej, która skupia się przede wszystkim na zrównoważonym zarządzaniu finansami oraz innymi zasobami. Szeroko dostrzegany jest już jednak fakt, że warto rozwijać wypracowane w tej dziedzinie rozwiązania i wykorzystywać je na potrzeby bezpieczeństwa – w tym zarządzania kryzysowego. Należy zauważyć, że kompetencje w zakresie zarządzania ryzykiem występują i są wykorzystywane na wszystkich szczeblach administracyjnych państwa. Zasadnym i istotnym zadaniem byłoby ich rozszerzenie na całą instytucję i włączenie do jednolitego systemu zarządzania ryzykiem w administracji publicznej.
11. Rozważyć należałoby zastosowanie gotowych i sprawdzonych rozwiązań na potrzeby oceny ryzyka i ich właściwej interpretacji – zwłaszcza tam, gdzie analiza ekspercka wydaje się uzasadniona. Metodyka PomRisc powstawała przed 2009 r., na bazie literatury oraz metod australijskich, w tym projektu przygotowywanej normy ISO 31000. Opracowano metodykę unikatową i odkrywającą niezbadane obszary zastosowania oceny ryzyka w tamtym czasie. Metodyka PomRisc umożliwia diagnozę stanu systemów bezpieczeństwa oraz wskazanie optymalnych kierunków działań doskonalących. Istota metody zawiera się w powiązaniu systemowym wyników analizy ryzyka z jednoznacznym wskazaniem przyczyn, kierunków eliminacji i redukcji ryzyka oraz optymalnych kierunków rozbudowy i doskonalenia systemu reagowania (ratownictwa) czy innego systemu bezpieczeństwa. PomRisc stanowić może doskonale narzędzie do wykorzystania w planach i pracach zespołów zarządzania kryzysowego, zawierające elementy przydatne w wytyczaniu kierunków rozwoju bezpieczeństwa, a także pracach zespołów badawczych i zespołów praktyków.
12. Narzędzia teleinformatyczne w procesach zarządzania występują coraz powszechniej, wspomagając i porządkując codzienną pracę. Tym niemniej wciąż niewiele jest tych dedykowanych do specjalistycznych zastosowań, które umożliwią dokonanie oceny ryzyka, czy wręcz kompleksowe zarządzanie ryzykiem. Te funkcjonujące obecnie są głównie w sektorze finansowym oraz w procesach decyzyjnych organizacji różnego typu. Przykładem zastosowania narzędzia teleinformatycznego do wspomagania procesu oceny ryzyka w planowaniu cywilnym jest oprogramowanie RISK0, którego specjalny moduł do oceny ryzyka umożliwia obliczenie oraz wizualizację ryzyka scenariuszy zagrożeń w planach zarządzania kryzysowego.

13. Konieczne są działania prowadzące do pełnego wdrożenia i doskonalenia procesu zarządzania ryzykiem pożarowym w Polsce – także w zakresie zastosowania zaleceń międzynarodowych norm ISO, regulujących sposób zaprojektowania architektury zarządzania ryzykiem i jej formalnego uruchomienia.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

- Komenda Główna Państwowej Straży Pożarnej, „Biuletyn Informacyjny Państwowej Straży Pożarnej za rok 1993–2011”, Warszawa 1994–2012.
- Komenda Główna Państwowej Straży Pożarnej, „Biuletyn Informacyjny Państwowej Straży Pożarnej za rok 1993–2012”, Warszawa 1993–2012.
- Komenda Główna Państwowej Straży Pożarnej, „Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2000–2011”, Warszawa 2001–2012.
- Komenda Główna Państwowej Straży Pożarnej, „Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2002–2012”, Warszawa 2003–2013.
- Majda T., Wałdykowski P., Adamczyk J., Grygoruk M., *Typologia terenów narażonych na niebezpieczeństwo powodzi*, TUP, Warszawa 2012.
- Olszewski A., Krzywicki B., *Budowa systemu informatycznego wspierającego przygotowywanie planów zarządzania kryzysowego RISKÓ*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, D. Wróblewski (red.), wyd. CNBOP-PIB, Józefów 2015.
- Pilch T., *Zasady badań pedagogicznych*, wyd. Żak, Warszawa 1995.
- Roguski E. W., Wróblewski D., *Diagnostyczna metoda oceny ryzyk i systemów reagowania PomRisc jako narzędzie programowania zmian doskonalących systemy bezpieczeństwa i ich monitorowania*, BiTP, vol. 12, Issue 4, 2008.
- Wróblewski D. (red.), *Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, Józefów 2009.
- Wróblewski D. (red.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014.
- Wróblewski D. (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego*, CNBOP-PIB, Józefów 2014.
- Wróblewski D., Kędzierska M., Połec B., *Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne*, [w:] *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, Majchrzak D. (red.), AON, Warszawa 2014.
- Wróblewski D., Połec B., Maciak J., *Informatyczne wspomaganie zarządzania kryzysowego –oprogramowanie „RISKÓ*”, [w:] *Organy administracji publicznej i instytucje w zarządzaniu kryzysowym*, G. Sobolewski, D. Majchrzak, Z. Sobejko (red.), wyd. AON, Warszawa 2016.
- Wróblewski D., Połec B., *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, Majchrzak D. (red.), AON, Warszawa 2014.

Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce, wyd. Bentley Dennison, Warszawa 2007.

Akty prawne

- Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. Nr 35, poz. 230 z późn. zm.).
- Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. nr 95, poz. 425 z późn. zm.).
- Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. Nr 91, poz. 578 z późn. zm.).
- Ustawa z dnia 18 lipca 2001 r. Prawo wodne (Dz. U. nr 115, poz. 1229).
- Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. Nr 179, poz. 1485 z późn. zm.).
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.).
- Ustawa z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz. U. 2009 nr 131, poz. 1076 z późn. zm.).
- Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. nr 157, poz. 1240 z późn. zm.).
- Ustawa z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2017 r., poz. 1566).
- Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz. Urz. UE L 288 z 06.11.2007, s. 27–34).
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. Nr 83, poz. 540).
- Zarządzenie nr 13 prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych (tekst jedn. Dz. Urz. WUG z 2016 r. poz. 65).
- Zarządzenie nr 15 Ministra Spraw Wewnętrznych i Administracji z dnia 8 kwietnia 2016 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.
- Zarządzenie nr 27 Ministra Spraw Zagranicznych z dnia 27 lipca 2016 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez Ministra Spraw Zagranicznych.
- Zarządzenie nr 587 wojewody mazowieckiego z dnia 14 grudnia 2016 r. w sprawie systemu kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.
- Zarządzenie nr 828/2015 Prezydenta miasta stołecznego Warszawy z dnia 10 czerwca 2015 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.
- Zarządzenie nr 18/2015 Burmistrza Karczewa z dnia 30 stycznia 2015 r. w sprawie wprowadzenia polityki zarządzania ryzykiem.
- 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 poz. 56).
- Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego.

Normy i standardy

AS/NZS 4360:1999 Risk Management.

