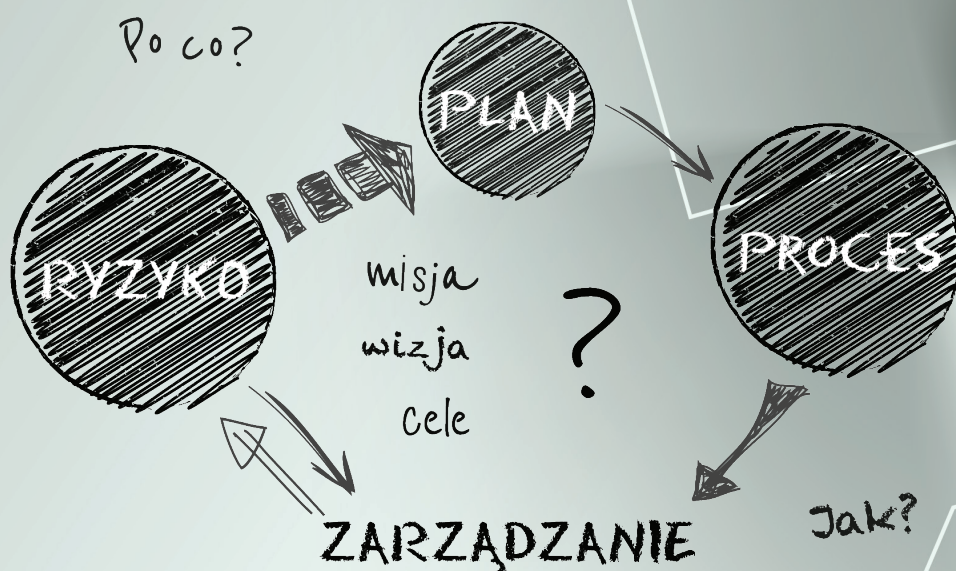


Zarządzanie ryzykiem



Przegląd wybranych metodyk

Redakcja naukowa
bryg. dr inż. Dariusz Wróblewski



Wydawnictwo CNBOP-PIB



GRSECO
POLAND

ZARZĄDZANIE RYZYKIEM – PRZEGLĄD WYBRANYCH METODYK

Praca pod redakcją

bryg. dr. inż. Dariusza Wróblewskiego

Publikacja finansowana przez NCBiR w ramach projektu
„Zintegrowany system budowy planów zarządzania kryzysowego
w oparciu o nowoczesne technologie informatyczne”
nr DOBR/0016/R/ID2/2012/03

Józefów 2015



ASSECO
POLAND

RISK MANAGEMENT – A REVIEW OF THE SELECTED METHODOLOGIES

**The work edited by
Dariusz Wróblewski, Brig. PhD**

The publication financed by NCBiR under the project
"Integrated system of creating emergency management plans
based on modern information technologies"

No. DOBR/0016/R/ID2/2012/03

Józefów, 2015

Praca zbiorowa pod redakcją

bryg. dr. inż. Dariusza Wróblewskiego

Zespół autorski w składzie:

Grzegorz Abgarowicz

Inga Abgarowicz

Anna Banulska

Jan Gołębiewski

Piotr Guzewski

Maria Kędzierska

Daniel Małozieć

Maciej Napiórkowski

Bartłomiej Połec

Witold Skomra

Ewa Sobór

Tomasz Sowa

Paweł Stępień

Małgorzata Trzcńska

Recenzenci:

st. bryg. dr inż. Paweł Janik

mł. bryg. dr inż. Paweł Kęпка

dr hab. inż. Bogdan Kosowski

st. bryg. mgr inż. Dariusz Marczyński

DOI: 10.17381/2015.1

ISBN 978-83-61520-18-4

Przygotowanie do druku:

Fundacja Edukacja i Technika Ratownictwa

Projekt okładki:

Julia Pinkiewicz

© Copyright by Wydawnictwo Centrum Naukowo-Badawczego Ochrony
Przeciwpożarowej im. Józefa Tuliszkowskiego Państwowego Instytutu Badawczego

Wydawca:

Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej

im. Józefa Tuliszkowskiego

Państwowy Instytut Badawczy

05-420 Józefów k. Otwocka, ul. Nadwiślańska 213

www.cnbop.pl

Druk i oprawa:

Fundacja Edukacja i Technika Ratownictwa

Liczba arkuszy wydawniczych: 18

Nakład: 250 egz.

A collective work edited by Dariusz Wróblewski, Brig. PhD

A team of authors composed of:

Grzegorz Abgarowicz

Inga Abgarowicz

Anna Banulska

Jan Gołębiewski

Piotr Guzowski

Maria Kędzierska

Daniel Małozieć

Maciej Napiórkowski

Bartłomiej Połec

Witold Skomra

Ewa Sobór

Tomasz Sowa

Paweł Stępień

Małgorzata Trzcńska

Reviewers:

Sr Brig. PhD Paweł Janik

Jr Brig. PhD Paweł Kępka

PhD Bogdan Kosowski

Sr Brig. M. Eng. Dariusz Marczyński

DOI: 10.17381/2015.1

ISBN 978-83-61520-18-4

Prepared for printing by:

Fundacja Edukacja i Technika Ratownictwa

Cover design by:

Julia Pinkiewicz

© Copyright by Wydawnictwo Centrum Naukowo-Badawczego
Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego Państwowego Instytutu Badawczego

Publisher:

Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej

im. Józefa Tuliszkowskiego

Państwowy Instytut Badawczy

05-420 Józefów k. Otwocka, ul. Nadwiślańska 213

www.cnbop.pl

Printed and bound by:

Fundacja Edukacja i Technika Ratownictwa

Number of author's sheets: 18

Circulation: 250 copies

Spis treści

WYKORZYSTANE SPRAWOZDANIA Z BADAŃ	16
SPIS OZNACZEŃ	17
CZĘŚĆ I ZAGADNIENIA OGÓLNE Z ZAKRESU ZARZĄDZANIA RYZYKIEM	21
WPROWADZENIE.....	22
1. ZARZĄDZANIE RYZYKIEM WEDŁUG NORMY ISO 31000.....	26
1.1. Norma ISO 31000:2009 – zakres i przeznaczenie.....	27
1.2. Zasady zarządzania ryzykiem.....	30
1.3. Struktura ramowa zarządzania ryzykiem	32
1.4. Proces zarządzania ryzykiem	37
1.5. Dokumentowanie zarządzania ryzykiem	52
2. METODY WYKORZYSTYWANE W OCENIE RYZYKA.....	55
2.1. Metoda, metodyka, metodologia.....	56
2.2. Analiza przyczyn i konsekwencji (cause and consequence analysis)	62
2.3. Analiza przyczynowo – skutkowa (cause and effect analysis).....	64
2.4. Analiza warstw ochrony – LOPA (layer protection analysis)	67
2.5. Analiza drzewa decyzji (decision tree analysis).....	69
2.6. Analiza drzewa błędów (fault tree analysis).....	71
2.7. Analiza drzewa zdarzeń (event tree analysis)	73
2.8. Ocena niezawodności człowieka (human reliability analysis)	74
2.9. Analiza muchy (bow tie analysis)	77
2.10. Metoda konserwacji ukierunkowana na niezawodność – RCM (reliability centred maintenance).....	79
2.11. Zapowiedź analizy – SA (sneak analysis) i zapowiedź analizy obwodu – SCA (sneak circuit analysis)	81
2.12. Metoda SWIFT – co jeśli? (structured „what if?” technique).....	82
2.13. Analiza scenariuszowa (scenario analysis)	83
2.14. Analiza wpływu na działalność – BIA (business impact analysis)	84
2.15. Matryca skutek/prawdopodobieństwo (consequence/probability matrix).....	86
PODSUMOWANIE I WNIOSKI	91
LITERATURA.....	99
CZĘŚĆ II ZARZĄDZANIE RYZYKIEM NA SZCZEBLU UE	103
WPROWADZENIE.....	104
1. ZARZĄDZANIE RYZYKIEM POWODZIOWYM	108
1.1. Wstępna ocena ryzyka powodziowego	110
1.2. Mapy zagrożenia powodziowego i mapy ryzyka	112
1.3. Plany zarządzania ryzykiem powodziowym	113
2. KONTROLA ZAGROZEŃ POWAŻNYMI AWARIAMI ZWIĄZANYMI Z SUBSTANCJAMI NIEBEZPIECZNYMI – Seveso III	115
3. ZARZĄDZANIE RYZYKIEM ZWIĄZANYM Z ELEKTROWNIAМИ JĄDROWYMI – TESTY WYTRZYMAŁOŚCIOWE	119
4. ZARZĄDZANIE RYZYKIEM W DZIEDZINIE ZDROWIA UE	124
5. ZARZĄDZANIE RYZYKIEM NIELEGALNEJ IMIGRACJI – FRONTEx	129
6. PRZYKŁADOWE PROJEKTY BADAWCZE Z ZAKRESU OCENY RYZYKA	133
6.1. KultuRisk.....	133
6.2. Matrix.....	135

6.3. Catalyst	136
PODSUMOWANIE I WNIOSKI	138
LITERATURA.....	148
CZĘŚĆ III ZARZĄDZANIE RYZYKIEM W WYBRANYCH PAŃSTWACH	151
WPROWADZENIE.....	152
1. ZARZĄDZANIE RYZYKIEM W AUSTRALII	156
1.1. Narodowe ramy oceny ryzyka	157
1.2. Opis procesu zarządzania ryzykiem	166
2. ZARZĄDZANIE RYZYKIEM W IRLANDII.....	182
2.1. Ramy zarządzania poważnymi sytuacjami kryzysowymi	182
2.2. Narodowa ocena ryzyka Irlandii	186
3. ZARZĄDZANIE RYZYKIEM W REPUBLICE FEDERALNEJ NIEMIEC	195
3.1. Metoda analizy ryzyka dla ochrony ludności.....	195
4. ZARZĄDZANIE RYZYKIEM W SZWECJI	207
4.1. Przewodnik po analizie ryzyka i podatności	207
4.2. Szwedzka narodowa ocena ryzyka 2012	225
5. ZARZĄDZANIE RYZYKIEM W WIELKIEJ BRYTANII	237
5.1. Krajowy rejestr ryzyka	237
5.2. Standard zarządzania ryzykiem FERMA.....	243
PODSUMOWANIE I WNIOSKI	257
LITERATURA.....	276
CZĘŚĆ IV ZARZĄDZANIE RYZYKIEM W RP	279
WPROWADZENIE.....	280
1. ZARZĄDZANIE RYZYKIEM W PLANOWANIU CYWILNYM	284
1.1. Plany zarządzania kryzysowego.....	287
1.2. Raport o zagrożeniach bezpieczeństwa narodowego	289
1.3. Ochrona infrastruktury krytycznej	295
2. METODA WDROŻENIA ZARZĄDZANIA RYZYKIEM W PROCES PLANOWANIA CYWILNEGO.....	298
2.1. Metoda wykorzystania norm ISO w zakresie zarządzania ryzykiem w planowaniu cywilnym.....	299
2.2. Szczegółowy opis procesu z uwzględnieniem istniejących ograniczeń formalno- prawnych	303
3. ZARZĄDZANIE RYZYKIEM POWODZIOWYM	321
3.1. Implementacja dyrektywy do polskiego systemu prawnego	321
3.2. Proces wdrażania polityki zarządzania ryzykiem	324
3.3. Plany zarządzania ryzykiem powodziowym	333
4. ZARZĄDZANIE RYZYKIEM W KONTROLI ZARZĄDCZEJ	338
4.1. Zarządzanie ryzykiem na szczeblu centralnym	340
4.2. Zarządzanie ryzykiem w województwie, powiecie i gminie	360
5. METODYKA DIAGNOZOWANIA SYSTEMÓW REAGOWANIA POMRISC – ELEMENTY ZARZĄDZANIA RYZYKIEM	374
5.1. Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego	375
5.2. Metody badawcze wykorzystane na potrzeby analizy oceny ryzyka – PomRisc	377
5.3. Identyfikacja i ocena wielkości ryzyka	384
5.4. Diagnoza systemu reagowania jako komponentu zarządzania ryzykiem	398
6. DOCHODZENIE W SPRAWACH O POŻARY JAKO ELEMENT ZARZĄDZANIA RYZYKIEM POŻAROWYM W POLSCE.....	413

6.1. Społeczno-ekonomiczne koszty pożarów jako bodziec rozwoju zarządzania ryzykiem pożarowym	416
6.2. Zarządzanie ryzykiem pożarowym w aspekcie teoretycznym i praktycznym.....	423
PODSUMOWANIE I WNIOSKI	429
LITERATURA.....	453
INDEKS POJĘĆ.....	459
SPIS RYSUNKÓW.....	463
SPIS TABEL.....	466
NOTKI BIOGRAFICZNE AUTORÓW I RECENZENTÓW	469

Table of Contents

USE OF THE STUDY REPORT	16
INDEX OF SYMBOLS	17
PART I GENERAL ISSUES IN SCOPE OF RISK MANAGEMENT	21
INTRODUCTION	24
1. RISK MANAGEMENT ACCORDING TO ISO 31000	26
1.1. ISO 31000:2009 – scope and purpose	27
1.2. Risk management principles	30
1.3. Framework for managing risk	32
1.4. Risk management process	37
1.5. Evidencing of risk management	52
2. METHODS USED IN RISK ASSESSMENT	55
2.1. Technique, methodology	56
2.2. Cause and consequence analysis	62
2.3. Cause and effect analysis	64
2.4. Layer Protection Analysis (LOPA)	67
2.5. Decision tree analysis	69
2.6. Fault tree analysis	71
2.7. Event tree analysis	73
2.8. Human reliability analysis	74
2.9. Bow tie analysis	77
2.10. Reliability centred maintenance (RCM)	79
2.11. Sneak analysis (SA) and Sneak circuit analysis (SCA)	81
2.12. Structured “what if?” technique	82
2.13. Scenario analysis	83
2.14. Business impact analysis (BIA)	84
2.15. Consequence/probability matrix	86
SUMMARY AND CONCLUSIONS	95
REFERENCES	99
PART II RISK MANAGEMENT AT THE EU LEVEL	103
INTRODUCTION	106
1. FLOOD RISK MANAGEMENT	108
1.1. Preliminary assessment of flood risk	110
1.2. Flood hazards and flood risks maps	112
1.3. Flood risk management plans	113
2. CONTROL OF HAZARDS OF SERIOUS FAILURES RELATED TO HAZARDOUS SUBSTANCES – Seveso III	115
3. RISK MANAGEMENT RELATED TO NUCLEAR PLANTS – STRENGTH TESTS	119
4. RISK MANAGEMENT IN THE AREA OF EU HEALTH	124
5. RISK MANAGEMENT FOR ILLEGAL IMMIGRATION – FRONTEX	129
6. EXAMPLES OF RESEARCH PROJECTS FOR RISK ASSESSMENT	133
6.1. Kulturisk	133
6.2. Matrix	135
6.3. Catalyst	136
SUMMARY AND CONCLUSIONS	143
REFERENCES	148
PART III RISK MANAGEMENT IN SELECTED COUNTRIES	151

INTRODUCTION	154
1. RISK MANAGEMENT IN AUSTRALIA.....	156
1.1. National Risk Assessment Framework	157
1.2. Description of risk management process.....	166
2. RISK MANAGEMENT IN IRELAND.....	182
2.1. Management framework for serious emergency situations.....	182
2.2. National Risk Assessment for Ireland.....	186
3. RISK MANAGEMENT IN GERMAN FEDERAL REPUBLIC.....	195
3.1. Risk analyses methods for civil protection	195
4. RISK MANAGEMENT IN SWEDEN	207
4.1. Guide to risk and vulnerability analysis.....	207
4.2. Swedish National Risk Assessment 2012.....	225
5. RISK MANAGEMENT IN THE GREAT BRITAIN	237
5.1. National Risk Register of Civil Emergencies	237
5.2. FERMA Risk Management Standard.....	243
SUMMARY AND CONCLUSIONS	267
REFERENCES	276
PART IV RISK MANAGEMENT IN THE REPUBLIC OF POLAND	279
INTRODUCTION	282
1. RISK MANAGEMENT IN CIVIL EMERGENCY PLANNING	284
1.1. Emergency management plans.....	287
1.2. Report on threats to national security.....	289
1.3. Protection of Critical Infrastructure	295
2. METHODS OF RISK MANAGEMENT IMPLEMENTATION IN CIVIL EMERGENCY PLANNING PROCESS.....	298
2.1. Method of using ISO standards for risk assessment in civil emergency planning.....	299
2.2. Detailed process description according to the existing formal and legal limitations ...	303
3. FLOOD RISK MANAGEMENT.....	321
3.1. Directive implementation into Polish legislative system	321
3.2. Risk management policy implementation process	324
3.3. Flood risks management plans.....	333
4. RISK MANAGEMENT IN GOVERNANCE CONTROL	338
4.1. Risk management at central level	340
4.2. Risk management in voivodeship, powiat and commune.....	360
5. DIAGNOSTICS METHODOLOGY OF POMRISC RESPONSE SYSTEMS – RISK MANAGEMENT ELEMENTS	374
5.1. Functioning concept of the regional integrated rescue system in Pomeranian Voivodeship.....	375
5.2. Research methods used for risk assessment analysis – PomRisc.....	377
5.3. Identification and assessment of risk level	384
5.4. Diagnosis of the response system as a component of risk management	398
6. INVESTIGATION IN FIRE CASES AS PART OF FIRE RISK MANAGEMENT IN POLAND	413
6.1. Social and economic costs of fire as a stimulus for development of fire risk management	416
6.2. Fire risk management in the theoretical and practical aspect.....	423
SUMMARY AND CONCLUSIONS	441
REFERENCES	453
INDEX OF TERMS	459
LIST OF FIGURES	463

LIST OF TABLES	466
BIOGRAPHICAL NOTES OF AUTHORS AND REVIEWERS.....	469

Szanowni Państwo,

przed Państwem piąta już publikacja pt. „Zarządzanie ryzykiem – przegląd wybranych metodyk”. Zawiera ona wyniki badań zespołu Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowego Instytutu Badawczego uzyskane podczas realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”. Projekt ten finansowany jest przez Narodowe Centrum Badań i Rozwoju. Jego realizacja została zaplanowana na lata 2012-2015, zaś wykonawcą jest konsorcjum naukowo-przemysłowe w składzie:

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

Zespół autorski w ramach badań dokonał identyfikacji i analizy standardów i norm w zakresie zasad oraz wytycznych zarządzania ryzykiem, metod zarządzania ryzykiem w procesie planowania cywilnego, metodyk oceny ryzyka i zagrożeń w przepisach prawa międzynarodowego i krajowego – z uwzględnieniem prawa miejscowego oraz metodyk oceny ryzyka i zagrożeń w normach i projektach norm z zakresu zarządzania ryzykiem. Na potrzeby opracowania tej monografii dokonano również przeglądu wybranych pozycji literatury przedmiotu. Głównym celem analizy powyższych zagadnień jest dostarczenie specjalistom i organizacjom wdrażającym procesy zarządzania ryzykiem uniwersalnych modeli oraz dobrych praktyk i wskazówek do zastosowania, ze szczególnym uwzględnieniem wytycznych do planowania cywilnego w obszarze zarządzania ryzykiem. Analiza opisanego materiału badawczego miała dać przegląd najważniejszych dokumentów normatywnych, a także terminologii z zakresu zarządzania ryzykiem – przy zastosowaniu kryterium użyteczności dla projektu. Analizując obcojęzyczne dokumenty, zespół autorski zdefiniował problem właściwego zrozumienia i tłumaczenia

pojęć. Związane to było między innymi z wieloznacznością nazewnictwa, wynikającą ze stosowania terminów wymiennie.

Aby uniknąć niejednoznaczności, które pojawiają się również w przetłumaczonych opracowaniach, autorzy zdecydowali się większość pojęć zaczerpnąć z uznanej normy ISO Guide 73:2009 *Risk Management – Vocabulary* i dokonać ujednoczenia terminologii. Jeżeli norma nie wyczerpywała danej definicji, korzystano z innych uznanych źródeł, np. z wiedzy słownikowej oraz literaturowej.

Sprawne porozumiewanie się, czy to w sferze naukowej, czy praktycznej, zależy od stosowania jednolitej i zrozumiałej dla wszystkich terminologii, zazwyczaj jest ona bowiem uwarunkowana odmiennymi doświadczeniami różnych państw, organizacji, sektorów działalności i branż, a także niedoskonałym tłumaczeniem i posługiwaniem się terminami wymiennie. Publikacja ta nie zawiera słownika, a jedynie indeks pojęć, kierujący czytelnika do objaśnień podstawowych terminów, pozwalający na właściwy odbiór poruszanych zagadnień.

Niniejsze opracowanie składa się z czterech zasadniczych części:

- Część I. Zagadnienia ogólne z zakresu zarządzania ryzykiem,
- Część II. Zarządzanie ryzykiem na szczeblu UE,
- Część III. Zarządzanie ryzykiem w wybranych państwach,
- Część IV. Zarządzanie ryzykiem w RP.

W części pierwszej, w rozdziale „Zarządzanie ryzykiem według normy ISO 31000”, przedstawione zostały potrzeby i korzyści związane z systemowym podejściem do problemu zarządzania ryzykiem na podstawie badań normy ISO 31000:2009. Opisano w niej także wybrane metody, które mogą zostać wykorzystane w procesie oceny ryzyka, również w ramach planowania cywilnego.

W części II „Zarządzanie ryzykiem na szczeblu UE” znalazły się wyniki analizy metodyk oceny ryzyka dla poszczególnych rodzajów zagrożeń, odnoszących się do wybranych aktywności Unii Europejskiej. Badaniom literaturowym poddano pięć obszarów oraz trzy przykładowe projekty badawcze z zakresu oceny ryzyka.

W ramach części III „Zarządzanie ryzykiem w wybranych państwach” dokonano analizy metodyk oceny ryzyka stosowanych w Australii, Irlandii,

Niemczech, Szwecji i Wielkiej Brytanii, a także sposobów identyfikacji zagrożeń na szczeblu krajowym, szacowania ryzyka ich wystąpienia oraz ewaluacji.

Część IV „Zarządzanie ryzykiem w RP” zawiera opis metodyk i rozwiązań wykorzystujących elementy zarządzania ryzykiem w procesie planowania cywilnego, związanych z ryzykiem powodziowym czy pożarowym, a także występujących w kontroli zarządczej. Opisana została również nowatorska metodyka diagnozowania systemów reagowania PomRisc.

Dokumenty poddane badaniom w niniejszej publikacji wskazują, że dzięki sprawnemu, efektywnemu, strategicznemu, zrównoważonemu projektowaniu oraz planowaniu działań i środków, a także konkretnie zdefiniowanym celom możliwe jest zapobieganie ryzyku oraz ograniczanie jego rozmiarów.

Wszystkie osoby zainteresowane pogłębieniem wiedzy w tym zakresie zachęcam również do sięgnięcia do czterech pozycji prezentujących wyniki projektu: „Planowanie cywilne w systemie zarządzania kryzysowego” (ISBN 978-83-61520-19-1), „Wybrane zagadnienia z zakresu planowania cywilnego w systemie zarządzania kryzysowego RP” (ISBN 978-83-61520-23-8), „Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem” (ISBN 978-83-61520-27-6), „Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego – analiza wybranych przepisów” (ISBN 978-83-61520-31-3), a także kolejnych publikacji przygotowywanych w ramach tego projektu.

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

<http://czytelnia.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, zarządzania ryzykiem i planowania.

Z poważaniem

bryg. dr inż. Dariusz Wróblewski
kierownik projektu

Dear Readers,

It is our pleasure to present you the fifth publication titled “Risk Management – A Review of the Selected Methodologies” containing the selected results of the studies led by Scientific and Research Centre for Fire Protection – the National Research Institute, obtained during implementation of the project titled “Integrated system of creating emergency management plans based on modern information technologies”. The project is financed by the National Centre for Research and Development, and its implementation has been planned for the years of 2012-2015, and the contractor is a scientific and industrial consortium composed of:

1. Scientific and Research Centre for Fire Protection – the National Research Institute;
2. National Defence University – National Security Faculty;
3. The Main School of Fire Service;
4. The Association of Voluntary Fire Brigades of the Republic of Poland;
5. Asseco Poland S.A.

The team of authors has identified and analysed the following documents under the studies: standards and norms in the field of risk management principles and guidelines; risk management methods in a civil emergency planning process; risk and hazard assessment methodologies in international and national laws with consideration to the local law; risk and hazard assessment methodologies in risk management standards and draft standards. Moreover, the selected thematic literature has been analysed for the purpose of preparing the monograph. The principal aim of analysing the above issues is to deliver universal models for specialists and organisations implementing risk management processes, and also to furnish good practices and hints for use, with special regard to civil emergency planning guidelines in the field of risk management. The research material in question has also been analysed in order to review the most essential normative documents, and also terminology in the field of risk management using project usefulness evaluation criteria. When analysing documents in foreign languages, the authors’ team defined the problem of correct understanding

and translation of terms, mainly due to the ambiguity of nomenclature resulting from the interchangeable usage of terms.

In order to avoid disambiguates occurring also in translated papers, the authors have decided that the majority of terms would be based on the standard ISO Guide 73:2009 *Risk Management – Vocabulary* and that terminology would be harmonised. If the standard was not exhaustive for a given definition, other recognised references were also used, e.g. knowledge from vocabularies and literature.

Efficient communication in the scientific or practical field is dependent on the usage of consistent terminology understandable for everyone, despite the fact that such terminology is conditioned by various experiences of different countries, organisations or sectors of activity and industries, and also by imperfect translation and the interchangeable use of terms. The publication does not include a glossary, only an index of terms, referring the reader to the explanation of basic terms in order to understand correctly the issues discussed.

This publication is comprised of the four major parts:

Part I General issues in scope of risk management;

Part II Risk management at the EU level;

Part III Risk management in selected countries;

Part IV Risk management in the Republic of Poland.

The first part “Risk management according to ISO 31000” presents the needs and benefits associated with a system-based approach to risk management based on the study of the standard ISO 31000:2009 and describes selected methods which can be potentially used in the risk assessment process, also under civil emergency planning.

Part II “Risk management at the EU level” presents the results of an analysis of risk assessment methodologies for particular types of hazards referring to the selected activities of the European Union. Five areas and three examples of research projects in scope of risk assessment were subject to literature studies.

Part III “Risk management in selected countries” analyses the risk assessment methodologies applied in Australia, Ireland, Germany, Sweden,

the Great Britain and solutions related to hazard identification at the national level, to estimation of their occurrence risk, as well as evaluation.

Part IV “Risk management in the Republic of Poland” describes a number of methodologies and solutions using risk management elements in a civil emergency planning process, associated with the flood or fire risk, and also those occurring in governance control. An innovative methodology of diagnosing the PomRisc response systems was also described.

The documents subject to the studies in this publication in scope of risk management indicate that there is a chance to prevent and mitigate a risk owing to the effective, efficient, strategic and sustainable programming and planning of measures and resources, as well as precisely defined objectives.

Therefore, all the persons interested in broadening the knowledge of the topics discussed are encouraged to familiarise themselves with the four publications presenting the project’s outcomes, i.e. “Civil Emergency Planning in the Emergency Management System” (ISBN 978-83-61520-19-1), “Selected aspects in scope of civil emergency planning in the emergency management system of the Republic of Poland” (ISBN 978-83-61520-23-8), “A review of selected normative documents in scope of emergency management and risk management with a lexicon” (ISBN 978-83-61520-27-6) and “General aspects of risk management and emergency management – analysis of selected regulations” (ISBN 978-83-61520-31-3), and also the future publications being prepared under the implemented project.

Wishing you interesting reading, I invite you also to visit our web-sites:

<http://czytelnia.cnbop.pl>,

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

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

where, I hope, you will find other interesting source materials concerning emergency management, rescue service, risk management and planning.

With kind regards

Dariusz Wróblewski, Brig. PhD
Project Manager

WYKORZYSTANE SPRAWOZDANIA Z BADAŃ

Na potrzeby niniejszej monografii wykorzystanych zostało 11 sprawozdań z badań:

1. G. Abgarowicz Czynniki ryzyka (*risk factors*).
2. G. Abgarowicz Normy ISO w procesie planowania cywilnego.
3. G. Abgarowicz Wykorzystanie metod zarządzania ryzykiem w procesie planowania cywilnego.
4. I. Abgarowicz
J. Smoła Analiza metodyk oceny ryzyka i zagrożeń ujętych w przepisach krajowego prawa powszechnie obowiązującego z elementami zarządzania ryzykiem i związanego z zarządzaniem ryzykiem – diagnoza stanu.
5. A. Banulska
T. Sowa Analiza metodyk oceny ryzyka i zagrożeń ujętych w normach z zakresu zarządzania ryzykiem – diagnoza stanu.
6. J. Gołębiwski Analiza metodyk oceny ryzyka i zagrożeń ujętych w przepisach międzynarodowych z wyłączeniem UE związanych z zarządzaniem ryzykiem – diagnoza stanu.
7. M. Napiórkowski Analiza metodyk oceny ryzyka i zagrożeń w przepisach krajowego prawa resortowego związanego z zarządzaniem ryzykiem – diagnoza stanu.
8. B. Połec Analiza metodyk oceny ryzyka i zagrożeń w przepisach krajowego prawa miejscowego związanego z zarządzaniem ryzykiem – diagnoza stanu.
9. W. Skomra Opracowanie metod oceny ryzyka na potrzeby planowania cywilnego.
10. E. Sobór
P. Stępień Analiza metodyk oceny ryzyka i zagrożeń ujętych w projektach norm z zakresu zarządzania ryzykiem – diagnoza stanu.
11. M. Trzcńska Analiza metodyk oceny ryzyka i zagrożeń ujętych w przepisach UE związanych z zarządzaniem ryzykiem – diagnoza stanu.

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
KPZK – Krajowy Plan Zarządzania Kryzysowego
KRS – Krajowy Rejestr Sądowy
KZGW – Krajowy Zarząd Gospodarki Wodnej
MAiC – Ministerstwo Administracji i Cyfryzacji
MEN – Ministerstwo Edukacji Narodowej
MON – Ministerstwo Obrony Narodowej
MSB (ang. *Swedish Civil Contingencies Agency*) – Szwedzka Agencja ds. Cywilnych Sytuacji Kryzysowych
MSW – Ministerstwo Spraw Wewnętrznych
MSWiA – Ministerstwo Spraw Wewnętrznych i Administracji
MSZ – Ministerstwo Spraw Zagranicznych
MTBiGM – Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej
NCBR – Narodowe Centrum Badań i Rozwoju
NFPA (ang. *National Fire Protection Association*) – Narodowe Stowarzyszenie Ochrony Przeciwpożarowej
NGO (ang. *non-governmental organization*) – organizacja pozarządowa
NIP – numer identyfikacji podatkowej
NPOiK – Narodowy Program Ochrony Infrastruktury Krytycznej
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

SAMG (ang. *Sevère Accident Management Guidelines*) – wytyczne dotyczące zarządzania poważnymi awariami

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

CZĘŚĆ I
ZAGADNIENIA OGÓLNE Z ZAKRESU
ZARZĄDZANIA RYZYKIEM

PART I
GENERAL ISSUES IN SCOPE
OF RISK MANAGEMENT

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. Odbyło się wiele spotkań, służących wymianie myśli i doświadczeń. Organizowane 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 POL-RISK.

Wynikiem prac ekspertów w takiej formule był pełen kompromis w postaci nowej normy, zalecanej do zaadaptowania w każdych uwarunkowaniach. 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 ryzy-

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_wyplywajace_z_kryzysu_tcm75-25681.pdf [dostęp 9 czerwca 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. nauk.), *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*.

kiem do zaadaptowania w systemach, służące poprawie ich skuteczności. Wdrożenie tych komponentów nie komplikuje działań organizacji, ale zwiększa szanse osiągnięcia jej celu. Podkreśla się, 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.

INTRODUCTION

A diagnosis is formulated in numerous publications devoted to the last financial crisis that it had been caused by imperfect risk management⁴. It is also implied that an approach to the area of a so-called residual risk⁵ had been treated too leniently. The case was approached seriously and independently of the sources of the crisis, an attempt was made to make many improvements in scope of risk management. Principles and a guideline for new risk management standards were introduced in 2009. A starting point was to admit that failure to take risks does not lead to successes nor ensures any progress, but on the other hand, similar consequences may occur if an excessive risk is taken. Many principles of such an activity were therefore formulated. First of all it was found that the effectiveness of risk management depends on an appropriate risk assessment. Such a risk cannot be either overestimated or underrated. The new standards of risk management are an outcome of the work of a team of experts from 28 countries from all continents. Numerous meetings of such experts were organised and the exchange of thoughts and experiences in many countries, collecting each time from 40 to 60 delegates. A constant group, being a leading body for coordination and continuation of the team's works, was always taking part in such meetings. The team's works were supported by national risk management teams, for example by POLRISK in Poland.

As a result of such a framework of the experts' activity, a full compromise was reached in the form of a new standard recommended for adaptation in any conditions. The standard, ISO 31000:2009⁶, is a group of principles, framework and processes for use by any organisation in scope of risk management and, more broadly, emergency management. It does not provide ready solutions,

⁴ *Conclusions drawn from the financial crisis from the management perspective*, a presentation from a meeting of the heads of the banks operating in Poland with the management of the Polish Financial Supervision Authority UKNF (Warsaw, 25 February 2011).

⁵ Residual risk – a risk remaining after application of actions specified in a risk management procedures. Reference: ISO Guide 73:2009 *Risk Management – Vocabulary*, definitions 3.8.1.6. See more: D. Wróblewski, (scientific edit.), *A review of selected normative documents in scope of emergency management and risk management with a lexicon*, CNBOP-PIB, Józefów 2014, p. 174.

⁶ The Polish version of the standard: PN-ISO 31000:2012 *Risk Management. Principles and Guidelines*.

but components of risk management to be adopted within systems to increase their efficiency. The implementation of such components does not complicate an organisation's activities, but increases the likelihood of achieving its objectives. It is emphasised that it can be fulfilled provided: a common, understandable terminology is used, clear processes and the right information is possessed.

The first chapter presents the needs and benefits associated with a system-based approach to the problem of risk management. ISO 31000:2009 was indicated as an example in the context of the studies performed, thus the document was recommended as a basis for the most universal and comprehensive use in organisations facing a broadly conceived risk on a daily basis. The examples of documenting the risk management process were also presented. The second chapter describes selected methods which can be potentially utilised in a risk assessment process, also under civil emergency planning.

1. ZARZĄDZANIE RYZYKIEM WEDŁUG NORMY ISO 31000

Zarządzanie ryzykiem⁷ stało się wyznacznikiem i integralnym elementem kultury organizacyjnej⁸, co oznacza przełożenie na cele strategiczne⁹, taktyczne i operacyjne¹⁰ oraz ścisłe sprecyzowanie odpowiedzialności¹¹ 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 zebrali na polu swojej działalności. Procedury opracowania norm przewidują obowiązkowy etap ankietowania, tj. poddawania normy publicznej dyskusji – po to, by wyeliminować

⁷ Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka. Źródło: ISO Guide 73:2009, definicja 2.1.

⁸ 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: Cz. Sikorski, *Kultura organizacyjna*, C.H. Beck, Warszawa 2002, s. 4.

⁹ 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 w zakresie bezpieczeństwa narodowego*, AON, Warszawa 2008, s. 25.

¹⁰ 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 14 marca 2015].

¹¹ *A Risk Management Standard*, IRM 2002, s. 2.

wać 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 nakreślonego 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 się poruszać. Wspierają je także w¹²:

1. Działaniach organizacyjnych polegających na:
 - 1.1. zwiększeniu prawdopodobieństwa osiągnięcia celu,
 - 1.2. uświadomieniu potrzeby identyfikacji ryzyka¹³,
 - 1.3. stosowaniu właściwych, wymaganych regulacji prawnych i norm międzynarodowych,
 - 1.4. zwiększaniu zaufania i pewności wśród zainteresowanych podmiotów,

¹² PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 14-16.

¹³ Identyfikacja ryzyka – proces wyszukiwania, rozpoznawania i opisywania ryzyka. Źródło: ISO Guide 73:2009, definicja 3.5.1.

- 1.5. ustanowieniu dogodnej bazy dla planowania i podejmowania decyzji,
 - 1.6. efektywnej alokacji i wykorzystaniu zasobów w zakresie postępowania z ryzykiem¹⁴,
 - 1.7. zapewnieniu ustalonych norm zdrowia i bezpieczeństwa oraz ochrony środowiska,
 - 1.8. minimalizowaniu strat.
2. Działaniach doskonalących w zakresie:
- 2.1. identyfikacji szans i zagrożeń,
 - 2.2. sprawozdawczości finansowej,
 - 2.3. organizacji procesów,
 - 2.4. procesu kontroli,
 - 2.5. operacyjnej skuteczności i efektywności systemu,
 - 2.6. zapobiegania stratom i kierowania w miejscach zdarzeń (incydentów),
 - 2.7. wykorzystania doświadczeń w organizacji,
 - 2.8. elastyczności organizacyjnej.

Międzynarodowa norma zarządzania ryzykiem wprowadziła cztery zasadnicze ustalenia¹⁵:

1. zmieniła definicję ryzyka¹⁶ na „wpływ niepewności na cele”,
2. wdrożyła jedenaście zasad zarządzania ryzykiem,
3. podała pięć atrybutów określających ramy zarządzania ryzykiem,
4. włączyła rekomendacje w zakresie podejścia do rozwoju ram zarządzania ryzykiem w skali całej organizacji.

¹⁴ 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.

¹⁵ 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 11 czerwca 2013].

¹⁶ Ryzyko – wpływ niepewności na cele. Źródło: ISO Guide 73:2009, definicja 1.1. Patrz szerzej: D. Wróblewski, (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 173.

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 ryzyka¹⁷, 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 ryzykiem¹⁸. 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 fizyczne¹⁹.

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 ryzyka²⁰ lub wystąpienia jego potencjalnych konsekwencji²¹. Wszystkie trzy filary zostały scharakteryzowane poniżej.

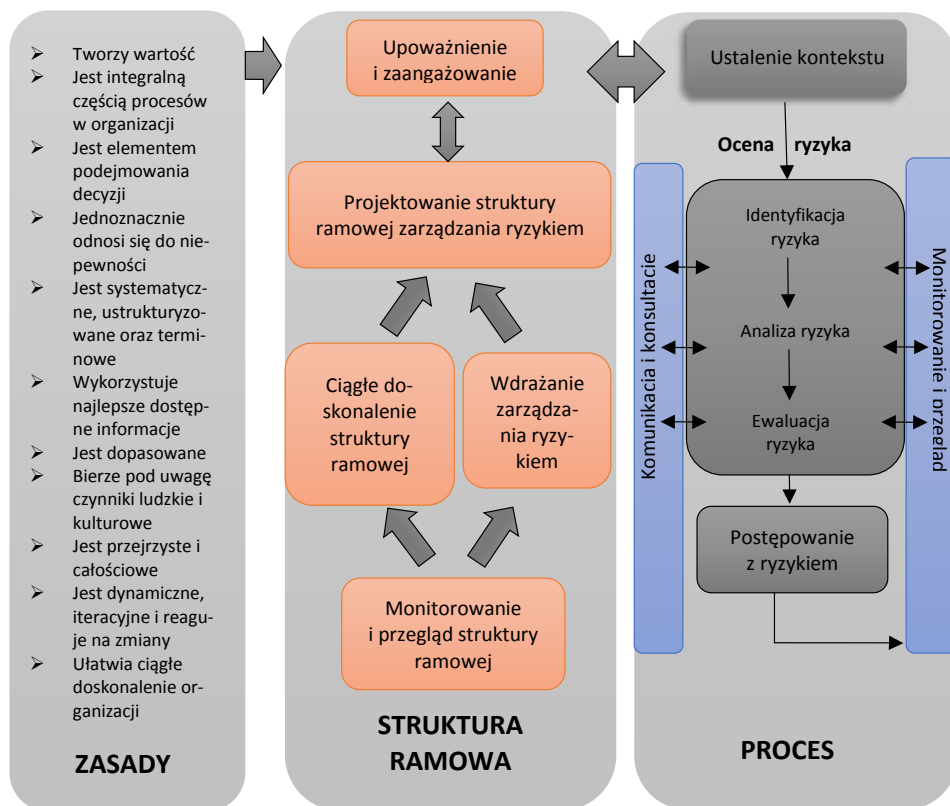
¹⁷ Ocena ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz ewaluacji ryzyka. Źródło: ISO Guide 73:2009, definicja 3.4.1. Patrz szerzej: D. Wróblewski (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 161.

¹⁸ <http://www.pbsg.pl/wiadomosci/analiza-ryzyka/iso-31000-pbsg.html>, dostęp: czerwiec 2013.

¹⁹ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 198-199.

²⁰ Patrz: ograniczanie ryzyka, s. 157.

²¹ Konsekwencje – rezultat zdarzenia mający wpływ na cele. Źródło: ISO Guide 73:2009, definicja 3.6.1.3.



Rys. 1. Relacje między zasadami, strukturą ramową i procesem zarządzania ryzykiem²²

1.2. Zasady zarządzania ryzykiem

W pierwszym filarze wyodrębnionych zostało jedenaście zasad, których kompleksowe wdrożenie w całej organizacji i poszczególnych obszarach jej działalności wpływa na efektywność zarządzania ryzykiem. Po pierwsze – zarządzanie ryzykiem powinno tworzyć oraz chronić wartość, która przekłada się na wyższą skuteczność osiągania celów. Pozwala to również stale doskonalić pro-

²² Źródło: opracowanie własne na podstawie PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*.

wadzoną działalność na każdym kierunku²³. 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 ograniczyć²⁴. Po piąte – w kontekście osiąganych 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 kontekstu²⁵, czy niewłaściwie przeprowadzonej identyfikacji bądź analizy ryzyka²⁶ i dalej – wątpliwie oszacowanej niepewności²⁷. 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

²³ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 200-201.

²⁴ PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 27-29.

²⁵ 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.

²⁶ Analiza ryzyka – proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka. Źródło: ISO Guide 73:2009, definicja 3.6.1.

²⁷ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 201.

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 ryzyka²⁸, ponieważ poszczególni decydenci mogą nie być świadomi niektórych ryzyk występujących w organizacji. Zwiększa to skuteczność podejmowanych działań, a tym samym jakość funkcjonowania całej organizacji²⁹. 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 ryzykiem³⁰

Ramy zarządzania ryzykiem określone zostały poprzez pięć atrybutów³¹:

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),

²⁸ 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. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 181-182.

²⁹ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 201.

³⁰ 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.

³¹ 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_F A3_23082010_0.pdf [dostęp 11 czerwca 2013].

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 procesie tym 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.

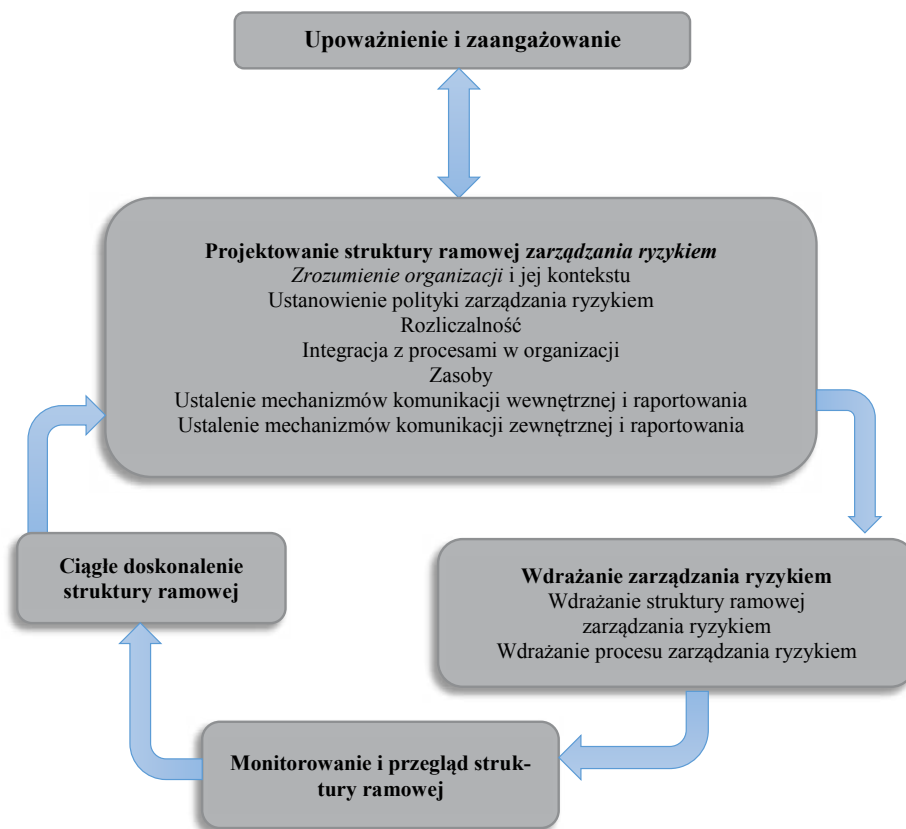
Norma akcentuje potrzebę doskonalenia ram³², które pomogą zintegrować zarządzanie ryzykiem z zarządzaniem organizacją. Dlatego zachęca się do zapewnienia bliższych powiązań ram zarządzania ryzykiem z celami organizacji. Ramy zarządzania ryzykiem powinny być osadzone na strategii³³ ogólnej oraz polityce³⁴ prowadzonych działań i praktyce. Powinny uwzględniać związki zewnętrzne i wewnętrzne, zakresy odpowiedzialności, zasoby, procesy i prowadzone działania.

Struktura ramowa, którą nakreśla ISO, umożliwi skuteczną 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.

³² Tamże.

³³ Strategia – oznacza logicznie skonstruowany plan lub metodę osiągnięcia celów, szczególnie w długim okresie. Źródło: PN-ISO 9004:2009 *Zarządzanie ukierunkowane na trwałą sukces organizacji. Podejście wykorzystujące zarządzanie jakością*, s. 17.

³⁴ 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.



Rys. 2. Relacje pomiędzy elementami struktury ramowej³⁵

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 w dalszym ciągu procesu. Pod pojęciem upoważnienia i zaangażowania rozumie się mechanizm zapewniający silny i trwały udział kierownictwa w procesie zarządzania ryzykiem³⁶. Funkcja ta powinna być realizowana przede

³⁵ Źródło: opracowanie własne na podstawie PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*.

³⁶ Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 31.

wszystkim na poziomie strategicznego planowania polityki organizacji i zawierać się między innymi w procesach:

1. definiowania i zatwierdzania polityki zarządzania ryzykiem,
2. zapewnienia spójności kultury organizacyjnej i polityki zarządzania ryzykiem,
3. określania wskaźników wyników zarządzania ryzykiem, które są spójne ze wskaźnikami rozwoju organizacji³⁷,
4. dostosowania celów zarządzania ryzykiem do celów i strategii organizacji,
5. zapewnienia zgodności zarządzania ryzykiem z przepisami prawa i wymaganiami regulacyjnymi,
6. zagwarantowania zasobów niezbędnych do zarządzania ryzykiem,
7. ciągłej weryfikacji, czy struktura ramowa zarządzania ryzykiem pozostaje właściwa³⁸.

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 kontekstu³⁹. 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 organiza-

³⁷ 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.

³⁸ PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 33.

³⁹ Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 33.

cyjnego⁴⁰ 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 organizacji⁴¹.

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 raportowania⁴².

Powyższe zasady powinny zostać uzupełnione poprzez wprowadzenie w organizacji odpowiedzialności za poszczególne ryzyka poprzez przypisanie jej konkretnym członkom instytucji⁴³, 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 ryzykiem⁴⁴.

⁴⁰ Ład organizacyjny – system, według którego organizacja podejmuje i wdraża decyzje służące realizacji jej celów. Źródło: PN-ISO 26000:2012 *Wytyczne dotyczące społecznej odpowiedzialności*.

⁴¹ Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 33.

⁴² Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 35.

⁴³ Osoby odpowiedzialne zarówno za wdrożenie i utrzymanie struktury ramowej, jak i proces zarządzania ryzykiem.

⁴⁴ Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 37.

Kolejnym krokiem po zaprojektowaniu struktury jest jej wdrożenie oraz ciągłe monitorowanie⁴⁵ i przegląd⁴⁶. Podczas wdrażania struktury ramowej ISO zaleca między innymi:

1. określenie harmonogramu i strategii wdrażania struktury ramowej,
2. respektowanie wymagań formalnych (w tym prawnych),
3. organizowanie szkoleń i kampanii informacyjnych,
4. 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 do wewnętrznego i zewnętrznego kontekstu organizacji. To właśnie monitorowanie umożliwia ciągłe doskonalenie kultury zarządzania ryzykiem⁴⁷.

1.4. Proces zarządzania ryzykiem

Zgodnie z międzynarodowymi normami proces zarządzania ryzykiem sprowadza się do: oceny ryzyka – w tym jego identyfikacji, analizy i ewaluacji⁴⁸, 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

⁴⁵ Monitorowanie – ciągłe 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.

⁴⁶ 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.

⁴⁷ 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.

⁴⁸ 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.

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:

1. właściwie sprecyzuje się cel (bądź cele),
2. dysponuje się zrozumiałym i przejrzystym procesem planowania,
3. stworzy się adekwatną do wymogów strukturę organizacyjną,
4. 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 metodykę⁴⁹ zarządzania ryzykiem, a nie odwrotnie.

Zarządzanie ryzykiem to proces leżący w kompetencji dyrekcji, zarządu, menedżerów i personelu, desygnowanych do identyfikacji ryzyka i zajmujących się 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 akceptowalne⁵⁰. Zarządzanie ryzykiem to również ograniczanie niepewności i możliwość sprostania jej.

⁴⁹ 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. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 159.

⁵⁰ Ryzyko akceptowalne – wielkość ryzyka, którą organizacja może zaakceptować bez żadnych dodatkowych działań zaradczych bądź zmian w funkcjonowaniu. Patrz: D. Wróblewski (red.

Percepcja ryzyka⁵¹ w społeczeństwie informacyjnym jest szczególna i może się znacząco różnić w zależności od grupy bądź nawet jednostki, która nieradko 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 ekspozycji⁵² na dane ryzyko, liczebność grup wystawionych na ryzyko, skala i trwałość jego skutków oraz poziom ryzyka⁵³ w odniesieniu do konkretnego środowiska. Niebagatelne znaczenie mają również możliwe zmiany ryzyka lub odporności⁵⁴ 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 ryzyka⁵⁵ reliktoowego artykułowane jest po to, by uwzględnić je podczas zarządzania ryzykiem, ustalania wartości kryteriów ryzyka⁵⁶

nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 174.

⁵¹ 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*.

⁵² 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. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 182. Za: J. Gołębiwski, *Vademecum zarządzania kryzysowego*, część III, Warszawa 2009, s. 84.

⁵³ 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.

⁵⁴ Odporność – zdolność radzenia sobie z ryzykiem. Źródło: J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 30.

⁵⁵ 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 zmniejsza-

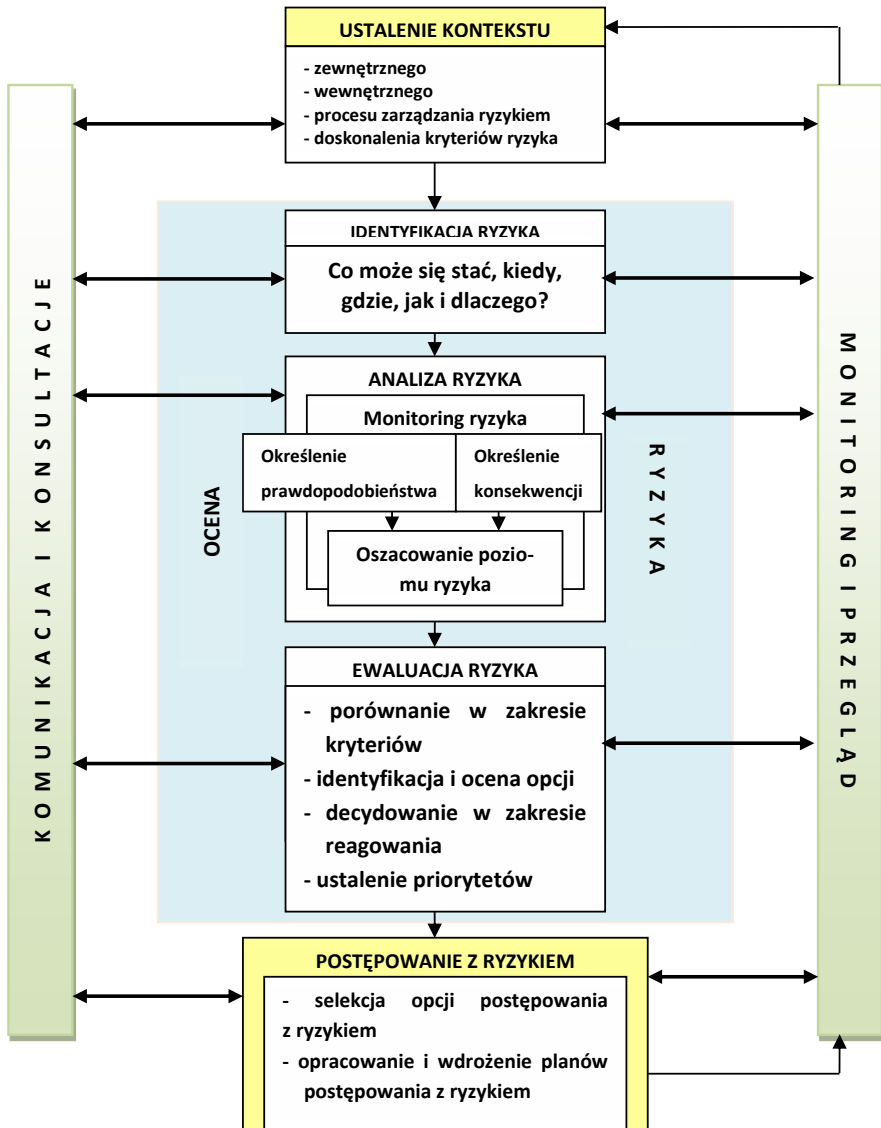
i zarysowania całego procesu. Bardzo ważne są parametry organizacji, które muszą spełniać kryteria ryzyka. Norma z serii ISO 31000 jest bez wątpienia dokumentem wartym zastosowania, pozwala bowiem wdrożyć w organizacji skuteczny proces zarządzania ryzykiem. Oczywiście w opracowaniach krajowych, w przypadku 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 konsultacje⁵⁷, ustalenie kontekstu, ocenę ryzyka, postępowanie z ryzykiem oraz monitorowanie i przegląd.

niem 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 teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 183.

⁵⁶ 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.

⁵⁷ Komunikacja i konsultacje – ciągłe 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.



Rys. 3. Proces zarządzania ryzykiem⁵⁸

⁵⁸ Źródło: K. W. Knight, *The New Standard For Risk Management*, materiał przygotowany na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.

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 interesariuszami⁵⁹. 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 kontekstu⁶⁰. 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

⁵⁹ 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*.

⁶⁰ Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 43-47.

odwołanie się do wartości organizacji oraz jej celów i misji⁶¹. Norma wskazuje, że definiując kryteria, należy brać pod uwagę⁶²:

1. charakter i rodzaje przyczyn i następstw, które mogą wystąpić, a także sposób ich mierzenia,
2. sposób definiowania prawdopodobieństwa⁶³ wystąpienia,
3. ramy czasowe wystąpienia prawdopodobieństwa i/lub następstw,
4. sposób ustalania poziomu ryzyka⁶⁴,
5. poziom ryzyka akceptowalnego⁶⁵ lub tolerowanego⁶⁶.

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. Kompetencje⁶⁷ i odpowiedzialność personelu powin-

⁶¹ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 205-206.

⁶² Opracowanie własne na podstawie: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 47.

⁶³ Prawdopodobieństwo – możliwość, szansa wystąpienia zdarzenia. Źródło: ISO Guide 73:2009 *Risk Management – Vocabulary*, definicja 3.6.1.1.

⁶⁴ Patrz: definicja na s. 38.

⁶⁵ Patrz: definicja na s. 39.

⁶⁶ 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.

⁶⁷ 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 osiągnięcia zamierzonych wyników. Źródło: PN-EN ISO/IEC

ny być precyzyjnie rozdzielone, kryteria ryzyka zdefiniowane i zgodne z celami organizacji. Wszystkie te działania powinny być prowadzone pod kątem szeroko pojmowanego planowania oraz być użyteczne w planowaniu.

1.4.3. Ocena ryzyka

Kolejnym istotnym działaniem jest ocena ryzyka. Wymaga ona wytypowania wyczerpującej listy zagrożeń⁶⁸. 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 zaistnienie⁶⁹. Dokonując identyfikacji, należy pamiętać o efekcie kaskadowym (domina)⁷⁰, który wpływa na pojawienie się kolejnych ryzyk⁷¹. 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:

17021:2011 *Ocena zgodności. Wymagania dla jednostek prowadzących audyty i certyfikację systemów zarządzania.*

⁶⁸ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 206.

⁶⁹ Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 47-49.

⁷⁰ 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.

⁷¹ Element ten jest istotny, ponieważ niektóre ryzyka (zagrożenia) mogą występować jedynie jako następstwa innych ryzyk.

1. źródła ryzyka⁷² lub zagrożenia,
2. zdarzenia lub incydenty będące źródłami ryzyka,
3. konsekwencje dla organizacji i otoczenia,
4. przyczyny obecnych zagrożeń lub występujących zdarzeń,
5. skuteczność monitoringu i systemów detekcyjnych,
6. miejsce i czas wystąpienia ryzyka.

Komponenty te rozpatrujemy oddzielnie w odniesieniu do każdego zdarzenia mogącego stworzyć zagrożenie (huragany, mecze piłkarskie, powódzie, 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, zaniedbania i zaniedbania, ignorancja, niekompetencja, korupcja (systemowa).
3. **Możliwe obszary ryzyka**⁷³: państwo, dział administracji rządowej, środowisko naturalne, społeczeństwo, społeczności, wspólnoty, działalność gospodarcza, organizacja, procesy rozwojowe, otoczenie bezpieczeństwa, informowanie i inne nieustalone.

⁷² 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”.

⁷³ 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.

W dalszej kolejności właściwie zagregowane ryzyka⁷⁴ należy poddać analizie. Analiza ryzyka służy jego szczegółowemu zrozumieniu. Wiedza zdobyta na tym etapie pozwala na podjęcie decyzji o sposobie postępowania z ryzykiem (wybór strategii⁷⁵ i dobór metod⁷⁶). 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 matryca 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 ryzykiem⁷⁷.

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

⁷⁴ Agregacja ryzyka – opis zestawu ryzyk. Źródło: opracowanie autorskie w ramach realizacji projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne”.

⁷⁵ 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 6/2002, Bellona 2002 oraz ISO Guide 73:2009, definicja 3.8.1.

⁷⁶ 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.

⁷⁷ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 206.

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.

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 ryzyk⁷⁸, który zostanie sporządzony w wyniku oceny, pomoże zrationalizować zarządzanie ryzykiem, a w konsekwencji – zarządzanie kryzysowe.

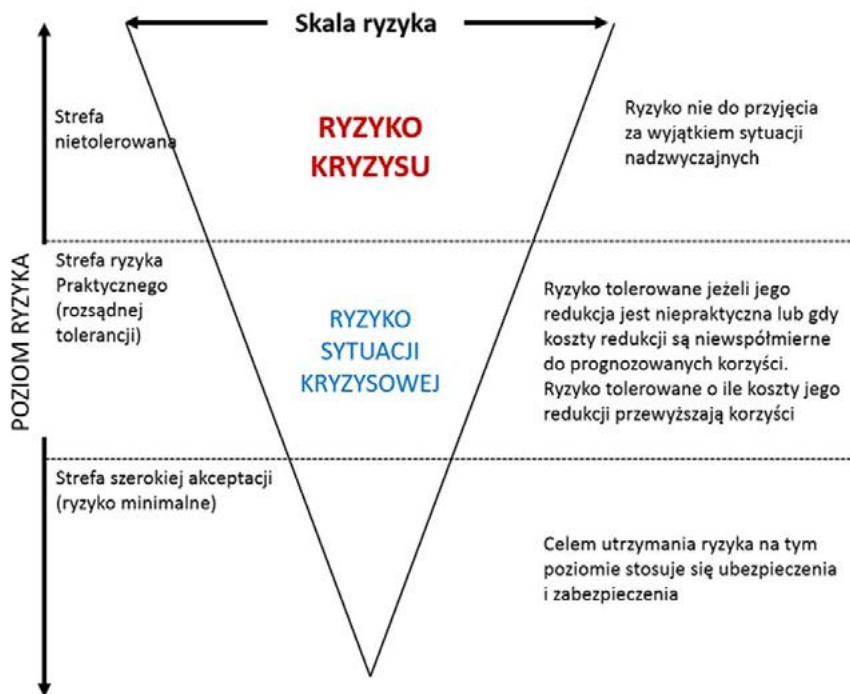
1.4.4. Postępowanie z ryzykiem

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), np. w zarządzaniu ryzykiem powodziowym. Ryzyko nie jest jednak czymś stałym i może eskalować w stronę granicy nietolerancji. Takie ryzyko wymaga więcej 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

⁷⁸ 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. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 172.

lub ograniczenia ryzyka oraz zapobieżenia zdarzeniu⁷⁹, które może je spowodować, a także zapobieżenia zagrożeniu będącemu skutkiem ryzyka.



Rys. 4. Koncepcja reagowania na ryzyko⁸⁰

Ocena ryzyka warunkuje sposób postępowania z ryzykiem. Sposoby te zdefiniowane w normie to⁸¹:

1. unikanie ryzyka poprzez decyzję o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko,

⁷⁹ 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”.

⁸⁰ Źródło: K. W. Knight, *The New Standard for Risk Management*, materiał przygotowany na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.

⁸¹ PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 51.

2. podjęcie lub zwiększenie ryzyka w celu wykorzystania szansy,
3. usunięcie źródła ryzyka,
4. zmiana prawdopodobieństwa (wystąpienia ryzyka),
5. zmiana konsekwencji,
6. dzielenie ryzyka z inną stroną lub stronami (łącznie z umowami i finansowaniem ryzyka),
7. 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 dotkliwie (o dużych, negatywnych następstwach, ale o niskim prawdopodobieństwie)⁸².

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 więc⁸³:

1. uzasadnienie wyboru danej opcji postępowania,
2. osoby odpowiedzialne za jego wdrożenie,
3. proponowane działania,
4. wymagania dotyczące zasobów z uwzględnieniem zasobów na wypadek sytuacji kryzysowych,
5. wymagania raportowania i monitorowania,
6. 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 oto-

⁸² D. Wróblewski, B. Połeć, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 207.

⁸³ PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 53.

czeniu, 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. 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)*⁸⁴.

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.

⁸⁴ P. Urbanek (red.), *Ekonomia i zarządzanie w teorii i praktyce*, WUŁ, Łódź 2011, s. 45.

1.5. Dokumentowanie zarządzania ryzykiem⁸⁵

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 ryzyk wskazują co najmniej dwa typy stosowanych dokumentów. Pierwszy 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 ryzyka⁸⁶, 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*. 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 zo-

⁸⁵ 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.

⁸⁶ Patrz: D. Wróblewski (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 172.

staje 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 ryzyka⁸⁷

Stanowisko:		Zestawił:		Data:	
Data przeglądu ryzyka:		Sprawdził:		Data	

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

W drugim przykładzie 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, har-

⁸⁷ Źródło: *Risk Management Guidelines Companion to AS/NZS 4360:2004*.

monogram zaplanowanych działań oraz zasady monitorowania ich realizacji, w tym poziomu ryzyka.

Tabela 2. Rejestr ryzyka⁸⁸

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	Zasady monitorowania działań i ryzyka

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.

⁸⁸ Źródło: *Risk Management Guidelines Companion to AS/NZS 4360:2004*.

2. METODY WYKORZYSTYWANE W OCENIE RYZYKA⁸⁹

W ostatnim czasie pojęcie oceny ryzyka⁹⁰ zyskało na popularności w niemalże wszystkich dziedzinach życia, poczynwszy 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 ryzyka⁹¹. 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 dla 31 metod oceny ryzyka oraz ich wzajemne porównanie w kontekście przydatności do identyfikacji ryzyka⁹², analizy ryzyka⁹³ pod względem konsekwencji, prawdopodobieństwa i poziomu ryzyka oraz ewaluacji ryzyka⁹⁴ (możliwość uzyskania wyników ilościowych, a nie tylko jakościowych)⁹⁵.

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 najskuteczniej ocenę ryzyka. Każda z wybranych metod została krótko scharakteryzowana pod kątem ogólnego zastosowania, cech korzystnych i niekorzystnych, jak również możliwych zastosowań.

⁸⁹ Patrz: definicja na s. 29.

⁹⁰ Patrz: D. Wróblewski (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 161.

⁹¹ Patrz: definicja na s. 39.

⁹² Patrz: definicja na s. 27.

⁹³ Patrz: definicja na s. 31.

⁹⁴ Patrz: definicja na s. 37.

⁹⁵ Patrz: D. Wróblewski (red. nauk.), *Przegląd wybranych dokumentów...*, 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”⁹⁶, „sposób uświadomiony i systematyczny”⁹⁷, „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”⁹⁸. 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 problemu⁹⁹. 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 stosowania¹⁰⁰.

⁹⁶ T. Kotarbiński, *Traktat o dobrej robocie*, Ossolineum, Wrocław 1973, s. 85.

⁹⁷ Tamże, s. 61.

⁹⁸ Tamże, s. 86-87.

⁹⁹ T. Pilch, T. Bauman, *Zasady badań pedagogicznych: strategie ilościowe i jakościowe*, wyd. „Żak”, Warszawa, 2001, s. 42.

¹⁰⁰ T. Kotarbiński, *Traktat o dobrej robocie*, Ossolineum, Wrocław 1973, s. 85-87.

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, osiągania 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 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 *cucmema* (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 *metod* (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*. Doku-

ment ten wskazuje, którymi narzędziami w których etapach oceny ryzyka należy się posługiwać. Metody te wskazuje poniższa tabela:

Tabela 3. Możliwe metody do zastosowania przy ocenie ryzyka¹⁰¹

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

¹⁰¹ Źródło: opracowanie własne na podstawie ISO/IEC 31010:2009 *Risk Management – Risk Assessment Techniques*.

CZĘŚĆ I
ZAGADNIENIA OGÓLNE Z ZAKRESU ZARZĄDZANIA RYZYKIEM

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>)	-	++	++	++	++	-
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
Metoda konserwa-	++	++	++	++	++	2.10

Publikacja finansowana przez NCBiR w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne” nr DOBR/0016/R/ID2/003

CZĘŚĆ I
ZAGADNIENIA OGÓLNE Z ZAKRESU ZARZĄDZANIA RYZYKIEM

cji ukierunkowana na niezawodność (ang. <i>reliability centred maintenance</i>)						
Zapowiedź analizy – SA i zapowiedź analizy obwodu – SCA (ang. <i>sneak analysis & sneak circuit analysis</i>)	+	-	-	-	-	2.11
Analiza Markova (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 skutków/prawdopodobieństwo (ang. <i>consequence/probability matrix</i>)	++	++	++	++	+	2.15
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. 156						

Legenda:

++ – zdecydowanie dotyczy

+ – dotyczy

-- nie dotyczy

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

1. analizę przyczyn i konsekwencji,
2. analizę przyczynowo-skutkową,
3. analizę warstw ochrony,
4. analizę drzewa decyzji,
5. analizę drzewa błędów,
6. analizę drzewa zdarzeń,
7. ocenę niezawodności człowieka,
8. analizę muchy,
9. metodę konserwacji ukierunkowaną na niezawodność,
10. zapowiedź analizy i zapowiedź analizy obwodu,
11. metodę „co, jeśli?”,
12. analizę scenariuszową,
13. analizę wpływu na działalność,
14. macierz 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 nierozdzielnie 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*)¹⁰²

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.

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 dokładnie ich awarie¹⁰³. Umożliwia ona wskazanie różnych ścieżek rozwoju w momencie wystąpienia niepożądanego zdarzenia, zależnych od zachowania poszczególnych podsystemów. Może ponadto służyć do dokładniejszej analizy

¹⁰² ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, annex B.16.

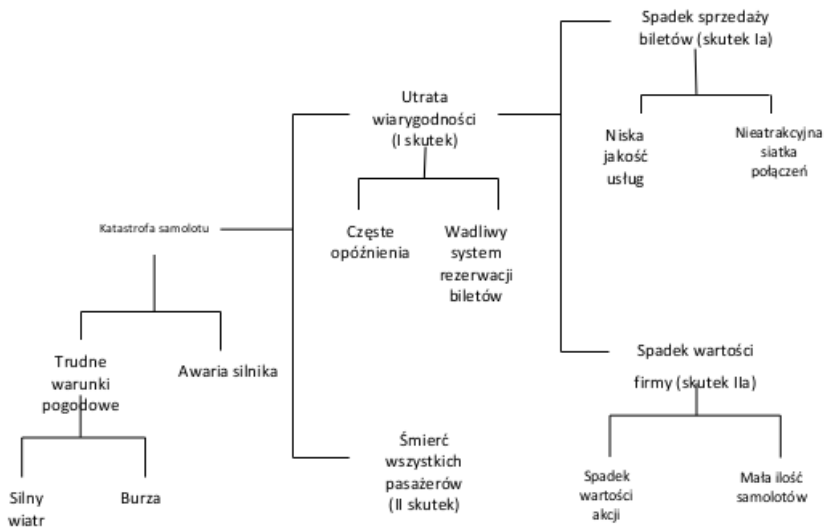
¹⁰³ Awaria – przerwanie pracy urządzenia technicznego w wyniku jego uszkodzenia. Źródło: *Wielki słownik języka polskiego*, Instytut Języka Polskiego PAN: http://www.wsjp.pl/index.php?id_hasla=33068&ind=0&w_szukaj=awaria, dostęp: marzec 2015.

przyczyn wystąpienia sytuacji kryzysowej. Postępowanie obejmuje pięć etapów:

1. wybór zdarzenia lub sytuacji do analizy,
2. identyfikację funkcji bezpieczeństwa dla poszczególnych elementów systemu,
3. określenie ścieżek zdarzenia, począwszy od zdarzenia inicjującego (drzewo zdarzeń),
4. wyznaczenie zdarzeń elementarnych dla zdarzenia inicjującego (drzewo skutków),
5. 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)¹⁰⁴.

Niniejszą metodę można przedstawić schematycznie, obrazując przyczyny i konsekwencje konkretnego zdarzenia.



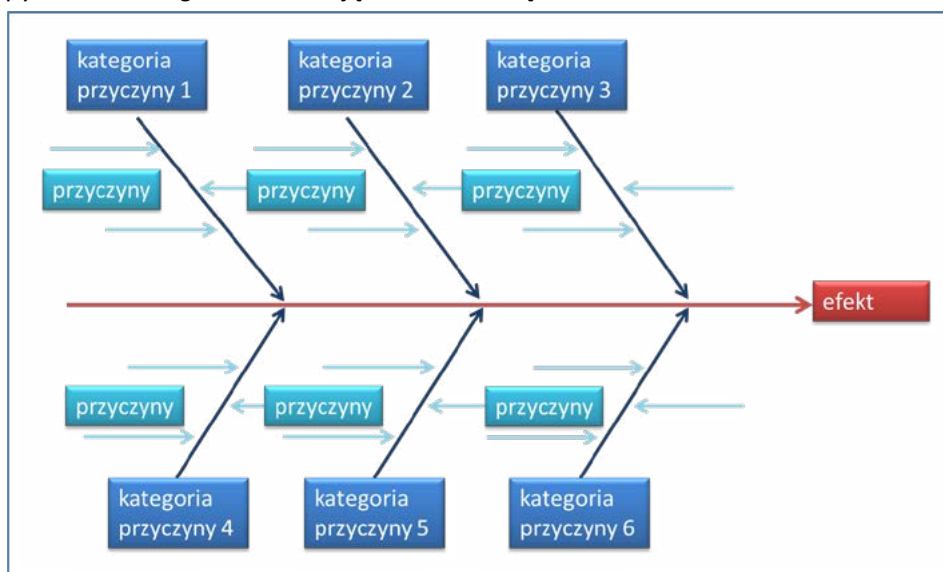
Rys. 5. Przykład analizy przyczyn i konsekwencji¹⁰⁵

¹⁰⁴ 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*)¹⁰⁶

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?*



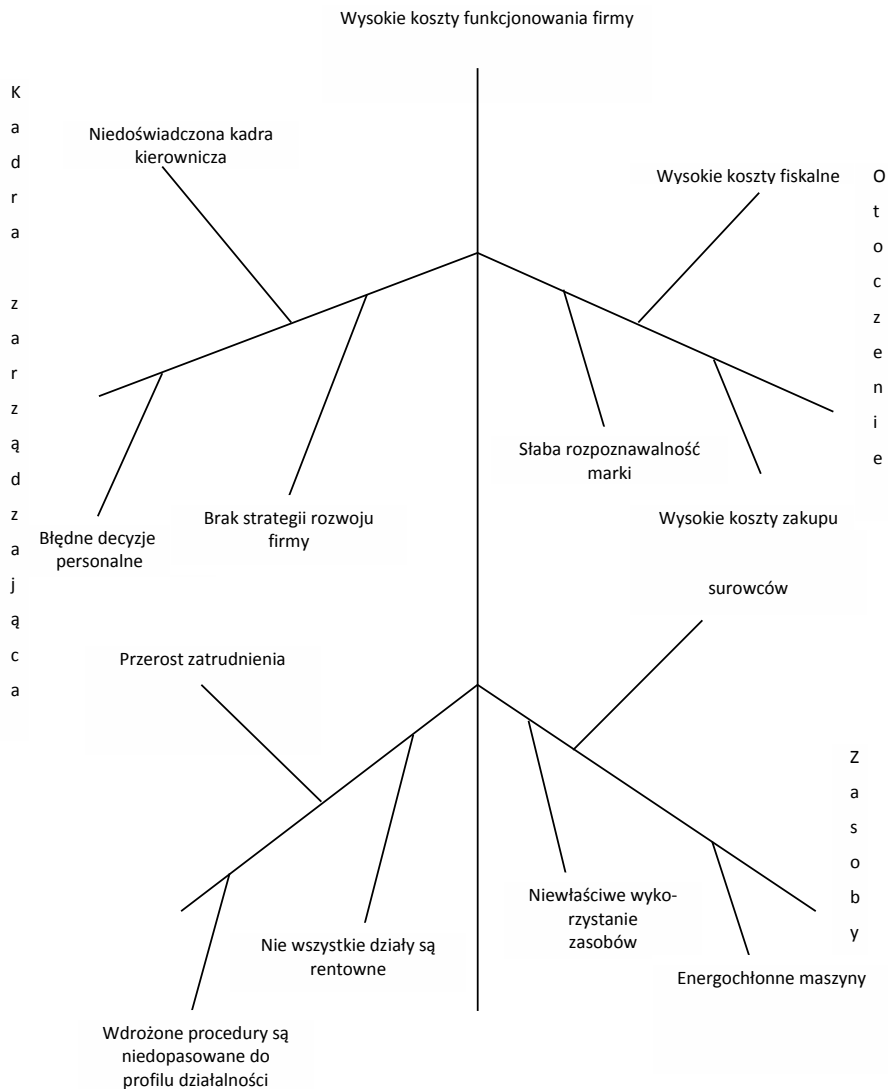
Rys. 6. Model diagramu Ishikawy¹⁰⁷

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

¹⁰⁵ Źródło: opracowanie własne.

¹⁰⁶ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, annex B.17.

¹⁰⁷ Źródło: opracowanie własne.



Rys. 7. Przykład analizy przyczynowo-skutkowej¹⁰⁸

¹⁰⁸ 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 mózgów¹⁰⁹) 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 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:

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

Korzyści z analizy przyczynowo-skutkowej to:

1. koncentrowanie uwagi członków zespołu na konkretnym problemie,
2. pomoc w ustaleniu przyczyny wystąpienia problemu dzięki zastosowaniu usystematyzowanego podejścia,

¹⁰⁹ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques* p. B.1.

3. zachęcenie do udziału w procesie analizy całej grupy i wykorzystanie wiedzy grupy,
4. uporządkowana forma przedstawienia wyników w postaci diagramu,
5. wskazanie możliwej przyczyny zmienności w procesie,
6. 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:

1. zaangażowanie ekspertów,
2. zorganizowany sposób dokonania analizy,
3. rozważenie wszystkich możliwych hipotez,
4. graficzna, łatwa do odczytania ilustracja wyników.

Częstym problemem związanym z wykorzystywaniem tej metody jest:

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

2.4. Analiza warstw ochrony – LOPA (*layer protection analysis*)¹¹⁰

LOPA to ilościowa metoda oceny ryzyka związanego z niepożądanym zdarzeniem lub scenariuszem zdarzeń. W tej metodzie analizuje się, czy istnieją wystarczające środki kontroli, aby zmniejszyć ryzyko wystąpienia zdarzenia niekorzystnego¹¹¹. 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.

¹¹⁰ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, annex B.18.

¹¹¹ 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 teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005, s. 174.



Rys. 8. Przykład analizy warstw ochrony – LOPA¹¹²

Podstawą analizy warstw ochrony jest odwołanie do pojęcia ryzyka rozumianego jako wzajemna relacja między zagrożeniami procesowymi a zastosowanymi systemami bezpieczeństwa i ochrony¹¹³.

Zalety metody LOPA:

1. wymaga mniej czasu i środków niż analiza drzewa błędów lub ryzyka całkowitego¹¹⁴ czy analiza ilościowa¹¹⁵,

¹¹² Źródło: opracowanie własne.

¹¹³ Zapis ten precyzuje definicję ryzyka zawartą w normie PN-ISO 31000, według której ryzyko jest to wpływ niepewności na cele.

¹¹⁴ 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 przynajm-

2. pomaga zidentyfikować zasoby i skupić je na najistotniejszych poziomach ochrony,
3. identyfikuje operacje, systemy i procesy, dla których nie ma wystarczających zabezpieczeń,
4. koncentruje się na najpoważniejszych konsekwencjach.

Ograniczenia metody:

5. LOPA koncentruje się na jednej parze przyczyn-konsekwencji i jednym scenariuszu następstw,
6. 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*)¹¹⁶

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 danej sytuacji obciążonej niepewnością.

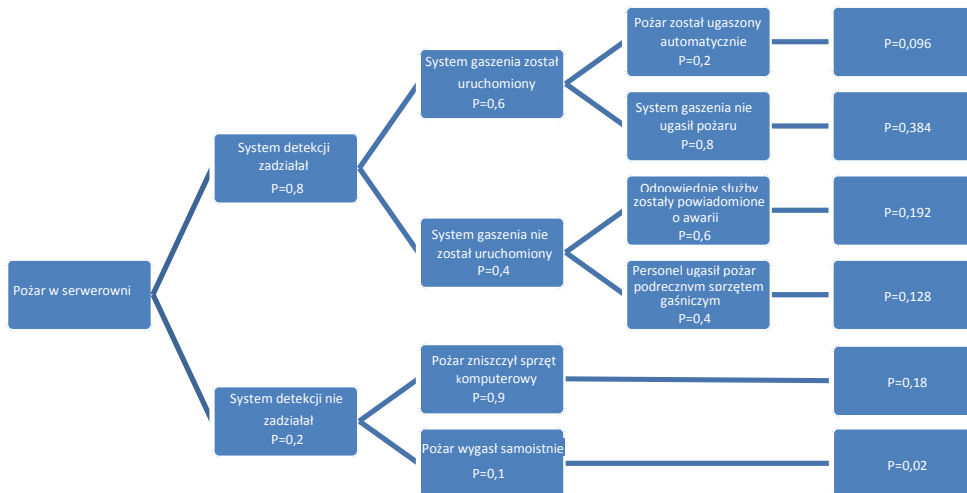
Drzewo decyzyjne rozpoczyna się od pierwszego inicjującego zdarzenia. Następnie określa się możliwe decyzje – zarówno rozwiązania korzystne, jak i niekorzystne oraz prawdopodobieństwo ich podjęcia. Kolejnym krokiem w budowie drzewa decyzji jest oszacowanie konsekwencji, jakie pociągają za sobą potencjalne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

niej 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.

¹¹⁵ 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.

¹¹⁶ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, annex B.19.

ga 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.



Rys. 9. Przykład analizy drzewa decyzji¹¹⁷

Informacjami wejściowymi niezbędnymi do zastosowania metody drzew decyzji są:

1. plan danego przedsięwzięcia czy projektu, którego analiza ma dotyczyć – wraz z punktami decyzyjnymi,
2. 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.

¹¹⁷ Źródło: opracowanie własne.

Informacjami wyjściowymi z zastosowanej metody są:

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

Największymi atutami przedstawianej metody są:

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

Ograniczenia metody:

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

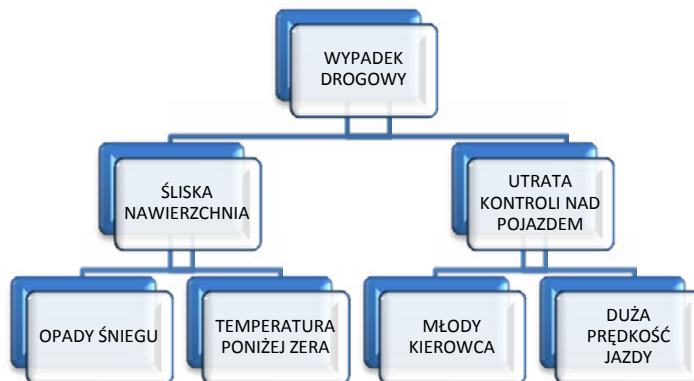
2.6. Analiza drzewa błędów (*fault tree analysis*)

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 liczbowych¹¹⁸. 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 jakościową¹¹⁹. Technika polega na pokazaniu głównego zdarzenia i rozrysowania w formie diagramu wszystkich czynników mogących doprowadzić do jego powstania. Po rozrysowaniu należy rozważyć metody redukcji bądź eliminacji potencjalnych zagrożeń/ich źródeł. Metoda ta jest pomocna przy identyfikowaniu potencjalnych przyczyn i rozwoju sytuacji i wyliczaniu prawdopodobieństwa wystąpienia zdarzenia.

¹¹⁸ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, pkt 5.3.1.

¹¹⁹ Patrz: AS/NZS 4360:2004 *Risk Management*, s. 18-19.



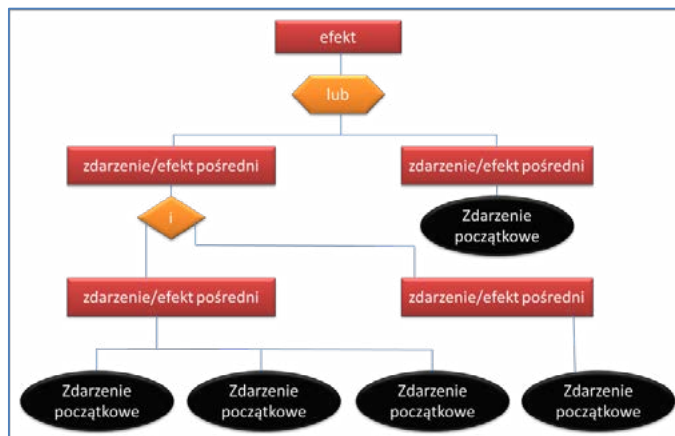
Rys. 10. Przykład analizy drzewa błędów¹²⁰

Metodę tę stosuje się w fazie projektowania systemu, w celu wskazania jego słabych punktów. Służy ona także do przeanalizowania rzeczywistej sytuacji – pozwala wówczas pokazać, jak poszczególne zdarzenia, połączone w całość, miały wpływ na powstanie/rozwój sytuacji. Dzięki tej metodzie uzyskujemy przedstawione w formie graficznej zdarzenie oraz ścieżki rozwoju do niego prowadzące, 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 nastąpi, gdy zaistnieje przynajmniej jedno ze zdarzeń „wychodzących”. Bramka „i” przedstawia sytuację, w której następane wydarzenie nastąpi tylko i wyłącznie wtedy, gdy zaistnieją wszystkie zdarzenia „wchodzące”¹²¹.

¹²⁰ Źródło: opracowanie własne.

¹²¹ Na podstawie: P. T. Mitkowski, *Ocena ilościowa ryzyka: analiza drzewa błędu (konsekwencji)*, materiały dydaktyczne, Politechnika Poznańska.



Rys. 11. Przykładowe drzewo logiczne wykorzystywane w analizie drzewa błędów¹²²

2.7. Analiza drzewa zdarzeń (*event tree analysis*)

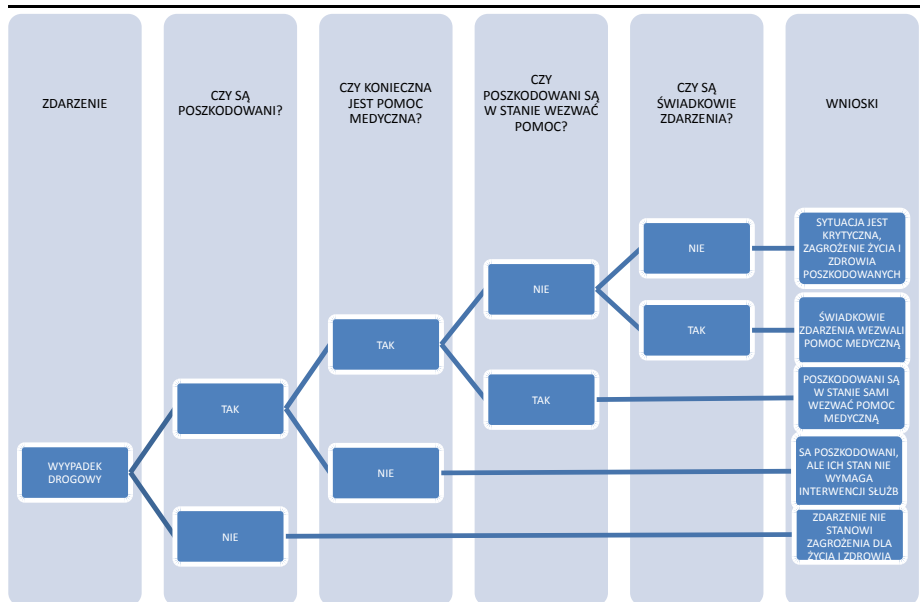
Drzewa zdarzeń są tworzone po analizie drzewa błędów. Analizują zdarzenia, które wynikają z pojedynczego zdarzenia w postaci prostych bramek logicznych. Drzewo zdarzeń pozwala na analizę możliwego skutku konkretnego zdarzenia inicjującego¹²³.

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).

¹²² Źródło: opracowanie własne na podstawie: P. T. Mitkowski, *Ocena ilościowa ryzyka: analiza drzewa błędów (konsekwencji) materiały dydaktyczne*. 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. 19.

¹²³ Zdarzenie inicjujące – zdarzenie początkowe w całym łańcuchu zdarzeń, prowadzące do kolejnych, sekwencyjnie występujących zdarzeń niekorzystnych. Źródło: J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, DANMAR, Warszawa 2005, s. 174.

CZĘŚĆ I
ZAGADNIENIA OGÓLNE Z ZAKRESU ZARZĄDZANIA RYZYKIEM



Rys. 12. Przykład analizy drzewa zdarzeń¹²⁴

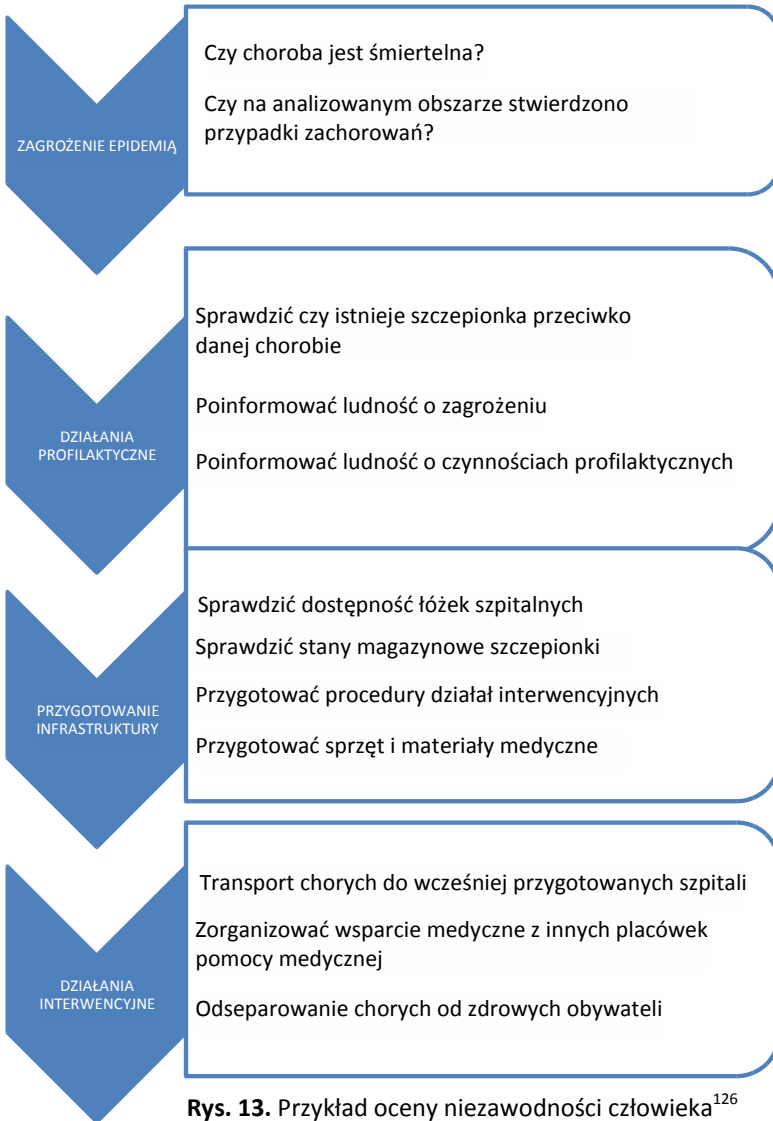
2.8. Ocena niezawodności człowieka (*human reliability analysis*)¹²⁵

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 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 wy-

¹²⁴ Źródło: opracowanie własne.

¹²⁵ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, annex B.20.

dajność prowadzonych procesów, wskaże również miejsca, gdzie można wprowadzić działania korygujące, które zapobiegną tym błędom.



Rys. 13. Przykład oceny niezawodności człowieka¹²⁶

¹²⁶ 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:

1. **określenie rodzaju problemu** – co ma być badane/oceniane,
2. **analiza zadań** – w jaki sposób proces jest wykonywany i w jaki sposób można wesprzeć to zadanie,
3. **analiza błędów ludzkich** – jakie błędy mogą wystąpić i jak można im zapobiec,
4. **przedstawienie** powiązań zadania z innymi elementami systemu (sprzęt, oprogramowanie, środowisko) i określenie ich relacji,
5. **oddzielenie błędów** ważnych od tych, które nie wymagają szczególnej analizy,
6. **ocena błędów** pod kątem prawdopodobieństwa wystąpienia,
7. **ocena skutków** – które błędy lub zadania są najbardziej wrażliwe, czyli które z nich mają największy wpływ na wysokość ryzyka,
8. **redukcja błędów** – jak można uzyskać większą niezawodność prowadzonych działań,
9. **dokumentowanie** – wszystkie działania muszą zostać udokumentowane.

Największe atuty metody HRA:

1. stanowi formalny mechanizm w ocenie roli błędów człowieka,
2. 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*)¹²⁷

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.

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 (*brainstorming*)¹²⁸. 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 *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.)¹²⁹.

¹²⁷ IEC/ISO 31010 *Risk Management – Risk Assessment Techniques*, annex B.21.

¹²⁸ IEC/ISO 31010 *Risk Management – Risk Assessment Techniques*, annex B.1.

¹²⁹ 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.

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.

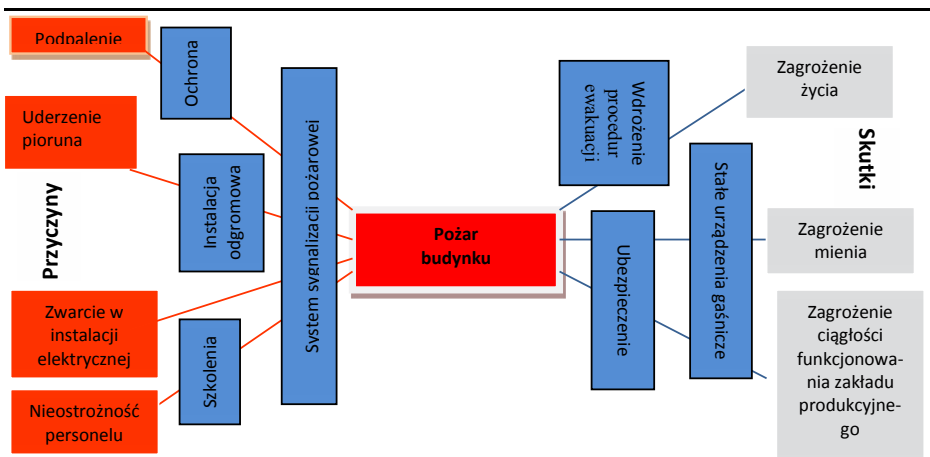
Obecnie istnieją narzędzia informatyczne, które wspomagają i ułatwiają stworzenie diagramu. Jeżeli takie właśnie oprogramowanie jest używane, wiedza ekspercka na temat ryzyka może być ograniczona.

Efektem analizy ryzyka metodą muchy jest schemat przedstawiający główne szlaki ryzyka oraz bariery, które mają zapobiegać skutkom zagrożenia lub łagodzić je.

Zaletą tej metody jest łatwość w zrozumieniu i przejrzysta forma pokazania zdarzenia. Wymaga ona zrozumienia przyczyn i skutków ryzyka oraz barier i kontroli, które mogą mu zapobiec, zmniejszyć je lub stymulować. W rezultacie otrzymujemy główne ścieżki rozwoju ryzyka.

Ograniczenia metody:

1. nie może posłużyć do opisu zdarzenia mającego kilka przyczyn (jednocześnie),
2. może nadmiernie upraszczać skomplikowane sytuacje.



Rys. 14. Przykład analizy muchy¹³⁰

2.10. Metoda konserwacji ukierunkowana na niezawodność – RCM (*reliability centred maintenance*)¹³¹

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.