ISO 31000:2009 Risk Management – Principles and Guidelines

ISO/IEC 31010:2010 Risk Management – Risk Assessment Techniques.

PN-ISO 31000:2012 Zarządzanie ryzykiem – Zasady i wytyczne.

Dokumenty elektroniczne, strony internetowe i inne

All Hazards Risk Assessment – Methodology Guidelines 2012–2013 [dok. elektr.], <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ll-hzrds-sssmnt/ll-hzrds-sssmnt-eng.pdf>.

Gawęcki K., PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym, materiał szkoleniowy BSI, Warszawa 2012.

<http://www.isok.gov.pl>.

<http://www.kzgw.gov.pl>.

Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych, KZGW, Warszawa 2013.

Raport z opracowania wstępnej oceny ryzyka powodziowego, KZGW, Warszawa 2011.

Umowa z dn. 05.05.2008 r. na wykonanie projektu pt. „Koncepcja Funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego”.

Wróblewski D., *Zarządzanie ryzykiem jako element kształtowania bezpieczeństwa lokalnego*, szkolenie podstawowe dla: starostów, wójtów, burmistrzów i prezydentów miast województwa dolnośląskiego z zakresu ochrony ludności i obrony cywilnej „Zarządzanie w stanach zagrożeń i doskonalenie systemu ochrony ludności”, Józefów 2011.

CZEŚĆ VI

SŁOWNIK WYBRANYCH POJEŃ Z ZAKRESU ZARZĄDZANIA RYZYKIEM

WPROWADZENIE

Niniejsza część powstała w oparciu o wybrane definicje z zakresu zarządzania ryzykiem pochodzące:

- ze słownika pojęć (s. 64–67) i słownika rekomendowanych pojęć (s. 69–166) opublikowanego w monografii *Rekomendacje formalno-prawne z zakresu zarządzania kryzysowego*¹ – pojęcia te zostały oznaczone (*). Słownik rekomendowanych pojęć został opracowany przez zespół projektowy w ramach zadania VI.1.2 pn. Analiza porządku terminologicznego w obszarze zarządzania kryzysowego (sierpień 2013), pod kierunkiem prof. dr. hab. inż. W. Kitlera;
- z części IV *Wybrane pojęcia z zakresu zarządzania kryzysowego i zarządzania ryzykiem* (s. 129–192) opublikowanej w monografii *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*² – pojęcia te zostały oznaczone (**). Zebrane pojęcia zostały opracowane przez zespół projektowy CNBOP-PIB w ramach zadania VI.1.1 pn. Zebranie (opracowanie) podstawowych definicji i pojęć związanych z bezpieczeństwem i zarządzaniem kryzysowym – opracowanie wspólnej terminologii pojęć (czerwiec 2013), pod kierunkiem dr. inż. D. Wróblewskiego;

oraz aktualizację lub uzupełnienie o nowe definicje – pojęcia te zostały oznaczone (***)

Obie ww. publikacje powstały i zostały wydane w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne” finansowanego przez Narodowe Centrum Badań i Rozwoju na podstawie umowy nr DOBR/0016/R/ID2/2012/03.

Odpowiednio przy definicjach podano każdorazowo oryginalne źródło, z którego pochodzi definicja, a w odniesieniu do pojęć definiowanych przez zespół autorski jednej z ww. publikacji takie autorstwo zostało odpowiednio wskazane opisem: „Opracowanie zespołu autorskiego pod kierunkiem (...)”, „Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem (...)”, „Opracowanie zespołu autorskiego

¹ D. Wróblewski (red.), *Rekomendacje formalno-prawne z zakresu zarządzania kryzysowego*, CNBOP-PIB, Józefów 2015, s. 64–166.

² D. Wróblewski (red.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 129–192.

(...) na podstawie” oraz w odniesieniu do jednej definicji wskazano indywidualne autorstwo członka zespołu projektowego.

Niniejsza część została podzielona na angielsko-polski i polsko-angielski słownik obejmujący 51 podstawowych pojęć z zakresu zarządzania ryzykiem, a także słownik obejmujący 127 wybranych pojęć z zakresu zarządzania ryzykiem.

ANGIELSKO-POLSKI SŁOWNIK PODSTAWOWYCH POJĘĆ Z ZAKRESU ZARZĄDZANIA RYZYKIEM

1. business continuity management – zarządzanie ciągłością działania (*)
2. communication and consultation – komunikacja i konsultacje (*)
3. consequence – konsekwencje (*)
4. decision-maker – decydent (*)
5. establishing the context – ustalanie kontekstu (**)
6. external context – kontekst zewnętrzny (**)
7. hazard – zagrożenie (*)
8. hazard identification – identyfikacja niebezpieczeństwa (*)
9. hazard map – mapa zagrożeń (*)
10. hazard mitigation – minimalizowanie zagrożeń (*)
11. impact – wpływ (*)
12. impact analysis – analiza wpływu (**)
13. internal context – kontekst wewnętrzny (**)
14. likelihood – prawdopodobieństwo (*)
15. mitigation – łagodzenie (**)
16. monitoring – monitorowanie (*)
17. organization – organizacja (*)
18. outrage – wzburzenie społeczne (**)
19. people at risk – ludność zagrożona (*)
20. policy – polityka (*)
21. residual risk – ryzyko rezydualne /reliktowe/ (**)
22. resilience – odporność (*)
23. review – przegląd (*)
24. risk – ryzyko (*)
25. risk acceptance – akceptacja ryzyka (**)
26. risk analysis – analiza ryzyka (**)
27. risk assessment – ocena ryzyka (**)
28. risk attitude – nastawienie do ryzyka (**)
29. risk avoidance – unikanie ryzyka (**)
30. risk criteria – kryteria ryzyka (**)
31. risk control strategy – strategia kontroli ryzyka (**)
32. risk evaluation – ewaluacja ryzyka (**)
33. risk identification – identyfikacja ryzyka (**)
34. risk level – poziom ryzyka (**)
35. risk management – zarządzanie ryzykiem (*)
36. risk management framework – struktura ramowa zarządzania ryzykiem (**)
37. risk management plan – plan zarządzania ryzykiem (**)
38. risk map – mapa ryzyka (*)

39. risk owner – właściciel ryzyka (**)
40. risk perception – percepcja ryzyka (**)
41. risk profile – profil ryzyka (**)
42. risk register – rejestr ryzyk (**)
43. risk scenario – scenariusz ryzyka (**)
44. risk sharing – dzielenie się ryzykiem (**)
45. risk source – źródło ryzyka (**)
46. risk treatment – postępowanie z ryzykiem (**)
47. stakeholder – interesariusz (**)
48. strategy – strategia (*)
49. threat – zagrożenie (*)
50. uncertain – niepewność (*)
51. vulnerability – podatność (*)