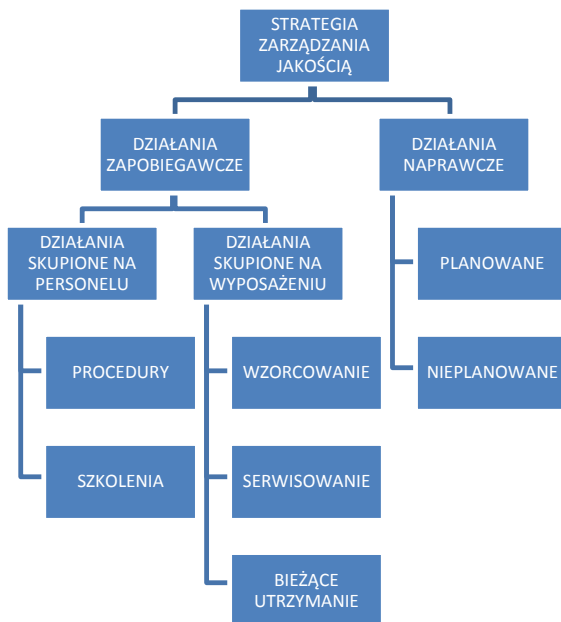
RCM jest uznana za sprawdzoną metodę i stosowana w wielu gałęziach przemysłu. Zapewnia ona, że w procesie decyzyjnym określane są właściwe i skuteczne działania zapobiegawcze dla urządzeń. Efektem końcowym procesu oceny ryzyka metodą RCM jest decyzja o konieczności wykonywania zadań konserwacyjnych lub 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 operacyjnie skuteczna, ale może mieć mniej rygorystyczne kryte-

¹³⁰ Źródło: opracowanie własne.

¹³¹ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, annex B.22.

ria bezpieczeństwa i ekonomiczności. Największe korzyści można osiągnąć poprzez ukierunkowanie analizy na te obszary, w których miałyby miejsce poważne błędy.



Rys. 15. Przykład metody konserwacji ukierunkowanej na niezawodność – RCM¹³²

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:

1. inicjowanie i planowanie,
2. analiza błędów funkcjonalnych,
3. wybór zadań,
4. wdrożenie,
5. ciągłe doskonalenie.

¹³² Źródło: opracowanie własne.

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*)¹³³

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.

¹³³ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, annex B.23.

Podstawowe kroki analizy stanowią:

1. przygotowanie danych,
2. budowa drzewa sieci,
3. ocena ścieżek sieciowych,
4. ostateczne rekomendacje i raport.

Atuty metody SA:

1. pomocna przy identyfikacji błędów projektowych,
2. działa najefektywniej w połączeniu z metodą HAZOP.

Wady:

1. proces może się różnić w zależności od tego, do czego jest stosowany – np. obwodów elektrycznych, instalacji technologicznych czy urządzeń mechanicznych,
2. metoda jest uzależniona od ustanowienia właściwej sieci drzew.

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.:

1. nie nosić wszystkich pieniędzy i kart razem,

2. znać numer telefonu, pod którym możemy zastrzec kartę, a przynajmniej numer infolinii swojego banku,
3. nie udostępniać nikomu numeru PIN i zastępować klawiaturę w bankomacie,
4. 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 opcję”, „najgorszą opcję”, „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 zabezpieczeniu 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 zabezpieczeniu 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*)¹³⁴

Analizę taką przeprowadza się, by pokazać, jak poszczególne zagrożenia wpływają na funkcjonowanie organizacji i jakich przedsięwzięć wymagają.

¹³⁴ Charakterystyka BIA przygotowana na podstawie: R. Kaszubski, D. Romańczuk (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, wyd. Związek Banków Polskich, Warszawa 2012.

Służy ona określenia ram czasowych i powiązanych zasobów niezbędnych do zapewnienia ciągłej realizacji zadań.

Do zalet tej metody można zaliczyć:

1. umożliwienie zrozumienia procesów, które zapewniają ciągłość działania i osiągnięcie celu,
2. pokazanie niezbędnych zasobów,
3. zdefiniowanie procesu operacyjnego pozwalającego zwiększyć odporność podmiotu¹³⁵.

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 RTO¹³⁶ i RPO¹³⁷ 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.

¹³⁵ ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*, s. 42–44.

¹³⁶ RTO (ang. *Recovery Time Objective*) – parametr określający maksymalny czas po awarii potrzebny do przywrócenia działania aplikacji, systemów i procesów biznesowych.

¹³⁷ RPO (ang. *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.

Kluczowe działania to:

1. określenie strat finansowych i niefinansowych, na jakie organizacja jest narażona w sytuacji zatrzymania procesu/procesów,
2. określenie RTO, czyli czasu, po którego upływie określone straty są już dla organizacji nieakceptowalne,
3. określenie RPO, czyli akceptowalnego przez organizację poziomu utraty danych – na podstawie technicznych zdolności ich odtworzenia;
4. 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 4. Przykład analizy wpływu na działalność – BIA¹³⁸

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.

2.15. Matryca skutek/prawdopodobieństwo (*consequence/probability matrix*)

Matryca skutek/prawdopodobieństwo jest wykorzystywana do klasyfikacji ryzyka¹³⁹, hierarchizacji¹⁴⁰ źródeł ryzyka i postępowania z ryzykiem (tabela 5

¹³⁸ Źródło: opracowanie własne.

i 6). Metoda ta stanowi wsparcie w procesie ustalania, które ryzyka wymagają dalszej 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 5. Określenie prawdopodobieństwa wystąpienia zdarzenia¹⁴¹

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

Określenie prawdopodobieństwa jest czynnością złożoną, ale przy ocenie jakościowej nie wymaga przeprowadzania skomplikowanych kalkulacji. Metoda podana w tabeli 6 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.

¹³⁹ 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”.

¹⁴⁰ Hierarchizacja ryzyka – w rozumieniu dosłownym oznacza ustalenie 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”.

¹⁴¹ Źródło: K. W. Knight, *The New Standard For Risk Management*, materiał konferencyjny na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.

Tabela 6. Ocena poziomu ryzyka¹⁴²

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

Poszczególne kategorie konsekwencji oraz prawdopodobieństwa¹⁴³, jak również poziomu ryzyka mogą zostać nazwane i zdefiniowane na wiele sposobów. Także rozpiętość matryc 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 7).

¹⁴² Tamże.

¹⁴³ Opis jakościowy/ilościowy dla konsekwencji i prawdopodobieństwa lub ich kombinacja.

Tabela 7. Szablon do sporządzania listy priorytetów dla każdego ryzyka¹⁴⁴

Prawdopodobieństwo	Konsekwencje		
	bardzo wysokie	średnie	bardzo niskie
bardzo wysokie	1	1	2
możliwe	1	2	3
rzadkie	2	3	3

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 matrycy prognozowania konsekwencji zarówno pozytywnych (korzyści), jak i negatywnych (strat).

Tabela 8. Przykładowa matryca prognozowania konsekwencji pozytywnych i negatywnych¹⁴⁵

-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	mniej		mniej	większe	wyjatkowe	ekstremalne
Konsekwencje negatywne					Konsekwencje pozytywne			

Legenda

S – szczególne, wymaga szczególnego zaangażowania szczebla kierowniczego,

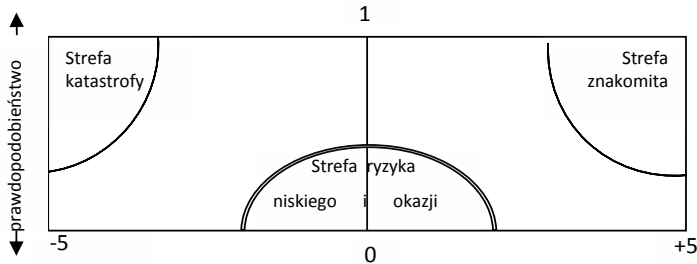
W – wysokie, wymaga zaangażowania właściwego menedżera,

M – małe, wymaga uwagi,

N – niskie, procedury rutynowe.

¹⁴⁴ Źródło: K. W. Knight, *The New Standard For Risk Management*, materiał przygotowany na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.

¹⁴⁵ Tamże.



Rys. 16. Diagram stref rozmieszczenia ryzyka (pozytywnego i negatywnego)¹⁴⁶

Analiza powinna dać odpowiedzi 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?
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.

¹⁴⁶ Tamże.

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 Management – Vocabulary* oraz normy ISO/IEC 31010 *Risk Management – 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 umożliwi 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 przedsięwzięcia¹⁴⁷.

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 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

¹⁴⁷ <http://wartowiedziec.org/index.php/pracownik-samorzadowy/zarzdanie/16316-jakociowa-i-ilociowa-analiza-ryzyka>, dostęp: luty 2015.

Pomaga w opisanii każdego rodzaju ryzyka, zarówno dłuogo-, 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 względu na biznesowe czy też publiczne.

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.

SUMMARY AND CONCLUSIONS

It can be pointed out by analysing the standards recommended by ISO as well as those adopted by The Polish Committee for Standardization (PKN) that the topic of risk management is emerging in many standards in numerous fields. Until ISO 31000:2009 *Risk Management – Principles and Guidelines*, ISO Guide 73:2009 *Risk Management – Vocabulary* and ISO/IEC 31010 *Risk Management – Risk Assessment Techniques* have been adopted, this aspect was tackled by the following standards, in particular: ISO 14000 – *Environmental impact assessment*, ISO/IEC 27001 – *Information security management systems*, PN-EN ISO 9001:2008 – *Enterprise organisation and management* or standards related to the safety of technical devices, i.e.: EN ISO 14121-1 and EN ISO 12100:2010. The standards recommended the use of the risk assessment process without indicating, however, detailed codes of procedure regarding the entire process.

It should be noted that the relevance of the standards was not only reflected in the minds of theorists and practitioners creating and applying them, but has been confirmed by, in particular, Polish legal regulations. Article 2 of the Standardisation Act (Journal of Law of 2002 No. 169, item 1386, as amended) specifies the status of standards as documents issued by *authorised* organisational entities, which are establishing, for a given field of activity, principles, guidelines or characteristics based on long-term practices and experience.

The first substantial advantage of applying standards from a family of ISO 31000 is that terminologies are harmonised according to readable groups of terms and their definitions. The documents allow understanding and applying a consistent terminology referring to risk management, its elements and processes in all fields of activity in which it is present.

Another important matter is possibly the most universal and unified approach of ISO 31000 to risk management processes, which allows its flexible use by any organisation operating in any public or private sector. The standard provides principles, structure and processes which can be permanently implemented in all areas of an organisation's activity regardless the type of risks encountered.

Another significant benefit of implementing ISO 31000 guidelines, apart from its abovementioned flexible accommodation to an organisation's current

needs, is openness to the changes resulting from changing conditions and needs.

One can realise by analysing carefully the principles described in the standard what, in particular, are the benefits that an organisation can obtain as a result of implementing the system. To a certain extent they provide an answer to the following question: why should we implement the system or what can we obtain in return? An answer to the following question: how to implement the system within an organisation in an effective and efficient manner? is clearly indicated by scrutinising the provisions concerning the framework structure. The description of processes allows answering the following question on the other hand: how to manage a risk in an organisation?

An important advantage is that the risk management process is defined in a comprehensive and orderly manner. It covers all processes occurring within an organisation. An important aspect of the process is that all the prerequisites to determine the context are specified at the beginning. A risk can be assessed appropriately by using such knowledge. An organisation can approach the risk management process properly by adhering to such recommendations at this stage. Depending on the needs, it is recommended to conduct consultations and communicate the risk, and also to carry out monitoring and review as supplementary and aiding tools for all the stages. The reliable evidencing of actions is an inherent component of risk management within an organisation recommended by ISO 31000, the benefits of which are frequently influencing an organisation's future: supporting the decision-making process, development and improvement of methods and processes within an organisation.

The current approach to risk assessment relies, most of all, on know-how and experience with the existing threats. Various risk assessment methods considerably improving emergency management are also applied.

This part presents also selected risk management methods positively influencing risk management when implemented in decision-making processes.

A planned response to a risk is an outcome of a risk assessment performed. Alternative procedures and activities reducing the threats and heightening the potential benefits for the objectives set are established under the process. A risk response plan is a key phase of the risk management process as methods of responding to favourable and unfavourable events are elaborated in the

plan. A risk of increasing or decreasing the successfulness of the entire project is immediately influenced by the efficiency of risk response planning for the threatened tasks¹⁴⁸.

The planned reactions must be proportional to the consequences of occurrence of unfavourable events; they must eliminate (or mitigate) the effects of a given threat in a cost-effective fashion and be carried out in a timely manner. Several strategies are commonly employed in a risk response planning process. An emergency plan has to be developed for each of the risks in such a way that the measures taken are as effective as possible.

A myriad of methods have been identified in the process of analysing risks and threats assessment. 31 methods are described in ISO/IEC 31010:2009. These are not all the existing risk assessment methods, but those described in this part permit to learn about diverse approaches to the topic in question. The methods have been so chosen as to analyse different approaches to risk assessment. The methods allow to represent the array of risk management starting with expert's considerations to methods based on the building of diagrams and logical scenarios of events. It is recommended to use the following methods:

1. SWIFT method
questions such as: "what if...?" "if ever...?" "what could happen...?" force us to analyse the majority of potential scenarios, their causes and consequences; the method can be applied broadly;
2. event tree
useful for calculating, modelling and allocating various follow-up scenarios related to the main event; it displays event progression depending on the scenario selected; the method is useful when analysing safety systems and emergency procedures;
3. cause and effect analysis
the method eliminates certain constraints of the event tree and fault tree methods by analysing events evolving over time; it delivers an extensive review of system operation;

¹⁴⁸ <http://wartowiedziec.org/index.php/pracownik-samorzadowy/zarzadzanie/16316-jakociowa-i-ilociowa-analiza-ryzyka>, access: February 2015.

4. scenario analysis
useful for depicting each type of risk, both, a long-term and short-term risk;
5. bow tie analysis
easy to understand and transparent in communicating an event.
6. consequence/probability matrix
very legible, with the possibility application of different scale (4x4, 5x5, 6x6) and weights.

The practical application of risk management standards indicates that they are a universal source of knowledge ensuring proven tools aiding the management of all organisational processes in the conditions of uncertainty. By applying them, organisations can more effectively fulfil the mission they were created for, as well as the objectives and tasks relevant for business or public purposes.

Since introducing the elements of risk management in 2009, its importance has been continuously growing. It is thus recommended to use recognised guidelines for risk management, which unify the terminology, offer universal principles, a flexible framework structure, appropriately matched processes, including tools supporting risk assessment and risk management evidencing.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

1. Chrószcz B., *Analiza i ocena ryzyka zawodowego osób obsługujących systemy maszynowe transportu pionowego w polskich kopalniach węgla kamiennego*, rozprawa doktorska, AGH, Kraków 2007.
2. Gołębiowski J., *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, Kraków 2011.
3. Kaszubski R., Romańczuk D. (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, wyd. Związek Banków Polskich, Warszawa 2012.
4. Kotarbiński T., *Traktat o dobrej robocie*, Ossolineum, Wrocław 1973.
5. Nogalski B., *Kultura organizacyjna. Duch organizacji*, Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz 1998.
6. Peszko A., *Podstawy zarządzania organizacjami*, Skrypty uczelniane AGH, nr 1485, Wydawnictwa AGH, Kraków 1997.
7. Pilch T., Bauman T., *Zasady badań pedagogicznych: strategie ilościowe i jakościowe*, wyd. Żak, Warszawa 2001.
8. Sikorski Cz., *Kultura organizacyjna*, C.H. Beck, Warszawa 2002.
9. *Słownik terminów z zakresu bezpieczeństwa narodowego*, Myśl Wojskowa 6/2002, Bellona, Warszawa 2002.
10. Urbanek P. (red.), *Ekonomia i zarządzanie w teorii i praktyce*, WUŁ, Łódź 2011.
11. Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, DANMAR, Warszawa 2005.
12. Wróblewski D. (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014.
13. Wróblewski D., Połeć B., *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014.

Akty prawne

1. 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

1. AS/NZS 4360:2004 *Risk Management*.
2. CAN/CSA-Q850-97 (2009) *Risk Management: Guidelines for Decision-makers*.
3. ISO 31000:2009 *Risk Management – Principles and Guidelines*.
4. ISO Guide 73:2009 *Risk Management – Vocabulary*.
5. ISO/IEC 31010:2009 *Risk Management – Risk Assessment Techniques*.
6. PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.
7. PN-EN ISO/IEC 17021:2011 *Ocena zgodności. Wymagania dla jednostek prowadzących audyty i certyfikację systemów zarządzania*.
8. PN-ISO 26000:2012 *Wytyczne dotyczące społecznej odpowiedzialności*.
9. PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*.
10. PN-ISO 9000:2006 *System zarządzania jakością. Podstawy i terminologia*.
11. PN-ISO 9004:2009 *Zarządzanie ukierunkowane na trwałą sukces organizacji. Podejście wykorzystujące zarządzanie jakością*.
12. *Risk Management Guidelines Companion to AS/NZS 4360:2004*.

Słowniki, leksykony i encyklopedie

1. *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2008.

Dokumenty elektroniczne, strony internetowe i inne

1. *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 [dostęp 11 czerwca 2013].

2. Fabbri 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.
3. <http://www.wsjp.pl>.
4. <http://mfiles.pl>.
5. <http://wartowiedziec.org>.
6. *IIF Report Reform In the Financial Services Industry: Strengthening Practices for a More Stable System*, Institute of International Finance, 2009.
7. Knight K. W., *The New Standard For Risk Management*, materiał przygotowany na Międzynarodową Konferencję Stowarzyszenia Zarządzania Ryzykiem POLRISK, 8 czerwca 2010 r., Warszawa.
8. Maas P., *Wiedza praktyczna: Zarządzanie poprzez cele*, wyd. Verlag Dashofer, Warszawa 2004 [dok. elektr.],
<http://www.dashofer.pl/przyklady/ED-ZPC.pdf> [dostęp 14 marca 2015].
9. Mitkowski P. T., *Ocena ilościowa ryzyka: analiza drzewa błędu (konsekwencji)*, materiały dydaktyczne, Politechnika Poznańska.
10. *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 [dostęp 9 czerwca 2013].

CZĘŚĆ II
ZARZĄDZANIE RYZYKIEM NA SZCZEBLU UE

PART II
RISK MANAGEMENT AT THE EU LEVEL

WPROWADZENIE

Unia Europejska podejmuje na swoim poziomie prace w zakresie oceny zagrożeń i ryzyka, na które są narażeni obywatele UE w różnych obszarach życia i działalności. Niemal każdy obszar funkcjonowania UE można powiązać z koniecznością dokonania oceny ryzyka wystąpienia danego zagrożenia, np.: przepływ statków Morzem Bałtyckim, zagrożenie piractwem morskim u wybrzeży Afryki, zagrożenie terroryzmem, zagrożenia przestępczością zorganizowaną czy handlem ludźmi w UE, ryzyko wystąpienia katastrof naturalnych lub technologicznych.

Prowadząc prace w dziedzinie oceny ryzyka i zagrożeń, Unia korzysta z: wypracowanych metodyk – w tym z norm Międzynarodowej Organizacji Normalizacyjnej, terminologii wypracowanej na forum Organizacji Narodów Zjednoczonych, metodologii wypracowanych w państwach członkowskich oraz w wyniku analiz, sama też proponuje państwom członkowskim terminologię, która dotyczy analizy ryzyka i oceny zagrożeń. W niniejszej części diagnozy zostaną przedstawione standardy i definicje uznane przez Unię Europejską i zapisane w dokumentach unijnych, rozporządzeniach, wytycznych oraz dyrektywach.

W Strategii bezpieczeństwa wewnętrznego UE z 2010 r. podkreślono, że należy opracować wytyczne diagnozowania, oceniania i analizowania niebezpieczeństw i ryzyka oraz dokonywać przeglądu zagrożeń naturalnych i wynikających z działalności ludzkiej, przed którymi może w przyszłości stanąć Unia. Kwestie te uregulowała 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.¹⁴⁹. Ponadto ustanowiono, iż kraje te przygotowują plany zarządzania ryzykiem związanym z klęskami i katastrofami na szczeblu krajowym lub odpowiednio niższym, stale je doskonaląc. Komisja Europejska planowała do 22 grudnia 2014 r. opracować wspólnie z państwami członkowskimi wytyczne w sprawie treści, metodologii i struktury tych ocen.

¹⁴⁹ A następnie co 3 lata.

W tej części publikacji przedstawiono analizę metodyk oceny ryzyka dla poszczególnych rodzajów zagrożeń, odnoszących się do wielu dziedzin aktywności UE. Podejmując działania w zakresie oceny zagrożeń i ryzyk, Unia dotychczas prowadziła takie oceny w sektorach i obszarach. Prace UE w poszczególnych obszarach w niniejszej diagnozie zostaną przedstawione na przykładzie zarządzania ryzykiem powodziowym, zagrożeń wypadkami chemicznymi, testów wytrzymałościowych, transgranicznych zagrożeń zdrowia oraz ochrony granic zewnętrznych Unii. Przywołana zostanie również aktywność naukowo-badawcza UE w zakresie projektów zgłębiających tematykę oceny ryzyka.

INTRODUCTION

The European Union has been pursuing efforts internally to evaluate threats and risks posed to the EU citizens in different areas of life and activities. Nearly each area of the EU's functioning can be linked to the necessity of applying a risk assessment for the likelihood of a particular threat: e.g. the crossing of ships through the Baltic Sea, a threat of sea piracy at the coasts of Africa, a threat of terrorism, organised crime or human trafficking in the EU, a risk of natural or technological catastrophes.

The EU, while conducting works in the field of risk and threat assessment, has been using the methodologies developed, including standards established by the International Organisation for Standardisation; the terminologies established at the forum of the United Nations; the methodologies established by the Member States and as a result of the analyses undertaken; it also proposes itself to the Member States a terminology concerning a risk analysis and evaluation of threats. The standards and definitions recognised by the European Union and included in EU documents, regulations, guidelines and directives are presented in this part of the diagnosis.

The EU Internal Security Strategy of 2010 highlights that guidelines for diagnosing, assessing and analysing threats and risks should be established, and natural threats and those resulting from human activity, likely to occur in the EU in the future, should be reviewed. Such matters are governed by Decision No. 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism. The Decision provides that the Member States are obliged to create a risk assessment at the national level or, respectively, at a lower level and to present to the Commission a summary of essential elements of such assessments by 22 December 2015¹⁵⁰. It was also specified that the states prepare risk management plans connected with disasters and catastrophes at the national level or, respectively, a lower level, and would improve them continuously. The European Commission has planned to set up, together with the Member States, guidelines concerning the

¹⁵⁰ And every 3 years thereafter.

contents, methodology and structure of the above assessments until 22 December 2014.

This part of the publication is analysing risk assessment methodologies for particular types of threats relating to multiple areas of the EU's activity. The EU, while carrying out works in scope of risk and threat assessment, has performed such assessments so far for particular sectors or areas of its activity. The EU's works in particular areas will be presented in this diagnosis with the example of managing a flood risk, threats of chemical accidents, strength tests, cross-boundary threats, protection of the European Union's external borders. The EU's research and scientific activity in scope of projects embarking on the subject of risk assessment is discussed towards the end.

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 powodzią. Katastroficzne w skutkach dla naszego regionu były powodzie w dorzeczach Dunaju i Elby w 2002 r. oraz 2005 r. To one wymogły na UE skupienie nad bardziej skoordynowanymi działaniami na jej forum.

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 EUR¹⁵¹. 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. Ostatnie duże powodzie wystąpiły w Europie w 2010 r. Objęły Europę Środkową, w szczególności Polskę, Republikę Czeską, Słowację, Węgry, Rumunię i Francję.

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 powodzi”¹⁵², 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

¹⁵¹ Dane Europejskiej Agencji Środowiskowej.

¹⁵² Komunikat Komisji dla Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Zarządzanie zagrożeniem powodziowym – zapobieganie powodziom, ochrona przeciwpowodziowa i ograniczanie skutków powodzi*, Bruksela, 12 lipca 2004 r., COM(2004) 472 wersja ostateczna, Bruksela, 12 lipca 2004 r.

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”¹⁵³.

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 inżynierjno-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”.

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, potwierdziła 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.

¹⁵³ Komunikat Komisji dla Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Zarządzanie zagrożeniem powodziowym – zapobieganie powodziom, ochrona przeciwpowodziowa i ograniczanie skutków powodzi*, Bruksela, 12 lipca 2004 r., COM(2004) 472 wersja ostateczna, Bruksela, 12 lipca 2004 r.

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”¹⁵⁴.

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*.

1.1. Wstępna ocena ryzyka powodziowego

Wstępna ocena ryzyka powodziowego dokonywana przez państwa członkowskie, opisana w art. 4 ww. dyrektywy, powinna obejmować co najmniej:

- a) *mapy obszaru dorzecza w odpowiedniej skali, zawierające granice dorzeczy, zlewni i – jeżeli takowe istnieją – obszarów wybrzeża, ukazujące topografię i zagospodarowanie przestrzenne,*
- b) *opis powodzi, które wystąpiły w przeszłości i miały znaczące negatywne konsekwencje dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz*

¹⁵⁴ Art. 1 dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim.

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,

c) 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:

d) 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 zamieszkanych, obszarów działalności gospodarczej oraz prognozę długofalowego rozwoju wydarzeń, w tym wpływu zmian klimatu na występowanie powodzi.

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:

a) bezpośredni wpływ powodzi na życie i zdrowie ludzi,

b) wpływ powodzi na obszary działalności gospodarczej wraz z infrastrukturą,

c) skuteczność istniejących budowli przeciwpowodziowych,

d) 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.

1.2. Mapy zagrożenia powodziowego i mapy ryzyka

Mapy zagrożenia powodziowego i mapy ryzyka¹⁵⁵ 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:

1. niskie prawdopodobieństwo powodzi lub scenariusze zdarzeń ekstremalnych,
2. średnie prawdopodobieństwo powodzi (częstotliwość występowania ≥ 100 lat),
3. wysokie prawdopodobieństwo powodzi, w odpowiednich przypadkach.

Dla każdego ze scenariuszy przedstawia się następujące elementy:

1. zasięg powodzi,
2. głębokość wody lub – w odpowiednich przypadkach – poziom zwierciadła wody,
3. tam, gdzie jest to właściwe, prędkość przepływu wody lub odnośny przepływ wody.

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:

1. „szacunkowa liczba mieszkańców potencjalnie dotkniętych powodzią,
2. rodzaj działalności gospodarczej prowadzonej na obszarze potencjalnie dotkniętym powodzią,
3. 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,
4. inne informacje uważane przez państwo członkowskie za przydatne, takie jak wskazanie obszarów, na których mogą wystąpić powodzie, któ-

¹⁵⁵ Por. definicje i przykłady: część IV, rozdział 3, podrozdziały 3.1-3.2.

rym towarzyszy transport dużej ilości osadów i rumowiska, oraz informacji o innych istotnych źródłach zanieczyszczenia”¹⁵⁶.

1.3. Plany zarządzania ryzykiem powodziowym

Ustalenie celów zarządzania ryzykiem powodziowym powierzono państwom członkowskim, przy czym w analizie tej szczególony 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 wód oraz kontrolowane zalewanie niektórych obszarów w przypadku wystąpienia powodzi”¹⁵⁷.

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 portowa. Są to aspekty, które wskazują na konieczność wzięcia pod uwagę czynników geograficznych, historycznych, ekonomicznych, gospodarki przestrzennej i infrastruktury. Następnie na podstawie map państwa członkowskie opracowują plany zarządzania ryzykiem powodziowym.

Harmonogram dalszych prac na forum UE oraz w państwach członkowskich przedstawia się następująco:

¹⁵⁶ Art. 6 dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim.

¹⁵⁷ Tamże.

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 lat¹⁵⁸.

¹⁵⁸ Art. 14 dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim.

2. KONTROLA ZAGROŻEŃ POWAŻNYMI AWARIAMI ZWIĄZANYMI Z SUBSTANCJAMI NIEBEZPIECZNYMI – SEVESO III

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 – 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.

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 dla 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:

1. potencjalnym wpływie zakładów na zdrowie ludzkie i środowisko,
2. 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.*

Minimalny zakres danych i informacji, które muszą zostać wzięte pod uwagę w raporcie o bezpieczeństwie, określa załącznik II do dyrektywy. W zakresie identyfikacji i analizy zagrożeń awariami oraz metod zapobiegawczych prowadzący zakład w raporcie o bezpieczeństwie uwzględnia:

1. „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:
 - a. przyczyny operacyjne,
 - b. 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,
 - c. przyczyny naturalne, na przykład trzęsienia ziemi lub powodzie;
2. ocenę zasięgu i skali skutków zidentyfikowanych poważnych awarii, w tym mapy, obrazowania lub, stosownie do potrzeb, równoważne opisy ukazujące obszary, które mogą zostać dotknięte takimi awariami mogącymi powstać w zakładzie;

3. 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;
4. opis parametrów technicznych i sprzętu użytego do celów bezpieczeństwa instalacji¹⁵⁹.

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 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.* Przyjęcie takiego podejścia w UE jest wynikiem analizy skutków katastrofy w Japonii 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.*

Zgodnie z przyjętym w dyrektywie harmonogramem państwa członkowskie miały wprowadzić w życie przepisy ustawowe, wykonawcze i administracyjne

¹⁵⁹ Załącznik nr II do dyrektywy Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi.

niezbędne do wykonania niniejszej dyrektywy w terminie do 31 maja 2015 r. Państwa członkowskie mają stosować niniejsze przepisy od dnia 1 czerwca 2015 r.

3. ZARZĄDZANIE RYZYKIEM ZWIĄZANYM Z ELEKTROWNIAМИ JĄDROWYMI – TESTY WYTRZYMAŁOŚCIOWE

W wyniku trzęsienia ziemi, do którego doszło 11 marca 2011 r. w Japonii, poniosło śmierć wielu ludzi. Efekt domina¹⁶⁰ w przypadku tej katastrofy przerosł oceny ryzyka dokonane przez zakład jądrowy. Trzęsienie ziemi spowodowało powstanie fali tsunami, która doprowadziła do wypadku w elektrowni jądrowej. 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 pomocy w Japonii. Przerosła ona zdolności reagowania służb kraju dotkniętego kaskadową katastrofą¹⁶¹.

Na forum Rady Unii Europejskiej już w dniach 24-25 marca 2011 r. przyjęto 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). Pilne prace po stronie Komisji Europejskiej, która miała określić zasady, na jakich będą dokonywane tzw. testy wytrzymałościowe (*stress tests*), wymuszała zwłaszcza obawa o ewentualny atak terrorystyczny na elektrownie atomowe w Europie. Rada Europejska miała natomiast

¹⁶⁰ Patrz: definicja na s. 44.

¹⁶¹ 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 strategię zarządzania kryzysowego). Katastrofy kaskadowe uwidoczniają 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, Vol. 3, No 1, 2015, s. 58-67 (tłumaczenie własne).

dokonać oceny wyników tej analizy. Plan działania Europejskiej Grupy Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego ENSREG zatwierdzono 1 sierpnia 2012 r. Z kolei 4 października 2012 r. Komisja wydała komunikat (COM(2012) 0571)¹⁶² 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 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 Fukushimie uwidocznily 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 Fukushimie, aby bardziej ograniczyć ryzyko incydentów jądrowych w Europie. Zadania sprawdzające określono jako celowane testy wytrzymałościowe marginesów bezpieczeństwa elektrowni jądrowych w świetle wniosków wyciągniętych z wydarzeń w Fukushimie, 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:

1. *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 ujęcia ciepła,*
2. *w 10 reaktorach nie zainstalowano przyrządów do pomiaru aktywności sejsmicznej wykorzystywanych na miejscu,*
3. *cztery kraje stosują obecnie dodatkowe systemy bezpieczeństwa w pełni niezależne od zwykłych systemów bezpieczeństwa, zlokalizowane*

¹⁶² Komunikat Komisji do Rady i Parlamentu Europejskiego dotyczący kompleksowych ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych, SWD(2012) 287, COM(2012) 571 wersja ostateczna, Bruksela, 4 października 2012 r.

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,

4. 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 innych.

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**¹⁶³. Istnieją luki w zapewnianiu kompleksowego i przejrzystego systemu identyfikacji oraz

¹⁶³ 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 ro-

zarządzania kluczowymi kwestiami bezpieczeństwa. *Jaskrawy przykład Fukushima pokazuje, że zagrożenie ze strony tsunami było zaniżone, głównie w wyniku działania czynników ludzkich, systemowych i organizacyjnych.*

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))*. Parlament przyjął do wiadomości komunikat Komisji w sprawie testów wytrzymałościowych i ich wyników po wypadku w Fukushima. 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 UE¹⁶⁴. *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 trzęsienia 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.*

Głównym czynnikiem gwarantującym wysoką jakość życia w społeczeństwie europejskim oraz ochronę naszej infrastruktury krytycznej stało się bez-

zumianego bezpieczeństwa, z pożytkiem dla siebie, ale i otoczenia. Źródło: M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, wyd. AP, Siedlce 2011, s. 210.

¹⁶⁴ Rezolucja Parlamentu Europejskiego w sprawie ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych (2012/2830(RSP)).

*pieczeństwo, polegające na zapobieganiu wspólnym zagrożeniom i ich usuwaniu*¹⁶⁵.

¹⁶⁵ Strategia Bezpieczeństwa Wewnętrznego UE, s. 13.

4. ZARZĄDZANIE RYZYKIEM W DZIEDZINIE ZDROWIA UE

Traktat o funkcjonowaniu Unii Europejskiej¹⁶⁶ przyznaje jej kompetencje do prowadzenia działań mających na celu wspieranie, koordynowanie lub uzupełnianie działań państw członkowskich w obszarze ochrony i poprawy zdrowia ludzkiego. Art. 168 określa dokładniej *działanie Unii, które uzupełnia polityki krajowe, nakierowane jest na poprawę zdrowia publicznego, zapobieganie chorobom i dolegliwościom 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 ostrzeżenie w przypadku takich zagrożeń i ich zwalczanie*. 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, środki dotyczące monitorowania poważnych transgranicznych zagrożeń dla zdrowia, wczesnego ostrzegania w przypadku takich zagrożeń oraz ich zwalczania, z wyłączeniem jakiegokolwiek harmonizacji przepisów ustawowych i wykonawczych państw członkowskich¹⁶⁷.

Koncepcja oceny ryzyka i zarządzania ryzykiem w dziedzinie zdrowia w UE obejmuje następujące elementy¹⁶⁸:

1. ocenę ryzyka (*risk assessment*),
2. zarządzanie ryzykiem (*risk management*),
3. przekazywanie informacji o ryzyku (*risk communication*).

W ramach niniejszej analizy skupiono się na ocenie ryzyka. W reagowaniu na transgraniczne kryzysy zdrowotne ocena ryzyka jest pierwszym działaniem.

¹⁶⁶ Traktat o funkcjonowaniu Unii Europejskiej, Dz.U. UE C 83/123 z 30 marca 2010 r.

¹⁶⁷ Tamże, art. 168.

¹⁶⁸ Por. decyzja Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, 2011/0421 (COD), COM(2011) 866 wersja ostateczna, Bruksela, 8 grudnia 2011 r. 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.

Inicjatywa UE dot. bezpieczeństwa zdrowotnego ma na celu szybkie uruchomienie 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.*¹⁶⁹ była odpowiedzią UE na potrzebę działań w obszarze bezpieczeństwa zdrowotnego. Unia wyciągnęła 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 na Islandii) oraz 2011 (skażenie żywności bakterią *E. coli*), co pozwoliło jej lepiej zarządzać w przypadku wirusa Ebola. Wzmocnienie roli UE w reagowaniu na kryzysy zdrowotne było więc sumą doświadczeń i te doświadczenia zawierała propozycja decyzji. Proponowano ustanowienie w niej również 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.

¹⁶⁹ Wniosek – Decyzja Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 wersja ostateczna, 2011/0421 (COD), Bruksela, 8 grudnia 2011 r.

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 pochodzenia¹⁷⁰.

Wniosek Komisji bazował na współpracy istniejących struktur, jednak proponował rozszerzenie dokonywanej oceny ryzyka oraz koordynację środków tak, aby poza chorobami zakaźnymi obejmowały 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.* 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.

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 rozważyć 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*

¹⁷⁰ Wniosek – Decyzja Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 wersja ostateczna, 2011/0421 (COD), Bruksela, 8 grudnia 2011 r., s. 3.

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.

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 Zdrowia, którego zadaniem jest koordynowanie 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 zdrowia¹⁷¹. Monitoring poważnych transgranicznych zagrożeń zdrowia innych niż choroby zakaźne opiera się jednak na systemach monitorowania państw członkowskich, a dostępne informacje są wymieniane za pośrednictwem EWRS.

Obecny program UE w dziedzinie zdrowia zawiera wiele działań związanych z ostrzeganiem, oceną ryzyka i monitorowaniem niektórych zagrożeń zdrowia. Po 2013 r. Komisja zamierzała objąć wszystkie te działania wnioskowanym programem „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

¹⁷¹ Tamże.

2014 r. w sprawie ustanowienia 3. Programu działań Unii w dziedzinie zdrowia (2014-2020)¹⁷² wskazało, że *program powinien wspierać skoordynowane środki 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 kryzysowymi.*

¹⁷² 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.U. L 86/3, t. 57, 21 marca 2014 r., s. 1.

5. ZARZĄDZANIE RYZYKIEM NIELEGALNEJ IMIGRACJI – FRONTEX

Agencja FRONTEX opracowała własny zintegrowany model analizy ryzyka,¹⁷³ tzw. CIRAM (*Common Integrated Risk Analysis Model*). Jego idea sięga 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.¹⁷⁴

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 nie-

¹⁷³ Agencja FRONTEX w ramach CIRAM umożliwia ocenę względnego ryzyka stwarzanego przez różne zagrożenia, dokonując ich identyfikacji i analizy.

¹⁷⁴ Za: S. Carrera, *The EU Border Management Strategy FRONTEX and the challenges of irregular immigration in the Canary Islands*, CEPS Working Document, nr 261, marzec 2007.

legalnej migracji czy przestępczości zorganizowanej, w tym handlu ludźmi. W razie konieczności podjęcia działań przez UE FRONTEX we współpracy z państwami członkowskimi może rozpocząć konkretne działanie 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.

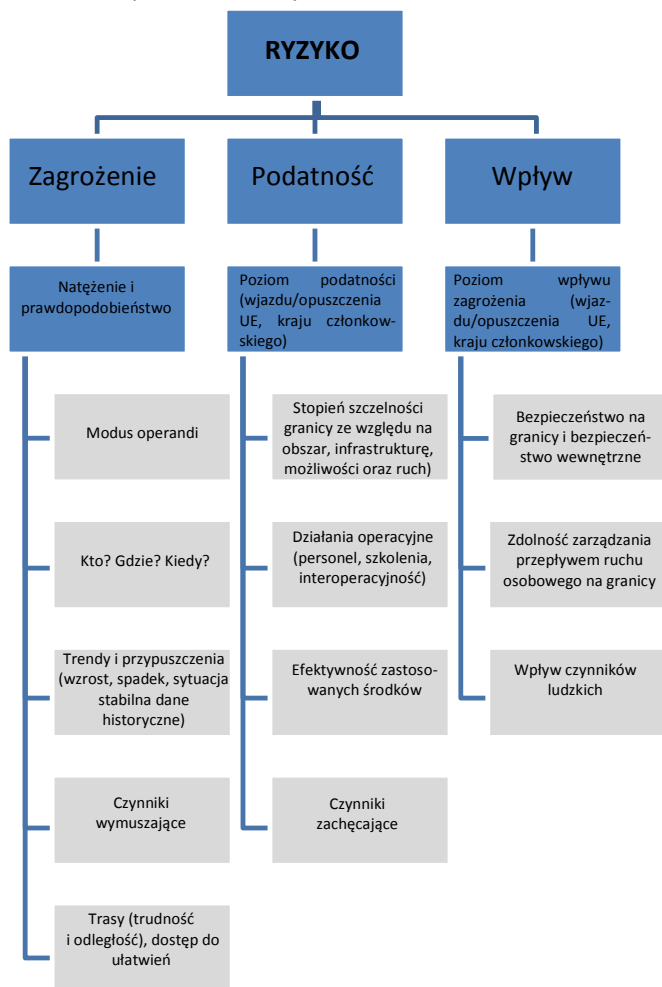
Zależności pomiędzy poszczególnymi elementami badane są ze względu na poziom podatności¹⁷⁵ (ang. *level of vulnerability*) dla Unii Europejskiej, danego wjazdu do państwa członkowskiego oraz miejsca opuszczenia UE. W tym obszarze bada się np. stopień szczelności granicy ze względu na obszar, infrastrukturę, możliwości oraz ruch. Badane są także działania operacyjne pod kątem personelu, szkolenia, interoperacyjności¹⁷⁶ oraz efektywność zastosowanych środków, jak i tzw. *pull factors* – czynników zachęcających do migracji (np. dostęp do pracy, bezpłatna opieka medyczna, bezpłatny dostęp do szkół).

W analizie ryzyka pod kątem wpływu rozpatruje się sytuację na granicy i sytuację wewnętrzną danego kraju członkowskiego (*border and internal security*),

¹⁷⁵ Poziom podatności – wartość podatności lub suma podatności. Źródło: opracowanie własne.

¹⁷⁶ 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.U. L 260 z 3 października 2009 r.

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. 17.



Rys. 17. Analiza ryzyka w ramach CIRAM¹⁷⁷

¹⁷⁷ Za: FRONTEX, Western Balkans, Annual Risk Analysis, 2012.

Kluczowe 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.).

6. 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”¹⁷⁸.

UE przeznacza także znaczne środki na projekty badawcze, które obejmują badania nad poszczególnymi rodzajami zagrożeń występującymi w Europie, np. powodziami, 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.*

6.1. 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

¹⁷⁸ Informacja prasowa KE, http://europa.eu/rapid/press-release_IP-13-317_pl.htm?locale=FR, dostęp: marzec 2015.

w ramach projektu ma pomóc ocenić, do 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 unaocznić 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 ziemni).
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: So-czy-Isonzo i Dunaju, pozwoliła na analizę aspektów transgranicznych. W tym projekcie widać podejście UE, które polega na rozpatrywaniu całościowo do-rzeczy 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 ana-lizy ryzyka, także na poziomie Unii Europejskiej, do polityki zapobiegania kata-strofom naturalnym. Zastosowane w projekcie środki, techniki oraz metodolo-

gia mają pozwolić na uwzględnienie zmian w zakresie użytkowania terenu, gospodarki przestrzennej oraz wpływu zmian klimatu.

6.2. Matrix

Projekt Matrix, 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 (*single-type hazards*) oraz dostarczenie bazy wiedzy do przeprowadzania złożonej oceny ryzyka w Europie.

Zgodnie z obserwacjami poczynionymi do założeń projektu w opinii jego realizatorów pewne obszary w Europie są narażone na ryzyko wystąpienia katastrof naturalnych i zdarzeń w pewnych kombinacjach. Analiza i ocena zagrożeń i ryzyka nie powinna opierać się na jednostkowej ocenie jednego zagrożenia, zawsze powinna uwzględniać zagrożenia z nim powiązane. Trzęsienie ziemi, erupcje wulkanu, osuwiska ziemi, tsunami, pożary, śnieżyce, 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. Projekt Matrix zakładał rozwinięcie metod i narzędzi badawczych, które będą przydatne w kontekście europejskim. Miejsce występowania danych zdarzeń (powodzie, trzęsienie ziemi, wulkany) jest 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 (*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 (*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 czasie¹⁷⁹ (*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. trzęsienie 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.

6.3. Catalyst

Projekt *Capacity Development for Hazard Risk Reduction and Adaptation Catalyst* 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,

¹⁷⁹ Podatność wystąpienia zdarzenia w czasie – oznacza zmienność charakterystyk podatności w czasie. Źródło: <https://crisma-cat.ait.ac.at/glossary/time-dependent-vulnerability>, dostęp: marzec 2015.

która będzie stanowiła miejsce wymiany wiedzy i zostanie udostępniona zainteresowanym ekspertom, badaczom i praktykom.

PODSUMOWANIE I WNIOSKI

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 usług¹⁸⁰. 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, scenariuszy, wprowadza się też zmienne do mierzenia ryzyka w postaci skutków dla obszaru.

UE stosuje metody ISO oraz ONZ, jak i państw członkowskich. Wspiera się przy tym metodologią wypracowaną już w ramach międzynarodowego standardu ISO. 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

¹⁸⁰ Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie wzmocnienia zdolności Unii do reagowania w przypadku katastrof, COM(2008) 130 wersja ostateczna, Bruksela, 5 marca 2008 r., s. 3.

na forum *Global Risk Assessment Dialogue* Unii Europejskiej udaje się w wymiarze globalnym osiągnąć przegląd systemów oraz rozumienia oceny ryzyka, wyłonić istotne kwestie, jak i określić wyzwania dla przyszłych ocen ryzyka, znaleźć obszary dla dialogu i współpracy oraz określić priorytety dla przyszłych inicjatyw w tym obszarze.

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. *multi-risk assessment* (ocena ryzyka uwzględniająca wiele rodzajów zagrożeń – tłum. własne). 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”¹⁸¹. Zasada pomocniczości ma na celu określenie odpowiedniego poziomu interwencji w dziedzinach kompetencji dzielonych między UE a państwami członkowskimi. Ochrona ludności jest

¹⁸¹ Art. 5 Traktatu o funkcjonowaniu Unii Europejskiej.

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 (...)”¹⁸².

Kolejną zasadą jest zasada proporcjonalności. Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka 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”¹⁸³. 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”¹⁸⁴.

¹⁸² Dyrektywa 2007/60/WE PE i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim, 6 listopada 2007 r., Dz.U. L 288/27.

¹⁸³ Art. 5 Traktatu o funkcjonowaniu Unii Europejskiej.

¹⁸⁴ 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.U. L 197/1 z dnia 24 lipca 2012 r.

W toku prac problematyczną kwestią okazała się porównywalność danych, analiz ryzyka i metodologii stosowanych przez poszczególne państwa członkowskie w ocenach ryzyka. Dlatego obecne 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 co raz 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”¹⁸⁵. 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, 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.

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. *Inte-*

¹⁸⁵ Art. 9 dyrektywy 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.U. L 197/1 z dnia 24 lipca 2012 r.

grated Risk Management – IRM), które obejmuje prewencję, przygotowanie, reagowanie oraz odbudowę w przypadku wszystkich zagrożeń w Europie.

Przegląd prac w zakresie analizy ryzyka i zagrożeń pokazuje sektorowe podejście UE do kwestii oceny ryzyka dla poszczególnych zagrożeń, przedstawia także zmianę podejścia UE i próby oraz cele osiągnięcia możliwości oceny zagrożeń w ramach efektu domina, czy zagrożeń powiązanych, mających wpływ na wiele sektorów. 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. Dlatego wspiera się w tych wysiłkach, rozwijając współpracę na forum międzynarodowym, a także korzystając z wyników prac poszczególnych państw członkowskich oraz wiedzy wypracowywanej w ramach polityki badawczej.

SUMMARY AND CONCLUSIONS

The European Commission, already in 2008, acknowledged the need of the EU's greater capacity of facing general challenges for prevention of catastrophes, mitigation of their consequences and response. The complexity and scope of these multidimensional challenges require a comprehensive approach by the EU to the continuum of disaster risk assessment, forecast, prevention, preparedness and mitigation (pre- and post-disaster), bringing together the different policies, instruments and services¹⁸⁶. In December 2010, the EC published the *Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management*, presenting guidelines for the member states for risk assessment and risk mapping, by assembling and harmonising methodologies, but leaving hints to the states. Risk assessment is crucial for the prevention of disasters in the member states, it may support prevention and reinforce resource planning in case of disaster response. The aim of the guidelines is to improve cohesion between risk assessments undertaken by the member states and the possibility of comparing them. This will hence facilitate collaboration, e.g. in border regions in case of a similar risk for a given region. It is significant that a number of options is discussed in the guidelines, e.g. variables for risk measurement, such as consequences for the area, are introduced for assessment of a single risk and for assessment of a risk considering multiple threats, the domino effect, scenarios.

The EU applies the ISO and UN's methods, as well as the member states' methods. The EU is using a methodology created under the international ISO standard. It is also using methodologies utilised by the member states, but also takes advantage of experiences from other countries, the USA, Canada, New Zealand. The 2nd international conference devoted to risk management, the Global Risk Assessment Dialogue, took place in Brussels in 2011. Its objective was to enable discussion concerning risk assessment priorities, assessment methods, principles of conducting a risk assessment. The meeting took place

¹⁸⁶ *Communication from the Commission to the European Parliament and the Council on reinforcing the Union's disaster response capacity*, COM(2008) 130, wersja ostateczna, Bruksela, 5 marca 2008 r., s. 3.

based on the collaboration between the EU and the USA and Canada. As a result of meetings held at the Global Risk Assessment Dialogue forum, the EU manages to achieve, globally, a review and understanding of risk assessment systems, to determine the important matters, to identify challenges for future risk assessments, to find space for a dialogue and cooperation, and to set up priorities for future initiatives in this field.

Risk and threat assessment methodologies have been elaborated at the EU level, notably for risks related to flood, drought, industrial failures, protection of critical infrastructure. The examples of important papers are discussed in this analysis for: floods, chemical failures and critical infrastructure failure, threats connected with safety at internal borders, health safety. Works in the field of risk assessment, threat assessment, risk management are seen in the sectoral approach. Measures in the field of so-called Multi-risk assessment (assessment of risk considering multiple threats – own translation) can already be observed in the European Union. The EU's strategic documents refer to this area as to a challenge. Moreover, the European Union, being interested itself in this subject and obliged by documents to make an overall analysis of threats for the EU, is taking advantage of research works in this domain. The works pertain not only to particular natural or technological risks, but, as seen from this analysis, also to more complex assessments presented with the example of KULTURISK, MATRIX, CATALYST projects.

The principle of subsidiarity spelled out in Article 5 of the Treaty is pivotal for understanding works at the EU forum. *Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and insofar as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level*¹⁸⁷. The purpose of the subsidiarity principle is to define the appropriate level of intervention in the areas of competences shared between the EU and the member states. For example, protection of people is the member states' responsibility, and the EU's task is to support, coordinate

¹⁸⁷ Article 5 of the *Treaty on European Union*.

or supplement their actions. The principle of subsidiarity concerns actions at the EU, national or regional level. The EU can intervene in any of the cases only if it is able to act more effectively than the Member States. The EU's flood risk assessment and management regulations are an example of this: *Since the objective of this Directive, namely the establishment of a framework for measures to reduce the risks of flood damage, cannot be sufficiently achieved by the Member States and can by reason of scale and effects of actions be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. (...)*¹⁸⁸.

Another principle is the principle of proportionality. Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks does not go beyond what is necessary to achieve that objective. *Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties. The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality*¹⁸⁹. Similar as in the case of Seveso III directive, the same provision has been applied: *Since the objective of this Directive, namely to ensure a high level of protection of human health and the environment, cannot be sufficiently achieved by Member States and can, therefore, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective*¹⁹⁰.

¹⁸⁸ Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks, 6.11.2007, L 288/27.

¹⁸⁹ Article 5 of the *Treaty on European Union*.

¹⁹⁰ Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC, L 197/1 of 24.07.2012.

A problem encountered during the works was the comparability of data, risk analyses and methodologies used by individual member states in risk assessments. For this reason, the EU's current works are aimed at achieving the possibility of data comparability, and are concentrated on performance of risk analyses which do not consider a single risk only, e.g. occurrence of flood or forest fire, but more and more often embark on the so-called domino effect for a chain of events cause by one event, which implies the occurrence of another one. The domino effect is described in the provisions of Seveso III directive adopted in 2012. *In order to reduce the risk of domino effects, where establishments are sited in such a way or so close together as to increase the likelihood of major accidents, or aggravate their consequences, operators should cooperate in the exchange of appropriate information and in informing the public, including neighbouring establishments that could be affected*¹⁹¹. On the other hand, the Commission's possible action may be to establish guidelines regarding safe distance and domino effects (Article 24). The EU's experience after a catastrophe in Japan in 2011 needs to be taken into account for domino effects and for inclusion of such provisions in the directive.

Hazard analyses and risk assessments are also pursued by EU agencies within their competences. The relevant EU agencies have developed risk and hazard assessment methodologies within their areas of competences, e.g. FRONTEX agency in scope of security evaluation at external borders, DG HOME in scope of terrorism threat analyses for the EU, DG SANCO in scope of hazards related to health, the European External Action Service in scope of European Union external security risk and hazard assessment.

Even though some EU policies incorporate the issue of risk analysis or works over the issue have commenced, the EU needs to take more efforts to adopt an approach of Integrated Risk Management (IRM) encompassing prevention, preparation, reaction and reconstruction for all hazards in Europe.

¹⁹¹ Article 9 of Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC, L 197/1 of 24.07.2012.

The undertaken review of works in scope of risk and hazard analysis shows the EU's sectoral approach to risk assessment for particular risks, it also indicates a shift in the EU's approach and the attempts and objectives to achieve a possibility of hazard assessment under the domino effect, or related hazards, having an effect on many sectors. The Union aims at achieving a possibility of assessing risks deriving from natural and man-induced risks which may occur in Europe, but also those the members states or neighbouring regions are exposed to. For this reason, the EU reinforces its efforts by developing international collaboration and by using the outcomes of the members states' works and knowledge created under the research policy.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

1. Cieślarczyk M., *Kultura bezpieczeństwa i obronności*, wyd. AP, Siedlce 2011.
2. Pescaroli G., Alexander D., *A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor*, Planet@Risk, Vol. 3, No 1, 2015, s. 58-67.

Akty prawne

1. Traktat o funkcjonowaniu Unii Europejskiej, Dz.U. UE C 83/123 z 30 marca 2010 r., Bruksela.
2. Dyrektywa 2007/60/WE PE i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim, L 288/27, 6 listopada 2007 r., Bruksela.
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, L 197/1 z dnia 24 lipca 2012 r., Bruksela.
4. 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. UE L 86/3, t. 57, 21 marca 2014 r.
5. Decyzja nr 922/2009/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie rozwiązań interoperacyjnych dla europejskich administracji publicznych (ISA), Dz.U. L 260 z 3 października 2009 r.
6. Decyzja Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, COM(2011) 866 wersja ostateczna, 2011/0421 (COD), Bruksela, 8 grudnia 2011 r.
7. 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.
8. Zarządzanie zagrożeniem powodziowym, Zapobieganie powodziom, ochrona przeciwpowodziowa i ograniczanie skutków powodzi, Komuni-

- kat Komisji dla Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, COM(2004) 472 wersja ostateczna, Bruksela, 12 lipca 2004 r.
9. Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie wzmocnienia zdolności Unii do reagowania w przypadku katastrof, COM(2008) 130 wersja ostateczna, Bruksela, 5 marca 2008 r.
 10. Komunikat Komisji do Rady i Parlamentu Europejskiego dotyczący kompleksowych ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych, SWD(2012) 287, COM(2012) 571 wersja ostateczna, Bruksela, 4 października 2012 r.
 11. Wniosek – decyzja Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia, 2011/0421 (COD), COM(2011) 866 wersja ostateczna, Bruksela, 8 grudnia 2011 r.
 12. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy, COM(2010) 673 wersja ostateczna, Bruksela, 22 listopada 2010 r.
 13. Rezolucja Parlamentu Europejskiego w sprawie ocen ryzyka i bezpieczeństwa (testów wytrzymałościowych) elektrowni jądrowych w Unii Europejskiej oraz działań powiązanych (2012/2830(RSP)), Bruksela.
 14. Risk Assessment and Mapping Guidelines for Disaster Management, Commission Staff Working Paper, SEC(2010) 1626 wersja ostateczna, Bruksela, 21 grudnia 2010 r.

Dokumenty elektroniczne, strony internetowe i inne

1. Carrera S., *The EU Border Management Strategy FRONTEX and the challenges of irregular immigration in the Canary Islands*, CEPS Working Document, nr 261, marzec 2007.
2. Frontex, Western Balkans, Annual Risk Analysis 2012.
3. <http://europa.eu>.
4. <https://crisma-cat.ait.ac.at/glossary>.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM W WYBRANYCH PAŃSTWACH

PART III
RISK MANAGEMENT IN SELECTED COUNTRIES

WPROWADZENIE

W części III niniejszego opracowania zawarta została analiza metodyk¹⁹² 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. Podane 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*, Swedish Civil Contingencies Agency, 2012 (Szwecja).
7. *The National Risk Register of Civil Emergencies (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 roz-

¹⁹² 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 w celu realizacji zadań z zakresu zarządzania ryzykiem poszczególnych państw.

wiązań 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. Umożliwiły również wskazanie korzyści z ich zastosowania, z uwzględnieniem potrzeb planowania cywilnego w Polsce. Rozważone zostały zarówno koncepcje przyjętych metodyk, jak również stosowane techniki i metody oceny ryzyka.

INTRODUCTION

An analysis of the risk assessment methodologies applied in other countries is analysed in part III¹⁹³. Literature studies included the solutions adopted in Australia, Ireland, Germany, Sweden and the Great Britain. Their selection was determined by the fact that such countries possess experience related to developing an own risk assessment methodology for the purpose of emergency planning. The documents analysed have the form of guides (guidelines) describing the particular countries' approach to this subject. Documents that consider the results of risk assessments conducted at the national level were taken into account. The following were the documents analysed:

1. National Emergency Risk Assessment Guidelines. Commonwealth of Australia and each of its states and territories 2010, October 2010 (Australia).
2. A National Risk Assessment for Ireland, Office of Emergency Planning, December 2012 (Ireland).
3. A Framework for Major Emergency Management. A Guide to risk Assessment in Major Emergency Management, January 2010 (Ireland).
4. Method of Risk Analysis for Civil Protection 2011; Federal Office of Civil Protection and Disaster Assistance 2011 (Germany).
5. Guide to risk and Vulnerability Analyses; Swedish Civil Contingencies Agency; 2012 (Sweden).
6. Swedish National Risk Assessment; Swedish Civil Contingencies Agency; 2012 (Sweden).
7. The National Risk Register of Civil Emergencies (NRR), Cabinet Office; 2010 (Great Britain).
8. National Risk Register for Civil Emergencies 2013 (NRR), Cabinet Office; 2013 (Great Britain).

The methodologies discussed vary in the extent of details presented in their contents. Nevertheless, the basic assumptions included therein referring to the

¹⁹³ Contrary to the methods discussed in part I and according to the definitions included there, methodologies are discussed in this part, as the sets of principles, codes of procedure (methods) indispensable to fulfil risk management tasks of particular countries are collected here.

risk assessment solutions adopted have allowed to present the approach of the particular countries in this field, and then to make a comparative analysis of risk assessment methodologies applied in the particular countries with regard to their strengths and weaknesses. They also enabled to indicate the benefits from their usage, considering the needs of civilian emergency planning in Poland. The concepts of the methodologies adopted were appraised for this purpose (represented by their individual stages and characteristics) as well as the risk assessment techniques and methods used.

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 niekorzystne¹⁹⁴ 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 przyszłości.

Taka koncepcja budowania bezpieczeństwa zmuszała do wyjścia poza reagowanie i udzielanie pomocy. Należało podjąć zdecydowane działania, uwzględniając analizę kosztów i korzyści¹⁹⁵, zmniejszenie wrażliwości ekspozy-

¹⁹⁴ Patrz: definicja na s. 67.

¹⁹⁵ 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.

cji¹⁹⁶, uodpornienie 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*¹⁹⁷. 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:

1. zwiększanie świadomości ryzyka zagrożeń w społeczeństwie i wdrażanie przedsięwzięć odpowiedniego postępowania z ryzykiem¹⁹⁸,
2. standaryzację oceny ryzyka¹⁹⁹ i doskonalenie alternatywnych propozycji ograniczania ryzyka²⁰⁰,
3. wzrost przejrzystości procesu, co ułatwiło jego realizację w zakresie ocen, kontroli i modelowania ryzyka w wyniku zdobywania wiedzy i informacji,
4. 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:

¹⁹⁶ Patrz: definicja na s. 39.

¹⁹⁷ *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.

¹⁹⁸ Patrz: definicja na s. 28.

¹⁹⁹ Patrz: definicja na s. 29.

²⁰⁰ 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.

1. umożliwia skupienie uwagi na ryzyku zarówno na szczeblu samorządu, jak i na wyższych szczeblach,
2. 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,
3. pozwala wykorzystać podejście scenariuszowe²⁰¹,
4. umożliwia klasyfikację ryzyka²⁰² w zakresie wiarygodnych poziomów konsekwencji,
5. pozwala identyfikować występujące ryzyka będące pod kontrolą oraz te, które wymagają wdrożenia dodatkowej kontroli lub wzmocnienia istniejącej,
6. zapewnia podstawy dla jakościowej oceny ryzyka oraz uruchomienie bardziej szczegółowej analizy,
7. umożliwia ewaluację ryzyka²⁰³ na różnych poziomach pewności,
8. 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.

²⁰¹ Podejście opisano w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 2 *Metody wykorzystywane w ocenie ryzyka*, podrozdział 2.13 *Analiza scenariuszowa*.

²⁰² Patrz: definicja na s. 87.

²⁰³ Patrz: definicja na s. 37.

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 redukujących²⁰⁴ ryzyko.
4. **Dokładne adresowanie niepewności.** Poprawnie realizowane zarządzanie ryzykiem pozwala ograniczać niepewność.
5. **Systematyczność, określoność i terminowość.** Czynniki te gwarantują spójność, elastyczność i adekwatność rezultatów.
6. **Dostępność najlepszych informacji**²⁰⁵. 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 różnicowania 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 ryzyka²⁰⁶.
8. **Uwzględnienie czynników ludzkich i kulturowych.** W zarządzaniu ryzykiem należy uwzględniać zdolności percepcyjne zarówno jednostek, jak i powołanych do tego zadania zespołów.

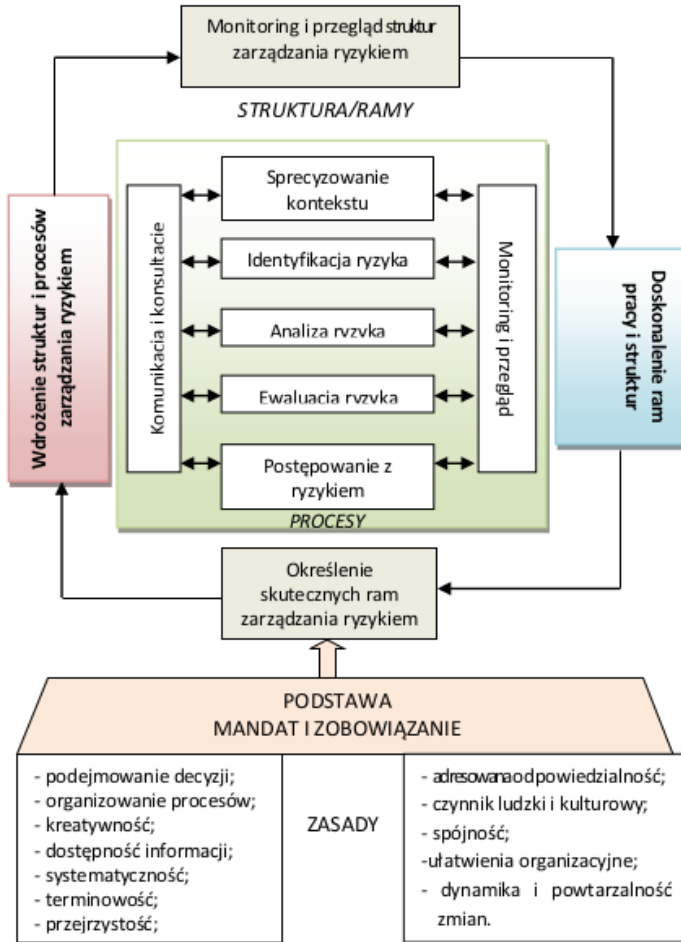
²⁰⁴ Patrz: ograniczanie ryzyka, s. 157.

²⁰⁵ Zgodnie z ISO 31000: pełny przekrój dostępnych danych oraz informacji na potrzeby bieżących oraz przyszłych działań.

²⁰⁶ Patrz: agregacja ryzyka, s. 46.

- 9. Transparentność i ogólność.** Zapewnienie skuteczności zarządzania ryzykiem zależy od angażowania wszystkich interesariuszy²⁰⁷, 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.

²⁰⁷ Patrz: definicja na s. 42.



Rys. 18. Zarządzanie ryzykiem: zasady, struktura i procesy²⁰⁸

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

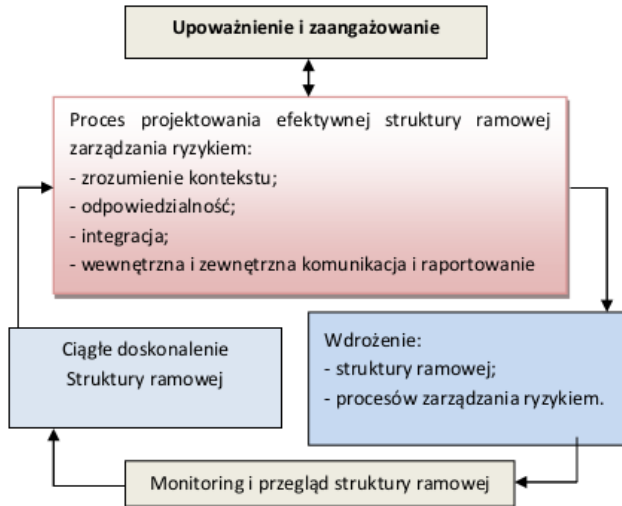
²⁰⁸ Źródło: *National Emergency Risk Assessment Guidelines*. Por.: rys. 1. Relacje pomiędzy zasadami, strukturą ramową i procesem zarządzania ryzykiem, s. 18.

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. 19):

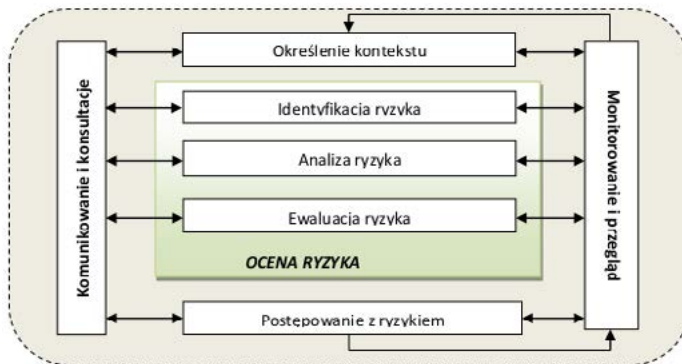
1. upoważnienie i zaangażowanie kierownictwa,
2. procesy ukierunkowane na projektowanie skutecznej struktury ramowej zarządzania ryzykiem,
3. programy wdrażania struktury i procesów zarządzania ryzykiem,
4. programy pozwalające monitorować i analizować tę działalność,
5. procesy ciągłego wdrażania tej działalności.

Proces zarządzania ryzykiem jest opisany w normie ISO 31000:2009 i zgodnie z nią powinien być integralną częścią zarządzania²⁰⁹. 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.

²⁰⁹ Standard zarządzania ryzykiem wyraźnie rozgranicza zarządzanie i decydowanie.



Rys. 19. Struktura ramowa zarządzania ryzykiem²¹⁰



Rys. 20. Ogólny schemat procesu zarządzania ryzykiem²¹¹

Proces zawiera pięć głównych składowych (rys. 20), wspieranych przez komunikowanie i konsultacje oraz monitorowanie i przegląd. Ma zastosowanie w każdej sytuacji, dotyczącej dowolnego zagrożenia.

Zrozumienie (określenie) kontekstu²¹² polega na zdefiniowaniu parametrów, w jakich będzie realizowane zarządzanie ryzykiem. Definiuje się je na podstawie

²¹⁰ Źródło: opracowanie na podstawie *National Emergency Risk Assessment Guidelines*.

²¹¹ Tamże.

²¹² Patrz: definicja na s. 31.

możliwości organizacji lub społeczności w całym przekroju zarządzania ryzykiem. Użyteczność tych działań polega na wspólnym zrozumieniu zakresu procesu i kryteriów ryzyka²¹³, 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 ryzyka²¹⁴ 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 ryzyka²¹⁵, 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 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 ryzyka²¹⁶ stanowi ten element procesu zarządzania ryzykiem, który pozwala określić poziom ryzyka²¹⁷. 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, prawdopo-

²¹³ Patrz: definicja na s. 40.

²¹⁴ Patrz: definicja na s. 27.

²¹⁵ Patrz: definicja na s. 45.

²¹⁶ Patrz: definicja na s. 31.

²¹⁷ Patrz: definicja na s. 39.

dobieństwo 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 hierarchizacji²¹⁸, 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 ryzyka²¹⁹ 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 rozłącznie. Przedsięwzięcia w zakresie postępowania z ryzykiem obejmują: unikanie, podjęcie lub zwiększenie ryzyka, usunięcie źródła ryzyka, zmianę (konsekwencji lub prawdopodobieństwa), optymalizację,

²¹⁸ Patrz: definicja na s. 87.

²¹⁹ Modyfikacja ryzyka – działania podejmowane samodzielnie lub w kombinacji w celu ograniczenia ryzyka. Źródło: opracowanie autorskie.

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 konsultacje²²⁰ 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.

Monitorowanie²²¹ i **przegląd**²²² 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.

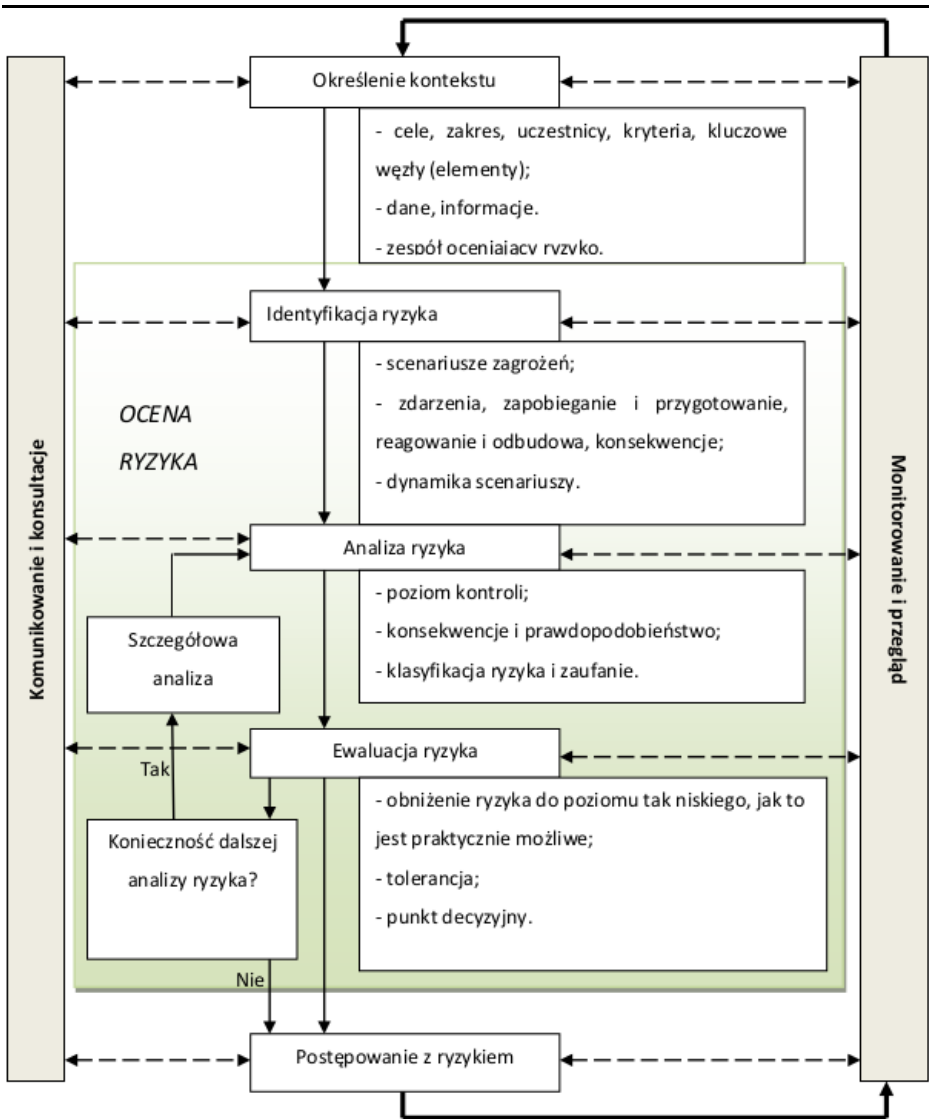
²²⁰ Patrz: definicja na s. 40.

²²¹ Patrz: definicja na s. 37.

²²² Patrz: definicja na s. 37.

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. 21). Punktem wyjścia 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. 21. Metodyka oceny ryzyka wystąpienia zdarzeń niekorzystnych²²³

²²³ Źródło: *National Emergency Risk Assessment Guidelines*.

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** (gdy 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:

1. stosowanie scenariuszy zdarzeń w całym procesie oceny ryzyka,
2. 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,
3. 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.
4. 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,

5. 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 unikać błędnych rezultatów, wynikających np. z subiektywnego postrzegania,
6. 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:

1. zgromadzenie wiedzy specjalistycznej odpowiadającej zakresowi tematu warsztatów,
2. prawidłowość zastosowania oraz dyscyplinę w przebiegu procesu oceny ryzyka,
3. dostęp do właściwych informacji i baz danych (jeszcze przed warsztatami),
4. 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 kryzysową²²⁴ czy możliwości sprostania potencjalnym zagrożeniom. Wspólne zrozumienie celów tej oceny jest najważniejsze dla zapewnienia

²²⁴ 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.

nia, że wszystkie istotne ryzyka zostały uwzględnione. Potwierdzenie celów będzie wspierało inne aspekty 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:

1. definicje konsekwencji (charakter i rodzaj oraz sposób pomiaru),
2. definicje prawdopodobieństw (rodzaj oraz sposób pomiaru),
3. kategorie poziomu ryzyka (sposób ustalenia),
4. definicje stopnia ufności,
5. kategorie ewaluacji (określenie poziomu ryzyka akceptowalnego lub tolerowanego).

Kryteria (opublikowane w Narodowych Wytycznych Oceny Ryzyka Zdarzeń Kryzysowych²²⁵) 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 klu-

²²⁵ Opublikowane w Australii w 2010 r.

czowe 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 w formie zorganizowanej lub w mediach²²⁶. 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 9).

²²⁶ 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 ostrzeżenie i alarmowanie ludności. Wspomagają również zapobieganie zagrożeniom poprzez edukację. Z drugiej jednak strony, poprzez rozpowszechnienie niezweryfikowanej informacji, same mogą doprowadzić do trudnego do opanowania kryzysu.

Tabela 9. Rejestr ryzyka (przykład)²²⁷

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.					

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 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 prowadzenia skutecznych kontroli:

²²⁷ Źródło: *National Emergency Risk Assessment Guidelines*.

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 objęgu. 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 10 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 10. Tabela prawdopodobieństwa²²⁸

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

²²⁸ Źródło: *National Emergency Risk Assessment Guidelines*.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

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

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 11. 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 11. Procentowy rozkład prawdopodobieństwa nasilenia w latach przy szansie 1%²²⁹

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%

Matryca ryzyka (tabela 12) 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.

²²⁹ Tamże.

Tabela 12. Matryca ryzyka²³⁰

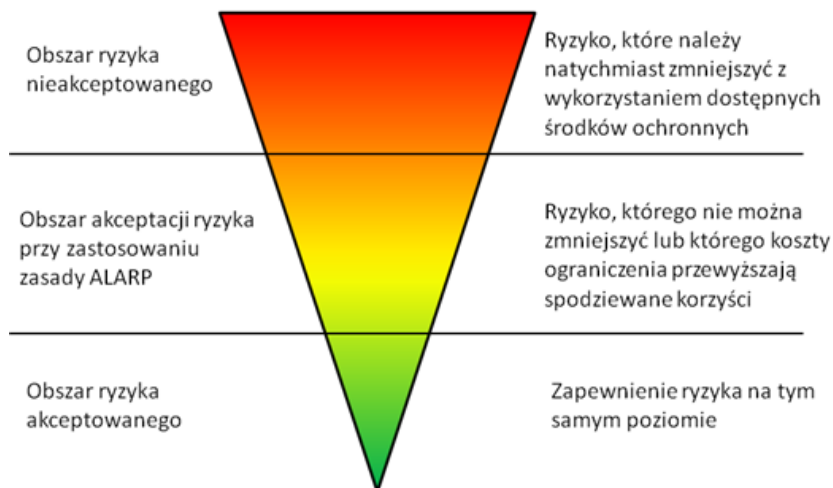
Prawdopodobieństwo	Konsekwencje				
	nieznaczące	małe	średnie	wysokie	katastrofalne
prawie pewne	średni	średni	wysoki	ekstremalny	ekstremalny
prawdopodobne	niski	średni	wysoki	wysoki	ekstremalny
możliwe	niski	niski	średni	wysoki	wysoki
nieprawdopodobne	niski	niski	średni	średni	wysoki
rzadkie	niski	niski	niski	średni	średni
bardzo rzadkie	niski	niski	niski	niski	średni
niewiarygodne	niski	niski	niski	niski	niski

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 informacji²³¹. Zgodnie z zasadą ALARP (rys. 22) 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).

²³⁰ Źródło: *National Emergency Risk Assessment Guidelines*.

²³¹ 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*.

Akceptacja ryzyka przy uwzględnieniu zasady ALARP



Rys. 22. Zasada ALARP²³²

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 macierzach tolerancji (tabela 13, 14 i 15). Poszczególne macierze tolerancji należy stosować w zależności od stopnia ufności dla konkretnego ryzyka.

Tabela 13. Ewaluacja ryzyka – wysoki poziom wiarygodności²³³

Poziom prawdopodobieństwa	Poziom konsekwencji				
	nieznaczny	mały	średni	wysoki	katastrofalny
prawie pewne	tolerowane	tolerowane	tolerowane	nietolerowane	nietolerowane
prawdopodobne	akceptowane	tolerowane	tolerowane	tolerowane	nietolerowane
możliwe	akceptowane	akceptowane	tolerowane	tolerowane	tolerowane

²³² Źródło: <http://www.ryzykozawodoweonline.pl/proces-oceny-ryzyka-id64.html>, dostęp: marzec 2015.

²³³ Źródło: *National Emergency Risk Assessment Guidelines*.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

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

Tabela 14. Ewaluacja ryzyka – średni poziom wiarygodności²³⁴

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

Tabela 15. Ewaluacja ryzyka – niski poziom wiarygodności²³⁵

Poziom prawdopodobieństwa	Poziom konsekwencji				
	nieznaczny	mały	średni	wysoki	katastrofalny
prawie pewne	tolerowane	tolerowane	nietolerowane	nietolerowane	nietolerowane
prawdopodobne	tolerowane	tolerowane	nietolerowane	nietolerowane	nietolerowane

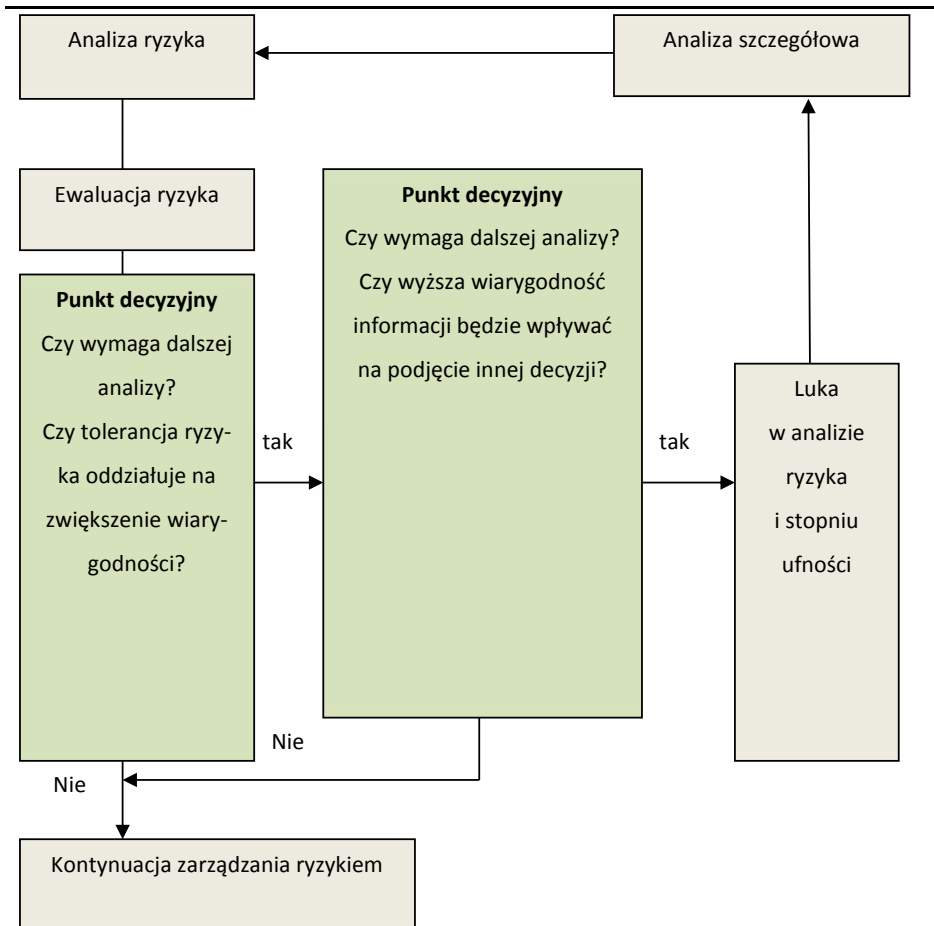
²³⁴ Tamże.

²³⁵ Tamże.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

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

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 13, 14, 15).



Rys. 23. Schemat działalności w „punkcie decyzyjnym”²³⁶

²³⁶ Źródło: *National Emergency Risk Assessment Guidelines*.

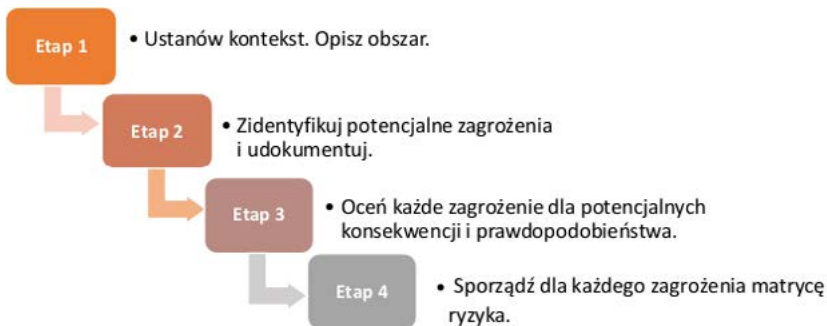
2. ZARZĄDZANIE RYZYKIEM W IRLANDII

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*²³⁷. 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. 24. Schemat procesu oceny ryzyka²³⁸

²³⁷ 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.

²³⁸ Źródło: opracowanie własne na podstawie *A Framework for Major Emergency Management*, s. 21.

Przedstawiony powyżej schemat procesu oceny ryzyka²³⁹ 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 ryzyka²⁴⁰, w etapie trzecim – analiza ryzyka²⁴¹ oraz w etapie czwartym – ewaluacja ryzyka²⁴². 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 podatność²⁴³ i odporność²⁴⁴ 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.

²³⁹ Patrz: definicja na s. 29.

²⁴⁰ Patrz: definicja na s. 27.

²⁴¹ Patrz: definicja na s. 31.

²⁴² Patrz: definicja na s. 37.

²⁴³ Podatność – patrz: część II *Zarządzanie ryzykiem na szczeblu UE*, rozdział 5 *Zarządzanie ryzykiem nielegalnej imigracji – FRONTEx*, s. 115.

²⁴⁴ Odporność – termin stosowany do opisu nieodłącznej zdolności społeczności, służb i infrastruktury oparcia się konsekwencjom zdarzenia i przywrócenia stanu normalności. Źródło: *A Framework for Major Emergency Management*, s. 29. Por.: definicja, s. 39.

Drugi etap to identyfikacja zagrożeń²⁴⁵. 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:

1. naturalne,
2. w transporcie,
3. technologiczne,
4. cywilne²⁴⁶.

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 matrycy.

Rodzaj i charakter zjawiska może być rozpatrywany w trzech aspektach:

1. wpływu na życie, zdrowie i dobrobytu społeczności,
2. wpływu na gospodarkę w zakresie kosztów/zniszczeń infrastruktury, jak również kosztów odbudowy lub utraty produkcji gospodarczej,
3. społecznych/oddziaływania na środowisko.

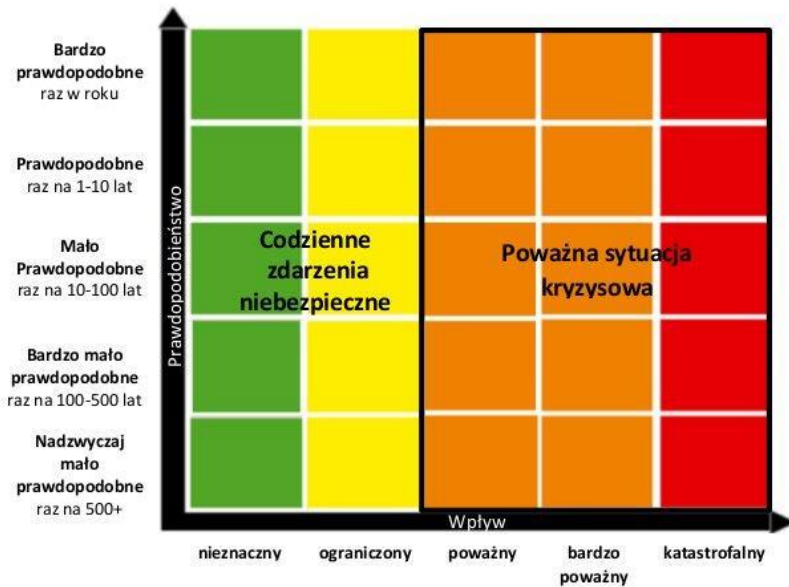
W uwagach metodyka wskazuje, jak ważne jest uwzględnienie możliwości eskalacji zdarzenia lub jego kombinacji z innymi zagrożeniami. Mimo tego zastrzeżenia i tak wszystkie wyniki analizy pozostają jedynie subiektywnymi ocenami

²⁴⁵ Por.: identyfikacja ryzyka wg PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

²⁴⁶ *A Framework for Major Emergency Management*, s. 23.

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 matrycy ryzyka (5 x 5), uwzględniającej prawdopodobieństwo wystąpienia zdarzenia (od bardzo rzadkiego – raz na 500 lat do bardzo prawdopodobnego – raz na rok) oraz jego rozmiaru/skutki (od znikomych do katastrofalnych). W normie ISO 31000 etapem porównania poziomów ryzyka²⁴⁷ w celu ułatwienia podjęcia decyzji jest ewaluacja ryzyka, jednak dokument ten nie narzuca zastosowania w tym celu matrycy ryzyka. Tzw. matryca irlandzka dodatkowo podzielona jest według dwóch stref (rys. 25) – pierwsza mieści zdarzenia umiarkowane, druga zaś dotyczy zdarzeń, które wymagają najwyższego stopnia gotowości.



Rys. 25. Strefy matrycy ryzyka²⁴⁸

²⁴⁷ Patrz: definicja na s. 39.

²⁴⁸ Źródło: opracowanie własne na podstawie *A Framework for Major Emergency Management*, s. 26.

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, 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.

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:

1. przyczynić się do stworzenia kompleksowej oceny ryzyka i wspólnego rozumienia wyzwań narodowych/społecznych,
2. wesprzeć w porównaniu różnych rodzajów zagrożeń z punktu widzenia narodowego/społecznego, pozwalając na ocenę ryzyk według wcześniej zdefiniowanych kryteriów prawdopodobieństwa i wpływu²⁴⁹,
3. stanowić podstawę do ustalenia priorytetów w zarządzaniu kryzysowym, które ułatwią koordynację międzysektorową i zapewnią równowagę środków na potrzeby zapobiegania i/lub ograniczania ryzyka²⁵⁰,
4. 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.

²⁴⁹ Wpływ – w odniesieniu do normy ISO 31000: konsekwencje.

²⁵⁰ Patrz: definicja na s. 157.

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 16. Klasyfikacja prawdopodobieństwa²⁵¹

Lp.	Klasyfikacja	Prawdopodobieństwo
1.	skrajnie nieprawdopodobne	może nastąpić tylko w wyjątkowych okolicznościach, raz na 500 lub więcej lat

²⁵¹ Źródło: opracowanie własne na podstawie *A National Risk Assessment for Ireland*, Office of Emergency Planning, grudzień 2012, s. 15.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

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
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

Tabela 17. Klasyfikacja wpływu²⁵²

Lp.	Klasyfikacja	Wpływ	Opis
1.	bardzo mały wpływ	życie, zdrowie, opieka środowisko	ograniczona liczba osób dotkniętych; 0-4 ofiary śmiertelne i ograniczona liczba drobnych urazów wymagających leczenia lub pierwszej pomocy nieznaczne, miejscowe zanieczyszczenia

²⁵² Źródło: opracowanie własne na podstawie *A National Risk Assessment for Ireland*, Office of Emergency Planning, December 2012, s. 16-17.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

		infrastruktura społeczeństwo	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
3.	umiarkowany wpływ	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	20 do 50 wypadków śmiertelnych, do 100 poważnych obrażeń, do 16 000 ewakuowanych

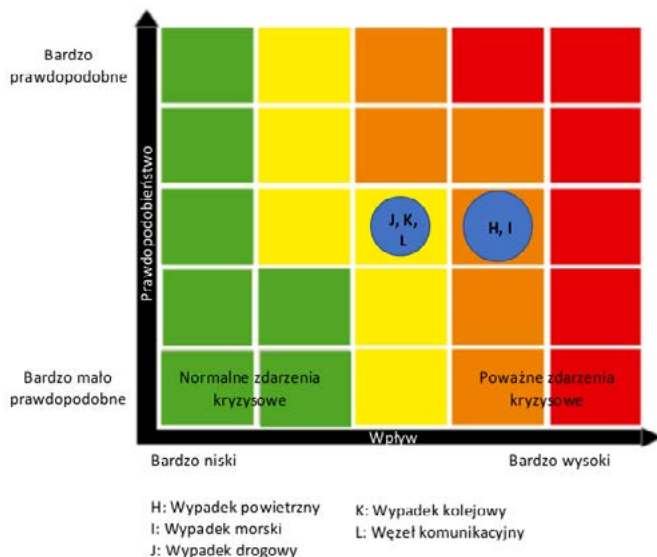
CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

		<p style="text-align: center;">środowisko</p> <p style="text-align: center;">infrastruktura</p> <p style="text-align: center;">społeczny</p>	<p style="text-align: center;">duże zanieczyszczenia, w długim okresie</p> <p style="text-align: center;">80-200 mln EUR</p> <p style="text-align: center;">społeczność działa słabo, minimalne usługi zapewnione</p>
5.	<p style="text-align: center;">bardzo duży</p> <p style="text-align: center;">wpływ</p>	<p style="text-align: center;">życie, zdrowie, opieka</p> <p style="text-align: center;">środowisko</p> <p style="text-align: center;">infrastruktura</p> <p style="text-align: center;">społeczny</p>	<p style="text-align: center;">duża liczba osób miała w obszarze zagrożonym - znaczna liczba zgonów (> 50), znaczne obrażenia, ponad 16 000 ewakuowanych</p> <p style="text-align: center;">bardzo duże zanieczyszczenia, rozległe, długotrwałe skutki</p> <p style="text-align: center;">powyżej 200 mln EUR</p> <p style="text-align: center;">poważne uszkodzenia infrastruktury powodujące znaczne zakłócenia lub utratę, kluczowych usług przez dłuższy okres; społeczność nie może funkcjonować bez znaczącego wsparcia</p>

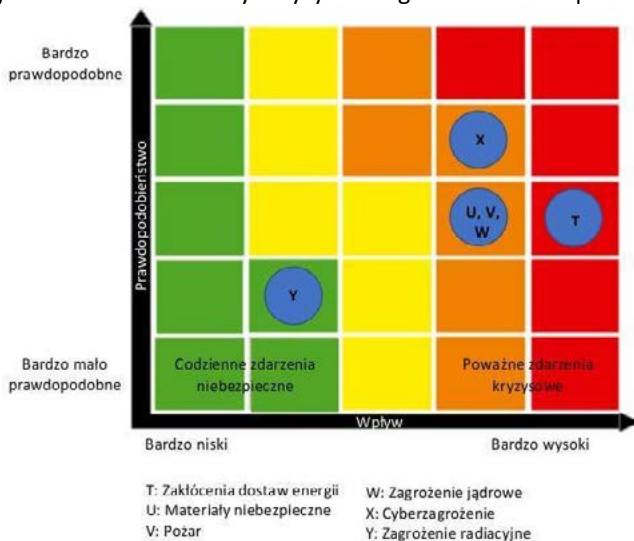
Kryteria ryzyka²⁵³ (mniej lub bardziej szczegółowe) nie są narzucone przez normę ISO, zaleca ona jedynie ich adekwatny dobór, według potrzeb. W metodyce irlandzkiej zarówno wpływ, jak i prawdopodobieństwo sklasyfikowano w sposób jakościowy oraz ilościowy, stosując wystarczająco precyzyjny opis.

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 zagrożeń od regionalnych grup sterujących w połączeniu z danymi zespołu eksperckiego ze szczebla centralnego przynosi równowagę

²⁵³ Patrz: definicja na s. 40.