POLSKO-ANGIELSKI SŁOWNIK PODSTAWOWYCH POJĘĆ Z ZAKRESU ZARZĄDZANIA RYZYKIEM

1. akceptacja ryzyka – risk acceptance (**)
2. analiza ryzyka – risk analysis (**)
3. analiza wpływu – impact analysis (*)
4. decydent – decision-maker (*)
5. dzielenie się ryzykiem – risk sharing (**)
6. ewaluacja ryzyka – risk evaluation (**)
7. identyfikacja niebezpieczeństwa – hazard identification (*)
8. identyfikacja ryzyka – risk identification (**)
9. interesariusz – stakeholder (**)
10. komunikacja i konsultacje – communication and consultation (**)
11. konsekwencje – consequence (*)
12. kontekst wewnętrzny – internal context (**)
13. kontekst zewnętrzny – external context (**)
14. kryteria ryzyka – risk criteria (**)
15. ludność zagrożona – people at risk (*)
16. łagodzenie – mitigation
17. mapa ryzyka – risk map (*)
18. mapa zagrożeń – hazard map (*)
19. minimalizowanie zagrożeń – hazard mitigation (*)
20. monitorowanie – monitoring (*)
21. nastawienie do ryzyka – risk attitude (**)
22. niepewność – uncertain (**)
23. ocena ryzyka – risk assessment (**)

24. odporność – resilience (*)
25. organizacja – organization (*)
26. percepcja ryzyka – risk perception (**)
27. plan zarządzania ryzykiem – risk management plan (**)
28. podatność – vulnerability (*)
29. polityka – policy (*)
30. postępowanie z ryzykiem – risk treatment (**)
31. poziom ryzyka – risk level (**)
32. prawdopodobieństwo – likelihood (*)
33. profil ryzyka – risk profile (**)
34. przegląd – review (**)
35. rejestr ryzyka – risk register (**)
36. ryzyko – risk (*)
37. ryzyko rezydualne (reliktowe) – residual risk (**)
38. scenariusz ryzyka – risk scenario (**)
39. strategia – strategy (*)
40. strategia kontroli ryzyka – risk control strategy (**)
41. struktura ramowa zarządzania ryzykiem – risk management framework (**)
42. unikanie ryzyka – risk avoidance (**)
43. ustalanie kontekstu – establishing the context (**)
44. właściciel ryzyka – risk owner (**)
45. wpływ – impact (*)
46. wzburzenie społeczne – outrage (**)
47. zagrożenie – hazard (*)
48. zagrożenie – threat (*)
49. zarządzanie ciągłością działania – business continuity management (*)
50. zarządzanie ryzykiem – risk management (*)
51. źródło ryzyka – risk source (**)

SŁOWNIK WYBRANYCH POJĘĆ Z ZAKRESU ZARZĄDZANIA RYZYKIEM

1. **Agregacja ryzyka** (***) – kombinacja kilku ryzyk w jedno ryzyko w celu uzyskania szerszego spojrzenia na całość ryzyka³.
2. **Akceptacja ryzyka** [ang. risk acceptance] (*) – świadoma decyzja o gotowości określonego podmiotu do narażenia się na dane ryzyko⁴.
3. **Akceptowany poziom ryzyka** (*) – jest wartością umowną. Jest rezultatem oceny ryzyka, która obejmuje porównanie poziomu ryzyka zidentyfikowanego

³ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁴ Tamże.

w procesie analizy z przyjętymi kryteriami. Ocenia się, czy oczekiwane ryzyko mieści się w granicach akceptacji lub tolerancji czy jest poza tymi granicami. Każde ryzyko, którego wartość wykracza poza poziom akceptowany, ale znajduje się jeszcze w granicach tolerancji, powinno wzmocnić czujność i uruchomić działania mające na celu jego monitorowanie, kontrolę i mechanizmy jego redukcji. Zanim jednak podejmie się jakiegokolwiek działania należy ocenić skuteczność monitoringu, wiarygodność informacji, poprawność analizy, możliwe straty lub korzyści wystąpienia ryzyka, przewidywane nakłady jego redukcji i ekonomiczność całego przedsięwzięcia⁵.

4. **Analiza** (*) – to teoretyczne i empiryczne wyodrębnienie właściwości, lub składników badanego zjawiska, czy przedmiotu w celu określenie znaczących faktów i późniejszej ich interpretacji⁶.
5. **Analiza ryzyka** [ang. *risk analysis*] (*) – proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka⁷.
6. **Analiza ryzyka** (*) – jest to analiza częstości wystąpienia zdarzenia niekorzystnego wraz z analizą jego skutków. Analiza ryzyka może być ilościowa, półilościowa, jakościowa⁸.
7. **Analiza ryzyka** (**) – oznacza proces składający się z trzech powiązanych elementów: oceny ryzyka, zarządzania ryzykiem i informowania o ryzyku⁹.
8. **Analiza skutków wystąpienia zagrożenia** (*) – zidentyfikowanie wpływu skutków zagrożenia na określony podmiot¹⁰.
9. **Analiza wpływu** [ang. *impact analysis*] (**) – analiza wykonywana na poziomie zarządczym, której celem jest zidentyfikowanie wpływu utraty zasobów przez organizację¹¹.
10. **Analiza zagrożeń** (*) – jest procesem ciągłym polegającym na identyfikacji zagrożeń i aktualizacji ich katalogu dla danego podmiotu¹².

⁵ J. Gołębiowski, *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, SA PSP, Kraków 2011, s. 120–121.

⁶ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera na podstawie: *Słownik terminów z zakresu bezpieczeństwa narodowego*, wersja elektroniczna, AON, Warszawa 2008, s. 9.

⁷ PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

⁸ J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 239.

⁹ Art. 3 rozporządzenia (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, (Dz. U. L 31 z 1.2.2002).

¹⁰ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

¹¹ NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs 2007 Edition.

¹² J. Gołębiowski, *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, SA PSP, Kraków 2011, s. 338.

11. **Audit (audyt) (**)** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z auditu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów auditu¹³.
12. **Audit (audyt) (**)** – systematyczny, niezależny i udokumentowany proces uzyskiwania zapisów, stwierdzenia faktów lub innych odpowiednich informacji i ich obiektywnej oceny w celu określenia stopnia spełnienia wyspecyfikowanych wymagań¹⁴.
13. **Audyt (*)** – jest rodzajem kontroli polegającej głównie na sprawdzeniu wykonania czegoś zgodnie z przyjętymi założeniami¹⁵.
14. **Bezpieczeństwo (*)** – to stan i/lub procesy zachodzące w otoczeniu cywilizacyjnym i **środowisku naturalnym, określone przez poziom całkowitego ryzyka**¹⁶.
15. **Cel (*)** – przyszły, pożądany stan rzeczy, możliwy i przewidziany do osiągnięcia w określonym przedziale czasu lub terminie¹⁷.
16. **Cel zarządzania ryzykiem powodziowym (**)** – rozumie się przez to ograniczenie potencjalnych negatywnych skutków powodzi dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej¹⁸.
17. **Czynniki ryzyka (**)** – to przyczyny mające decydujący wpływ na powstawanie ryzyka. Mogą mieć charakter niezależny od nas (pogoda, zjawiska przyrody, natura) i w pełni zależny (budżet, prawo, dobór personelu, ryzykowne badania naukowe)¹⁹.
18. **Działania korygujące (*)** – działania w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanego sytuacji²⁰.
19. **Działania zapobiegawcze (*)** – działania w celu wyeliminowania przyczyny potencjalnej niezgodności lub innej potencjalnej sytuacji niepożądanego²¹.
20. **Dzielenie się ryzykiem (*)** – rozdział ryzyka na kilku uczestników określonego podmiotu²².
21. **Efekt domina (*)** – teoria zakładająca, że jedno zdarzenie wywołuje ciąg kolejnych wydarzeń²³.