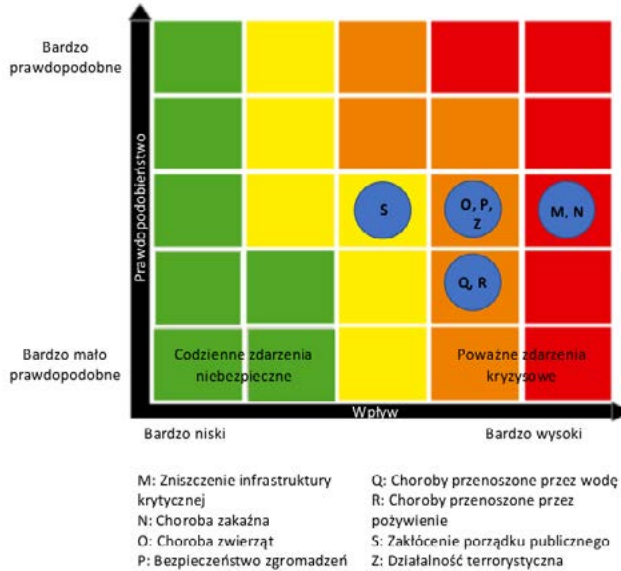
Rys. 27. Narodowa matryca ryzyka – zagrożenia w transporcie²⁵⁶



Rys. 28. Narodowa matryca ryzyka – zagrożenia technologiczne²⁵⁷

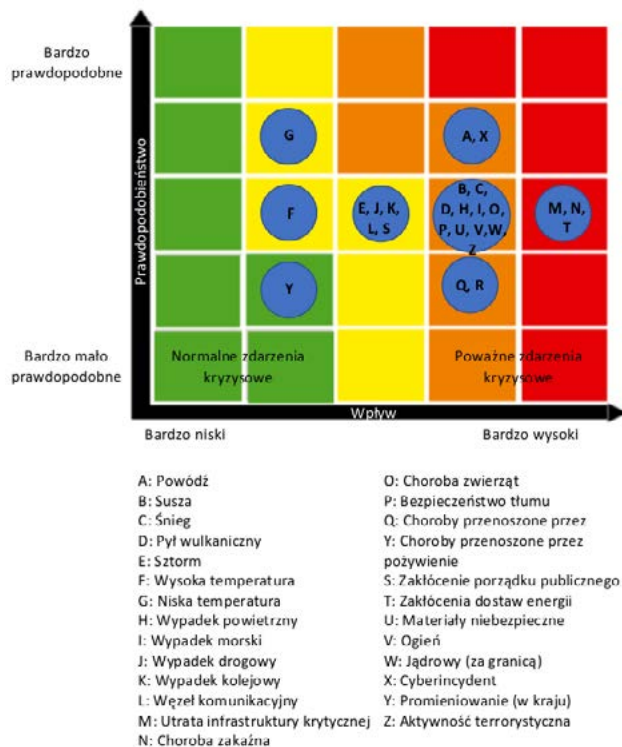
²⁵⁶ Źródło: opracowanie własne na podstawie *A National Risk Assessment for Ireland*, Office of Emergency Planning, grudzień 2012, s. 22.

²⁵⁷ Źródło: opracowanie własne na podstawie *A National Risk Assessment for Ireland*, Office of Emergency Planning, grudzień 2012, s. 24.



Rys. 29. Narodowa matryca ryzyka – zagrożenia cywilne²⁵⁸

²⁵⁸ Źródło: opracowanie własne na podstawie *A National Risk Assessment for Ireland*, Office of Emergency Planning, grudzień 2012, s. 28.



Rys. 30. Narodowa matryca ryzyka – wszystkie zagrożenia²⁵⁹

Aktualna ocena

Dane z czterech pojedynczych matryc ryzyka zagrożeń zostały skonsolidowane w narodowej matrycy ryzyka (rys. 30). 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.

²⁵⁹ Źródło: opracowanie własne na podstawie *A National Risk Assessment for Ireland*, Office of Emergency Planning, grudzień 2012 r., s. 32.

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 ryzyka²⁶⁰, 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 wpływ²⁶¹. Prawdopodobieństwo odnosi się do niebezpiecznych zdarzeń o pewnym natężeniu²⁶², wpływ tyczy się zaś różnorodnych zniszczeń obiektów chronionych, które są spodziewane, jeśli ryzykowne zdarzenie wystąpi. Po drugie, proces analizy ryzyka²⁶³ powinien wykorzystywać najlepsze dane i informacje, w tym badania naukowe, dane statystyczne oraz szacunki eksperckie zapewniające możliwie najwyższy poziom wiarygodności. Po trzecie, wszystkie kroki procesu analizy ryzyka powinny być wnikliwie dokumentowane w celu zagwarantowania uzyskania jej rezultatów. Po czwarte, za dopuszczalne uważa się ogranicze-

²⁶⁰ Patrz: definicja na s. 29.

²⁶¹ Wpływ – w odniesieniu do normy ISO 31000: konsekwencje.

²⁶² Natężenie – stopień nasilenia czegoś, intensywność. Źródło: <http://sjp.pl/nat%C4%99%C5%BCenie>, dostęp: marzec 2015.

²⁶³ Patrz: definicja na s. 31.

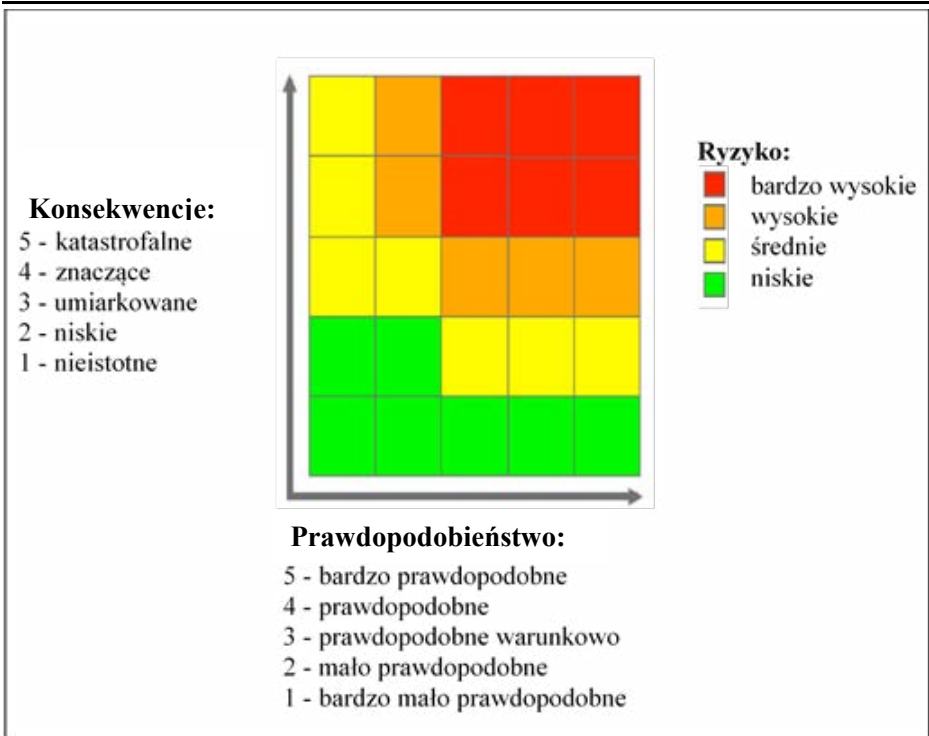
nie analizy do tych ryzyk, które konfrontowałyby szczebel administracyjny z tak znacznymi wyzwaniem, w których poradzenie sobie ze zniszczeniami lub podjęcie odpowiednich środków zapobiegawczych wymagałoby wsparcia poziomu centralnego. Po piąte, analiza ryzyka powinna rozważać także zagrożenia, które 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, ewaluację²⁶⁴, postępowanie z ryzykiem²⁶⁵ oraz monitorowanie²⁶⁶ ryzyk.

Celem analizy ryzyka w obszarze ochrony ludności jest porównanie różnych rodzajów zagrożeń za pomocą matrycy ryzyka (rys. 31) 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.

²⁶⁴ Patrz: definicja na s. 37.

²⁶⁵ Patrz: definicja na s. 28.

²⁶⁶ Patrz: definicja na s. 37.



Rys. 31. Matryca ryzyka wykorzystywana przez niemieckie Federalne Biuro Ochrony Ludności²⁶⁷

Budowa scenariusza opiera się na odpowiedziach na zdefiniowane wcześniej pytania dotyczące przedstawionych poniżej parametrów, które stanowią pewien substytut dla podprocesu identyfikacji ryzyka²⁶⁸ w normie ISO 31000.

²⁶⁷ Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 22.

²⁶⁸ Patrz: definicja na s. 27.

Tabela 18. Parametry i centralne pytania do opisu scenariusza²⁶⁹

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 przyście? Czy władze publiczne są w stanie się przygotować na jego przyście?
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?

Tabela 18 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 19).

²⁶⁹ Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 26.

Tabela 19. Przykładowy model klasyfikacji prawdopodobieństwa²⁷⁰

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

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 20. Przykładowe parametry charakteryzujące miejsce²⁷¹

Klasa	Informacja	Możliwe źródła informacji
Ludność	liczba mieszkańców	biura statystyczne
	gęstość zaludnienia	główny urząd statystyczny
	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

²⁷⁰ Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 27.

²⁷¹ Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 30-31.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

Gospodarka	wydajność gospodarki	władza/administracja właściwa ds. ekonomicznych biura statystyczne
	wpływy podatkowe	
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

Kolejnym krokiem jest opisanie atrybutów zdarzenia (według określonych parametrów – patrz tabela 21).

Tabela 21. Przykładowe parametry charakteryzujące zdarzenie²⁷²

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

²⁷² Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 30-31.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

	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
	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

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

	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
	konsekwencje psychologiczne	stopień utraty zaufania publicznego do organów władzy (np. rządu lub administracji)	zasięg

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

	zniszczenia dóbr kultury	zniszczenia dóbr kultury w wyniku incydentu (np. będących pod ochroną konwencji haskiej)	liczba uszkodzonych obiektów i stopień tych uszkodzeń
--	--------------------------	--	---

Kolejnym krokiem jest przypisanie właściwych poziomów konsekwencji, zgodnie ze wskazaną jednostką miary. Tabela 22 wskazuje przykładowy model bez wskazania wartości (symbol „_” pokazuje miejsce wskazania wartości).

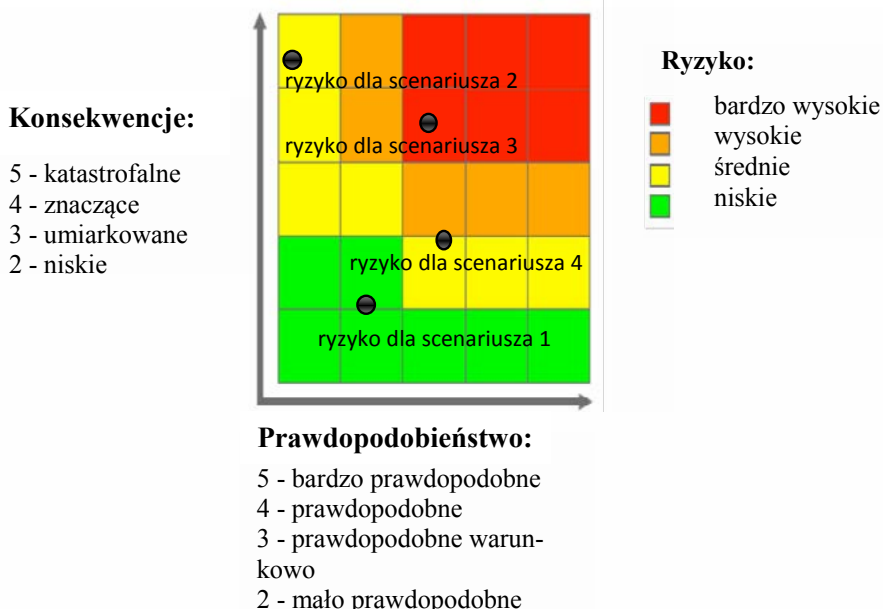
Tabela 22. Model klasyfikacji kategorii Ludność²⁷³

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

²⁷³ Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 33.

1	nieistotne	= lub < _	= lub < _	= lub < _	= lub < _ osób przez = lub < _ godz./dni
----------	------------	-----------	-----------	-----------	--

Po określeniu (zgodnie z powyżej wskazanymi zasadami) wartości wpływu i prawdopodobieństwa wyniki analizy ryzyka są wizualizowane na macierzach ryzyka, w których ryzyka dla poszczególnych scenariuszy, warunkowane przez czynniki prawdopodobieństwa i wpływu, ujęte zostały jako punkty.



Rys. 32. Przykładowe zestawienie porównawcze różnorodnych zagrożeń w macierzy²⁷⁴

Wizualizacja ryzyk 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*

²⁷⁴ Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 41.

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 osiągnięty²⁷⁵. Ujęcie analizy ryzyka jako centralnego elementu zarządzania ryzykiem prezentuje rys. 33.



Rys. 33. Analiza ryzyka jako centralny element zarządzania ryzykiem (na podstawie ISO 31000)²⁷⁶

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*.

²⁷⁵ *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 45.

²⁷⁶ Źródło: opracowanie własne na podstawie *Method of Risk Analysis for Civil Protection*, Federal Office of Civil Protection and Disaster Assistance, 2011, s. 45.

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 ryzyka²⁷⁷), 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 wystandardyzowanych 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.

²⁷⁷ Por. definicja na s. 157.

4. ZARZĄDZANIE RYZYKIEM W SZWECJI

W niniejszym rozdziale omówione zostaną dwa istotne dokumenty, które odnoszą się do zarządzania ryzykiem w Szwecji – szczególnie w kontekście zarządzania kryzysowego, a w tym planowania cywilnego. Pierwszym jest opublikowany w 2012 r. *Przewodnik po analizie ryzyka i podatności*²⁷⁸, a kolejnym *Szwedzka narodowa ocena ryzyka*²⁷⁹, z tego samego roku.

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:

1. identyfikacja 27 zdarzeń narodowych – na podstawie analiz ryzyka i podatności przeprowadzonych w latach 2010-2011 przez odpowiednie organy,
2. 11 scenariuszy opartych na tych zdarzeniach,
3. analiza oraz ocena 7 zdarzeń,
4. opracowanie procesu i metodologii przeprowadzenia oceny,
5. 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^{280,281} w zarządzaniu przygotowaniem na stan kryzysowy. Przed-

²⁷⁸ *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012.

²⁷⁹ *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012.

²⁸⁰ Por. definicja na s. 130.

²⁸¹ Autorzy przewodnika stosują i konsekwentnie podkreślają w dokumencie istotne dla nich elementy: analizę ryzyka (jako najważniejszy podproces oceny ryzyka) i analizę podatności (jako

stawia także cel przewodnika i docelowe grupy jego odbiorców. Główne cele bezpieczeństwa społeczeństwa, które zgodnie z dokumentem należy chronić, to:

1. życie i zdrowie populacji,
2. funkcjonowanie społeczne,
3. 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 osiągane poprzez przygotowanie społeczeństwa na wystąpienie sytuacji kryzysowych to:

1. redukcja ryzyka²⁸² oraz skutków poważnych zakłóceń, kryzysów i wypadków,
2. zapewnienie zdrowia i bezpieczeństwa dzieci, kobiet i mężczyzn,
3. 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.

najważniejszy podproces oceny podatności). W dalszej części rozdziału dokonano próby ich charakterystyki.

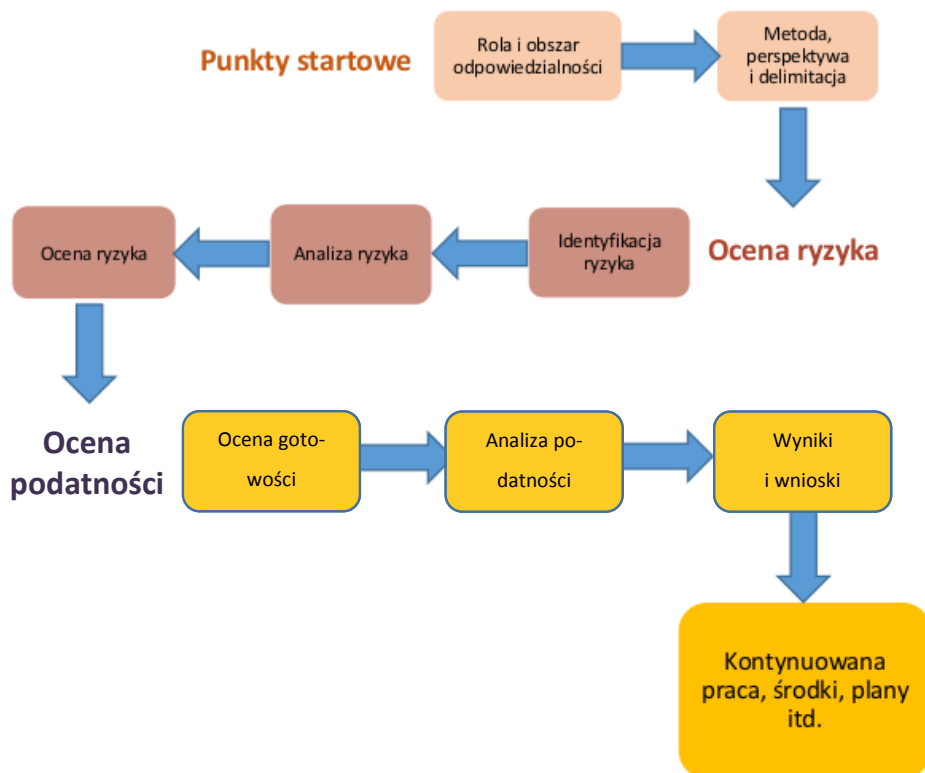
²⁸² Por. definicja na s. 157.

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),*
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.



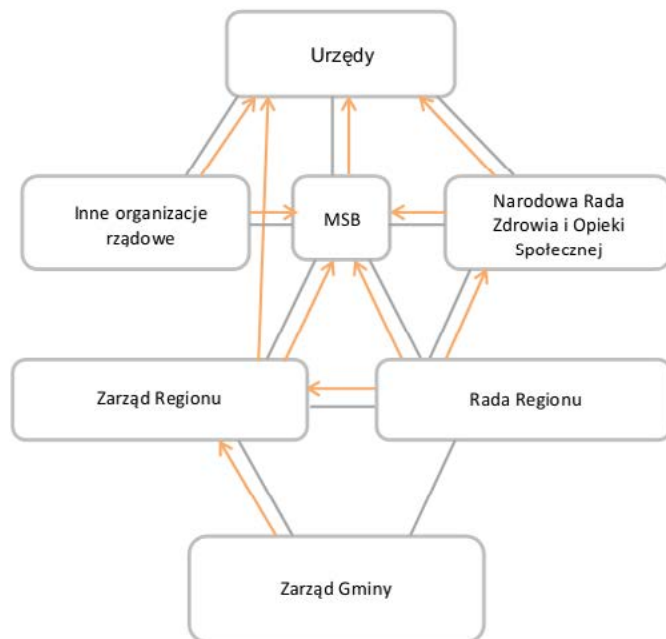
Rys. 34. Proces zarządzania ryzykiem²⁸³

Schemat Szwedzkiej Agencji ds. Cywilnych Sytuacji Kryzysowych (rys. 34) 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 ryzyka²⁸⁴ z kolei przeniesiono, zgodnie z wytycznymi normy. Novum 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

²⁸³ Źródło: opracowanie własne na podstawie *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 14.

²⁸⁴ Patrz: definicja na s. 29.

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 ryzykiem²⁸⁵, w którym wiodącą rolę przejmują decydenci właściwi dla danego obszaru administracyjnego.



- Informacja

- Sprawozdawczość

Rys. 35. Graficzny opis obiegu informacji na temat analizy ryzyka²⁸⁶

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 –

²⁸⁵ Patrz: definicja na s. 28.

²⁸⁶ Źródło: opracowanie własne na podstawie *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 17.

przede wszystkim nadrzędnego, jakim jest realizacja celów organizacji (w tym przypadku państwa na rzecz bezpieczeństwa społeczeństwa) oraz m.in.:

1. zapewnienie społeczeństwu informacyjnej bazy dotyczącej zagrożeń społecznych,
2. zapewnienie podstaw do podjęcia decyzji decydujących oraz osobom odpowiedzialnym za działania operacyjne,
3. zapewnienie podstawowych informacji dla społecznego planowania,
4. 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, zarządów regionów, gmin i rad regionów). Przewodnik omawia rolę 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:

1. infrastruktura techniczna,
2. transport,
3. substancje niebezpieczne,
4. bezpieczeństwo ekonomiczne,
5. geograficzny obszar odpowiedzialności,
6. 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:

1. sytuacje, które pojawiają się szybko, niespodziewanie i bez ostrzeżenia, lub czy istnieje zagrożenie bądź ryzyko, że tego typu sytuacja wyniknie,
2. sytuacje, które wymagają natychmiastowych decyzji i współpracy z innymi podmiotami,
3. potrzebę utrzymania najważniejszych funkcji społecznych,
4. 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 regionu²⁸⁷ 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 scenariuszami²⁸⁸, 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,

²⁸⁷ Odpowiednik zarządu województwa w Polsce.

²⁸⁸ Scenariusze w znaczeniu analogicznym do scenariuszy niemieckich, patrz: s. 196.

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:

1. służba zdrowia,
2. kontrola zachorowań (80% wydatków),
3. usługi stomatologiczne,
4. edukacja pielęgniarek,
5. kultura,
6. wsparcie przedsiębiorców z terenu regionu,
7. odpowiedzialność za rozwój regionalny.

Rada może sama wypełniać zadania lub je zlecać.

Analiza ryzyka zawiera m.in. odpowiedzi na trzy najważniejsze pytania:

1. co może się stać?
2. dlaczego może to nastąpić i jak często?
3. 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:

1. role i obszary odpowiedzialności,
2. metody i narzędzia pracy,
3. zakres prowadzonej oceny ryzyka i podatności,
4. 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 ryzyka²⁸⁹

Należy ustalić, co może się wydarzyć, określić źródła ryzyka²⁹⁰, 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, 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.

²⁸⁹ Patrz: definicja na s. 27.

²⁹⁰ Patrz: definicja na s. 45.

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 ryzyka²⁹¹ i podjęcie decyzji co do postępowania z nim.

Ocena prawdopodobieństwa

Na potrzeby oceny prawdopodobieństwa również stosuje się szereg metod, które zawierają różne przyjętą skalę dla wystąpienia danego zagrożenia. Wykorzystywane metody pogrupowane są w cztery grupy:

1. opis jakościowy prawdopodobieństwa wystąpienia zdarzenia,
2. opis jakościowy za pomocą skali,
3. opis ilościowy za pomocą skali i podziałów,
4. 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:

1. opis jakościowy skutków wystąpienia zdarzenia,
2. opis jakościowy z pomocą skali,
3. opis ilościowy z pomocą skali i podziałów,
4. opis ilościowy.

²⁹¹ Patrz: definicja na s. 37.

Tabela 23. Opis jakościowy z pomocą skali²⁹²

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
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

Tabela 24. Wyniki ilościowej analizy ryzyka²⁹³

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

²⁹² *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 48.

²⁹³ *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 50.

Ocena ryzyka²⁹⁴

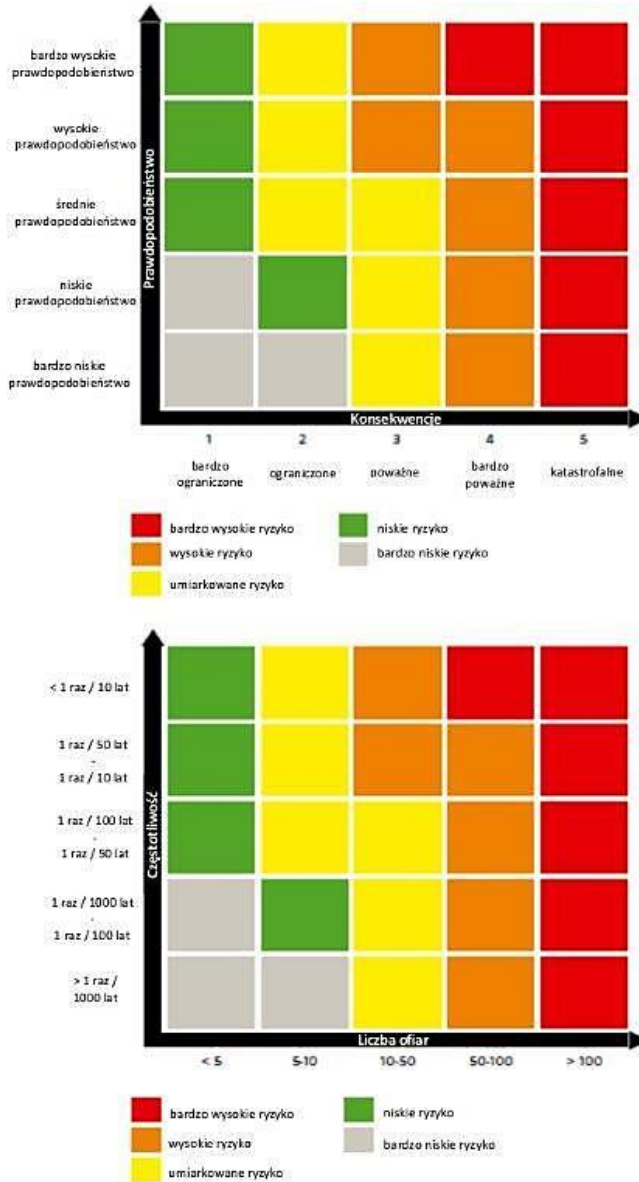
Ocena ryzyka oznacza analizę pozwalającą na określenie, czy poziom danego ryzyka²⁹⁵ jest akceptowalny, czy nie. Stanowi właściwą podstawę dla planowania oraz wdrażania środków ograniczających ryzyko. Ocena powinna zawierać analizę zalet i wad proponowanych rozwiązań i zostać uzupełniona o niezbędne wnioski: czy dane rozwiązanie powinno zostać zastosowane, czy też nie, a także jak znaczący 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.

²⁹⁴ W dokumencie zastosowano pojęcie oceny ryzyka, jednak etap ten odpowiada ewaluacji ryzyka, zgodnie z definicją i opisem w normie ISO 31000.

²⁹⁵ Patrz: definicja na s. 39.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH



Rys. 36. Przykładowe matryce ryzyka²⁹⁶

²⁹⁶ Źródło: opracowanie własne na podstawie *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 52.

Metodyka stosowana przez Szwedzką Agencję ds. Cywilnych Sytuacji Kryzysowych bazuje na wielowymiarowej analizie aktywności (MVA)²⁹⁷. 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 oprogramowaniem²⁹⁸. Praca jest podzielona i realizowana podczas trzech seminariów, poświęconych: identyfikacji, analizie i feedbackowi.



Rys. 37. Metoda MVA²⁹⁹

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 niekorzystne³⁰⁰ – 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.

²⁹⁷ Źródło: opracowanie własne na podstawie *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 62-63.

²⁹⁸ Por.: część I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 2 *Metody wykorzystywane w ocenie ryzyka*, podrozdział 2.13 *Analiza scenariuszowa*.

²⁹⁹ *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 62.

³⁰⁰ Patrz: definicja na s. 67.

Druga faza koncentruje się na analizie, podczas której szczegółowo przedstawia się podatność na zagrożenia oraz odporność³⁰¹ 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, 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)³⁰². Metoda ta kładzie duży nacisk na proces zarządzania ryzykiem³⁰³. 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

³⁰¹ Patrz: definicja na s. 39.

³⁰² *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 63-65.

³⁰³ Trzon tej metody zakorzeniony jest w procesie zarządzania ryzykiem normy ISO 31000. Patrz szerzej: *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012 s. 190-203.

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 ryzyka³⁰⁴ podmiotu (systemu lub obiektu), wraz ze wskazaniem istniejących słabych punktów (podatności). Aby wizualnie przedstawić wyniki, używa się trzech kolorów (dokument nie określa koloru) odpowiadających trzem poziomom oceny:

1. bardzo dobrej,
2. dobrej,
3. niewystarczającej.

³⁰⁴ Profil ryzyka – opis zestawu ryzyk. Źródło: ISO Guide 73:2009 *Risk Management – Vocabulary*, definicja 3.8.2.5.



Rys. 38. Metoda ROSA³⁰⁵

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 scenariuszowej³⁰⁶ i jest najbliższa metodzie wypracowanej przez stronę niemiecką³⁰⁷;
2. wstępna analiza ryzyka (ang. *Preliminary Risk Analysis* oraz *Broad Analysis*) – ogólna analiza jakościowa stosowana przy sporządzaniu map ryzyka, skoncentrowana na identyfikacji i scenariuszu ryzyka. Analiza ta jest

³⁰⁵ Źródło: opracowanie własne na podstawie *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 64.

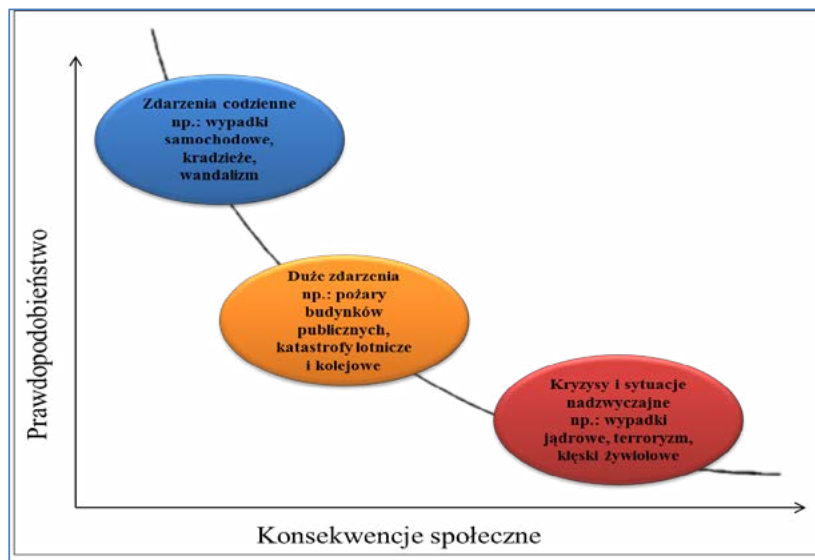
³⁰⁶ Patrz szerzej: *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 65-66.

³⁰⁷ Patrz: s. 197.

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 zidentyfikowanych zagrożeniach, ich możliwe przyczyny i konsekwencje, dokonać ewaluacji ryzyka oraz przedstawić ogólne rekomendacje działań redukujących konsekwencje³⁰⁸;

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. 39.



Rys. 39. Zależność pomiędzy skalą ryzyka a rodzajami zdarzeń³⁰⁹

³⁰⁸ Patrz szerzej: *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, s. 67-68.

³⁰⁹ Źródło: opracowanie własne na podstawie *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012, 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* 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 uwzględniać zagrożenia wszystkich z tych wartości.

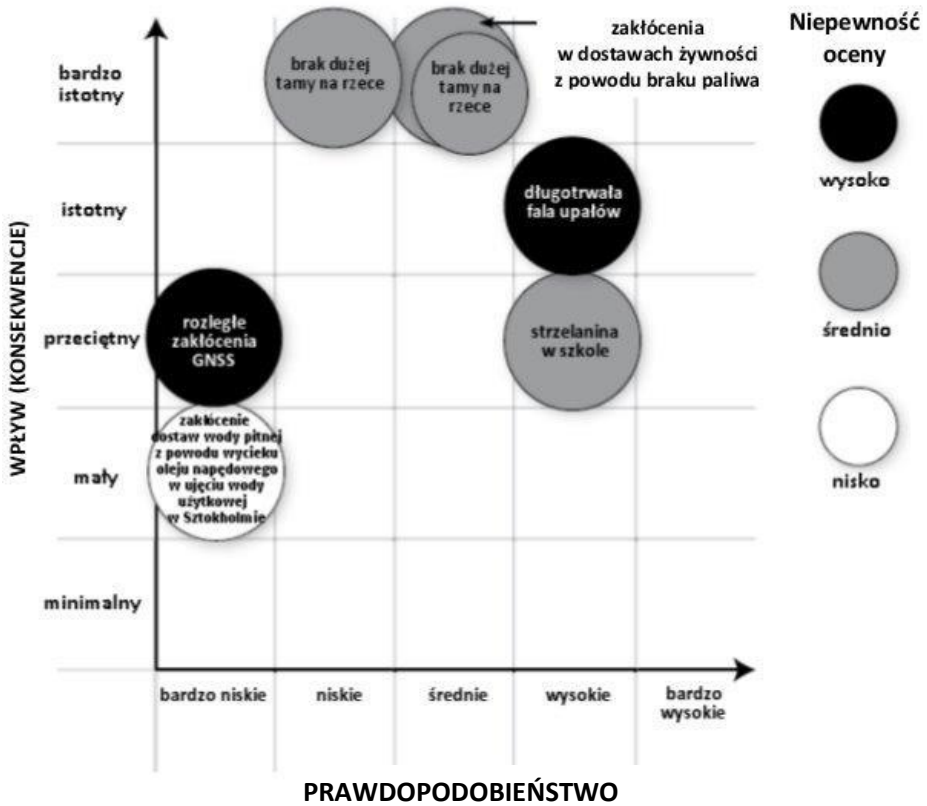
Są to tzw. czarne scenariusze, co oznacza, że zakładają zdarzenia, które mogą powodować poważne lub bardzo poważne skutki i są uważane za realne na podstawie wiedzy eksperckiej w dziedzinie, której scenariusz dotyczy. Scenariusze powstające w ramach *Szwedzkiej narodowej oceny ryzyka* są spójne z elementami 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 Europejskiej³¹⁰ (2010) 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, niepewności³¹¹ (prawdopodobieństwa i konsekwencji) dla każdego zdarzenia. Taka matryca nazywana jest matrycą 5 x 5, ponieważ składa się z pięciu kolumn i pięciu rzędów z 25 możliwymi kombinacjami oceny prawdopodobieństwa i wpływu.

³¹⁰ European Commission: *Commission Staff Working Paper: Risk Assessment and Mapping Guidelines for Disaster Management*, 2010, SEC(2010) 1626 wersja ostateczna (17899/10).

³¹¹ 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. 40. Matryca ryzyka analizowanych scenariuszy w Narodowej ocenie ryzyka 2012³¹²

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.

³¹² Źródło: opracowanie własne na podstawie *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012, s. 23.

Tabela 25. Skala prawdopodobieństwa³¹³

Skala jakościowa (matryca ryzyka)	Skala ilościowa oceny prawdopodobieństwa		
	dolna granica	środek przedziału	górną granicą
bardzo wysokie	≥ 0,2 w ujęciu rocznym (≥ 0,5 raz na 5 lat)	1 w ujęciu rocznym (raz do roku)	1 (raz do roku)
wysokie	≥ 0,02 w ujęciu rocznym (≥ raz na 50 lat)	0,1 w ujęciu rocznym (raz na 10 lat)	< 0,2 w ujęciu rocznym (< raz na 5 lat)
średnie	≥ 0,002 w ujęciu rocznym (≥ raz na 500 lat)	0,0001 w ujęciu rocznym (raz na 1000 lat)	< 0,02 w ujęciu rocznym (< raz na 50 lat)
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)

Tabela 26. Skala konsekwencji³¹⁴

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




³¹³ Źródło: opracowanie własne na podstawie *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012, s. 23.

³¹⁴ Źródło: opracowanie własne na podstawie *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012, s. 24.

minimalne	brak martwych lub ciężko rannych, kilka drobnych urazów	< SEK 20 mln	minimalny
-----------	---	--------------	-----------

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 27. Skala niepewności³¹⁵

Oznakowanie w matrycy 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. Eksperti 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

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

³¹⁵ Źródło: opracowanie własne na podstawie *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012, s. 24.

ofiara śmiertelna) oraz dwie strzelaniny w szkołach w Finlandii. Strzelaninę udaremnilo 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 po 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 zniżenie 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.

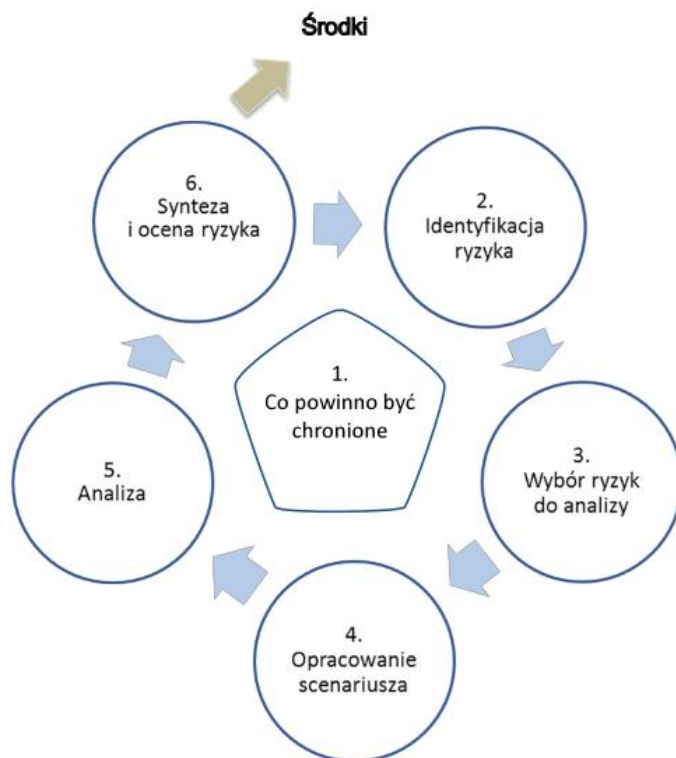
Ogólny proces i metodyka

Praca nad *Narodową oceną ryzyka* wyłoniła sześć kroków prowadzących do osiągnięcia założonego wyniku:

1. określenie, co powinno być chronione,
2. identyfikacja ryzyka (zdarzeń niekorzystnych),
3. wybór zdarzeń do analizy,
4. opracowanie scenariuszy dla wybranych zdarzeń,
5. analiza scenariuszy: konsekwencji, prawdopodobieństwa i niepewności oceny,
6. 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 Europejskiej³¹⁶. Stąd wśród kroków *Narodowej oceny ryzyka* nie zabrakło głównych podprocesów stanowiących komponent procesu zarządzania ryzykiem, zgodnie ze wspomnianą normą.

³¹⁶ European Commission, Commission Staff Working Paper: *Risk Assessment and Mapping Guidelines for Disaster Management*, 2010, SEC(2010) 1626 wersja ostateczna (17899/10).



Rys. 41. Sześć kroków oceny ryzyka³¹⁷

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.

³¹⁷ Źródło: opracowanie własne na podstawie *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012, s. 27.

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 rządów regionów. Na warsztatach dokonano przeglądu katalogów zdarzeń³¹⁸ 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 połączenia³¹⁹ 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:

1. poważne zakłócenia nawigacji satelitarnej,

³¹⁸ Katalog zdarzeń – uporządkowany wykaz lub spis zdarzeń. Źródło: opracowanie autorskie.

³¹⁹ Np. połączony scenariusz aktu terrorystycznego z rozproszeniem bomby chemicznej.

2. ostrzał z broni na terenie szkoły,
3. zakłócenia dostaw wody pitnej w wyniku zanieczyszczenia paliwem źródła wody w Sztokholmie,
4. zakłócenia dostaw żywności w wyniku niedoboru paliwa,
5. duży pożar na statku rejsowym,
6. awaria tamy na rzece,
7. długa fala upałów,
8. pandemia spowodowana wirusem grypy A/H5N1 (wirus ptasiej grypy),
9. katastrofa nuklearna z emisją radioaktywną,
10. atak terrorystyczny w Sztokholmie (bomby w Sergels i na dworcu centralnym),
11. 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 28. Wskaźniki dla wartości narodowych podlegających ochronie³²⁰

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
	brak kontroli nad instytucjami publicznymi
suwerenność narodowa	wpływ na międzynarodową reputację Szwecji
	brak kontroli nad terytorium kraju

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.

³²⁰ Źródło: opracowanie własne na podstawie *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, 2012, s. 31.

5. ZARZĄDZANIE RYZYKIEM W WIELKIEJ BRYTANII

W rozdziale tym analizie poddano dokument *National Risk Register* (*Krajowy rejestr ryzyka*³²¹ – 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 ryzyka³²², 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 ryzyka³²³. Istnieją trzy etapy analizy. Pierwszym jest identyfikacja ryzyka³²⁴ poprzez konsultacje eksperckie, co daje obraz potencjalnych zdarzeń, wypadków, zagro-

³²¹ 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.

³²² 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.

³²³ Patrz: definicja na s. 222.

³²⁴ Patrz: definicja na s. 27.

żeń 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 nagłych³²⁵. W związku z tym eksperci uważają, że mogą wziąć je pod uwagę w przyszłości i że powinny zostać poddane przeglądowi³²⁶.

Ustanawiając kontekst ryzyka³²⁷, 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:

1. liczbę ofiar śmiertelnych,
2. zranienia i urazy,
3. zakłócenia społeczne, biorąc pod uwagę brak uzyskania dostępu do opieki zdrowotnej lub edukacji, przerwy w świadczeniu podstawowych

³²⁵ 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.

³²⁶ *The National Risk Register of Civil Emergencies (NRR)*, Cabinet Office, 2010 edition, s. 53.

Przegląd – patrz: definicja na s. 37.

³²⁷ Patrz: definicja na s. 31.

usług (dostęp do wody i prądu), a także konieczność ewakuacji osób z danego obszaru,

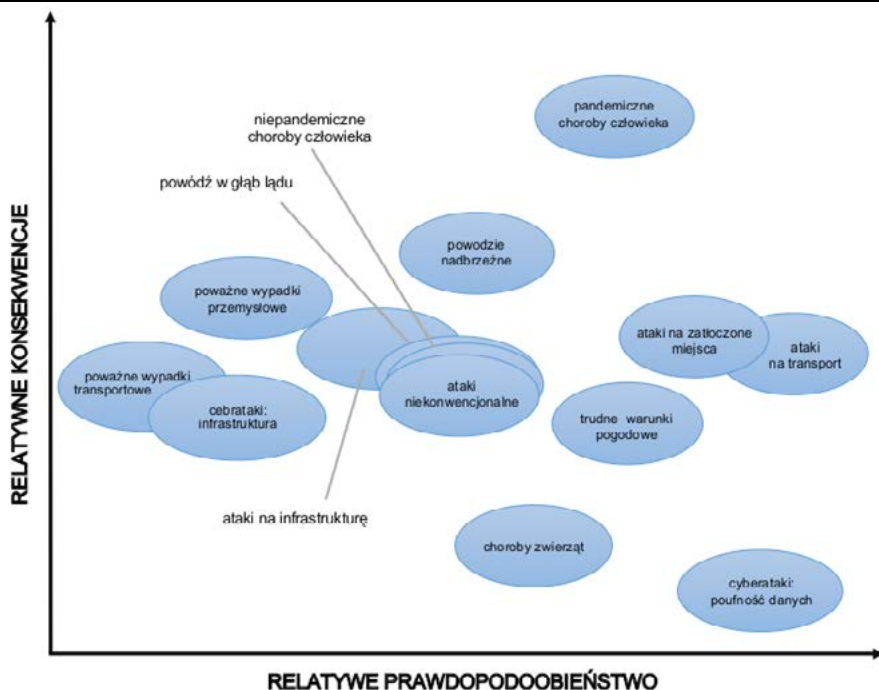
4. straty ekonomiczne.

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 określa się, biorąc także pod uwagę różne rodzaje ryzyka. Przyjmuje się skalę od 1 do 5. Kombinacja prawdopodobieństwa i konsekwencji wyznacza poziom ryzyka³²⁸, 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. 42 przedstawia relatywne³²⁹ 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.

³²⁸ Poziom ryzyka – patrz: definicja na s. 39.

³²⁹ Dotyczy prognozy prawdopodobieństwa i konsekwencji na najbliższe 5 lat.



Rys. 42. Zagrożenia umieszczone na wykresie w kontekście prawdopodobieństwa i konsekwencji³³⁰

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 kategorie³³¹ (np. ataki na zatłoczone miejsca). Kategorie oraz ryzyka te przedstawiają matryce na rys. 43. Ponadto można zauważyć, że obie skale nie są bezpośrednio porównywalne ze sobą, na przykład „wysokie” zagrożenia niekoniecznie mają „większą niż 50 proc.” szansę wystąpienia.

Zagrożenia w górnej prawej ćwiartce mają ten sam priorytet wystąpienia.

³³⁰ Źródło: opracowanie własne na podstawie *The National Risk Register of Civil Emergencies (NRR)*, Cabinet Office, 2010, s. 5.

³³¹ Kategoria – klasa obiektów mających określone cechy i powiązanych wzajemnymi relacjami. Źródło: <http://s.jp.pl/kategoria>, dostęp: marzec 2015.

Prawa strona matrycy przedstawia prawdopodobieństwo wystąpienia ataku terrorystycznego, lewa zaś – innych zagrożeń możliwych. Dla obu prawdopodobieństwo zakładane jest w perspektywie najbliższych 5 lat.

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.

Całociowa ocena konsekwencji	5		katastrofalne ataki terrorystyczne			
	4					
	3		cyberataki: infrastruktura	ataki na infrastrukturę cyberataki na mniejszą skalę	ataki na zatłoczone miejsca	ataki na systemy transportu
	2					
	1					cyberataki: poufność danych
		niskie	średnio niskie	średnie	średnio wysokie	wysokie

Względne prawdopodobieństwo wystąpienia w kolejnych 5 latach

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

Całociowa ocena konsekwencji	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	
		od 1/20000 do 1/2000	od 1/2000 do 1/200	od 1/200 do 1/20	od 1/20 do 1/2	więcej niż 1/2

Względne prawdopodobieństwo wystąpienia w kolejnych 5 latach

Rys. 43. Podstawowe zagrożenia, na jakie narażona jest Wielka Brytania³³²

Wszystkie zagrożenia mające wpływ na bezpieczeństwo narodowe, łącznie z zagrożeniem katastrofami naturalnymi³³³ oraz atakami terrorystycznymi,

³³² Źródło: opracowanie własne na podstawie *The National Risk Register of Civil Emergencies (NRR)*, Cabinet Office, 2013, s. 10.

obejmuje dokument niejawną *National Security Risk Assessment* (NSRA). Wielka Brytania uważana jest na świecie za jednego z pionierów zarządzania ryzykiem w sytuacjach nadzwyczajnych³³⁴.

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 szkodom³³⁵ 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.

³³³ 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.).

³³⁴ Sytuacja nadzwyczajna (ang. *emergency*) – nagłe, 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*.

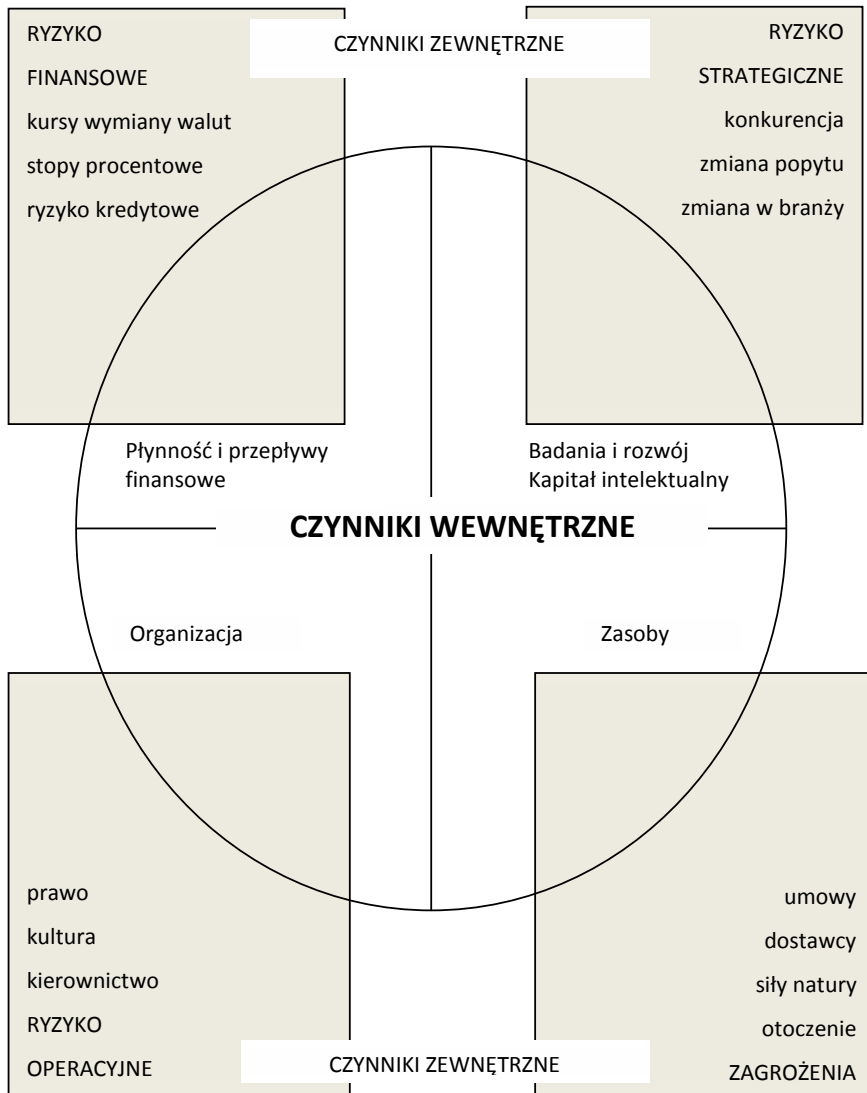
³³⁵ Szkoła (ang. *harm*) – uraz fizyczny lub uszczerbek na zdrowiu, uszkodzenie mienia lub degradacja środowiska,

http://www.ciop.pl/CIOPPortalWAR/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.

Rys. 44 prezentuje przykładowy zbiór czynników ryzyka³³⁶. 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 ryzyka te zestawiono w postaci czynników (strategiczne, finansowe, operacyjne, zagrożenia³³⁷ itd.).

³³⁶ 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.

³³⁷ 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. 44. Przykładowy rozkład czynników ryzyka³³⁸

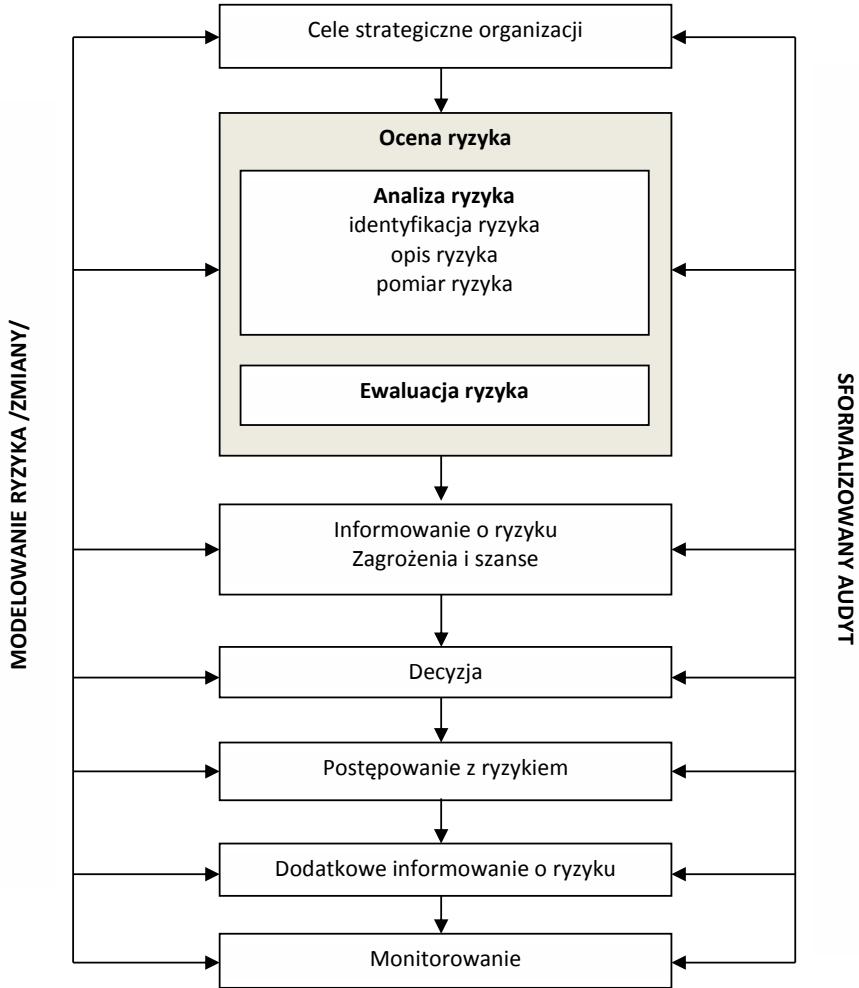
³³⁸ Źródło: opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, s. 4.

Zarządzanie ryzykiem stanowi o wartości organizacji systemu, przyczyniając się do realizacji celów organizacji poprzez³³⁹:

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,
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.

³³⁹ *Standard zarządzania ryzykiem FERMA 2003*, s. 5.



Rys. 45. Proces zarządzania ryzykiem

Ocena ryzyka³⁴⁰ jest procesem złożonym. Norma ISO Guide 73:2009 definiuje ocenę ryzyka jako całościowy proces złożony z identyfikacji, analizy ryzyka³⁴¹

³⁴⁰ Patrz: definicja na s. 29.

³⁴¹ Patrz: definicja na s. 31.

oraz ewaluacji ryzyka³⁴². 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 metod czy międzynarodowych norm. Norma ISO 31000 rozumie ją wprost, jako proces poszukiwania, rozpoznawania i opisywania ryzyka. Proces ten wymaga szczegółowej 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 kryteriów³⁴³, np.³⁴⁴:

1. Kwestie strategiczne – związane z długofalowymi celami strategicznymi³⁴⁵ 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.

³⁴² Patrz: definicja na s. 37.

³⁴³ Patrz: definicja na s. 40.

³⁴⁴ *Standard zarządzania ryzykiem FERMA 2003*, s. 6.

³⁴⁵ Patrz: definicja na s. 26.

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.

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 ryzyka³⁴⁶ 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), 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 operacyjne³⁴⁷. W obszarze bezpieczeństwa nic się nie zmieni. Zarządzanie ryzykiem to działalność, która rozpoczyna się na etapie projekcyjnym już w fazie koncepcyjnej i jest prowadzona przez cały okres realizacji.

Tabela 29. Opis ryzyka (przykład)³⁴⁸

Parametr ryzyka	Opis ryzyka
Nazwa ryzyka	
Zakres ryzyka	rodzaj, skala, zdarzenia pochodne
Charakter ryzyka	z czym jest związane: z wiedzą, prawem, umiejętnościami

³⁴⁶ Patrz: definicja na s. 222.

³⁴⁷ *Standard zarządzania ryzykiem FERMA 2003*, s. 5.

³⁴⁸ Źródło: opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, s. 7.

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

Pomiar ryzyka³⁴⁹ 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 30). Prawdopodobieństwo także można przyjąć jako duże, średnie lub małe. Podczas rozważania zarówno szans, jak i zagrożeń należy je definiować osobno (tabela 31). Podany sposób klasyfikacji (ujęty w metodyce) jest przykładowy, dlatego w przypadku różnych organizacji właściwe mogą się okazać odmienne schematy klasyfikowania skutków i prawdopodobieństwa ryzyka (w dalszej części tego materiału). Przy zastosowaniu metody maczycy skutków/prawdopodobieństwa (patrz część I, rozdział 2, podrozdział 2.15) rekomenduje się zastosowanie wartości liczbowych co najmniej w układzie 4 x 4 lub wyższym, natomiast w celu eliminacji uśredniania wyników pomiaru – maczycy o liczbie parzystej.

Tabela 30. Pomiar skutków³⁵⁰

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

³⁴⁹ Por.: szacowanie ryzyka, s. 39.

³⁵⁰ Źródło: opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, s. 8.

W podanych przykładach przyjęto trójstopniową klasyfikację prawdopodobieństwa i skutków. Można jednak spotkać np. klasyfikację pięciostopniową, daje ona dokładniejsze wyniki.

Tabela 31. Prawdopodobieństwo wystąpienia zagrożenia³⁵¹

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

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 przypadkach³⁵². Te ostatnie mają charakter uniwersalny. Wyniki analizy ryzyka służą opracowaniu profilu ryzyka³⁵³. Do każdego ryzyka przypisana jest ocena opisująca jego znaczenie. Profil ryzyka porządkuje zidentyfikowane 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 ściślemu określeniu odpowiedzialności żadne ryzyka nie zostają

³⁵¹ Podobną tabelę sporządza się dla szans. Źródło: opracowanie własne na podstawie *Standardu zarządzania ryzykiem FERMA 2003*, s. 8.

³⁵² Rekomendowane metody użyteczne do zastosowania w procesie oceny ryzyka opisano w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*.

³⁵³ Patrz: definicja na s. 222.

pominięte. Każdemu ryzyku zostają przyporządkowane odpowiednie zasoby menedżerskie, a właścicielom – obszary zainteresowań ryzykiem³⁵⁴.

Wynik analizy ryzyka umożliwi porównanie szacunków wartości ryzyka³⁵⁵ 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 ryzyka³⁵⁶, 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 ryzyka³⁵⁷, 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 gwarantować³⁵⁸:

1. skuteczne i sprawne funkcjonowanie organizacji,

³⁵⁴ *Standard zarządzania ryzykiem FERMA 2003*, s. 9.

³⁵⁵ Por.: poziom ryzyka, s. 39.

³⁵⁶ Patrz: definicja na s. 157.

³⁵⁷ 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*, s. 10.

³⁵⁸ *Standard zarządzania ryzykiem FERMA 2003*, s. 10.

2. skuteczne mechanizmy kontroli wewnętrznej,
3. zgodność działań z przepisami prawa i innymi obowiązującymi uregulowaniami.

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 za-

kresie 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, że³⁵⁹:

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,
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.

³⁵⁹ *Standard zarządzania ryzykiem FERMA 2003*, s. 11.

Każdy podmiot, organizacja, instytucja, agencja powinna³⁶⁰:

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, powinni³⁶¹:

1. być świadomi odpowiedzialności za rodzaj ryzyka leżący w ich kompetencjach,
2. znać metody postępowania w zakresie sprostania wymogom i stałego doskonalenia procesu zarządzania ryzykiem,
3. mieć świadomość, w jaki sposób zarządzanie ryzykiem wynika z kultury organizacyjnej,
4. 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

³⁶⁰ Tamże.

³⁶¹ Tamże.

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, opisu poszczególnych jego procesów czy też metod szacowania ryzyka³⁶² na 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)³⁶³ 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

³⁶² Patrz: definicja na s. 39.

³⁶³ Siłą rzeczy występują elementy podobne (między przeanalizowanymi metodykami a normą ISO 31000), jednak nie można uznać za pewnik, że są zbieżne albo jedno 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.

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.

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.

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).

Poniższa tabela przedstawia porównanie poszczególnych metodyk, z uwzględnieniem etapu identyfikacji ryzyka.

Tabela 32. Identyfikacja ryzyka (zagrożeń) w metodykach oceny ryzyka wybranych państw³⁶⁴

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

³⁶⁴ Źródło: opracowanie własne na podstawie poddanych analizie dokumentów opisujących metodyki oceny ryzyka stosowane w wybranych krajach.

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.
------------------------	--

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 zregulowania 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 33 prezentuje porównanie poszczególnych metodyk, z uwzględnieniem etapu analizy ryzyka.

Tabela 33. Analiza ryzyka w metodykach oceny ryzyka wybranych państw³⁶⁵

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>

³⁶⁵ Źródło: opracowanie własne, na podstawie poddanych analizie dokumentów opisujących metodyki oceny ryzyka stosowane w wybranych krajach.

CZĘŚĆ III
ZARZĄDZANIE RYZYKIEM WYBRANYCH PAŃSTWACH

Irlandia	Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości Wpływ ³⁶⁶ : ludzie (liczbowo), środowisko, infrastruktura (straty finansowe), społeczeństwo (pięciostopniowa skala jakościowa)
Niemcy	Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości Wpływ ³⁶⁷ : 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
Szwecja	Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości Konsekwencje: ludzie (liczba rannych, poszkodowanych), gospodarka/środowisko (kwota strat finansowych), polityka/społeczeństwo (jakościowo)
Wielka Brytania	Prawdopodobieństwo: pięciostopniowa skala jakościowa ze wskaźnikami częstości Konsekwencje: gospodarka, ludzie (ofiary i poszkodowani), wzburzenie społeczne, skutki psychologiczne

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 x 5 (Australia: 7 x 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

³⁶⁶ Pod pojęciem zgodnie z normą ISO 31000 należy rozumieć konsekwencje, jednak tłumaczenie pochodzi od słowa impact (ang.).

³⁶⁷ Uzasadnienie jak w komentarzu powyżej.

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 umożliwia ich porównanie. Oprócz parametru wartości ryzyka na matrycach (wykresie) zaznacza się poziom niepewności wyniku (Szwecja).

Tabela 34. Porównanie poszczególnych metodyk oceny ryzyka z uwzględnieniem etapu oceny ryzyka³⁶⁸

Kraj/Etap oceny ryzyka	Ocena ryzyka
Australia	Wartość ryzyka: czterostopniowa skala jakościowa Wizualizacja ryzyka: matryce ryzyka 7 x 5, ocena ryzyka zależy od wiarygodności informacji.
Irlandia	Wartość ryzyka: pięciostopniowa skala jakościowa Wizualizacja ryzyka: matryce ryzyka 5 x 5 dla każdej z czterech kategorii zagrożeń + zbiorcza matryca ryzyka
Niemcy	Wartość ryzyka: czterostopniowa skala jakościowa Wizualizacja ryzyka: matryca ryzyka 5 x 5 dla każdego scenariusza + zbiorcza matryca ryzyka
Szwecja	Wartość ryzyka: pięciostopniowa skala jakościowa Wizualizacja ryzyka: matryce ryzyka 5 x 5 uwzględniające parametry jakościowe oraz ilościowe, obejmujące częstość zdarzenia; matryca ryzyka 5 x 5 (ze wskaźnikiem oceny niepewności wyniku) w krajowej ocenie ryzyka
Wielka Brytania	Wartość ryzyka: pięciostopniowa skala Wizualizacja ryzyka: matryce ryzyka 5 x 5, uwzględniające parametry jakościowe oraz ilościowe, obejmujące częstość zdarzenia, oddzielne dla zagrożeń intencjonalnych, w tym terrorystycznych, oraz dla pozostałych zagrożeń

³⁶⁸ 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 ryzyk 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 powyższą 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, środowi-

ska/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 matrycy 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 dziesiętnymi) 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.

SUMMARY AND CONCLUSIONS

A variety of solutions for the risk assessment methodologies presented in part III results, most of all, from the basis of establishing them, namely the internal regulations of the particular countries and institutions. The methodologies subject to the analysis incorporate common elements, though. This is evident in those documents which were based on the guidelines of international risk assessment norms and standards.

The German, Australian and, partly, Swedish risk assessment methodologies were established in line with ISO 31000:2009 *Risk Management – Principles and Guidelines* and ISO/IEC 31010:2009 *Risk Management – Risk Assessment Techniques*. It is incontestably a strong point of such methodologies that they use such guidelines. It is because by applying them, good practices in scope of the above risk management principles and guidelines can be put into life, along with a description of individual risk management processes or risk assessment methods for the purpose of emergency management (civil emergency planning, or civil protection).

In the majority of the methodologies given in the analysis, risk assessment is seen in the context of the entire risk management process (also those which directly do not recommend the use of ISO standards in this scope, i.e. Ireland and Great Britain)³⁶⁹.

The solutions used in the chosen countries were compared in order to present clearly an approach of the countries to risk assessment and indicate their strengths and weaknesses. The particular phases of the discussed methodologies were adopted as an evaluation criterion, including their description, together with risk assessment tools and methods.

The phases of national methodologies are often distinguished by a varied number, as well as by terminology relating to the particular stages, including their names. Particular methodologies are scrutinised further in the paper, with a special emphasis on risk identification, risk analysis and risk evaluation as the

³⁶⁹ Similar elements exist therefore (between the methodologies analysed and ISO 31000), it cannot be taken for granted, though, that they are concurrent or benefit from them. For example, FERMA standard was prepared about 7 years prior to ISO 31000, and even before the preceding standard which entered into force in 2004.

elements common for all the represented approaches, and such considerations are summarised with tables characterising such 3 phases for the purpose of a comparative analysis.

The whole process in the Swedish methodology starts by identifying the roles and responsibilities of the entities taking part in risk assessment. The organisational context is defined in the first phase in the Irish methodology, though. The first phase in the Irish methodology (context determination) and in the German methodology (description of the area defined) concentrates on the description of the area subject to risk assessment and provides information about the geography of the identified area, climate, population, environment, supplies or economy.

A common stage for all the discussed methodologies is the identification of potential hazards with the determination of scenarios of unfavourable inter-linked events. It is because they are a starting point for risk analysis and evaluation. Scenarios are considered under particular risk assessment elements, i.e. under an analysis, including the estimation of likelihood and consequences, as well as risk evaluation. Therefore the need to describe them as accurately as possible. The necessary constituent parts are indicated for the particular methodologies, such as: a base event (and other events related directly or indirectly), their description with the causes of event occurrence, consequences and context relating to the circumstances of occurrence of a given event.

The German methodology approaches scenario description in detail. It provides an answer to a number of questions connected with the determination of the type of a hazardous event, spatial dimension, intensity and duration.

The methodologies discussed indicate the necessity to focus on scenarios having a nationwide impact, affecting the national values/vital interests and being 'black scenarios'. An innovative solution consists of the preparation of a scenario of events under a series of seminars, considering public participation in appraising the consequences of an event scenario (multivariate analysis (MVA) in Sweden).

The table below compares the particular methodologies considering the phase of risk identification.

Table 32. Risk (hazard) identification in risk assessment methodologies of selected countries³⁷⁰

Country/Risk assessment phase	Risk (hazard) identification
Australia	Risk identification is carried out based on an appropriately high standard of information, knowledge and experience of an organisation's staff and personnel. Hazards and sensitivity of exposure to a specific examined and described risk are both considered. The sources of risks controlled routinely and potential events and areas of their likely occurrence are considered. The exclusion of a considerable risk or its significant reduction is ensured considering that such measures are systematic and widespread. Care is taken that high class experts participate in such measures and scenarios of potential event progression are created. Scenarios backed up with past events may clearly strengthen knowledge on potential phases of event progression. All potential risks are identified, regardless they are under control or not, as well as all the existing and potential problems requiring risk reduction solutions.
Ireland	The area defined is described prior to hazard identification, hazards are classified according to: natural, transport, technological and civilian, 'black scenarios' are taken into account
Germany	The area defined is described prior to hazard identification, an event scenario is created based on the chosen hazards, events are considered at the national scale in relation to the worst case possible
Sweden	Risk identification as part of risk and vulnerability analysis conducted by state and local administration bodies; the phase is started with describing a system (of a given organisation), considering a structural, functional and mixed model with identification of internal and external factors likely to disrupt the system; a developed scenario approach using multiple methods, e.g. MVA, ROSA; scenarios described as 'black scenarios' in national risk assessment, with serious consequences, being a threat to at least one national value
Great Britain	Risk identification through expert consultations, events are selected being "worst possible case" with high risk of occurrence (high likelihood and consequences), scenarios consistent with the definition of a sudden event are selected or others are excluded by placing them on a reserve list for review at a later date.

³⁷⁰ Reference: an own paper based on the analysed documents describing risk assessment methodologies applied in the selected countries.

The next phase is a risk analysis, usually done based on historical, scientific, statistical data and expert estimations taking into account the indicated event scenarios. Its results is quantitative and qualitative data. An analysis of the selected risk assessment methodologies points out that the risk is estimated according to two basic factors, i.e. likelihood and consequences. A likelihood assessment as a secondary measure after the determination of consequences in seen the Irish methodology only. The following factors are additionally taken into account also: result estimation uncertainty in relation to the both basic parameters and vulnerability (assessment) as a part of the entire risk management process (Sweden).

The necessity to aggregate impact results by means of mathematic calculations is emphasized in the German methodology subject to the analysis. The overall result of the impact (consequence) in the German case is determined through calculations. The particular results of the impact value for individual impact parameters under a given category are added and divided by the number of parameters (weight can also be determined for particular elements of impact).

Table 33 below compares the particular methodologies considering the phase of risk analysis.

Table 33. Risk analysis in risk assessment methodologies of the selected countries³⁷¹

Country/Risk assessment phase	Risk analysis
Australia	<p>Likelihood: Seven-degree quantitative and qualitative scale with frequency/average interval/chance cycle occurrence indicators</p> <p>Consequences: Five-degree qualitative scale with consequence indicators</p>
Ireland	<p>Likelihood: Five-degree qualitative scale with frequency indicators</p> <p>Impact³⁷²: Population (in number), environment, infrastructure (financial losses), society (5-degree qualitative scale)</p>

³⁷¹ Reference: an own paper based on the analysed documents describing risk assessment methodologies applied in the selected countries.

³⁷² The term according to ISO 31000 is understood as consequences, however it is translated from *impact*.

Germany	<p>Likelihood: Five-degree qualitative scale with frequency indicators</p> <p>Impact³⁷³: 20 impact parameters under the category: man, environment, economy, supplies and intangible (e.g. political, psychological) considered quantitatively, i.e. number, time, amount (apart from the intangible category estimated qualitatively), adopting the aggregation method of impact results</p>
Sweden	<p>Likelihood: Five-degree qualitative scale with frequency indicators</p> <p>Consequences:</p> <p>Population (the number of injured, affected)</p> <p>Economy/Environment (the amount of financial losses)</p> <p>Politics/Society (qualitatively)</p>
Great Britain	<p>Likelihood: Five-degree qualitative scale with frequency indicators</p> <p>Consequences:</p> <p>Economy,</p> <p>People (victims and affected people), social unrest, psychological consequences</p>

Another stage is a risk assessment including the determination of the risk value based on the estimated likelihood parameters and consequences, as well as its visualisation. A risk matrix is a common tool serving this purpose. This allows to present comparatively the identified risks. A 5x5 risk matrix (7x5 for Australia) with five-degree scales of: likelihood and consequences (from 1 to 5) are adopted in the majority of the methodologies discussed. The points highlighted on the matrix determine the estimated risk value result. Depending on the country, either 4 (e.g. Germany) or 5 (e.g. Sweden) risk value parameters are adopted. A risk value in some countries is estimated not only based on a qualitative, but also quantitative description, considering event frequency, e.g. once every 100 years in relation to the number of victims (Sweden), or also a mixed (quantitative – qualitative) description, i.e. a consequence parameter at a qualitative scale of 1-5 and a quantitative parameter determining frequency in relation to event likelihood (Great Britain). Separate risk matrices for particular groups of hazards are created in some countries, i.e. for natural, transport, technological and civilian hazards (Ireland), as well as intentional hazards (such as terrorist attacks) and others (Great Britain). A collective risk

³⁷³ The justification as in the comment above.

matrix is the final effect in each of the methodologies, however, where all the risks of individual hazards are presented aggregately (event scenarios), which allows to compare them. A result uncertainty level is also marked on matrices (chart) apart from the risk value parameter (Sweden).

Table 34. Comparison of the particular risk assessment methodologies considering the phase of risk assessment³⁷⁴

Country/risk Assessment phase	Risk assessment
Australia	Risk value: Four-degree qualitative scale Risk visualisation: 7 x 5 risk matrices, risk assessment depends on information credibility.
Ireland	Risk value: Five-degree qualitative scale Risk visualisation: 5 x 5 risk matrices for each of four hazard categories + collective risk matrix
Germany	Risk value: Four-degree qualitative scale Risk visualisation: 5 x 5 risk matrix for each scenario + collective risk matrix
Sweden	Risk value: Five-degree qualitative scale Risk visualisation: 5 x 5 risk matrices including qualitative and quantitative parameters including event frequency; 5x5 risk matrix (with result uncertainty result indicator) in the National Risk Assessment
Great Britain	Risk value: Five-degree scale Risk visualisation: 5 x 5 risk matrices including qualitative and quantitative parameters including event frequency, separate for intentional hazards, including terrorist hazards and for other hazards

It is argued in the documents analysed that decision-makers determine, based on the risk assessment results, which risks need to be handled and set up response priorities. A vulnerability appraisal is additionally carried out in the Swedish methodology. It permits to answer the question what are weaknesses under the available forces and resources necessary to reduce risks and which of

³⁷⁴ Reference: an own paper based on the analysed documents describing risk assessment methodologies applied in the selected countries.

them should be reinforced. The analysis, therefore, greatly complements the risk assessment undertaken in an earlier phase.

A number of tools, supporting the persons conducting a risk assessment and analysis, has been identified for the analysed methods. In particular, the Guide to risk and vulnerability analyses prepared by the Swedish Civil Contingencies Agency presents a considerable number of tools used, also the ones recognised notably by ISO/IEC 31010, i.e. *Risk Management — Risk Assessment Techniques*. It should be remarked that from amongst the countries indicated in the paper, all of them have developed their own scenario analyses: MVA, ROSA, IBERO (Swedish proposals), NRA documents (for the Irish and British methodology). If we look at the tools recommended by ISO/IEC 31010, the ones worth recommending for the purpose of civil emergency planning are qualitative tools, i.e. preliminary risk analysis, “what if?” analysis and a fault tree analysis. The first one, the preliminary risk analysis, is rather of limited usage. It enables, however, to adopt a general view on all the identified hazards and after taking into account the recorded causes, consequences and likelihood, to carry out an assessment and indicate proposed solutions. In turn, the SWIFT method offers an inquisitive analysis of all the possible causes and impacts for a broad array of scenarios, which marks its versatility. A fault tree analysis is indicating in a clear way the linkage between the specific consequences and their causes. The method also permits to estimate occurrence likelihood or frequency in the next step for the quantitative method used. The picture created helps to understand how a given event is created by the existence of subsequent factors contributing to its occurrence. Appropriate preventive measures can be taken in longer term owing to this. Risk matrices are used most often for the purpose of risk evaluation and presentation. The ones used most often in national methodologies included two five-degree scales of likelihood and consequences (three degrees of uncertainty of the estimated result are also used in Sweden).

An analysis of the risk assessment methodologies used in the selected countries has shown that the process, similar as in Poland, sets a basis for emergency management planning (civil protection). The approaches presented in this part contain numerous examples of solutions relating to the identification of hazards at the national level, estimation of their occurrence risk, as well as evaluation. Some of them could be used in Polish conditions.

It should hence be concluded based on the analysis of documents from different countries that the perception of risk assessment in relation to the entire risk management process is common these days. In this approach, the process comprises such elements as: context determination, risk identification, risk analysis, risk evaluation, as well as risk handling. It also seems substantiated to provide a legal framework for such a process in Poland (the process, until now, comprises only selected elements, including risk assessment). Especially that it is recommended, in the methodologies analysed, to use guidelines of selected risk management standards, including solutions appropriate for a given country, as well as the directives of international standards, e.g. ISO 31000 and ISO/IEC 31010. These could be used for the terminology, for the construction of the entire risk management process, as well as for risk assessment methods.

A possibility of developing a scenario-based approach should be considered for the solutions used in selected countries in the context of their implementation in Polish conditions, according to which scenarios are a starting point for risk analysis, therefore, the main focus is put on describing them precisely, on the possibility of using experts' support for preparing them and the application of methods and techniques to establish scenarios of events, or to select them by choosing only "the worst possible scenarios" having the nationwide impact.

In connection with the abovementioned concept of broadening a risk assessment to encompass the entire risk management process, it is worth considering to supplement the risk assessment method with an element connected with the determination of an organisation's (to which the risk assessment process relates) internal and external context considering, in particular, its goals, organisation structure, environment/surrounding, law. It is therefore possible to determine its vulnerability likely to cause an increased estimated value of likelihood and consequences, and in turn the change of the forecast risk value. What is more, it should be considered to present handling procedures for the identified risks on the risk matrix.

It should be pointed out as a result of analysing the country methodologies presented in part III that:

- An advantage of the Australian methodology is that it approaches risk management comprehensively, while introducing at the same time universal and unified risk management principles, frameworks (structures) and processes

consistent with national documents as well as the international standard ISO 31000:2009.

- An advantage of the Irish methodology that in the beginning of the analysis it draws attention to the necessity to determine its context, i.e. to describe the area/region for which a risk assessment is established, allowing to realise the given area's vulnerability and resilience in case of danger.

- An advantage of the German methodology is that the risk assessment process relates to a precisely defined area covered by the analysis, i.e. in relation to the defined objects or places, which later facilitates to determine the impact, as well as a developed scenario approach (being a starting point for further analysis). The establishment of the impact results aggregation method (a parameter determined by means of quantitative and qualitative estimations) converted, after summing up, to a result close to the qualitative scale (allowed with decimals) is brought to attention for the purpose of presentation of results on the risk matrix together with the estimated likelihood.

- An advantage of the Swedish methodology is that individual groups of situations (daily events, large events, crises) are placed on the risk chart, and multiple useful tools can be used and described – methods aiding risk assessment, and that event scenarios are created under a series of seminars considering the participation of people in the evaluation of event scenario consequences.

- An advantage of the British methodology is that risk assessment activities are highly systematised for the purpose of emergency planning (carried out on a yearly basis). The use of experts' support at the stage of risk identification also comes to attention, as well as preliminary selection of event scenarios as to exclude the most improbable ones from a further analysis (based on selection of the "worst case", i.e. events with a high risk of occurrence, i.e. associated with high likelihood and consequences). An attempt to estimate a psychological effect of unfavourable events on the society can be regarded to be a strong point of the methodology used in the Great Britain. Moreover, its advantage is that it considers risks for their occurrence over the next five years.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

1. Boardman A., Greenberg D., Vining A., Weimer D., *Cost-Benefit Analysis: concepts and practice*, Prentice Hall 2010.
2. Gołębiowski J., *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, SA PSP, Kraków 2011.
3. Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, Danmar, Warszawa 2005.

Akty prawne

1. Civil Contingencies Act 2004, UK.
2. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558, z późn. zm.).
3. Zarządzenie nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie
4. Zarządzenie nr 80 wojewody mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia Polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.
5. European Commission: Commission Staff Working Paper: Risk Assessment and Mapping Guidelines for Disaster management, 2010, SEC(2010) 1626 final (17899/10).

Normy i standardy

1. ISO 31000:2009 *Risk Management – Principles and Guidelines*.
2. ISO Guide 73:2009 *Risk Management – Vocabulary*.
3. PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.
4. PN-EN 15975-1:2011 *Bezpieczeństwo zaopatrzenia w wodę pitną. Przewodniki zarządzania kryzysowego i ryzyka. Część 1: Zarządzanie kryzysowe*.
5. PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*.
6. *Standard zarządzania ryzykiem FERMA 2003*.

Dokumenty elektroniczne, strony internetowe i inne

1. *A Framework for Major Emergency Management, A Guide to risk Assessment in Major Emergency Management*, January 2010 (Irlandia).
2. *A National Risk Assessment for Ireland*, Office of Emergency Planning, December 2012 (Irlandia).
3. *Guide to risk and vulnerability analyses*, Swedish Civil Contingencies Agency, 2012 (Szwecja).
4. <http://ciop.pl>.
5. <http://sjp.pl>.
6. <http://www.governica.com>.
7. <http://www.ryzykozawodoweonline.pl>.
8. *Method of Risk Analysis for Civil Protection 2011*, Federal Office of Civil Protection and Disaster Assistance 2011 (Niemcy).
9. *National Emergency Risk Assessment Guidelines. Commonwealth of Australia and Each of its States and Territories 2010*, grudzień 2010 (Australia).
10. *National Risk Register for Civil Emergencies 2013*, Cabinet Office, 2013 (Wielka Brytania).
11. *Swedish National Risk Assessment*, Swedish Civil Contingencies Agency, 2012 (Szwecja).
12. *The National Risk Register of Civil Emergencies*, Cabinet Office, 2010 (Wielka Brytania).

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

PART IV
RISK MANAGEMENT IN THE REPUBLIC OF POLAND

WPROWADZENIE

Zarządzanie ryzykiem stało się nieodzownym elementem wielu gałęzi aktywności państwa. Dotyczy to w szczególności działalności związanych z bezpieczeństwem pojmowanym szeroko (rozwiązania dla całego sektora) oraz wąsko (rozwiązania dla poszczególnych instytucji), ponieważ możemy mówić m.in. o bezpieczeństwie finansów publicznych, rozwoju gospodarczego czy resortów administracji rządowej z jednej strony i bezpieczeństwie powodziowym bądź też konkretnych jednostek terytorialnych i podmiotów z drugiej strony.

W całościowym przekroju zastosowania zarządzania ryzykiem w Polsce systemowe rozwiązanie, obejmujące kompleksowe podejście do ryzyka, obowiązuje w polskim systemie prawnym w sektorze finansów publicznych. Rozwiązania wzmacniające kontrolę nad wydatkowaniem środków publicznych wprowadziła ustawa o finansach publicznych³⁷⁵ 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 są 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 rozwiązań w nich zaproponowanych.

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 I. Stanowi on próbę przybliżenia metody wdrażania

³⁷⁵ 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.

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 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. Ostatni z rozdziałów części IV 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”.

INTRODUCTION

Risk management has become an inherent part of many fields of the state's activity. It especially holds true for activities related to a broadly (solutions for the entire sector) and narrowly (solutions for individual institutions) conceived safety, as one can speak, for instance, about the safety of public finance, economic development or branches of state administration on one hand, and flood safety or safety of specific territorial units and entities on the other hand.

For the overall spectrum of risk management in Poland, a system-based approach covering comprehensively an approach to risk has been in place in the public finance sector in the Polish legal system. The Public Finance Act has implemented solutions reinforcing control over the disbursement of public funds³⁷⁶ and mandates numerous entities, i.e. ministries, central administration, banks and other public administration entities and institutions to enforce such solutions.

This part presents a number of methodologies and solutions using risk management elements, which are implemented or are valid in various areas of activity in Poland. All those described in the next chapters are functioning directly or indirectly as an area of interest for emergency management and civil emergency planning. A relationship with the guidelines of recognised risk management standards are shown for the examples of the solutions given or a need is identified to consider the solutions proposed there.

The first chapter discussed the application of risk management elements in the documents prepared under the emergency management act (emergency management plans, Report on threats to state security and critical infrastructure protection plans). The second chapter, by referring to the considerations made in the first chapter as well as in part I, makes an attempt to bring closer the method of incorporating the good practices adopted in standards into civil emergency planning. The next chapter touches upon the issue of flood risk management in Poland. A risk assessment methodology for flood hazards es-

³⁷⁶ The act introduced under EU legislation subject to harmonisation with Polish law, in particular as delegation of the COUNCIL REGULATION (EC) No. 1466/97 of 7 July 1997 on the strengthening of the surveillance of budgetary positions and the surveillance and coordination of economic policies.

established at the EU level is thoroughly analysed. Chapter four is broadening the area of studies over risk management in Poland by focussing on governance control. This is a separate component mandatorily enforced by, among others, public administration bodies responsible for civil emergency planning. This offers a renewed focus on governance control as additional competences of state and local administration personnel in scope of risk management. The fifth chapter depicts a custom PomRisc methodology enabling to diagnose a safety status and rescue system with indicating the optimum directions of improvement measures. The methodology is an example how risk assessment and risk management methods and tools are utilised. The last chapter of part IV embarks indicatively on the aspect of fire risk management in Poland. This topic – being of paramount importance for national security and local communities, is incorporated into the area of interest of the research and development project for state defence and security titled “Creation of system-based solutions aiding post-fire investigations using modern information technologies, including technical and IT tools”.

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 ryzyka³⁷⁷. 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.

³⁷⁷ Patrz: definicja na s. 29.

Zarówno NPOIK, jak i *Procedura opracowania raportu cząstkowego na potrzeby RoZBN* poruszają problematykę zarządzania ryzykiem. Niemniej jednak żadne z nich nie opiera się na normach ISO ani ich nie rekomenduje.

Analiza formalna wskazanych wyżej dokumentów³⁷⁸ (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 ryzykiem³⁷⁹, natomiast organizacja ISO nie podejmuje się wskazania szczegółowych zaleceń pozwalających na dokonanie samej oceny ryzyka. Hipoteza ta brzmi:

³⁷⁸ Pod tym pojęciem rozumie się technikę badawczą służącą do gromadzenia wstępnych, opisowych, także ilościowych informacji o badanej instytucji czy zjawisku. Za: T. Pilch, *Zasady badań pedagogicznych*, wyd. Żak, Warszawa 1995, s. 76.

³⁷⁹ Patrz: definicja na s. 28.

Normy ISO można wykorzystać w procesie planowania cywilnego w zakresie ujednolicenia 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 ryzyka³⁸⁰ 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.

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.

³⁸⁰ Patrz: definicja na s. 45 (źródło 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. Nowela ta uzupełniła wymogi dla planowania cywilnego w obszarze planów zarządzania kryzysowego. W odniesieniu do planów zarządzania kryzysowego ustawa została uzupełniona o:

1. 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,
2. art. 5 ust 2 pkt 1 ppkt a, który mówi, że charakterystyka zagrożeń (będącą elementem planu głównego PZK) powinna zawierać także *ocenę ryzyka ich wystąpienia* (w tym zagrożeń dotyczących infrastruktury krytycznej) oraz *mapy ryzyka i mapy zagrożeń*³⁸¹.
3. 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 spo-

³⁸¹ Zgodnie z art. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. 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.

sób finansowania w dziedzinie zarządzania kryzysowego³⁸². W wymienionych definicjach omawianej ustawy na szczególną uwagę zasługują pojęcia:

1. 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 awarii³⁸³, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie³⁸⁴,
2. zdefiniowanej wcześniej mapy ryzyka³⁸⁵.

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 reagowania kryzysowego, dotyczących sposobu postępowania w sytuacjach kryzysowych. Kolejny-

³⁸² Art. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590, z późn. zm.).

³⁸³ Patrz: definicja na s. 62.

³⁸⁴ Art. 3 pkt 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590, z późn. zm.).

³⁸⁵ Art. 3 pkt 10 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590, z późn. zm.).

mi 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 kryzysowego³⁸⁶.

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 ryzyka³⁸⁷. 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 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 przygo-

³⁸⁶ Art. 5a pkt 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590, z późn. zm.).

³⁸⁷ Ustawodawca nie przewidział zasadności włączenia innych elementów procesu zarządzania ryzykiem.

towaniem *Raportu* kieruje dyrektor Rządowego Centrum Bezpieczeństwa. W dokumencie tym wskazuje się najważniejsze zagrożenia przedstawione na mapie ryzyka, określa cele strategiczne³⁸⁸ oraz priorytety w reagowaniu na wytypowane zagrożenia oraz siły i środki niezbędne do osiągnięcia celów strategicznych.

Rozporządzenie w sprawie *Raportu o zagrożeniach bezpieczeństwa narodowego*³⁸⁹ określa sposób, tryb i terminy jego opracowania. Na potrzeby *Raportu* przygotowywane są przez właściwego ministra raporty częściowe, w których skład wchodzi raporty częściowe wykonane przez podległego kierownika urzędu centralnego. Raporty częściowe zawierają informacje dotyczące wskazania najważniejszych zagrożeń i skutków ich wystąpienia zobrazowane na mapie ryzyka³⁹⁰. 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, oddziaływać na sąsiednie kraje. Raport określa również cele strategiczne, które należy osiągnąć w dążeniu do zminimalizowania możliwości wystąpienia zagrożenia, a także wskazanie sił i środków niezbędnych 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 częściowy 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.

³⁸⁸ Patrz: definicja na s. 26.

³⁸⁹ Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie *Raportu o zagrożeniach bezpieczeństwa narodowego* (Dz.U. nr 83, poz. 540).

³⁹⁰ Mapy ryzyka nie można utożsamiać z matrycą ryzyka. Mapy ryzyka obrazują skutki i są przygotowywane dla zagrożeń o określonym już prawdopodobieństwie (np. wysokim).

Rządowe Centrum Bezpieczeństwa opracowało metodykę na potrzeby *Raportu o zagrożeniach bezpieczeństwa narodowego*. Metodyka ta wykorzystywana jest w odniesieniu do zagrożeń³⁹¹:

1. 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;
2. których skutki mogą:
 - godzić w bezpieczeństwo państwa, jego porządek konstytucyjny; a w szczególności w suwerenność, niepodległość i nienaruszalność terytorium,
 - zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach;
 - oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa;
 - dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie;
3. występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych;
4. o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej.

Proces oceny ryzyka koncentruje się na czterech krokach:

1. identyfikacji zagrożeń – zgodnie z działami administracji rządowej,
2. opisanu scenariuszy – wskazanie potencjalnych miejsc wystąpienia zagrożenia oraz jego typu,
3. analizie skutków³⁹² – dla ludności, gospodarki, mienia, środowiska, infrastruktury krytycznej, wraz z danymi graficznymi i tabelarycznymi,

³⁹¹ Procedura opracowania raportu częściowego do *Raportu o zagrożeniach bezpieczeństwa narodowego*, s. 4-5.

³⁹² Pod pojęciem skutków należy rozumieć konsekwencje, zgodnie z definicją normy ISO. Patrz: s. 22.

4. ocenie ryzyka³⁹³ – określenie prawdopodobieństwa, skutków, wartości ryzyka³⁹⁴ oraz poziomu jego akceptacji.

Prawdopodobieństwo opisuje się według poniższej skali:

Tabela 35. Skala prawdopodobieństwa na potrzeby *Raportu (...)*³⁹⁵

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.
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.

Skutki opisywane są również w pięciostopniowej skali, ale rozpatruje się je ponadto w odniesieniu do: życia i zdrowia, mienia i środowiska (tabela 36).

³⁹³ Pojęcie zastosowano w dokumencie błędnie, powinno być rozumiane jako analiza ryzyka. Patrz: definicja na s. 31.

³⁹⁴ Patrz: definicja na s. 39 (poziom ryzyka).

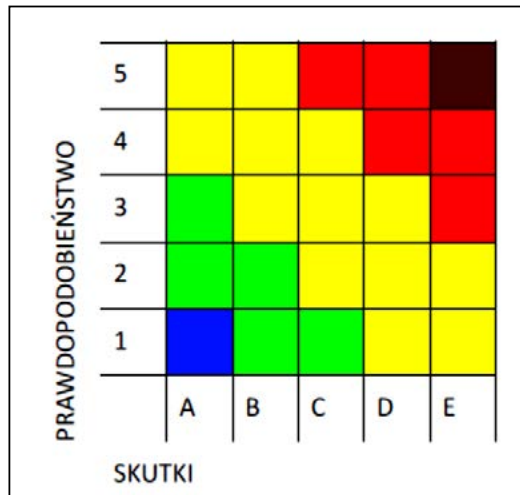
³⁹⁵ Źródło: Procedura opracowania raportu częściowego do *Raportu o zagrożeniach bezpieczeństwa narodowego*, s. 14.

Tabela 36. Skala konsekwencji na potrzeby *Raportu (...)*³⁹⁶

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.
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	Spoločność 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.

³⁹⁶ Źródło: Procedura opracowania raportu cząstkowego do *Raportu o zagrożeniach bezpieczeństwa narodowego*, s. 16.

Wyniki analizy prezentuje się na matrycy (5 x 5):



Rys. 46. Matryca ryzyka na potrzeby Raportu (...) ³⁹⁷

Metody przedstawione w części I niniejszej publikacji wskazują, w jaki sposób za ich pomocą można/należy:

1. identyfikować zagrożenia – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, drzewa zdarzeń, wpływu na działalność (BIA), przyczyn i skutków oraz przyczyn i efektów;
2. określać ich prawdopodobieństwo – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, *bow tie*, wpływu na działalność (BIA) oraz przyczyn i efektów;
3. określać ich konsekwencje – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, drzewa zdarzeń, *bow tie*, wpływu na działalność (BIA), przyczyn i skutków oraz przyczyn i efektów;
4. określać poziom ryzyka – metody: SWIFT – „co, jeśli?”, scenariuszowa, drzewa błędów, drzewa zdarzeń, *bow tie*, wpływu na działalność (BIA) oraz przyczyn i skutków;
5. prezentować wyniki analizy – matryca ryzyka.

³⁹⁷ Źródło: Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego, s. 17.

1.3. Ochrona infrastruktury krytycznej

Zgodnie ze wspomnianą już nowelą do 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. 6 pkt 2, mówiący, że dyrektor Rządowego Centrum Bezpieczeństwa przekazuje Komisji Europejskiej co 2 lata sprawozdanie zawierające ogólne dane dotyczące rodzajów ryzyka³⁹⁸ oraz zagrożeń i słabych punktów stwierdzonych w każdym z systemów, w których została wyznaczona europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej.

Rozporządzenie w sprawie *Narodowego programu ochrony infrastruktury krytycznej* uszczegóławia ogólną ocenę ryzyka dla funkcjonowania opisywanego obszaru zadaniowego, poprzez uwzględnienie w niej podatności³⁹⁹ na zagrożenie oraz konsekwencje zakłócenia funkcjonowania infrastruktury krytycznej⁴⁰⁰. Trzecie z rozporządzeń wydanych na podstawie noweli 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 przeznaczone do tego procesu narzędzie, jakim jest metoda scenariuszowa.

Na podstawie *Narodowego programu ochrony infrastruktury krytycznej* tworzone są warunki do poprawy jej bezpieczeństwa. Oznacza to podejmowanie

³⁹⁸ Pod pojęciem rodzajów ryzyka należy rozumieć czynniki ryzyka, zgodnie z definicją na s. 227.

³⁹⁹ Patrz: definicja na s. 130.

⁴⁰⁰ § 5 ust. 1 rozporządzenia nakłada ten obowiązek na ministrów i kierowników urzędów centralnych (tzw. gospodarzy systemów IK), którzy po okresie 6 miesięcy od otrzymania kryteriów pozwalających na wyznaczenie infrastruktury krytycznej powinni przesłać między innymi tę informację do dyrektora RCB.

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 nie znaleziono na etapie analizy dokumentu metodyki zarządzania ryzykiem.

Rozporządzenie w sprawie *Narodowego programu ochrony infrastruktury krytycznej*⁴⁰¹ 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, urzędzeń 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.

⁴⁰¹ Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie *Narodowego programu ochrony infrastruktury krytycznej* (Dz.U. nr 83, poz. 541).

Rozporządzenie w sprawie planów ochrony infrastruktury krytycznej⁴⁰² 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 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.

⁴⁰² Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. nr 83, poz. 542).

2. METODA WDROŻENIA ZARZĄDZANIA RYZYKIEM W PROCES 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:

1. Ustalanie kontekstu⁴⁰³.
2. Ocena ryzyka⁴⁰⁴:
 - 2.1. Identyfikacja ryzyka⁴⁰⁵.
 - 2.2. Analiza ryzyka⁴⁰⁶.
 - 2.3. Ewaluacja ryzyka⁴⁰⁷.
3. Postępowanie z ryzykiem⁴⁰⁸.

Każde z tych działań powiązane jest również z komunikacją i konsultacjami⁴⁰⁹ oraz monitorowaniem⁴¹⁰ i przeglądem⁴¹¹.

Przedstawione powyżej i zgodne z polską normą nazewnictwo działań zawiera pewną nieścisłość. Na przykład „identyfikacja ryzyka” może sugerować, że szacowania ryzyka⁴¹² już dokonano. W rzeczywistości o ryzyku możemy mówić dopiero po kroku „ewaluacja”. Wcześniejsze etapy dotyczą zagrożenia, jego cech i następstw. Dlatego w dalszej części niniejszego rozdziału, w celu uniknię-

⁴⁰³ Patrz: definicja na s. 31.

⁴⁰⁴ Patrz: definicja na s. 29.

⁴⁰⁵ Patrz: definicja na s. 27.