¹³ PN-EN ISO 19011:2012 Wtyczne dotyczące audytowania systemów zarządzania.

¹⁴ PN-EN ISO/IEC 17000:2006 Ocena zgodności. Terminologia i zasady ogólne.

¹⁵ A. Markowski, R. Pawelec (red.), *Nowy słownik wyrazów obcych i trudnych*, Wilga 2007.

¹⁶ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera na podstawie: J. Wolanin, *Zarys teorii bezpieczeństwa...*, dz. cyt., s. 35.

¹⁷ *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002.

¹⁸ Art. 9 ustawy z dnia 18 lipca 2001 r. Prawo wodne (Dz. U. z 2001 r. Nr 115, poz. 1229 z późn. zm.).

¹⁹ J. Gołębiowski, *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, SA PSP, Kraków 2011, s. 339.

²⁰ PN-EN ISO 9000:2006 Systemy zarządzania jakością. Podstawy i terminologia.

²¹ Tamże.

²² Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

²³ *Wielki słownik języka polskiego*, Instytut Języka Polskiego PAN: <http://www.wsjp.pl/>.

22. **Ewaluacja ryzyka** [ang. *risk evaluation*] (*) – proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane²⁴.
23. **Hierarchizacja ryzyka** (*) – w rozumieniu dosłownym oznacza ustalanie kolejności następujących po sobie rzeczy, zdarzeń, zagadnień od najważniejszych do najmniej ważnych²⁵.
24. **Identyfikacja ryzyka** [ang. *risk identification*] (*) – proces wyszukiwania, rozpoznawania i opisywania ryzyka²⁶.
25. **Identyfikacja ryzyka** (*) – proces wyszukiwania źródeł ryzyka, scenariuszy i potencjalnych skutków zagrożeń²⁷.
26. **Informowanie o ryzyku** (***) – oznacza interaktywną wymianę informacji i opinii podczas procesu analizy ryzyka, dotycząca zagrożeń i ryzyka, czynników związanych z ryzykiem i postrzeganiem ryzyka, między oceniającymi ryzyko, zarządzającymi ryzykiem, konsumentami, przedsiębiorstwami żywnościowymi i paszowymi, środowiskiem naukowym i innymi zainteresowanymi stronami, z uwzględnieniem wyjaśnienia wniosków z oceny ryzyka i powodów decyzji w zakresie zarządzania ryzykiem²⁸.
27. **Interesariusz** [ang. *stakeholder*] (***) – osoba, grupa osób lub organizacja wpływająca, na którą mogą wpływać, lub która jest przekonana że mogą na nią wpłynąć, podejmowane decyzje i zdarzenia²⁹.
28. **Klasyfikacja** (*) – to podział elementów rzeczywistości według przyjętych wcześniej kryteriów³⁰.
29. **Klasyfikacja ryzyka** (*) – jest to podział ryzyka według przyjętych wcześniej kryteriów³¹.
30. **Klasyfikacja zagrożeń** (*) – jest to podział zagrożeń według przyjętych wcześniej kryteriów³².
31. **Komunikacja i konsultacje** [ang. *communication and consultation*] (*) – ciągle i prowadzone w sposób iteracyjny procesy, które są przez organizację prowadzone w celu zapewnienia, przekazywania lub uzyskania informacji, jak również w celu porozumiewania się z interesariuszami, odnoszące się do zarządzaniem ryzykiem³³.

²⁴ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

²⁵ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

²⁶ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

²⁷ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

²⁸ Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (Dz. Urz. WE L 31 z 01.02.2002).

²⁹ CAN/CSA-Q850-97 (2009) Risk Management: Guideline for Decision-makers.

³⁰ A. Markowski, R. Pawelec, *Nowy słownik wyrazów obcych i trudnych*, Wilga 2007.

³¹ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego.

³² Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego.

³³ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

32. **Konsekwencje** [ang. *consequence*] (*) – rezultat zdarzenia mający wpływ na cele³⁴.
33. **Kontekst wewnętrzny** [ang. *internal context*] (*) – środowisko wewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów³⁵.
34. **Kontekst zewnętrzny** [ang. *external context*] (*) – środowisko zewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów³⁶.
35. **Kryteria ryzyka** [ang. *risk criteria*] (*) – poziomy odniesienia, względem których określa się hierarchię (ważność) ryzyka, kryteria oparte są na celach organizacyjnych oraz na zewnętrznym i wewnętrznym kontekście danego podmiotu³⁷.
36. **Krzywa F-N** (*) – jest ilościową metodą szacowania ryzyka opartą o analizę historii zdarzeń niekorzystnych³⁸.
37. **Ludność zagrożona** [ang. *people at risk*] (**) – wszystkie osoby przebywające na określonym terenie, na które może oddziaływać zdarzenie niekorzystne³⁹.
38. **Łagodzenie skutków zdarzeń niekorzystnych** (*) – zespół przedsięwzięć podjętych w celu ograniczenia skutków zdarzeń niekorzystnych⁴⁰.
39. **Mapa ryzyka** (*) – to mapa lub opis przedstawiający negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę wraz z prawdopodobieństwem wystąpienia tego zagrożenia⁴¹.
40. **Mapa ryzyka** (*) – to mapa lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę⁴².
41. **Mapa zagrożeń** (*) – to mapa, która przedstawia wielkość prawdopodobieństwa wystąpienia różnych zagrożeń na określonym obszarze⁴³.
42. **Mapa zagrożeń** (*) – mapa przedstawiająca obszar geograficzny objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń⁴⁴.

³⁴ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia. W literaturze przedmiotu zastępczo stosowane jest także pojęcie: skutek.

³⁵ Tamże.

³⁶ Tamże.

³⁷ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera na podstawie: PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

³⁸ J. Wolanin, *Zarys teorii bezpieczeństwa...*, dz. cyt., s. 229.

³⁹ ISO/DIS 22322 Societal security – Emergency Management – Public warning, projekt normy międzynarodowej z dnia 09.01.2013.

⁴⁰ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

⁴¹ Opracowanie autorskie prof. dr. hab. Jerzego Wolanina.

⁴² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm.).

⁴³ European Commission, Risk Assessment and Mapping Guidelines for Disaster Management, Commission Staff Working Paper, SEC(2010) 1626 final z dnia 21 grudnia 2010.

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

43. **Mapy ryzyka powodziowego** (*) – mapy przedstawiające potencjalne negatywne skutki powodzi⁴⁵.
44. **Mapy zagrożenia powodziowego** (*) – mapy przedstawiające obszary narażone na niebezpieczeństwo powodzi⁴⁶.
45. **Matryca ryzyka** (***) – graficzna ilustracja przedstawiająca poziom ryzyka w układzie współrzędnych: prawdopodobieństwa i skutków⁴⁷.
46. **Metoda postępowania z ryzykiem** (*) – sposób modyfikacji ryzyka, do którego można zaliczyć m.in.: unikanie ryzyka, podjęcie lub zwiększenie ryzyka, usunięcie źródła ryzyka, zmianę następstw, dzielenie ryzyka, retencję ryzyka⁴⁸.
47. **Mierniki ryzyka** (*) – określone w sposób ilościowy są wyrażone liczbowo i stanowią iloczyn prawdopodobieństwa i skutków i/lub ekspozycji na zagrożenie, określone w sposób jakościowy charakteryzują prawdopodobieństwo, skutki i/lub ekspozycję na zagrożenie⁴⁹.
48. **Mikrosystem zarządzania ryzykiem** (*) – to zamknięty obszar działania organizacji, instytucji, stowarzyszenia, na rzecz eliminacji lub ograniczania czynników ryzyka i samego ryzyka, będący w kompetencjach jednej lub kilku komórek⁵⁰.
49. **Minimalizowanie** (*) – to „przedsięwzięcia realizowane przed katastrofą, ukierunkowane na obniżenie lub wyeliminowanie jej wpływu na społeczeństwo i środowisko”, to całość działań podejmowanych celem ograniczenia lub wyeliminowania → *ryzyka wystąpienia zagrożenia* dla życia ludzi i ich mienia⁵¹. Minimalizowanie ma na celu eliminowanie lub ograniczanie → *czynników ryzyka*, wystąpienia zagrożeń i ich skutków. W tej fazie realizuje się: prace legislacyjne; inspekcje i kontrole; sporządza się mapy podwyższonego ryzyka; zawiera umowy; wdraża prawo; stosuje zachęty finansowe; planowanie przestrzenne; budowanie tam, grobli, zapór i innych budowli ograniczających ryzyko powodzi; doskonalą się sztuki planowania; sporządzania regionalnych stref zagrożeń; doskonalą prognozowania pogody; inwentaryzuje i organizuje zapasy oraz dostosowuje struktury.
50. **Minimalizowanie zagrożeń** [ang. *hazard mitigation*] (*) – działania mające na celu osłabienie skutków zagrożenia lub zmniejszenie prawdopodobieństwa

⁴⁵ Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim.

⁴⁶ Tamże.

⁴⁷ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera. W literaturze przedmiotu zastępczo stosowane jest także pojęcie: macierz ryzyka.

⁴⁸ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego na podstawie: PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

⁴⁹ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

⁵⁰ *Emergency Management: Principles and Practice for Local Government*, mat. FEMA, s. 263–264.

⁵¹ Tamże, s. 90.

- wystąpienia zagrożenia, polegające na czynnościach związanych z zapobieganiem, minimalizowaniem i przygotowaniem⁵².
51. **Modyfikacja ryzyka** (*) – działania podejmowane samodzielnie lub w kombinacji w celu ograniczenia ryzyka⁵³.
 52. **Monitorowanie** [ang. *monitoring*] (*) – ciągle sprawdzanie, nadzorowanie, krytyczne obserwowanie lub określanie stanu prowadzone w celu zidentyfikowania zmian w zakresie wymaganego lub oczekiwanego poziomu skuteczności⁵⁴.
 53. **Monitorowanie ryzyka** (**) – to obserwacja, zinventaryzowanie, sklasyfikowanie, analiza i ocena przy zastosowaniu przyjętych mierników ryzyka. Sporządzenie hierarchii ryzyka i prognoz rozwoju sytuacji. Monitorowanie ryzyka jest związane z monitorowaniem otoczenia bezpieczeństwa i inwentaryzacją zagrożeń. Rezultaty monitoringu ryzyka stanowią bazę planowania gotowości cywilnej⁵⁵.
 54. **Nastawienie do ryzyka** [ang. *risk attitude*] (**) – podejście organizacji do oceny i w konsekwencji monitorowania, zatrzymania, podjęcia lub unikania ryzyka⁵⁶.
 55. **Niepewność** [ang. *uncertain*] (*) – stan, również częściowy, braku informacji związanej ze zrozumieniem lub wiedzą na temat zdarzenia, jego następstw lub prawdopodobieństwa⁵⁷.
 56. **Obszar ryzyka** (*) – obszar, w którym występują istotne z punktu widzenia danego podmiotu czynniki ryzyka⁵⁸.
 57. **Ocena ryzyka** [ang. *risk assessment*] (*) – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz ewaluacji ryzyka⁵⁹.
 58. **Ocena ryzyka** (*) – określa całkowity poziom ryzyka spowodowanego różnymi zagrożeniami występującym w tym samym czasie albo następującymi szybko po sobie (z powodu wzajemnych zależności albo pochodzenia od tego samego źródła) albo narażającymi te same obszary bez chronologicznego porządku⁶⁰.
 59. **Ocena ryzyka** (**) – oznacza proces wsparty naukowo, składający się z czterech etapów: identyfikacji zagrożenia, charakterystyki niebezpieczeństwa, oceny ekspozycji i charakterystyki ryzyka⁶¹.

⁵² ISO/CD 22325 Societal security – Emergency management – Guidelines for emergency management security assessment.

⁵³ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego.

⁵⁴ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁵⁵ J. Gołębiewski, *Vademecum zarządzania kryzysowego*, część I, Warszawa 2008, s. 102, 127, 137–138.

⁵⁶ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁵⁷ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.

⁵⁸ Załącznik 1 do zarządzenia nr 80 Wojewody Mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

⁵⁹ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁶⁰ European Commission, Risk Assessment and Mapping Guidelines for Disaster Management, Commission Staff Working Paper, SEC(2010) 1626 final z dnia 21 grudnia 2010, s. 11.

⁶¹ Art. 3 rozporządzenia (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, (Dz. Urz. WE L 31 z 01.02.2002).