⁴⁰⁶ Patrz: definicja na s. 31.

⁴⁰⁷ Patrz: definicja na s. 37.

⁴⁰⁸ Patrz: definicja na s. 28.

⁴⁰⁹ Patrz: definicja na s. 40.

⁴¹⁰ Patrz: definicja na s. 37.

⁴¹¹ Patrz: definicja na s. 37.

⁴¹² Patrz: definicja na s. 39.

cia 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:

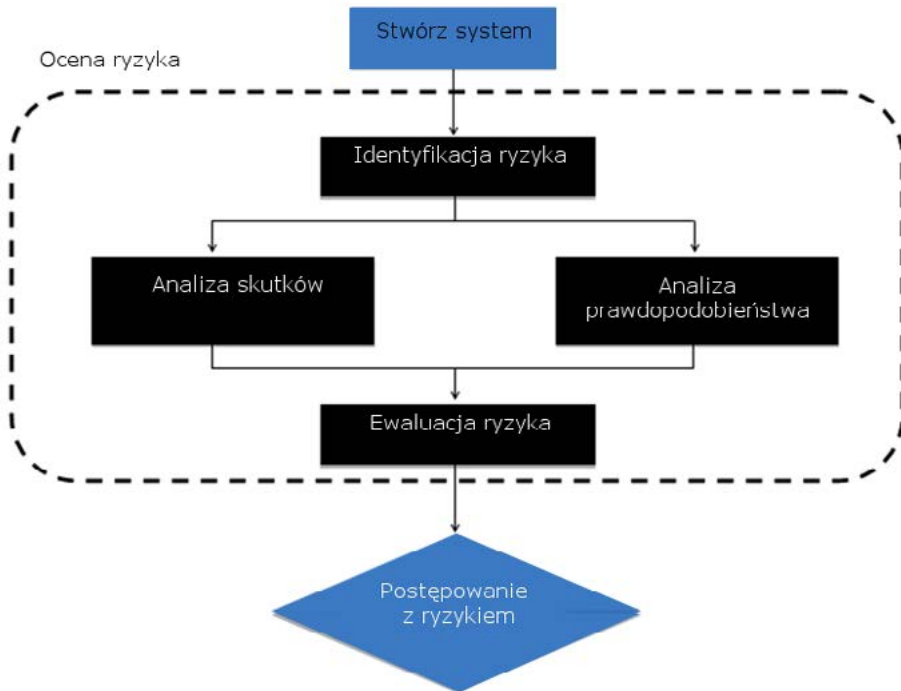
1. włączenia do planów zarządzania kryzysowego procedur oceny ryzyka oraz przygotowania na ich podstawie map ryzyka,
2. wykorzystania przy ocenie ryzyka metody scenariuszowej⁴¹³.

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:

1. identyfikacja ryzyka,
2. analiza ryzyka,
3. ewaluacja ryzyka.

Procesy te uporządkowano, proponując następujący schemat postępowania:

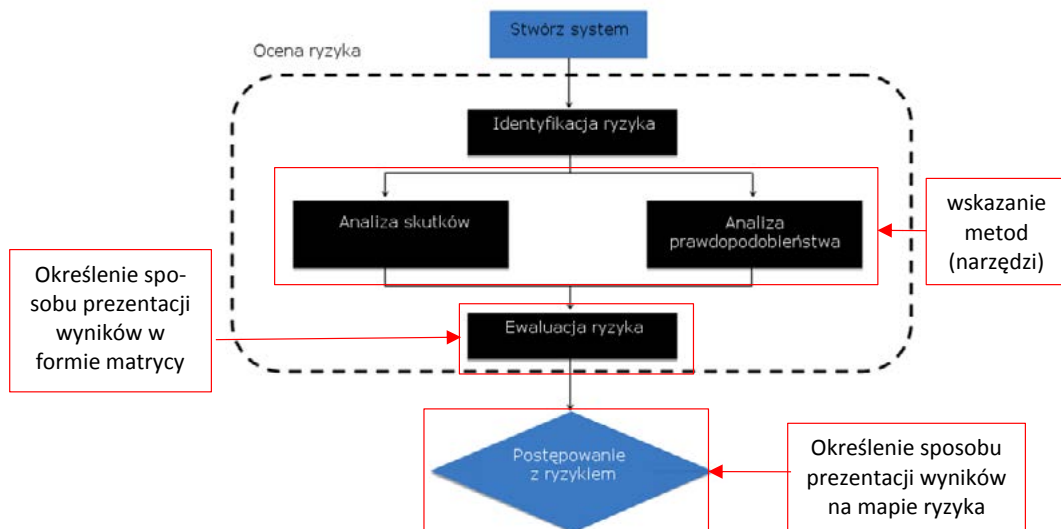
⁴¹³ Metoda ta jest wymagana (formalnie) jedynie przy analizie na potrzeby ochrony infrastruktury krytycznej.



Rys. 47. Proces oceny ryzyka⁴¹⁴

Biorąc pod uwagę wymagania stawiane przez ustawę o zarządzaniu kryzysowym oraz konieczność przypisania poszczególnym krokom narzędzi badawczych, powyższą rycinę należy rozszerzyć. Uzupełnienie to będzie wskazywało zakres koniecznych badań, które zostały zrealizowane w trakcie obecnego projektu.

⁴¹⁴ Źródło: na podstawie materiału szkoleniowego BSI: PN-ISO 31000:2012 *Wytyczne w zakresie zarządzania ryzykiem korporacyjnym*.



Rys. 48. Prezentacja obszarów badawczych na podstawie wniosków z poprzedniego etapu badań⁴¹⁵

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:

1. Jakie metodyki są stosowane w innych krajach i na ile można dokonać ich implementacji do warunków polskich?
2. Jakie metody oceny ryzyka są obecnie wykorzystywane w Polsce?
3. Na ile spełniają one wymagania stawiane planom zarządzania kryzysowego?

Wstępne badania literaturowe przeprowadzone przed przystąpieniem do zasadniczej części badania wskazują, że:

⁴¹⁵ Źródło: opracowanie własne.

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 awariami⁴¹⁶ 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*⁴¹⁷. 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 37.

⁴¹⁶ Patrz: definicja na s. 62.

⁴¹⁷ PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*, s. 49.

Tabela 37. Metody rekomendowane dla planowania cywilnego przy ocenie ryzyka⁴¹⁸

Metody oceny ryzyka	Procesy oceny ryzyka				
	Identyfikacja	Analiza ryzyka			Ewaluacja ryzyka
		Skutki ⁴¹⁹	Prawdopodobieństwo	Poziom ryzyka	
Analiza „co, jeśli?”	++	++	++	++	++
Analiza scenariuszy	++	++	+	+	+
Analiza drzewa błędów	+	-	++	+	+
Analiza drzewa zdarzeń	+	++	+	+	-
Analiza <i>bow tie</i>	-	+	++	++	-

Legenda:

++ – zdecydowanie dotyczy

+ – dotyczy

-- nie dotyczy

2.2. Szczegółowy opis procesu z uwzględnieniem istniejących ograniczeń formalnoprawnych

Jak już wcześniej wspomniano, ocena ryzyka to proces, na który składają się:

1. identyfikacja,
2. analiza,
3. 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

⁴¹⁸ Źródło: ISO/IEC 31010 *Risk Management – Risk Assessment Techniques* (tłumaczenie własne).

⁴¹⁹ Konsekwencje – w rozumieniu normy ISO 31000.

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 *All Hazards Risk Assessment – Methodology Guidelines 2012-2013*⁴²⁰ autorzy uwzględnili następujące aspekty: polityczny, ekonomiczny, społeczny, technologiczny oraz prawny i środowiskowy. W *National Security Programme – National Risk Assessment Method Guide 2008*⁴²¹ 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). W tym etapie określa się scenariusze prowadzące do powstania danego zjawiska.
2. Określenie sposobu postrzegania zdarzenia (okoliczności towarzyszących zagrożeniu). W 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

⁴²⁰ *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 24 lutego 2015 r.

⁴²¹ *National Security Programme – National Risk Assessment – Method Guide 2008*.

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 (*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:

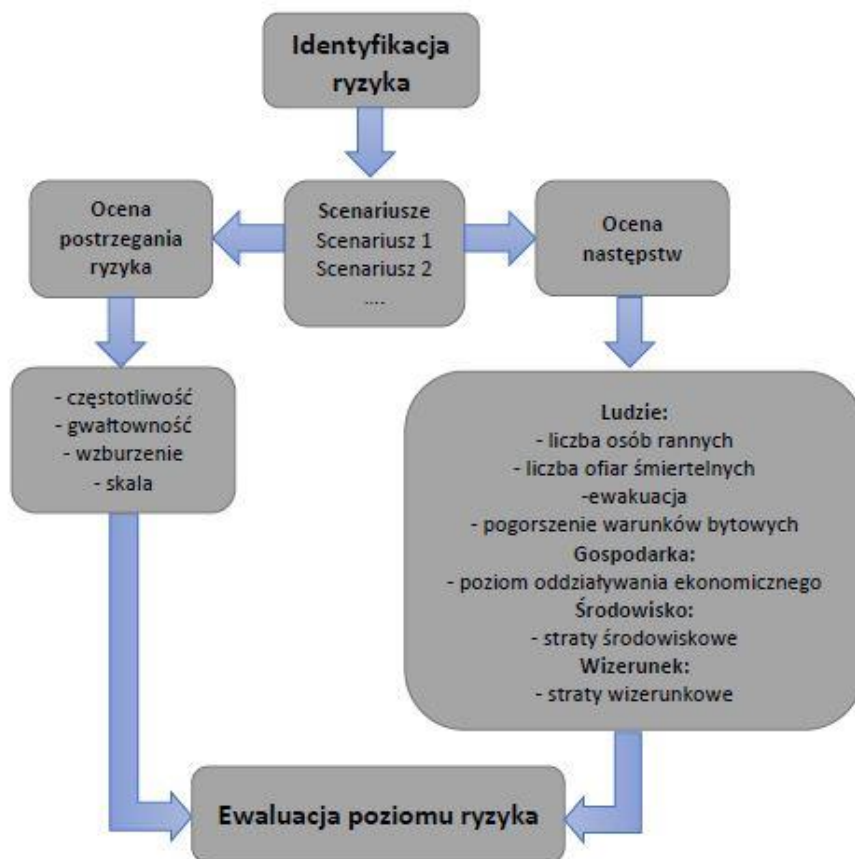
1. burzę mózgow – konfrontowanie ze sobą ocen przygotowanych przez różnych ekspertów,
2. grupowanie podobieństw (*affinity grouping*) – metoda polegająca na przyporządkowaniu zagrożeniom o podobnych cechach podobnego poziomu ryzyka,
3. listę kontrolną (*checklist*) – poziom ryzyka określany jest na podstawie listy pewnych cech zagrożenia,
4. analizę scenariuszy (*scenario analysis*) – dla danego zagrożenia opracowuje się różne scenariusze, a ryzyko ustalone jest dla scenariusza najbardziej reprezentatywnego i skrajnego (tzw. czarnego scenariusza),
5. analizę SWOT – gdzie dokonuje się oceny mocnych (*Strengths*) i słabych (*Weaknesses*) stron oraz szans (*Opportunities*) i zagrożeń (*Threats*) dla społeczności poddanej danemu zagrożeniu,

6. 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,
7. 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. 49.



Rys. 49. Schemat metody ilościowej⁴²²

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

⁴²² Źródło: opracowanie własne.

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 piętającej.

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:

- **Częstotliwość** – zależność wpływu ryzyka od tego, jak często dane zagrożenie występuje na danym poziomie administracji.

Tabela 38. Częstotliwość⁴²³

Wpływ	Częstotliwość występowania (co najmniej raz na [lat])
1	500 lub rzadziej
2	100
3	20
4	5
5	1

- **Gwałtowność** – zależność wpływu ryzyka od tego, jak szybko dane zjawisko się pojawia, czy możliwe jest jego monitorowanie oraz ostrzeżenie społeczeństwa.

Tabela 39. Gwałtowność⁴²⁴

Wpływ	Gwałtowność
1	zagrożenie pojawiające się powoli, możliwe do monitorowania, istnieje możliwość ostrzeżenia społeczeństwa z dużym wyprzedzeniem czasowym

⁴²³ Źródło: *Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego.*

⁴²⁴ Źródło: opracowanie własne.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

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 ⁴²⁵

- Wzburzenie – zależność wpływu ryzyka od tego jak jest ono postrzegane przez społeczeństwo nim dotknięte.

Tabela 40. Wzburzenie⁴²⁶

Wpływ	Wzburzenie
1	zagrożenie o znanym charakterze, mieszkańcy znają wzorce prawidłowych zachowań i posiadają zasoby własne pozwalające na łagodzenie jego skutków ⁴²⁷ 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) ⁴²⁸
3	zagrożenie o częściowo znanym charakterze, wymagane jest podanie mieszkańcom wzorców prawidłowych zachowań oraz interwencja służb ratowniczych i/lub administracji ⁴²⁹
4	zagrożenie o częściowo znanym charakterze, wymagane jest podanie mieszkańcom wzorców prawidłowych zachowań, nie ma możliwości zwalczania jego skutków w krótkim okresie ⁴³⁰
5	zagrożenie o niespotykanym charakterze, mieszkańcy nie znają wzorców prawidłowych zachowań, brak możliwości zwalczania jego skutków w krótkim czasie ⁴³¹

⁴²⁵ Przykładem takiego zdarzenia jest upadek samolotu na budynki mieszkalne. Zagrożenie takie jest standardowo rozważane na trasach dolotowych do lotnisk.

⁴²⁶ Źródło: opracowanie własne.

⁴²⁷ Przykładem jest grypa sezonowa.

⁴²⁸ Przykładem jest pożar wielkoobszarowy.

⁴²⁹ Przykładem są zagrożenia w pobliżu zakładów stwarzających ryzyko awarii przemysłowej.

⁴³⁰ Przykładem są zagrożenia radiologiczne.

⁴³¹ Przykładem takiego zdarzenia jest wystąpienie pandemii nowej, nieznannej choroby, jak np. wirus AH1N1.

- Skala – zależność wpływu zagrożenia od poziomu administracyjnego, który jest odpowiedzialny za zwalczanie zagrożenia bądź jego skutków.

Tabela 41. Skala⁴³²

Wpływ	Poziom administracji
1	gmina
2	powiat
3	województwo
4	kraj
5	międzynarodowy ⁴³³

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 42. Ranni⁴³⁴

Wpływ	Liczba rannych
1	< 10
2	< 100
3	< 500
4	< 1000
5	> 1000

2. Ofiary śmiertelne – zależność wpływu zagrożenia od liczby ofiar śmiertelnych.

⁴³² Źródło: opracowanie własne.

⁴³³ Dotyczy to zagrożeń, dla których konieczna jest współpraca o charakterze ponadnarodowym, np. migracji spowodowanych konfliktami polityczno-militarnymi.

⁴³⁴ Źródło: opracowanie własne.

Tabela 43. Ofiary śmiertelne⁴³⁵

Wpływ	Liczba ofiar śmiertelnych
1	< 5
2	< 10
3	< 100
4	< 500
5	> 500

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 44. Ewakuacja⁴³⁶

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

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, drogo, transport publiczny itp.

⁴³⁵ Źródło: opracowanie własne.

⁴³⁶ Źródło: opracowanie własne.

Tabela 45. Pogorszenie warunków bytowych⁴³⁷

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

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 46.

Tabela 46. Poziom oddziaływania ekonomicznego dla jednostek dysponujących budżetem własnym (samorząd terytorialny)⁴³⁸

Wpływ	Koszty
1	< 0,5% wydatków budżetu ⁴³⁹
2	< 5% wydatków budżetu
3	< 15% wydatków budżetu
4	> 15% wydatków budżetu
5	brak możliwości uchwalenia budżetu na kolejny rok – przekroczony indywidualny wskaźnik zadłużenia ⁴⁴⁰

⁴³⁷ Źródło: opracowanie własne.

⁴³⁸ Źródło: opracowanie własne.

⁴³⁹ 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 § 4 ustawy o zarządzaniu kryzysowym z 2007 r. (Dz.U. nr 89, poz. 590, z późn. zm.).

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. Nie uwzględnia się natomiast na poziomie poszczególnych resortów i poziomie wojewódzkim 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:

1. pomoc jednostkom samorządu terytorialnego w zakresie odbudowy infrastruktury,
2. 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).

⁴⁴⁰ 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.

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 47.

Tabela 47. Poziom oddziaływania ekonomicznego dla jednostek administracji rządowej (objętych regulacjami ustawy budżetowej)⁴⁴¹

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 Żywiotowych 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)

Kategoria – oddziaływanie na środowisko

Ocena wpływu skutków zagrożenia na środowisko rozpatrywana jest poprzez opis strat środowiskowych.

Tabela 48. Straty środowiskowe⁴⁴²

Wpływ	Wpływ na środowisko
1	mała powierzchnia (kilka hektarów) skażonego terenu, brak innych oddziaływań
2	powierzchnia skażonego terenu powyżej 10 ha, brak innych oddziaływań
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)

⁴⁴¹ Źródło: opracowanie własne.

⁴⁴² Źródło: opracowanie własne.

Kategoria – oddziaływanie na wizerunek

Wpływ zagrożenia na wizerunek danej społeczności określany jest na podstawie opisu strat wizerunkowych wywołanych przez zagrożenie.

Tabela 49. Straty wizerunkowe⁴⁴³

Wpływ	Wpływ na wizerunek
1	krótkotrwały, dotyczący do małej grupy ludzi, nie ma wpływu na gospodarkę danej jednostki terytorialnej, nie wywołuje napięć i niepokoїв 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

Etap ewaluacji ryzyka

Ewaluacja – określenie poziomu ryzyka poprzez:

1. zsumowanie wartości wskaźników dla postrzegania zagrożenia (suma liczb obrazujących wpływ z tabel 39 do 42),
2. zsumowanie wartości wskaźników dla następstw zagrożenia (suma liczb obrazujących wpływ z tabel 43 do 49, przy czym w zależności od rodzaju jednostki stosuje się jedną z tabel obrazujących wpływ na ekonomię – tabelę 46 albo 47),
3. odczyt poziomu ryzyka z tabeli.

Uzyskiwane wartości ryzyka⁴⁴⁴:

1. minimalne (kolor niebieski, 1),

⁴⁴³ Źródło: opracowanie własne.

⁴⁴⁴ Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego.

2. małe (kolor zielony, 2),
3. średnie (kolor żółty, 3),
4. duże (kolor czerwony, 4),
5. ekstremalne (kolor brązowy, 5).

Tabela 50. Szacowanie wartości poziomu ryzyka⁴⁴⁵

		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

Metodyka oceny ryzyka dla zagrożeń społecznych

Dla zagrożeń społecznych, ze względu na niemożliwość 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, umieszczone są w tabeli 51.

⁴⁴⁵ Źródło: opracowanie własne.

Tabela 51. Wykaz instytucji dysponującymi danymi wyjściowymi⁴⁴⁶

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

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:

1. komisji bezpieczeństwa i porządku – której zadaniem jest ocena zagrożeń porządku publicznego i bezpieczeństwa obywateli na terenie powiatu⁴⁴⁷,
2. spisów powszechnych – pozwalających na określenie wielkości migracji,
3. 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

⁴⁴⁶ Źródło: opracowanie własne.

⁴⁴⁷ Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym.

informowania dyrektorów szkół o zmianach w ewidencji dzieci jest nałożony przez ustawę o systemie oświaty⁴⁴⁸,

4. gminnego programu profilaktyki i rozwiązywania problemów alkoholowych – jego powstanie zakłada ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi⁴⁴⁹; na jego podstawie można określić skalę problemu alkoholowego na danym terenie, tzn. oszacować liczbę osób z problemem alkoholowym, liczbę osób żyjących w otoczeniu takiej osoby oraz skalę przemocy domowej spowodowanej tym nałogiem,
5. gminnego programu przeciwdziałania narkomanii – jego powstanie zakłada ustawa o przeciwdziałaniu narkomanii⁴⁵⁰; 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 52.

⁴⁴⁸ Ustawa z dnia 7 września 1991 r. o systemie oświaty.

⁴⁴⁹ Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.

⁴⁵⁰ Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii.

Tabela 52. Analiza SWOT⁴⁵¹

	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 niezbędnych 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.

⁴⁵¹ Źródło: opracowanie własne.

Po przeanalizowaniu wszystkich powyższych aspektów przez powołany zespół ekspertów należy przyporządkować danemu zagrożeniu poziom ryzyka, korzystając z następującej tabeli:

Tabela 53. Szacowanie wartości poziomu ryzyka⁴⁵²

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

⁴⁵² 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.

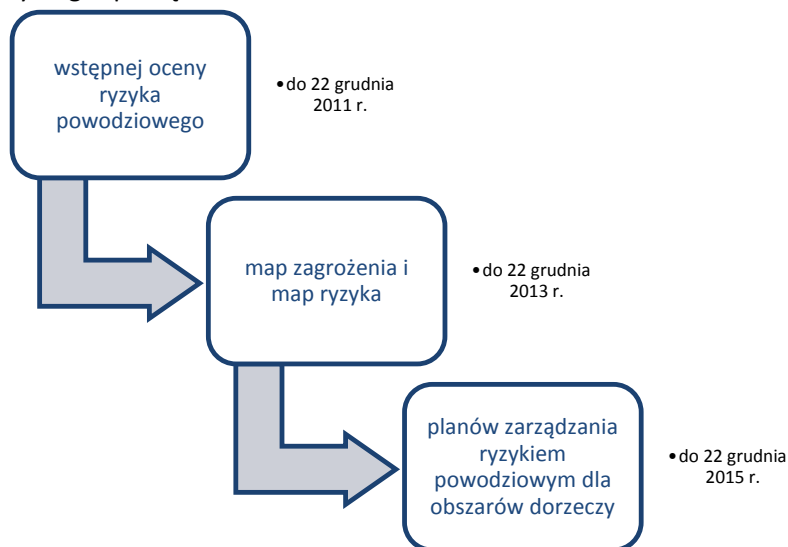
Celem niniejszego rozdziału jest wskazanie zasad zarządzania ryzykiem powodziowym opartych o rozwiązania przyjęte w dyrektywie powodziowej. W poszczególnych jego częściach zostaną zaprezentowane główne założenia dyrektywy oraz proces jej wdrażania, polityka zarządzania ryzykiem powodziowym oraz metodyka 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 przedstawiciele lokalnych społeczności, tak aby uzyskać maksymalne korzyści społeczne⁴⁵³.

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 ocen ryzyka powodziowego i zarządzania nim wymaga sporządzenia:



Rys. 50. Proces wprowadzania wymogów dyrektywy powodziowej⁴⁵⁴

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 gospodarczej⁴⁵⁵;
- **obszary narażone na niebezpieczeństwo powodzi** – rozumie się przez to określenie we wstępnej ocenie ryzyka powodziowego obszarów, na których

⁴⁵³ Art. 1 pkt 1, 3 ustawy z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. nr 115, poz. 1229).

⁴⁵⁴ Źródło: opracowanie własne na podstawie dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r.

⁴⁵⁵ Art. 9 pkt 1b ustawy z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. nr 115, poz. 1229).

istnieje znaczące ryzyko powodzi⁴⁵⁶ lub jest prawdopodobne wystąpienie znaczącego ryzyka powodzi^{457,458};

- **cele główne planów zarządzania ryzykiem** – cele odwołujące się do kolejnych faz zarządzania ryzykiem powodziowym: prewencji, ochrony, przygotowania, odbudowy i analiz⁴⁵⁹. 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 wodnych⁴⁶⁰;

- **wrażliwość** – odporność infrastruktury zlokalizowanej w terenach zagrożonych na podtopienia i zalanie, charakteryzuje stopień przygotowania zagrożonych 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 ostrzegania⁴⁶¹;

⁴⁵⁶ 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: *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, KZGW, Warszawa 2013, s. 6.

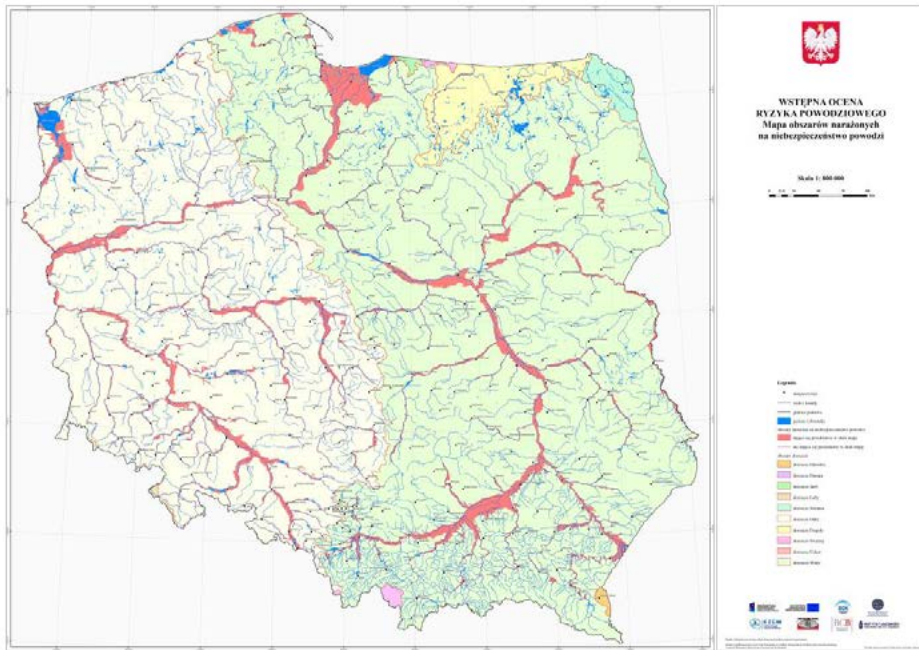
⁴⁵⁷ Art. 9 pkt. 6b ustawy z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. nr 115, poz. 1229).

⁴⁵⁸ Obszary, na których wystąpienie powodzi jest prawdopodobne – obszary z zasięgami powodzi prawdopodobnych – są to obszary wyznaczone głównie na podstawie studiów ochrony przeciwpowodziowej opracowanych przez regionalne zarządy gospodarki wodnej. Ponieważ zostały wyznaczone na podstawie modelowania hydraulicznego dla przepływów o określonym prawdopodobieństwie wystąpienia, traktowane są jako powodzie mogące wystąpić w przyszłości, o których mowa w art. 88b ust. 2 pkt 3 ustawy Prawo wodne oraz w art. 4.2d dyrektywy powodziowej. Źródło: *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, KZGW, Warszawa 2013, s. 6.

⁴⁵⁹ Wprowadzenie faz zarządzania ryzykiem powodziowym można zinterpretować jako przyjęcie w pewnym zakresie struktury ramowej niezbędnej do celów realizacji tego procesu.

⁴⁶⁰ *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, KZGW, Warszawa 2013, s. 8.

⁴⁶¹ Tamże.



Rys. 51. Wstępna ocena ryzyka powodziowego. Mapa obszarów narażonych na niebezpieczeństwo powodzi⁴⁶²

- **ryzyko powodzi** – to kombinacja prawdopodobieństwa wystąpienia powodzi i potencjalnych negatywnych skutków⁴⁶³ powodzi dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej⁴⁶⁴.

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 powodziowego⁴⁶⁵, map ry-

⁴⁶² http://www.kzgw.gov.pl/files/file/Materialy_i_Informacje/WORP/Polska/1.jpg,
dostęp: styczeń 2015.

⁴⁶³ Pod pojęciem skutków należy rozumieć konsekwencje, zgodnie z definicją normy ISO na s. 22.

⁴⁶⁴ Art. 9 pkt. 13c ustawy z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. nr 115, poz. 1229).

⁴⁶⁵ 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.

zyka powodziowego⁴⁶⁶, a także planów zarządzania ryzykiem powodziowym. Zgodnie z art. 88b przywołanej ustawy na wstępie dla obszarów dorzeczy przygotowuje się **wstępną ocenę ryzyka powodziowego** (rys. 56). *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 powodziowego⁴⁶⁷. Do sporządzenia oceny konieczne było przyjęcie poniższego procesu⁴⁶⁸:*

1. zebranie i zestawienie materiałów do wykonania WORP,
2. utworzenie wejściowej bazy danych WORP,
3. zlokalizowanie znaczących powodzi (historycznych i prawdopodobnych),
4. zlokalizowanie i zidentyfikowanie obszarów potencjalnie zagrożonych powodzią,
5. wydzielenie obszarów narażonych na niebezpieczeństwo powodzi,
6. utworzenie wynikowej bazy danych WORP,
7. opracowanie map wstępnej oceny ryzyka powodziowego.

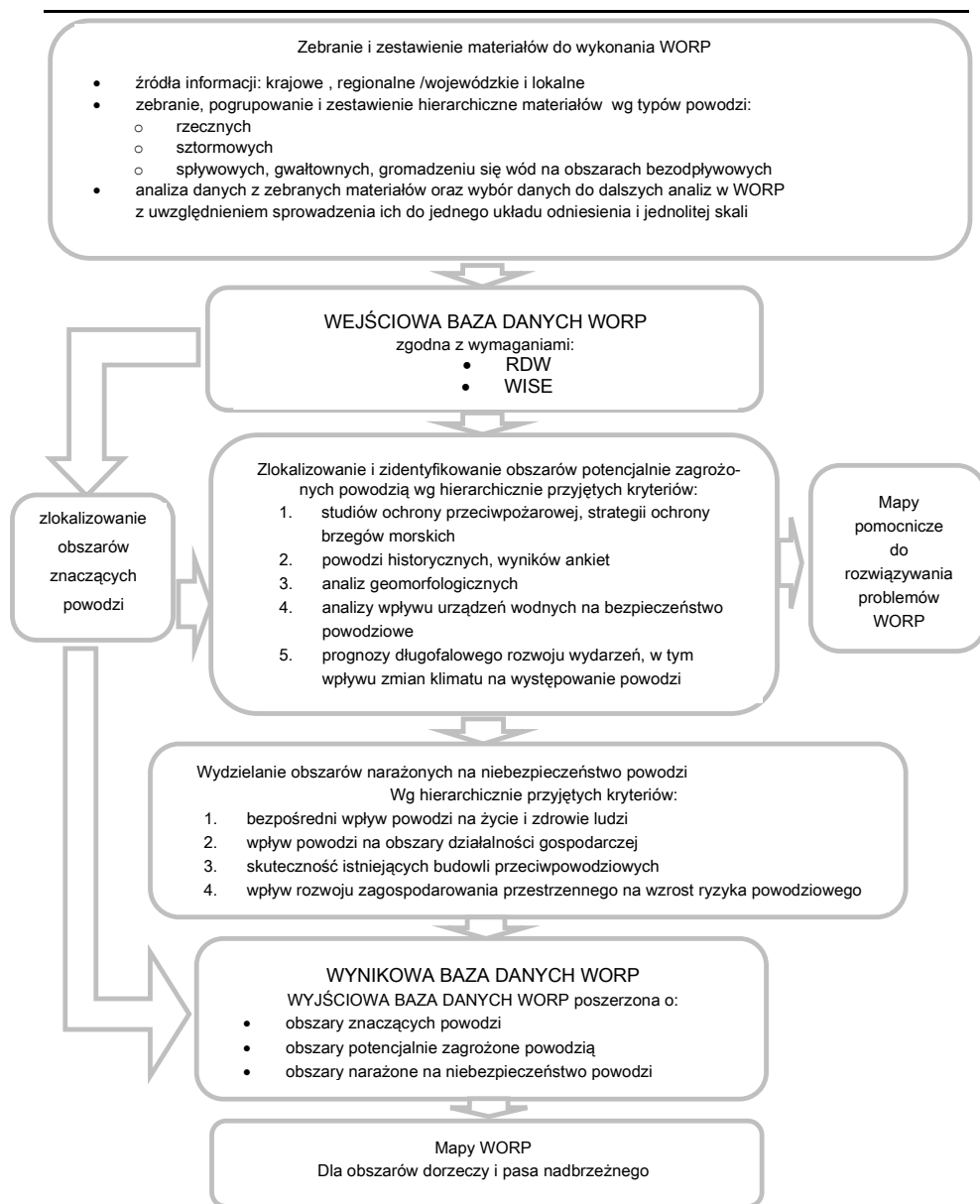
WORP stanowi jedynie materiał poglądowy, niewymagający danych o wysokiej dokładności, dlatego też do jego przygotowania wykorzystano dane powszechnie dostępne. W trakcie tego etapu dokonano analizy ponad 250 rzek o łącznej długości ponad 15 tys. km. Na mapie kolorem czerwonym zaznaczono obszary narażone na niebezpieczeństwo powodzi. Wyłonienie powyższych procesów pozwoliło na przygotowanie algorytmu dla wstępnej oceny (patrz rys. 52).

⁴⁶⁶ 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.

⁴⁶⁷ *Raport z wykonania wstępnej oceny ryzyka powodziowego*, KZWG, Warszawa 2011, s. 4.

⁴⁶⁸ Tamże, s. 8.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP



Rys. 52. Algorytm opracowania wstępnej oceny ryzyka powodziowego⁴⁶⁹

⁴⁶⁹ Źródło: *Raport z wykonania wstępnej oceny ryzyka powodziowego*, KZWG, Warszawa 2011, s. 9.

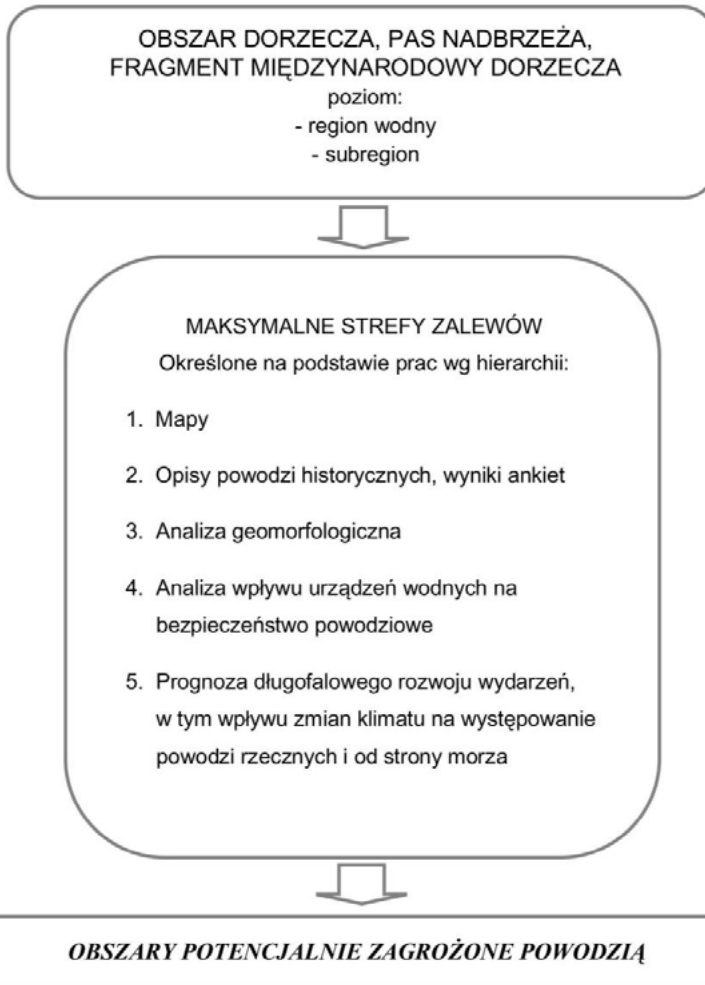
Obszary dorzeczy definiuje się jako tereny, z których wody powierzchniowe spływają do określonej rzeki lub jej dopływów. W Polsce występują dorzecza Wisły, Odry, Niemna oraz rzek pobrzeża bałtyckiego⁴⁷⁰. I właśnie dla obszarów dorzeczy prezes Krajowego Zarządu Gospodarki Wodnej, zgodnie z art. 88c, opracowuje wstępną ocenę ryzyka powodziowego, która zawiera mapy obszarów dorzeczy⁴⁷¹, 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 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 prezes Krajowego Zarządu Gospodarki Wodnej przedkłada dyrektorowi Rządowego Centrum Bezpieczeństwa. Omawiany dokument podlega przeglądowi co 6 lat, a także w razie potrzeby aktualizacji⁴⁷².

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. 53.

⁴⁷⁰ Art. 3 ust. 2 ustawy Prawo wodne.

⁴⁷¹ Mapy obszarów dorzeczy przedstawiają granice dorzeczy, granice zlewni, granice pasa nadbrzeżnego oraz topografię terenu wraz z jego zagospodarowaniem.

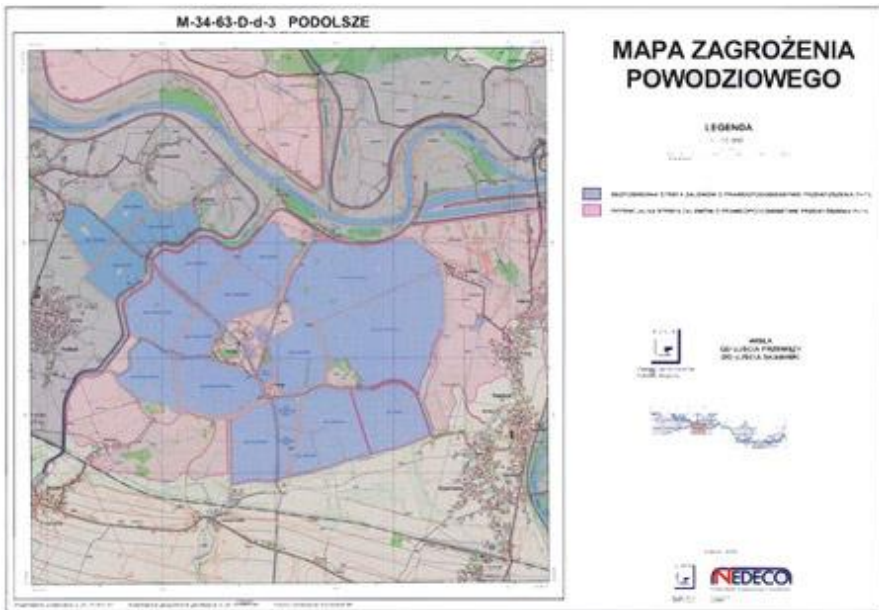
⁴⁷² Art. 88c ust. 8-9 ustawy Prawo wodne.



Rys. 53. Schemat blokowy lokalizacji i identyfikacji obszarów potencjalnie zagrożonych powodzią⁴⁷³

W przypadku obszarów narażonych na niebezpieczeństwo wystąpienia powodzi wymienionych we wstępnej ocenie ryzyka powodziowego konieczne jest sporządzenie mapy zagrożenia powodziowego, zgodnie z art. 88d.

⁴⁷³ Źródło: Raport z wykonania wstępnej oceny ryzyka powodziowego, KZWG, Warszawa 2011, s. 13.



Rys. 54. Przykładowa mapa zagrożenia powodziowego – Podolsze⁴⁷⁴

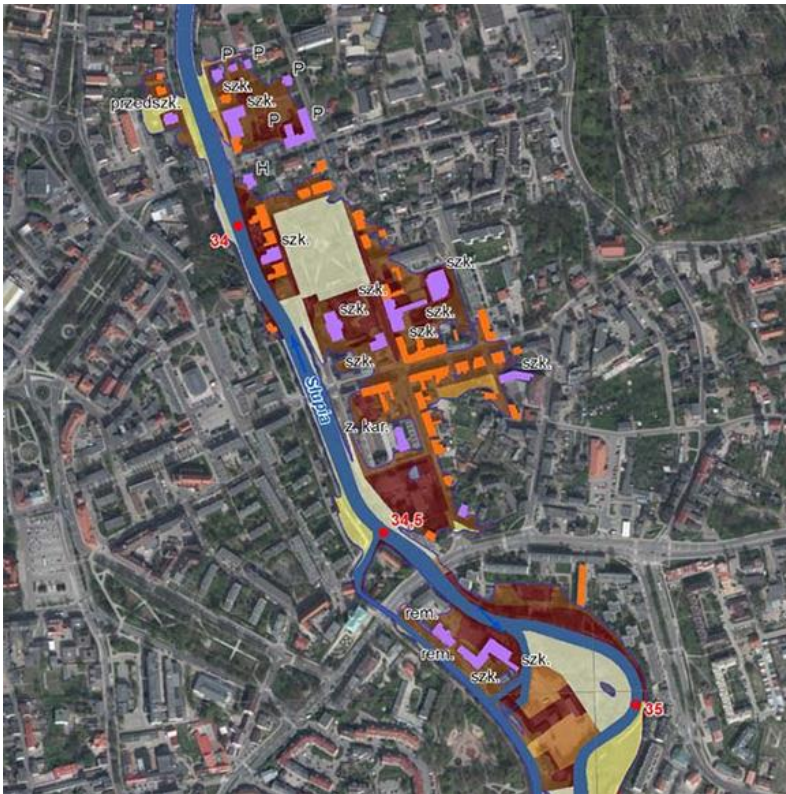
Zamieszczone w niej informacje dotyczą obszarów, gdzie prawdopodobieństwo wystąpienia powodzi jest niskie (raz na 500 lat), obszarów szczególnego zagrożenia powodzią, terenów narażonych na zalanie w razie przelania się wód przez koronę wału przeciwpowodziowego, a także jego zniszczenia lub uszkodzenia, 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 natężenie⁴⁷⁵. Kolorem niebieskim zaznaczono tereny bezpośredniego zagrożenia powodzią, natomiast fioletowym zalania potencjalnego. Obszary te, zgodnie z art. 84 ustawy Prawo wodne, uwzględnia się przy sporządzaniu planu zagospodarowania przestrzennego województwa, studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy, miejscowego planu zagospodarowania przestrzennego oraz

⁴⁷⁴ <http://geoforum.pl/?page=news&id=9007&link=trwaja-prace-nad-mapami-zagrozenia-powodziowego&menu=46815,46847>, fot. OKI Kraków, dostęp: styczeń 2015.

⁴⁷⁵ Art. 88d ustawy Prawo wodne.

decyzji o lokalizacji inwestycji celu publicznego oraz decyzji o warunkach zabudowy.

Dla obszarów szczególnego zagrożenia powodzią dodatkowo sporządza się **mapę ryzyka powodziowego**, z danymi zawierającymi szacunkową liczbę mieszkańców oraz rodzaje działalności gospodarczej⁴⁷⁶. Dane te gromadzi się przede wszystkim na potrzeby ewakuacji (rys. 55).



Rys. 55. Fragment mapy ryzyka powodziowego – negatywne konsekwencje dla ludności i wartość potencjalnych strat powodziowych⁴⁷⁷

Jako granicę terenów zurbanizowanych przyjęto granice działek usługowych, produkcyjnych i zabudowy mieszkaniowej oraz zasięg zabudowy dla zabudowy

⁴⁷⁶ Art. 88e ustawy Prawo wodne.

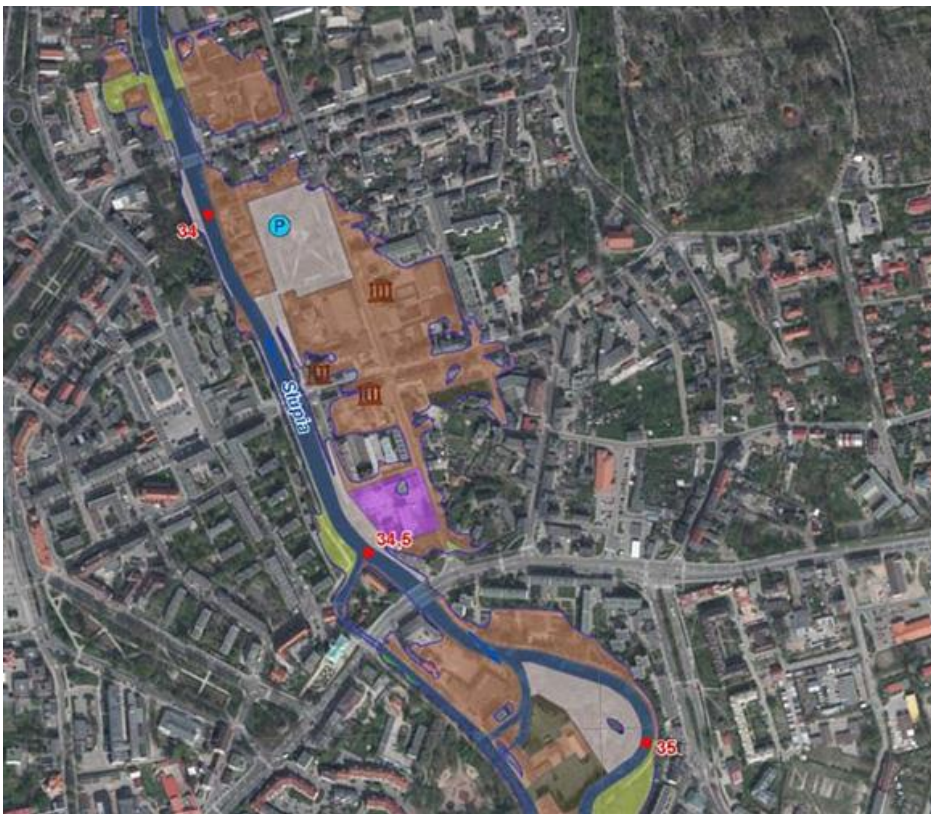
⁴⁷⁷ <http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego>, dostęp: styczeń 2015.

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/mieszkańca (średnia dla Polski $24m^2/osobę$)⁴⁷⁸. 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.

Mapy ryzyka powodziowego prezentują także negatywne konsekwencje dla środowiska, dziedzictwa kulturowego i działalności gospodarczej (rys. 56). 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)⁴⁷⁹.

⁴⁷⁸ T. Majda, P. Wałdykowski, J. Adamczyk, M. Grygoruk, *Typologia terenów narażonych na niebezpieczeństwo powodzi*, TUP, Warszawa 2012, s. 49.

⁴⁷⁹ Art. 88e ust. 2 ustawy Prawo wodne.



Rys. 56. Fragment mapy ryzyka powodziowego – negatywne konsekwencje dla środowiska, dziedzictwa kulturowego i działalności gospodarczej⁴⁸⁰

Przedstawione powyżej mapy sporządza prezes Krajowego Zarządu Gospodarki Wodnej, natomiast część opracowania, w zakresie map od strony morza, w tym morskich wód wewnętrznych, zlecane są do opracowania dyrektorom urzędów morskich. Gotowe mapy zagrożenia powodziowego i ryzyka powodziowego prezes KZGW, zgodnie z art. 88f, wydaje dyrektorom regionalnych zarządów gospodarki wodnej, głównemu geodecie kraju, głównemu inspektorowi ochrony środowiska oraz dyrektorowi Rządowego Centrum Bezpieczeństwa. Opracowane mapy przekazywane są ponadto właściwym wojewodom, marszałkom, starostom, wójtom (burmistrzom, prezydentom miast) oraz ko-

⁴⁸⁰ <http://www.isok.gov.pl/pl/mapy-zagrozenia-powodziowego-i-mapy-ryzyka-powodziowego>, dostęp: styczeń 2015.