60. **Ocena zagrożeń** (*) – jest procesem wartościującym poszczególne zagrożenia⁶².
61. **Odporność** (*) – zdolność systemu, społeczności narażonej na zagrożenia do odparcia, wchłonięcia, przystosowania i odbudowy związanej ze skutkami zagrożenia dokonanej w odpowiednim czasie i w skuteczny sposób, włączając w to utrzymanie i odtworzenie ich podstawowych struktur i funkcji⁶³.
62. **Odporność** (*) – zdolność radzenia sobie z ryzykiem⁶⁴.
63. **Ograniczanie ryzyka** (*) – proces zmniejszający ryzyko bądź przez zmniejszenie prawdopodobieństwa, bądź/i skutków wystąpienia zdarzenia stwarzającego zagrożenie⁶⁵.
64. **Organizacja** (*) – to pewien rodzaj całości ze względu na stosunek do niej jej własnych elementów, mianowicie takich całości, której większe składniki współprzyczyniają się do powodzenia całości⁶⁶.
65. **Percepcja ryzyka** [ang. *risk perception*] (*) – znaczenie przypisywane ryzyku przez poszczególnych interesariuszy. Percepcja ta jest pochodną potrzeb, zagadnień i spraw poszczególnych interesariuszy⁶⁷.
66. **Plan zarządzania ryzykiem** [ang. *risk management plan*] (*) – plan zawarty w strukturze ramowej zarządzania ryzykiem określający podejście, elementy zarządzania i zasoby, które będą zastosowane w zarządzaniu ryzykiem⁶⁸.
67. **Planowanie** (*) – to wytyczanie celów organizacji i określanie sposobu ich najlepszej realizacji⁶⁹.
68. **Podatność** (***) – wewnętrzne właściwości skutkujące narażeniem na źródło ryzyka, które może prowadzić do zdarzenia z jego następstwami⁷⁰.
69. **Polityka** (*) – ogół zamierzeń i ukierunkowanie organizacji odnoszące się do całokształtu lub określonego aspektu działalności organizacji⁷¹.
70. **Polityka zarządzania ryzykiem** [ang. *risk management policy*] (*) – deklaracja dotycząca ogółu zamierzeń i ukierunkowania organizacji odnoszących się do zarządzania ryzykiem⁷².
71. **Postępowanie z ryzykiem** [ang. *risk treatment*] (*) – proces modyfikacji ryzyka poprzez m.in. unikanie ryzyka, podjęcie lub zwiększenie ryzyka, usunięcie źródła ryzyka, dzielenie ryzyka, retencję ryzyka⁷³.

⁶² Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

⁶³ European Commission, Risk Assessment and Mapping Guidelines for Disaster Management, Commission Staff Working Paper, SEC(2010) 1626 final z dnia 21 grudnia 2010, s. 10.

⁶⁴ J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 30.

⁶⁵ Tamże, s. 177.

⁶⁶ T. Kotarbiński, *Traktat o dobrej robocie*, Ossolineum 1972, s. 74.

⁶⁷ CAN/CSA-Q850-97 (2009) Risk Management: Guidelines for Decision-makers.

⁶⁸ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁶⁹ R.W. Griffin, *Podstawy zarządzania organizacjami*, PWN, Warszawa 1998, s. 40.

⁷⁰ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁷¹ Opracowanie na podstawie: PN-ISO 9000:2006 System zarządzania jakością. Podstawy i terminologia.

⁷² PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁷³ Tamże.

72. **Poziom podatności** (*) – wartość podatności lub suma podatności⁷⁴.
73. **Poziom ryzyka** (***) – wielkość ryzyka lub suma ryzyk⁷⁵.
74. **Poziom ryzyka** [ang. *risk level*] (**) – wielkość ryzyka lub kombinacji ryzyk, wyrażona w postaci kombinacji następstw oraz ich prawdopodobieństwa⁷⁶.
75. **Prawdopodobieństwo** [ang. *likelihood*] (*) – możliwość wystąpienia, szansa wystąpienia zdarzenia, prawdopodobieństwo może być definiowane, mierzone i określane w sposób obiektywny lub subiektywny, jakościowo lub ilościowo, może być określane przy użyciu ogólnych terminów jak i terminów matematycznych⁷⁷.
76. **Prawdopodobieństwo obiektywne** (*) – względna częstotliwość zdarzeń. Częstotliwość względna zbliża się do wartości prawdopodobieństwa w miarę zwiększania próby statystycznej⁷⁸.
77. **Prawdopodobieństwo subiektywne** (*) – kategoria odnosząca się do stanu umysłu decydenta i wyrażająca jego przekonanie o możliwości wystąpienia określonego zdarzenia⁷⁹.
78. **Profil ryzyka** [ang. *risk profile*] (*) – opis zestawu ryzyk⁸⁰.
79. **Przegląd** [ang. *review*] (*) – działanie podejmowane w celu określenia przydatności, adekwatności oraz skuteczności przedmiotu rozważań do osiągnięcia ustalonych celów⁸¹.
80. **Rejestr ryzyk** [ang. *risk register*] (*) – wykaz informacji o zidentyfikowanych ryzykach⁸².
81. **Ryzyko** (*) – rozumie się przez to prawdopodobieństwo wystąpienia konkretnego skutku w określonym czasie lub w określonej sytuacji⁸³.
82. **Ryzyko** [ang. *risk*] (*) – wpływ niepewności na cele⁸⁴.
83. **Ryzyko** (*) – jest to suma iloczynu prawdopodobieństwa wystąpienia zdarzenia niekorzystnego i jego skutków oraz społecznego wzburzenia⁸⁵.
84. **Ryzyko** (**) – oznacza niebezpieczeństwo zaistnienia negatywnych skutków dla zdrowia oraz dotkliwość takich skutków w następstwie zagrożenia⁸⁶.

⁷⁴ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego.

⁷⁵ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego.

⁷⁶ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁷⁷ Tamże.

⁷⁸ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

⁷⁹ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera na podstawie: *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002.

⁸⁰ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁸¹ Tamże.

⁸² Tamże.

⁸³ Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz. U. 2008 Nr 62, poz. 627 z późn. zm.).

⁸⁴ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

⁸⁵ P. M. Sandman, *Responding to Community Outrage: Strategies for effective Risk Communication*. American Industrial Hygiene Association Fairfax, Va. Fourth Printing 1997.

⁸⁶ Art. 3 rozporządzenia (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd

85. **Ryzyko akceptowalne** (*) – wielkość ryzyka, którą organizacja może zaakceptować bez żadnych dodatkowych działań zaradczych bądź zmian w funkcjonowaniu⁸⁷.
86. **Ryzyko całkowite** (***) – suma ryzyka obliczeniowego i wzburzenia społecznego⁸⁸.
87. **Ryzyko eksperckie** (*) – jest iloczynem prawdopodobieństwa wystąpienia zdarzenia niekorzystnego oraz jego potencjalnych skutków⁸⁹.
88. **Ryzyko grupowe** (*) – jest to prawdopodobieństwo tego, że określona liczba osób znajdujących się na danym obszarze jest narażona na negatywne skutki zdarzenia niekorzystnego lub prawdopodobieństwo tego, że określona liczba osób poddana jest danemu poziomowi ryzyka indywidualnego⁹⁰.
89. **Ryzyko indywidualne** (*) – jest to prawdopodobieństwo wystąpienia zdarzenia niekorzystnego, w określonym przedziale czasu, negatywnie oddziałyującego na pojedynczego człowieka. W skrajnym przypadku oddziaływanie to może doprowadzić do śmierci, w takich przypadkach mówimy o indywidualnym ryzyku śmierci⁹¹.
90. **Ryzyko kryzysowe** (*) – jest to ryzyko o takim rozmiarze, któremu system (organizacja) nie może sprostać w dowolnym czasie przy wykorzystaniu normalnych środków i procedur⁹².
91. **Ryzyko obliczeniowe** (***) – techniczna strona ryzyka wyrażona liczbowo jako iloczyn prawdopodobieństwa wystąpienia zdarzenia niekorzystnego i jego skutków⁹³.
92. **Ryzyko powodziowe** (*) – rozumie się przez to kombinację prawdopodobieństwa wystąpienia powodzi i potencjalnych negatywnych skutków powodzi dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej⁹⁴.

ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, (Dz. Urz. WE L 31 z 01.02.2002).

⁸⁷ Załącznik do Zarządzenia Nr 80 Wojewody Mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

⁸⁸ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. hab. inż. Dariusza Wróblewskiego na podstawie P. M. Sandman, *Risk = Hazard + Outrage: Coping with Controversy about Utility Risks*, „Engineering News-Record” 1999, October 4, pp. A19–A23.

⁸⁹ P. M. Sandman, *Responding to Community Outrage: Strategies for effective Risk Communication*, American Industrial Hygiene Association Fairfax Va, Fourth Printing, 1997.

⁹⁰ J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 29.

⁹¹ Tamże.

⁹² W. K. Knight, *Praktyczne aspekty zarządzania ryzykiem*, materiał z seminarium Stowarzyszenia Zarządzania Ryzykiem POLRISK z 8.06.2010 w Warszawie, s. 13.

⁹³ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. hab. inż. Dariusza Wróblewskiego na podstawie P. M. Sandman, *Risk = Hazard + Outrage: Coping with Controversy about Utility Risks*, „Engineering News-Record” 1999, October 4, pp. A19–A23.

⁹⁴ Ustawa z dnia 18 lipca 2001 r. Prawo wodne (Dz. U. Nr 115, poz. 1229 z późn. zm.).

93. **Ryzyko powodziowe** (*) – to kombinacja prawdopodobieństwa wystąpienia powodzi i związanych z powodzią potencjalnych negatywnych konsekwencji dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej⁹⁵.
94. **Ryzyko reliktowe (szczątkowe, resztkowe, rezydualne)** [ang. *residual risk*] (*) – pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem⁹⁶.
95. **Ryzyko strukturalne** (*) – stanowi współzależność zagrożeń, na które narażona jest społeczność i jej podatność na te zagrożenia⁹⁷.
96. **Ryzyko zredukowane** (*) – ryzyko, które pozostaje w wyniku działań powodujących jego redukcję⁹⁸.
97. **Scenariusz ryzyka** (*) – jest przedstawieniem jednej sytuacji związanej z ryzykiem lub grupą ryzyk prowadzącej do określonych skutków, wybranej w celu bardziej szczegółowej oceny konkretnego typu ryzyka, będącego ryzykiem reprezentatywnym, stanowiącym przykład informacyjny lub ilustrację⁹⁹.
98. **Sekwencja zdarzeń** (*) – seria niezależnych zdarzeń prowadząca do zdarzenia niekorzystnego¹⁰⁰.
99. **Siatka bezpieczeństwa** (*) – to zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego przy ich usuwaniu oraz podmiotów współpracujących¹⁰¹.
100. **Skutek** (*) – efekt zdarzenia wyrażony jakościowo lub ilościowo¹⁰².
101. **Sterowanie ryzykiem** (*) – proces podejmowania decyzji niezbędnych do zarządzania ryzykiem, wybór i wdrożenie wybranych opcji obniżenia poziomu ryzyka oraz legislacja wraz okresem badaniem efektywności tych działań¹⁰³.
102. **Strategia** (*) – oznacza logicznie skonstruowany plan lub metodę osiągnięcia celów, szczególnie w długim okresie¹⁰⁴.
103. **Struktura ramowa zarządzania ryzykiem** [ang. *risk management framework*] (**) – zestaw elementów zapewniających podstawy i ustalenia organizacyjne

⁹⁵ Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz. Urz. UE L 288/27 z 2007).

⁹⁶ PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

⁹⁷ J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 29.

⁹⁸ Tamże.

⁹⁹ Commission staff working paper. Risk Assessment and Mapping Guidelines for Disaster Management, Bruksela, 21.12.2010, s. 12.

¹⁰⁰ J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 174.

¹⁰¹ Ustawa z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590 z późn. zm).

¹⁰² J. Wolanin, *Zarys teorii bezpieczeństwa...*, dz. cyt., s. 174. W literaturze przedmiotu zastępczo stosowane jest także pojęcie: konsekwencje.

¹⁰³ J. Wolanin, *Zarys teorii bezpieczeństwa...*, dz. cyt., s. 183.

¹⁰⁴ PN-ISO 9004:2009 *Zarządzanie ukierunkowane na trwały sukces organizacji. Podejście wykorzystujące zarządzanie jakością*.

- w zakresie projektowania, wdrażania, monitorowania, dokonywania przeglądów i ciągłego doskonalenia zarządzania ryzykiem w całej organizacji¹⁰⁵.
104. **Szacowanie ryzyka** (*) – określanie przybliżonej wielkości potencjalnego ryzyka¹⁰⁶.
 105. **Szacowanie strat** (*) – ocena skutków zdarzenia¹⁰⁷.
 106. **Unikanie ryzyka** (*) – świadoma decyzja podmiotu o niewystawianiu się na dane ryzyko¹⁰⁸.
 107. **Ustalanie kontekstu ryzyka** [ang. *establishing the context*] (*) – definiowanie zewnętrznych i wewnętrznych parametrów, które powinny być uwzględnione podczas zarządzania ryzykiem, jak również podczas określania profilu i kryteriów ryzyka dla polityki zarządzania ryzykiem¹⁰⁹.
 108. **Wielkość ryzyka** (***) – cecha ryzyka wyrażona ilościowo lub jakościowo¹¹⁰.
 109. **Właściciel ryzyka** [ang. *risk owner*] (*) – podmiot rozliczany z zarządzania ryzykiem i uprawniona do tego zarządzania¹¹¹.
 110. **Wrażliwość ekspozycji** (*) – słaba odporność na czynniki oddziaływania zewnętrznego lub wewnętrznego będące wynikiem incydentu lub katastrofy. To podatność na skutki zdarzenia niekorzystnego¹¹².
 111. **Wzburzenie społeczne** [ang. *outrage*] (**) – pozatechniczna strona ryzyka związana z odczuciami ludzi, skupiająca się na wszystkim negatywnym wokół danego zdarzenia, pomijając jego skutki. Czy jest dobrowolne czy wymuszone, czy jest znane czy egzotyczne, czy się go obawia czy nie. Względem ludzi: czy są wiarygodni czy nie, czy są skuteczni w działaniu czy też nie¹¹³.
 112. **Wzburzenie społeczne** (*) – jest to emocjonalne, subiektywne odczucie związane z postrzeganiem zagrożenia¹¹⁴.
 113. **Zagrożenie** (*) – to stan rzeczy lub okoliczności wywołujących możliwość wystąpienia jednego z negatywnych zjawisk lub sytuacja wymagająca rozwiązania gdy może ona stworzyć poważne trudności¹¹⁵.
 114. **Zagrożenie** (**) – źródło potencjalnej szkody¹¹⁶.

¹⁰⁵ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

¹⁰⁶ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego.

¹⁰⁷ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

¹⁰⁸ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

¹⁰⁹ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

¹¹⁰ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. hab. inż. Dariusza Wróblewskiego.

¹¹¹ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

¹¹² J. Gołębiowski, *Vademecum zarządzania kryzysowego*, część III, Warszawa 2009, s. 84.

¹¹³ Opracowanie zespołu autorskiego CNBOP-PIB pod kierunkiem dr. inż. Dariusza Wróblewskiego na podstawie P.M. Sandman, *Risk = Hazard + Outrage: Coping with Controversy about Utility Risks*, „Engineering News-Record” 1999, October 4, pp. A19–A23.

¹¹⁴ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

¹¹⁵ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

¹¹⁶ PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

115. **Zagrożenie** [ang. *hazard*] (**) – źródło potencjalnej szkody lub sytuacja posiadająca potencjał do spowodowania szkody np. utraty zdrowia, zniszczenia mienia, środowiska i innych wartościowych rzeczy lub kombinacja powyższych¹¹⁷.
116. **Zagrożenie** (**) – oznacza czynnik biologiczny, chemiczny lub fizyczny w żywności lub paszy, bądź stan żywności lub paszy, mogący powodować negatywne skutki dla zdrowia¹¹⁸.
117. **Zagrożenie** (**) – sytuacja, w której naruszone mogą być istotne dla danego podmiotu wartości¹¹⁹.
118. **Zagrożenie** (**) – to możliwość wystąpienia jednego z negatywnie wartościowanych zjawisk¹²⁰.
119. **Zarządzanie ciągłością działania** [ang. *business continuity management*] (**) – zdolność organizacji do planowania i reagowania na incydenty i zakłócenia działalności w taki sposób, aby kontynuować działalność na akceptowalnym zdefiniowanym poziomie¹²¹.
120. **Zarządzanie ryzykiem** [ang. *risk management*] (*) – skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka¹²².
121. **Zarządzanie ryzykiem** (*) – system metod i działań zmierzających do obniżenia ryzyka do akceptowalnego poziomu¹²³.
122. **Zarządzanie ryzykiem** (**) – oznacza proces, różniący się od oceny ryzyka, polegający na zbadaniu alternatywy polityki w porozumieniu z zainteresowanymi stronami, wzięciu pod uwagę oceny ryzyka i innych prawnie uzasadnionych czynników, i w razie potrzeby – na wybraniu stosownych sposobów zapobiegania i kontroli¹²⁴.
123. **Zdarzenie** (*) – wystąpienie lub zmiana określonego stanu rzeczy, który może wystąpić jeden raz bądź wielokrotnie i może mieć wiele przyczyn¹²⁵.

¹¹⁷ CAN/CSA-Q850-97 (2009) Risk Management: Guideline for Decision-makers.

¹¹⁸ Art. 3 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, (Dz. Urz. WE L 31 z 01.02.2002).

¹¹⁹ Z. Ciekanski, *Zagrożenia bezpieczeństwa państwa*, BiTP Vol. 21 Issue 1, 2011, pp. 69–77.

¹²⁰ Z. Ciekanski, R. Zięba, *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych*, [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wiek*, D. Bobrów, E. Haliżak, R. Zięba, Warszawa 1997, s. 4.

¹²¹ PAS 200:2011 Crisis management – Guidance and good practice.

¹²² PKN-ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia.

¹²³ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

¹²⁴ Art. 3 rozporządzenia (WE) NR 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, (Dz. Urz. WE L 31 z 01.02.2002).

¹²⁵ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

124. **Zdarzenie inicjujące** (*) – zdarzenie początkowe w całym łańcuchu zdarzeń prowadzące do kolejnych, sekwencyjnie występujących zdarzeń niekorzystnych¹²⁶.
125. **Zdarzenie niekorzystne** (*) – podzbiór zbioru zdarzeń niepożądanych i nieoczekiwanych, zdarzenie powstające nagle i powodujące śmierć lub uszczerbek zdrowia, szkody w mieniu lub/i negatywnie oddziałujące niekorzystnie na środowisko naturalne i przestrzeń cywilizacyjną¹²⁷.
126. **Źródła ryzyka** (*) – obiekty i okoliczności stwarzające zagrożenie¹²⁸.
127. **Źródło ryzyka** [ang. *risk source*] (**) – element, który sam lub w połączeniu z innymi ma wewnętrzny potencjał, aby powodować powstanie ryzyka¹²⁹.

¹²⁶ J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 174.

¹²⁷ Tamże.

¹²⁸ Opracowanie zespołu autorskiego pod kierunkiem prof. dr. hab. inż. Waldemara Kitlera.

¹²⁹ PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne.

Na podstawie danych z Systemu Informacji Prawnej LEX stwierdzono, że pojęcie „ryzyko” występuje w 4828 aktach prawnych, co daje prawie dwukrotny wzrost w ciągu ośmiu lat względem 2009 roku, w którym pojawiało się ono w 2686 dokumentach prawodawczych. Biorąc pod uwagę wyłącznie okres od pierwszego wydania niniejszej monografii do chwili obecnej, liczba aktów prawnych uwzględniających to pojęcie zwiększyła się o 621, co daje prawie 30-procentowy wzrost w ciągu niecałych trzech lat.

W związku z powyższym uzasadnione wydało się przygotowanie kolejnego wydania monografii *Zarządzanie ryzykiem. Przegląd wybranych metodyk* – rozszerzonego o komplementarne tematycznie treści zaczerpnięte z trzech publikacji:

1. *Rekomendacje formalno-prawne z zakresu zarządzania kryzysowego* – wykorzystano angielsko-polski i polsko-angielski słownik pojęć oraz słownik rekomendowanych pojęć.
2. *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem* – wykorzystano Część III Zarządzanie ryzykiem oraz Część IV Wybrane pojęcia z zakresu zarządzania kryzysowego i zarządzania ryzykiem.
3. *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego* – wykorzystano Część III Zarządzanie ryzykiem w Unii Europejskiej.

Z uwagi na czas, jaki upłynął od pierwszego wydania trzech powyższych publikacji, autorzy dokonali aktualizacji pierwotnych treści oraz uzupełnili je o istotne dla tego obszaru tematycznego wątki, czego efektem jest niniejsza monografia. Powstała ona z myślą zarówno o osobach zainteresowanych zawodowo przedmiotową problematyką, jak i studentach kierunków związanych z zarządzaniem – szczególnie jeżeli chodzi o przyjęty przez autorów i rekomendowany słownik terminów związanych z zarządzaniem.

brg. dr hab. inż. Dariusz Wróblewski
Redaktor wydania, Dyrektor CNBOP-PIB

ISBN: 978-83-948534-0-2
DOI : 10.17381/2018.1

Wydawnictwo CNBOP-PIB
www.cnbop.pl