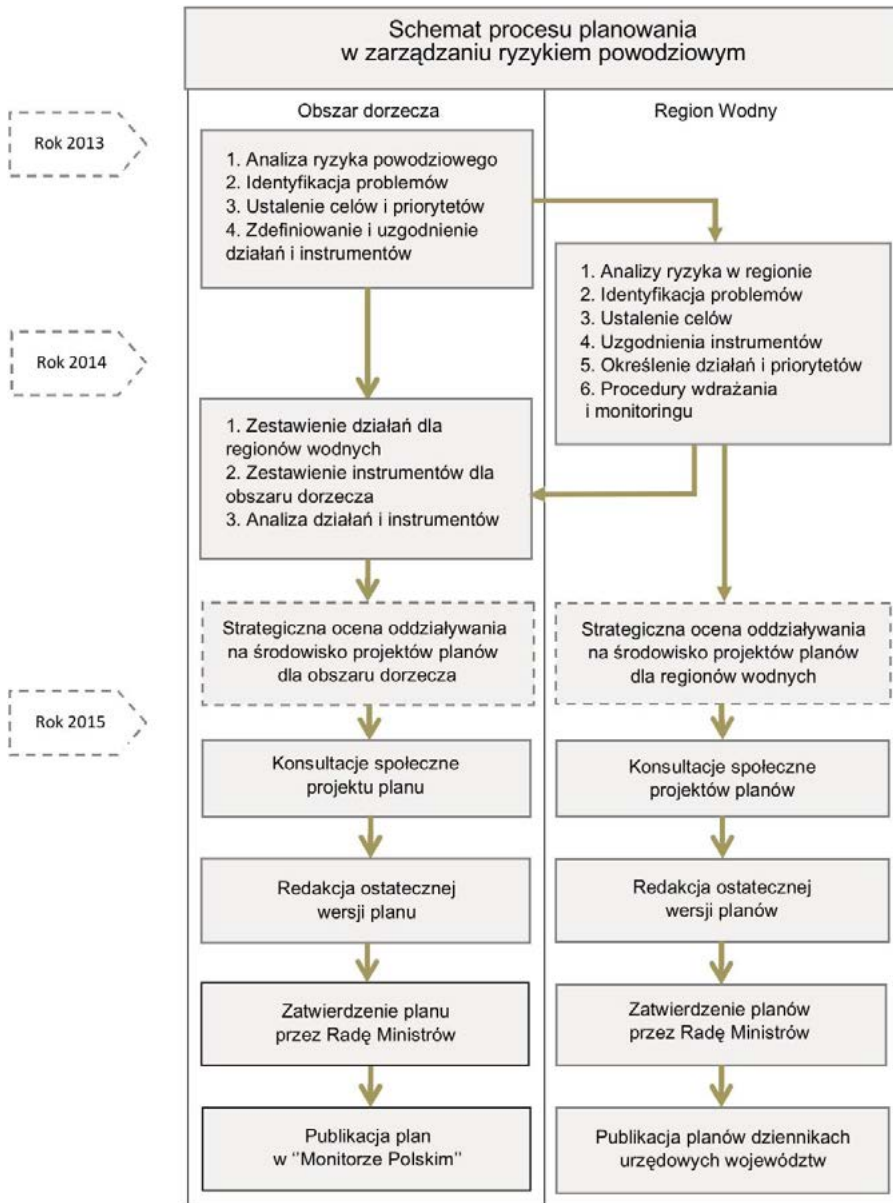
mentantom wojewódzkim i powiatowym (miejskim) Państwowej Straży Pożarnej, a także dyrektorom urzędów żeglugi śródlądowej. Mapy zagrożenia powodziowego oraz ryzyka powodziowego mogą być wykorzystywane na potrzeby zagospodarowania przestrzennego.

3.3. Plany zarządzania ryzykiem powodziowym

Powyżej wskazane 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 priorytetu⁴⁸¹. W przypadku planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy dokumenty te przygotowywane są przez prezesa Krajowego Zarządu Gospodarki Wodnej we współpracy z ministrem infrastruktury i rozwoju. Plany dla regionów wodnych opracowują dyrektorzy regionalnych zarządów gospodarki wodnej. Przedstawione plany podlegają przeglądowi w celu aktualizacji co 6 lat.

W 2011 r. KZGW przygotował dokument pod nazwą *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*. Zgodnie z nią proces planowania powinien przebiegać w następujący sposób:

⁴⁸¹ Art. 88g pkt 2 ustawy z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. nr 115, poz. 1229).



Rys. 57. Schemat procesu planowania w zarządzaniu ryzykiem powodziowym⁴⁸²

⁴⁸² Źródło: *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, KZGW, Warszawa 2011, s. 13.

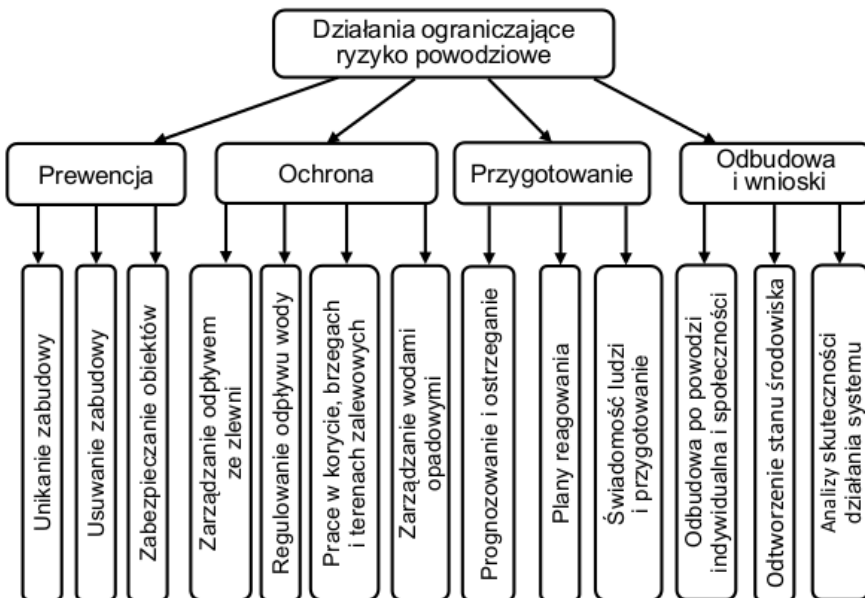
Metodyka zakłada, że strukturę planu powinny tworzyć następujące elementy:

1. streszczenie w języku nietechnicznym,
2. wprowadzenie – cele i zakres planu, podstawy prawne, relacje PZRP z innymi dokumentami,
3. opis obszaru planowania – topografia, hydrografia, gleby, geologia, hydrologia, charakter zagrożenia powodziowego w zlewni, użytkowanie terenu,
4. partnerzy procesu planowania i zasady udziału społecznego – analiza interesariuszy, zarządzanie procesem planowania, zasady udziału społecznego,
5. podsumowanie wstępnej oceny ryzyka powodziowego,
6. ocena zagrożenia powodziowego – wnioski z analiz map zagrożenia powodziowego, dodatkowe analizy, podsumowanie,
7. ocena ryzyka powodziowego – wnioski z analiz map ryzyka powodziowego, dodatkowe analizy, podsumowanie,
8. uwzględnienie wpływu zmian klimatu na ryzyko powodziowe,
9. analiza obecnego systemu zarządzania ryzykiem powodziowym,
10. cele zarządzania ryzykiem powodziowym – analiza problemów zarządzania ryzykiem powodziowym i wnioski, cele zarządzania ryzykiem powodziowym,
11. 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),
12. opis zakresu i sposobu koordynacji z ramową dyrektywą wodną,
13. podsumowanie strategicznej oceny oddziaływania na środowisko,
14. podsumowanie procesu konsultacji społecznych i informowania społeczeństwa – konsultacje społeczne, informowanie ogółu społeczeństwa,
15. opis zakresu i sposobu współpracy międzynarodowej,
16. sposób monitorowania postępów realizacji planu zarządzania ryzykiem powodziowym,
17. literatura/źródła.

Plan powinien także zawierać załączniki:

1. listę skrótów,
2. słownik pojęć,
3. listę interesariuszy,
4. katalog celów,
5. katalog działań,
6. wstępną ocenę ryzyka powodziowego,
7. mapy zagrożenia powodziowego,
8. mapy ryzyka powodziowego,
9. materiały dokumentujące proces konsultacji i udziału społecznego,
10. 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 je następująco:



Rys. 58. Struktura działań ograniczających ryzyko powodziowe⁴⁸³

⁴⁸³ Źródło: *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, KZGW, Warszawa 2011, s. 40.

Według tej klasyfikacji sporządzony został katalog działań podstawowych, czyli takich, które bezpośrednio wpływają na wielkość ryzyka powodziowego⁴⁸⁴.

W związku z tym, że zarządzanie ryzykiem powodziowym nie dotyczy działalności prowadzonej przez konkretną organizację i jej otoczenie, a wynika z prawa europejskiego⁴⁸⁵ 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.

⁴⁸⁴ *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, KZGW, Warszawa 2011, s. 40.

⁴⁸⁵ Komisja Europejska przygotowała w latach 200-2007 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 poprzez 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 jednostki⁴⁸⁶. Tym bardziej nie powinna dziwić tak szeroka kwalifikacja kontroli zarządczej w rozdziale 6 działu I ustawy⁴⁸⁷. W rozdziale tym zdefiniowano kontrolę zarządczą oraz sprecyzowano cele, które ma spełniać. A należą do nich:

1. zapewnienie zgodności prowadzonej działalności z przepisami prawa oraz procedurami wewnętrznymi,
2. skuteczność i efektywność działania,
3. wiarygodność sprawozdań,
4. ochrona zasobów,
5. przestrzeganie i promowanie zasad etycznego postępowania,
6. efektywność i skuteczność przepływu informacji,
7. **zarządzanie ryzykiem**⁴⁸⁸.

Załącznik do komunikatu nr 6 ministra finansów z dnia 6 grudnia 2012 r. tylko potwierdza powyższy fakt, 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*⁴⁸⁹. Przywołana defini-

⁴⁸⁶ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 197.

⁴⁸⁷ D. Wróblewski (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 95.

⁴⁸⁸ Art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. nr 157, poz. 1240, z późn. zm.).

⁴⁸⁹ 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).

cja 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 organizacji w odniesieniu do ryzyka, które stanowi wpływ niepewności na cele*.

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 zaakceptować⁴⁹⁰. Co istotne, z punktu widzenia niniejszej publikacji oraz przedstawianych w rozdziale rozważań do podmiotów odpowiedzialnych za sprawne wdrożenie i funkcjonowanie kontroli zarządczej należą: wójt, burmistrz, prezydent miasta, przewodniczący zarządu jednostki samorządu terytorialnego⁴⁹¹, jak również ministrowie i kierownicy jednostek i urzędów centralnych – organy wiodące bądź pełniące znaczące funkcje w systemie zarządzania kryzysowego. Ponadto, jako organizatorzy kontroli zarządczej w swoich jednostkach, przekazują w tym zakresie uprawnienia do swoich pracowników. Należy więc domniemywać, że w jednostkach tych istnieją i są sędowane na pracowników kompetencje w zakresie zarządzania ryzykiem⁴⁹², ponieważ dokonują oni identyfikacji i analizy ryzyka⁴⁹³, 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.

⁴⁹⁰ 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).

⁴⁹¹ Art. 69 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. nr 157, poz. 1240, z późn. zm.).

⁴⁹² Patrz szerzej: D. Wróblewski (red. nauk.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego*, CNBOP-PIB, Józefów 2014, s. 25-29.

⁴⁹³ A w jednostkach również opisanych w niniejszym rozdziale nawet pełny proces oceny ryzyka oraz w ograniczonym zakresie inne etapy procesu 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 kontekstu⁴⁹⁴, identyfikacji⁴⁹⁵, analizy⁴⁹⁶, oceny⁴⁹⁷, działania, nadzoru oraz informowania o ryzyku w sposób, który umożliwi organizacji minimalizację strat i maksymalizację możliwości”⁴⁹⁸.

W praktyce przekłada się to na:

1. możliwie najszybszą identyfikację ryzyka związanego z działaniem operacyjnym, ocenę stopnia wpływu ryzyka na wyniki lub cele organizacji oraz zastosowanie odpowiednich środków kontroli ryzyka,
2. upewnienie się, że środki kontroli stosowane przez organizację do zarządzania ryzykiem będą skuteczne⁴⁹⁹.

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.⁵⁰⁰. Przepisy te nie precyzują, w jaki sposób ocena ryzyka⁵⁰¹ 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 Administracji i Cyfryzacji, Ministerstwie

⁴⁹⁴ Patrz: definicja na s. 31.

⁴⁹⁵ Patrz: definicja na s. 27.

⁴⁹⁶ Patrz: definicja na s. 29.

⁴⁹⁷ Patrz: definicja na s. 37 (ewaluacja ryzyka).

⁴⁹⁸ Norma AS/NZS 4360:1999 *Risk Management*.

⁴⁹⁹ *Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce*, wyd. Bentley Dennison, Warszawa 2007, s. 8.

⁵⁰⁰ Rozdział 6 ustawy o finansach publicznych z dnia 27 sierpnia 2009 r. (Dz.U. nr 157, poz. 1240) – Kontrola zarządcza oraz koordynacja kontroli zarządczej w jednostkach sektora finansów publicznych.

⁵⁰¹ Patrz: definicja na s. 29.

Spraw Wewnętrznych, Ministerstwie Spraw Zagranicznych oraz w Wyższym Urzędzie Górniczym i to właśnie na nich w głównym stopniu oparto analizę metody 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:

1. zarządzenie nr 13 prezesa Wyższego Urzędu Górniczego z dnia 5 lipca 2013 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych,
2. zarządzenie nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych,
3. zarządzenie nr 4 ministra spraw zagranicznych z dnia 5 stycznia 2015 r. zmieniające zarządzenie w sprawie zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych,
4. zarządzenie nr 25 ministra administracji i cyfryzacji z dnia 31 grudnia 2013 r. w sprawie wprowadzenia *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*,
5. zarządzenie nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

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: osiągnięcie celów i realizacji priorytetów strategicznych, poprawa jakości zarządzania w całej strukturze WUG oraz

doskonalenie procesów wewnętrznych poprzez optymalne wykorzystanie posiadanych zasobów⁵⁰².

Odpowiedzialność za prawidłowe funkcjonowanie zarządzania ryzykiem w poddanych analizie jednostkach ponosi najwyższe kierownictwo. We wszystkich powołano jednak właściciela ryzyka⁵⁰³, który odpowiada na danym poziomie za monitorowanie ryzyka⁵⁰⁴. 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 ryzykiem^{505, 506}. Jeszcze inny zakres uprawnień ma właściciel ryzyka w MAiC, który może powołać zespół w razie potrzeby oszacowania ryzyka bądź przygotowania planów postępowania z ryzykiem⁵⁰⁷.

W MSW natomiast w celu zapewnienia wsparcia dla właścicieli ryzyk oraz prawidłowości realizacji procesu zarządzania ryzykiem minister może powołać zespół konsultacyjny do spraw ryzyka. W skład zespołu wchodzi pracownicy ministerstwa, jednostek, jak również inne wskazane osoby spoza ministerstwa lub jednostek. Przewodniczącego zespołu wyznacza minister, określając jednocześnie kompetencje przewodniczącego oraz przysługujące mu uprawnienia odpowiednio wobec komórek organizacyjnych i jednostek. W przypadku nieprawidłowości w ocenie ryzyka i postępowaniu z ryzykiem zespół proponuje niezbędne działania korekcyjne⁵⁰⁸ – rekomenduje się w tym przypadku odpowiednio: działania zapobiegawcze i działania korygujące⁵⁰⁹.

⁵⁰² § 1 zarządzenia 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 nr 24).

⁵⁰³ Patrz: definicja na s. 32.

⁵⁰⁴ Patrz: definicja na s. 37.

⁵⁰⁵ Patrz: definicja na s. 28.

⁵⁰⁶ § 2 zarządzenia 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 nr 24).

⁵⁰⁷ § 6 załącznika nr 1 do zarządzenia nr 25 ministra administracji i cyfryzacji z dnia 31 grudnia 2014 r. w sprawie wprowadzenia *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

⁵⁰⁸ § 18 zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁰⁹ Działania zapobiegawcze – działania w celu wyeliminowania przyczyny potencjalnej niezgodności lub innej potencjalnej sytuacji niepożądaney. Działania korygujące – działania w celu

W MSZ powołany jest natomiast 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 ryzyk⁵¹⁰ oraz planowanych działań zapobiegawczych w zakresie zgodności z zasadami wynikającymi z przepisów zarządzenia, adekwatności działań zapobiegawczych do zadań realizowanych przez właścicieli ryzyka oraz zgodności wykazu ryzyk i działań zapobiegawczych z najważniejszymi celami i zadaniami ministra spraw zagranicznych. Komitet przygotowuje także informacji na temat procesu zarządzania ryzykiem w ministerstwie i placówkach zagranicznych⁵¹¹.

Dyrektor generalny, na wniosek przewodniczącego komitetu, powołuje w drodze decyzji skład osobowy komitetu spośród dyrektorów albo zastępców dyrektorów komórek organizacyjnych ministerstwa, a właścicielem ryzyka, który odpowiada za zarządzanie ryzykiem, jest dyrektor komórki organizacyjnej lub kierownik placówki zagranicznej⁵¹².

Zarządzeniem nr 4 z dnia 5 stycznia 2015 r. minister spraw zagranicznych powołał pełnomocnika do spraw kontroli zarządczej i procedur antykorupcyjnych, który koordynuje w jego imieniu proces zarządzania ryzykiem w działach

wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanego sytuacji. Źródło: PN-EN ISO 9000:2006 *Systemy zarządzania jakością. Podstawy i terminologia*, definicja 3.6.4 i 3.6.5.

⁵¹⁰ Należy rozumieć jako rejestr ryzyk zgodnie z normą ISO 31000.

⁵¹¹ § 5 zarządzenia nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych.

⁵¹² Tamże, § 8.

administracji rządowej kierowanych przez ministra spraw zagranicznych oraz zapewnią obsługę prac komitetu⁵¹³.

Każdy pracownik komórki organizacyjnej lub placówki zagranicznej ma obowiązek zgłaszać ryzyka w odniesieniu do celów i zadań oraz sporządzać wykaz według wzoru do zarządzenia (załącznik nr 1). W przypadku zgłaszania zmian zidentyfikowanych ryzyk po akceptacji komitetu ryzyka podlegają procedurze określonej w zarządzeniu⁵¹⁴.

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 przeglądu⁵¹⁵. Cztery kompleksowo opracowane zarządzeniach (MAiC, MSW, MSZ i WUG) dotyczące zarządzania ryzykiem zawierają wyżej wymienione etapy bądź realizują je wybiórczo.

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. Dlatego też najczęściej korzysta się z kombinacji kilku metod (kwestionariuszy i burzy mózgów).

Identyfikację ryzyka w MAiC przeprowadza się z wykorzystaniem załącznika nr 2 do *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji* w odniesieniu do zdefiniowanych na poziomie strategicznym obszarów działania istotnych dla osiągnięcia celów operacyjnych⁵¹⁶. Zidentyfikowane ryzyko przyporządkowane jest do określonej poniżej kategorii ryzyka:

⁵¹³ § 9 zarządzenia nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych.

⁵¹⁴ Tamże, § 10.

⁵¹⁵ Patrz: definicja na s. 37.

⁵¹⁶ Patrz: definicja na s. 26.

1. zarządzanie,
2. finanse,
3. bezpieczeństwo,
4. czynniki zewnętrzne,
5. przepisy i procedury,
6. działalność operacyjna⁵¹⁷.

Tabela 54. Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałania ryzykom związanym z osiągnięciem celów⁵¹⁸

Określenie ryzyka dla celów/zadań ujętych w planie działalności komórki organizacyjnej											Reakcja na ryzyko ⁵¹⁹
L.p.	cel ogólny	cel szczegółowy/ zadanie	obszar działania ⁵²⁰	kategoria ryzyka	opis ryzyka ⁵²¹	prawdopodobieństwo	skutek ⁵²²	istotność ryzyka ⁵²³	priorityet Mini-stra	właściciel ryzyka	przyjęta metoda przeciwdziałania ryzyku (mechanizm kontroli wewnętrznej) ⁷
1.											
2.											

W MSZ brak szczegółowo opisanej procedury identyfikacji ryzyka. Dokonywana jest w odniesieniu do celów i zadań określonych w *Planie działalności ministra spraw zagranicznych*, którego integralnym elementem jest wykaz ryzyk zgodny ze wzorem w załączniku nr 1 do zarządzenia⁵²⁴. Pracownicy wszystkich komórek są zobowiązani do przekazywania przełożonym informacji na temat zidentyfikowanego ryzyka, które może wpływać na cele jednostki.

⁵¹⁷ § 8 *Polityka zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

⁵¹⁸ Załącznik nr 2 do *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

⁵¹⁹ Należy rozumieć jako postępowanie z ryzykiem zgodnie z ISO 31000.

⁵²⁰ Obszar działania dotyczy obszaru wyodrębnionego spośród działalności MAiC, np. legislacja.

⁵²¹ Opis zidentyfikowanego ryzyka.

⁵²² Skutek należy rozumieć jako konsekwencje zgodnie z normą ISO 31000.

⁵²³ Autorzy zarządzenia określili pod pojęciem iloczyn prawdopodobieństwa i skutku – w nomenklaturze normy ISO 31000 oznacza ryzyko (obliczeniowe).

⁵²⁴ § 10 zarządzenie nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych.

Tabela 55. Wykaz ryzyk i działań zapobiegawczych do planu działalności ministra spraw zagranicznych na rok ...⁵²⁵

Numer identyfikacyjny ryzyka	Cel	Zadanie	Ryzyko	Przyczyna wystąpienia ryzyka	Skutek wystąpienia ryzyka	Funkcjonujące mechanizmy kontrole	Prawdopodobieństwo (w pkt)	Istotność oddziaływania ⁵²⁶ (w pkt)	Punktowa ocena ryzyka ⁵²⁷ (kol. 8 x 9)	Akceptacja ryzyka ⁵²⁸ tak/nie	Postępowanie z ryzykiem	Właściciel ryzyka
1	2	3	4	5	6	7	8	9	10	11	12	13
Wymagane działania zapobiegawcze									Data wykonania			

Również w MSW wyniki przeprowadzonej identyfikacji ryzyka odnotowuje się w zbiorczym arkuszu całej oceny ryzyka (załącznik nr 3 do zarządzenia) w odniesieniu do konkretnego celu i zadania jednostki.

⁵²⁵ Załącznik 1 do zarządzenia nr 42 ministra spraw zagranicznych (...).

⁵²⁶ Należy rozumieć jako konsekwencje zgodnie z ISO 31000.

⁵²⁷ Należy rozumieć jako poziom ryzyka zgodnie z ISO 31000.

⁵²⁸ Akceptacja ryzyka (ang. *risk acceptance*) – świadoma decyzja o gotowości organizacji do narażenia się na dane ryzyko. Źródło: ISO Guide 73:2009 *Risk Management – Vocabulary*, definicja 3.7.1.6.

Tabela 56. Arkusz oceny⁵²⁹

Cel	Za- danie	Identyfikacja ryzyka			Analiza ryzyka			Ewalua- cja ryzy- ka (7)	Postępo- wanie z ryzykiem (8)
		zdarze- nie (1)	następ- stwo ⁵³⁰ (2) (N)	prawdo- podo- bieństwo (3) (P)	oce- na ⁵³¹ (N) (4)	oce- na ⁵³² (P) (5)	poziom ryzyka = N x P (6)		

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 planowania⁵³³.

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 wpływu⁵³⁴, natomiast w MSZ prawdopodobieństwo oraz wpływ składają z pięciu poziomów. Przy ocenie wpływu brane są pod uwagę zarówno skutki

⁵²⁹ Załącznik nr 3 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵³⁰ Następstwo należy rozumieć jako konsekwencje zgodnie z normą ISO 31000.

⁵³¹ W kolumnie wprowadza się punktową ocenę dla konsekwencji.

⁵³² W kolumnie wprowadza się punktową ocenę dla prawdopodobieństwa.

⁵³³ § 10 zarządzenia 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 nr 24).

⁵³⁴ Rozumianego jako określenie konsekwencji dla realizowanych celów i zadań.

finansowe, jak i niefinansowe. Poziom ryzyka⁵³⁵ mierzy się, mnożąc wartości prawdopodobieństwa wystąpienia zdarzenia oraz jego ewentualnego skutku⁵³⁶.

Tabela 57. Matryca istotności ryzyka⁵³⁷

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

W MSW wsparciem dla urzędnika w merytorycznym uzupełnieniu arkusza oceny (przedstawionego w tabeli 56) 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.

Arkusz oceny określa⁵³⁸:

1. Zdarzenie – wystąpienie lub zmiana konkretnego zestawu okoliczności.
2. Następstwo – konsekwencje, rezultat zdarzenia mający wpływ na cele. Następstwa powinno zostać ocenione w skali od 1 do 5 (tabela 58).
3. Prawdopodobieństwo – możliwość, szansa wystąpienia zdarzenia. Oceniając prawdopodobieństwo należy przeanalizować:
 - a. środek kontroli – wszystko, co modyfikuje ryzyko (działanie lub rozwiązanie, w szczególności organizacyjne lub techniczne, które

⁵³⁵ Patrz: definicja na s. 32.

⁵³⁶ § 12 zarządzenia nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych (Dz.Ur. MSZ nr 9, poz. 72).

§ 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 (Dz.Ur. WUG nr 24).

⁵³⁷ § 10 ust. 2 załącznika 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 (Dz.Ur. WUG nr 24).

⁵³⁸ Załącznik nr 3 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

- ogranicza prawdopodobieństwo wystąpienia zdarzenia lub minimalizuje jego negatywne następstwa oraz daje racjonalne zapewnienie osiągnięcia celów),
- b. podatność⁵³⁹ – słabość lub wrażliwość, która tworzy pozytywne środowisko do wystąpienia zagrożenia,
 - c. dane historyczne – informacje o występowaniu zdarzenia w przeszłości.
4. Prawdopodobieństwo powinno zostać ocenione w skali od 1 do 5 (tabela 59).
 5. 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)⁵⁴⁰ (tabela 60).
 6. Ewaluację ryzyka.
 7. Postępowanie z ryzykiem.

Tabela 58. Ocena następstw ryzyka⁵⁴¹

Poziom	Ocena (N)	Czynniki oceny następstw			
		finansowe	organizacyjne	zdrowie i bezpieczeństwo ludzkie	reputacja (zaufanie i wizerunek)
1	nieznaczne	nieznaczna strata	krótkotrwałe zakłócenia w działalności	nieznaczne obrażenia	nieznaczne pogorszenie reputacji
2	małe	mała strata	niewielkie zakłócenia w działalności	niewielkie obrażenia	małe pogorszenie reputacji
3	średnie	średnia strata	zakłócenia w działalności	poważne obrażenia	średnie pogorszenie reputacji

⁵³⁹ Por.: definicja na s. 130.

⁵⁴⁰ Załącznik nr 3 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁴¹ Tamże.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

4	poważne	poważna strata	częściowy brak realizacji celu	poważne i trwałe obrażenia	poważne pogorszenie reputacji
5	katastrofalne	katastrofalna strata	brak realizacji celu	utrata życia	poważne i długotrwałe pogorszenie reputacji

Tabela 59. Ocena prawdopodobieństwa ryzyka⁵⁴²

Ocena (P)	Środek kontroli	Podatność	Dane historyczne
1	w pełni skuteczne	brak podatności	nie wystąpiło
2	skuteczne	nieistotna podatność	jednostkowe wystąpienia
3	skuteczne, ale nie pełne	kilka nieistotnych podatności	wystąpienia
4	nieliczne	istotna podatność	częste wystąpienia
5	brak	kilka istotnych podatności	bardzo częste wystąpienia

Tabela 60. Poziom ryzyka wyrażony jest w postaci kombinacji następstw oraz ich prawdopodobieństwa

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

Po określeniu celów, obszarów działania, zadań, kategorii ryzyka i przypisaniu do nich czynników ryzyka⁵⁴³ zidentyfikowane w MAiC ryzyko podlega analizie mającej na celu oszacowanie wpływu, tj. prawdopodobieństwa wystąpienia

⁵⁴² Załącznik nr 3 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁴³ Patrz: definicja na s. 244.

ryzyka, a także ocenie skutku wystąpienia danego zdarzenia⁵⁴⁴. Na potrzeby szacowania ryzyka⁵⁴⁵ pod uwagę brane są uwarunkowania, okoliczności wpływające na prawdopodobieństwo i skutki. Wykorzystywana jest metoda punktowa (zakres od 1 do 5 dla prawdopodobieństwa i skutków), zaleca się również uwzględnianie poziomu wdrożenia i skuteczności dotychczasowych mechanizmów kontroli. Brane są także pod uwagę skutki finansowe i pozafinansowe⁵⁴⁶.

Tabela 61. Prawdopodobieństwo wystąpienia zagrożenia⁵⁴⁷

Prawdopodobieństwo wystąpienia zagrożenia		
Ocena	Punkty	Opis
rzadkie	1	istnieją uzasadnione powody, by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz lub nie zdarzy się w ciągu roku
mało prawdopodobne	2	istnieją uzasadnione powody, by sądzić, że zdarzenie objęte ryzykiem zdarzy się dwa lub trzy razy w ciągu roku
możliwe	3	istnieją uzasadnione powody, by sądzić, że zdarzenie objęte ryzykiem zdarzy się kilkakrotnie w ciągu roku
prawdopodobne	4	istnieją uzasadnione powody, by sądzić, że zdarzenie objęte ryzykiem zdarzy się więcej niż kilkakrotnie w ciągu roku
prawie pewne	5	istnieją uzasadnione powody, by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku

Tabela 62. Skutek związany z danym zagrożeniem⁵⁴⁸

Skutek związany z danym zagrożeniem		
Ocena	Punkty	Opis
nieznaczny	1	- zdarzenie objęte ryzykiem powoduje nieznaczne zakłócenie lub opóźnienie w wykonywaniu zadań, nie wpływa na wizerunek jednostki - skutki zdarzenia można łatwo usunąć
mały	2	- zdarzenie objęte ryzykiem powoduje małe zakłócenie lub opóźnienie w wykonywaniu zadań, częściowo wpływa na wizerunek jednostki - skutki zdarzenia można usunąć

⁵⁴⁴ § 9 *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

⁵⁴⁵ Patrz: definicja na s. 39.

⁵⁴⁶ § 9 *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

⁵⁴⁷ Tamże.

⁵⁴⁸ Tamże.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

średni	3	- zdarzenie objęte ryzykiem powoduje średnią stratę zasobów, małą stratę finansową, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań i wizerunek jednostki - z wystąpieniem zdarzenia może się wiązać trudny proces przywracania stanu poprzedniego
duży	4	- zdarzenie objęte ryzykiem powoduje poważną stratę zasobów, średnią stratę finansową, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań i wizerunek jednostki - z wystąpieniem zdarzenia wiąże się trudny proces przywracania stanu poprzedniego
krytyczny	5	- zdarzenie objęte ryzykiem powoduje uszczerbek mający krytyczny lub bardzo duży wpływ na realizację kluczowych zadań lub osiągnięcie założonych celów, poważny uszczerbek w jakości wykonywanych zadań, poważną stratę finansową albo niekorzystny wpływ na wizerunek jednostki - z wystąpieniem zdarzenia wiąże się długotrwały i trudny proces przywracania stanu poprzedniego

Istotność ryzyka⁵⁴⁹ określa się również ze skalą punktową od 1 do 25, przy czym liczba 20-25 określa ryzyko bardzo wysokie, a od 1 do 5 ryzyko niskie, będące ryzykiem akceptowalnym⁵⁵⁰.

Tabela 63. Istotność ryzyka⁵⁵¹

Istotność ryzyka	
Ocena	Punkcja
niska	1-5
średnia	6-10
wysoka	12-16
bardzo wysoka	20-25

Tabela 64. Graficzne przedstawienie analizy ryzyka⁵⁵²

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

⁵⁴⁹ Por.: poziom ryzyka – definicja na s. 39.

⁵⁵⁰ § 9 *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

⁵⁵¹ Tamże.

⁵⁵² Tamże.

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 ryzyka⁵⁵³.

Rezultatem sporządzenia hierarchizacji⁵⁵⁴ jest rejestr zawierający uszeregowane zagrożenia, który był brany pod uwagę podczas aktualizacji czy też tworzenia nowych planów. Obecnie zrezygnowano z niego na rzecz planów operacyjnych i planów pracy.

Tabela 65. Rejestr ryzyk⁵⁵⁵

Lp.	Cel lub zadanie zawarte w planie	Ryzyko	Istotność (prawdopodobieństwo x wpływ)	Właściciel	Reakcja	Działania w ramach reakcji	Stan faktyczny
1.							
2.							

⁵⁵³ § 11 ust. 1 pkt 7 zarządzenia nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych (Dz.Urz. MSZ nr 9, poz. 72).

§ 10 ust. 2 zarządzenia 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 nr 24).

⁵⁵⁴ Patrz: definicja na s. 87.

⁵⁵⁵ Załącznik nr 5 do zarządzenia nr 6 prezesa Wyższego Urzędu Górniczego z dnia 1 lutego 2012 r. w sprawie planowania działalności oraz zarządzania ryzykiem w urzędach górniczych.

Analogiczne podejście przyjęto w MSW, jednak kryteria ustalone w tej jednostce prezentują się następująco:

Tabela 66. Ewaluacja ryzyka⁵⁵⁶

Kryteria		Ewaluacja
Poziom	Ryzyko	
1-5	małe	akceptowalne
6-9	średnie	akceptowalne, wymagające decyzji kierownictwa
10-16 oraz gdzie P = 1, N = 5	duże	nieakceptowalne, wymagające decyzji kierownictwa
20-25	bardzo duże	kierownictwa

W MAiC wyniki uzyskane z analizy ryzyka także podlegają dalszej analizie, ale pod kątem możliwości ograniczenia ryzyka na poziomie operacyjnym i strategicznym, a dokument opracowywany i zaakceptowany przez kierownika komórki organizacyjnej oraz koordynatora przekazywany jest do właściwych członków kierownictwa ministerstwa. Po nadaniu priorytetu poszczególnym czynnikom ryzyka minister, stosownie do potrzeb, przedstawia na posiedzeniu kierownictwa ministerstwa informacje o ryzykach, które mogą zagrozić realizacji głównych celów ministerstwa oraz o podjętych i przewidywalnych działaniach zaradczych. Na podstawie arkuszy ewidencyjnych i zawartych w nich danych opracowywane są mapy⁵⁵⁷ ryzyka⁵⁵⁸.

W MAiC zdefiniowano cztery poziomy ryzyka w skali 0%-100% maksymalnego możliwego poziomu ryzyka:

1. **ryzyko niskie** zawiera się w przedziale do 25% – jest to ryzyko akceptowalne, które należy monitorować i w miarę potrzeby kontrolować,
2. **ryzyko średnie** zawiera się w przedziale od 26%-50% – może wywierać poważny wpływ na działalność ministerstwa, powinno być monitorowane, a w razie potrzeby poddane działaniom zaradczym i ewentualnie mechanizmom kontrolnym przez właściciela ryzyka,

⁵⁵⁶ Załącznik nr 3 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁵⁷ Mapy ryzyka w niniejszej publikacji oznaczają mapy przedstawiające potencjalne negatywne skutki zdarzenia, w tym dokumencie należy rozumieć je jako matryce ryzyka.

⁵⁵⁸ § 12 *Polityka zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

3. **ryzyko wysokie** zawiera się w przedziale od 51%-75% – może mieć wpływ na działalność ministerstwa i wymaga wprowadzenia na poziomie operacyjnym działań zaradczych i uzupełnienia wewnętrznych mechanizmów kontrolnych, które ograniczą prawdopodobieństwo wystąpienia ryzyka, a decyzję o akceptacji ryzyka może podjąć tylko minister,
4. **ryzyko bardzo wysokie** mieści się w przedziale od 76%-100% – stanowi poważne zagrożenie dla działalności ministerstwa lub osiągnięcia przez niego celów działania; wymaga natychmiastowego działania, poprzez ciągłe monitorowanie oraz wprowadzenie silnych mechanizmów kontroli⁵⁵⁹.

Postępowanie z ryzykiem

Po dokonanej ocenie ryzyka organizacja musi rozważyć wszystkie możliwe działania służące jego kontroli 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.

Kierownictwo MAiC zobowiązane jest do zaprojektowania mechanizmów ograniczających poziom ryzyka bardzo wysokiego. Ryzyko wysokie i bardzo wysokie stanowi ryzyko kluczowe dla działalności, w odniesieniu do nich podejmuje się działania polegające na: zmniejszeniu poziomu ryzyka do akceptowalnego poprzez zapobieganie, przeniesieniu ryzyka, tolerowaniu ryzyka – w przypadku, gdy koszty podjętych działań mogą przekroczyć przewidywalne korzyści oraz zaprzestanie lub zawieszenie działań rodzących ryzyko. Sposób postępowania wobec zidentyfikowanego ryzyka podejmuje właściciel ryzyka, uwzględniając sytuację oraz wielkość kosztów ograniczenia danego ryzyka. Minister podejmuje decyzję o akceptacji ryzyka na poziomie niskim, średnim i wysokim oraz niepodejmowaniu działań zaradczych⁵⁶⁰.

MSW w zakresie postępowania z ryzykiem przyjmuje analogiczne podejście, jak w pozostałych jednostkach, stosując jednak własne, następujące kryteria:

⁵⁵⁹ Tamże.

⁵⁶⁰ Tamże, § 13.

Tabela 67. Postępowanie z ryzykiem⁵⁶¹

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
20-25	bardzo duże	1. unikanie 2. przeniesienie 3. zapobieganie 4. tolerowanie (wraz z pisemnym uzasadnieniem)

Decyzję dotyczącą postępowania z ryzykiem podejmuje właściciel ryzyka, kierując się celowością, adekwatnością i racjonalnością. 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 zarządzenia⁵⁶².

Tabela 68. Plan postępowania z ryzykiem⁵⁶³

Cel	Zadanie	Zdarzenie	Poziom ryzyka	Postępowania z ryzykiem	Działania	Terminy	Odpowiedzialni	Informacje o realizacji

⁵⁶¹ Załącznik nr 3 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁶² § 19 zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁶³ Załącznik nr 4 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

Zmiany uwarunkowań dotyczących zidentyfikowanych zdarzeń lub spostrzeżenia dotyczące pojawienia się nowych zdarzeń lub czynników, właściciel ryzyka odnotowuje w rejestrze ryzyk. Wzór rejestru ryzyk stanowi załącznik nr 5⁵⁶⁴. Właściciel ryzyka 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 kierownika właściwej komórki nadzorującej⁵⁶⁵.

Tabela 69. Rejestr ryzyk⁵⁶⁶

Cel	Zadanie	Zdarzenie	Informacje o zmaterializowaniu się ryzyka

Monitorowanie i przegląd

W zarządzaniu ryzykiem bardzo ważnym elementem jest monitoring, który powinien obejmować:

1. dokonanie przeglądu w celu określenia, czy ryzyko uległo zmianie,
2. sprawdzenie, czy punktowa ocena ryzyka jest wciąż odpowiednia,
3. zapewnienie skuteczności dotychczasowych mechanizmów kontrolnych,
4. monitorowanie rozwoju uzgodnionych działań w zakresie zarządzania ryzykiem.

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 roku⁵⁶⁷.

⁵⁶⁴ § 20 zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁶⁵ § 21 zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁶⁶ Załącznik nr 5 do zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁶⁷ § 13, § 15 i § 16 zarządzenia nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych (Dz.Urz. MSZ nr 9, poz. 72).

Tabela 70. Informacja na temat procesu zarządzania ryzykiem w roku ... ⁵⁶⁸

Numer identyfikacyjny ryzyka	Właściciel ryzyka	Wymagane działania zapobiegawcze oraz nazwa komórki organizacyjnej /placówki zagranicznej odpowiedzialnej za realizację działania	Stopień realizacji działań zapobiegawczych	Przyczyny braku realizacji działań zapobiegawczych	Uwagi (np. czy ryzyko wystąpiło w roku, którego dotyczy informacja)
1	2	3	4	5	6

Nie rzadziej niż raz na rok koordynator ds. zarządzania ryzykiem przedstawia ministrowi administracji i cyfryzacji informację o zagrożeniach w realizowanych zadaniach obarczonych największym ryzykiem i o podjętych działaniach zaradczych lub przedstawia wstępną propozycję postępowania z ryzykiem w przypadkach, gdy kompetencje do podjęcia działań w tym zakresie należą do ministra. Przekazuje także na bieżąco innym właścicielom obszarów ryzyka informację o tych ryzykach, które wykraczają poza obszar funkcjonowania ministerstwa. Wyniki uzyskane podczas oceny ryzyka wykorzystywane są przez audytora wewnętrznego na etapie przygotowywania rocznego planu audytu wewnętrznego w ministerstwie⁵⁶⁹. Proces monitorowania ryzyka jest procesem ciągłym, realizowanym przez kierownictwo ministerstwa na każdym szczeblu zarządzania i prowadzony jest pod kątem ich adekwatności, efektywności i skuteczności. W ramach monitoringu dokonywany jest przegląd aktualności ryzyk, aktualności przypisanej do ryzyk oceny, a także przegląd mechanizmów kontrolnych i ich skuteczności. Koordynator odpowiada za monitoring na szczeblu

§ 12, § 16, § 17, § 18 zarządzenia 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 r. 24).

⁵⁶⁸ Załącznik nr 5 do zarządzenia nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r.

⁵⁶⁹ § 14 *Polityka zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

strategicznym, natomiast niezależną ocenę zarządzania ryzykiem może przeprowadzić audytor wewnętrzny ministerstwa lub audytorzy zewnętrzni⁵⁷⁰.

Polityka zarządzania ryzykiem wraz z załącznikami podlega corocznym przeglądom, dokonywanym w celu ich aktualizacji. Każda aktualizacja *Polityki* podlega akceptacji ministra⁵⁷¹.

Nadzór nad dokumentowaniem systemu kontroli zarządczej, ciągłości działalności, ochrony zasobów, szczegółowych mechanizmów kontroli dotyczących operacji finansowych, gospodarczych oraz kontroli dotyczących systemów informatycznych sprawuje kierownictwo ministerstwa i kierownicy jednostek. Zobowiązani są do przygotowania dokumentacji systemu kontroli zarządczej, obejmującej wytyczne, regulaminy, procedury, instrukcje i inne dokumenty wewnętrzne właściwe do rodzaju zadań, a także nadzorowania wykonania zadań w celu zapewnienia ich skutecznej, efektywnej, prawidłowej i oszczędnej realizacji⁵⁷². W przypadku zidentyfikowania obszarów krytycznych, dla których niezbędne jest zachowanie ciągłości działania, uwzględniają wyniki oceny ryzyka, a w szczególności takie zdarzenia, których prawdopodobieństwo oceniane jest jako niskie, a następstwa na poziomie katastrofalnym – w takim przypadku należy ustalić w formie udokumentowanej plan ciągłości działania i inne dokumenty określające zapewnienie ciągłości działania w sytuacjach kryzysowych. Szczególnej uwagi wymaga opracowanie szczegółowych mechanizmów kontroli operacji finansowych i gospodarczych, a także mechanizmów zapewniających bezpieczeństwo elektronicznych baz danych i systemów informatycznych⁵⁷³. Za monitorowanie systemu kontroli zarządczej, samoocenę, audyt wewnętrzny i uzyskanie zapewnienia o stanie kontroli zarządczej odpowiada kierownictwo ministerstwa oraz kierownicy jednostek, którzy są także zobowiązani do bieżącego monitorowania i samooceny oraz przeprowadzonych audytów i kontroli⁵⁷⁴.

⁵⁷⁰ Tamże, § 15.

⁵⁷¹ Tamże, § 17.

⁵⁷² § 22 zarządzenia nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.

⁵⁷³ Tamże, § 23.

⁵⁷⁴ Tamże, § 27.

W przypadku analizowanych jednostek szczebla centralnego dokumenty dotyczące oceny ryzyka zostały oparte na strukturze ramowej zaproponowanej w normie ISO 31000 bądź są z nią tożsame. Ponieważ norma ta zawiera ramy, procesy i zasady dotyczące procesu oceny ryzyka mające pomóc w ujednoczeniu procesów zarządzania ryzykiem, zarówno MSW, MAiC, 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. Zawierająca pięć niezbędnych atrybutów opisanych w części pierwszej, została skutecznie zaimplementowana do tych jednostek. Zarówno w MSW, MAiC, 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 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 zarządczej⁵⁷⁵, 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

⁵⁷⁵ Patrz: D. Wróblewski (red. nauk.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego*, CNBOP-PIB, Józefów 2014, s. 24.

w oparciu o nowoczesne technologie informatyczne⁵⁷⁶. W związku z powyższym na szczeblu wojewódzkim przeanalizowanym dokumentem było zarządzenie nr 80 wojewody mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia *Polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie*. Na szczeblu powiatowym analizie poddano zarządzenie nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie. Spośród mazowieckich gmin wybrano Legionowo, gdzie metodykę ujęto w zarządzeniu nr 204/2012 prezydenta miasta Legionowa z dnia 15 października 2012 r. w sprawie zasad zarządzania ryzykiem w Urzędzie Miasta Legionowa.

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 terytorialnym⁵⁷⁷, 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 I *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

⁵⁷⁶ D. Wróblewski (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014, s. 108.

⁵⁷⁷ Tamże.

ukierunkowanie na cele⁵⁷⁸ 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 ryzyka⁵⁷⁹, odpowiedź bądź reakcja na ryzyko oraz raportowanie o ryzyku i jego monitorowanie⁵⁸⁰. Inne rozbieżności wskazanych dokumentów wobec zaleceń normy we wskazanym powyżej zakresie to m.in.: tryb raportowania – kwartalne (województwo), roczne i niezwłoczne⁵⁸¹ (powiat). 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.

Szczebel wojewódzki

Załącznik do zarządzenia⁵⁸² 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, mechanizm kontrolny, czynniki ryzyka, obszar ryzyka, ewaluacja ryzyka, właści-

⁵⁷⁸ Tu rekomenduje się na potrzeby definiowania celów m.in. wykorzystanie metodyki SMART (*Simple, Measurable, Achievable, Relevant, Timely*): prosty (rozumienie 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 dołącznie określony horyzont czasowy, w jakim zamierzamy go osiągnąć).

⁵⁷⁹ Zarządzenie prezydenta m.st. Warszawy zastępuje analizę ryzyka oceną ryzyka, podczas której wyznaczany jest poziom ryzyka.

⁵⁸⁰ D. Wróblewski, B. Połec, *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014, s. 210.

⁵⁸¹ Raportowanie bieżące w razie zaistniałych incydentów.

⁵⁸² Zarządzenie nr 80 wojewody mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia *Polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie*.

ciel ryzyka, ocena ryzyka, analiza ryzyka, prawdopodobieństwo wystąpienia ryzyka, skutek ryzyka czy ryzyko akceptowalne⁵⁸³.

Polityka zarządzania ryzykiem ustalona przez wojewodę wiąże się ściśle z celami kontroli zarządczej. Jest ukierunkowana na zwiększenie prawdopodobieństwa osiągnięcia zamierzonych celów oraz efektywną realizację zadań⁵⁸⁴. Zarządzanie ryzykiem odbywa się poprzez sześć etapów:

1. identyfikacja ryzyka – rozpoznanie wszystkich ryzyk, mogących oddziaływać na realizację celów,
2. analiza ryzyka – etap obejmujący hierarchizację ryzyk według ich oddziaływania oraz prawdopodobieństwa wystąpienia,
3. ewaluacja ryzyka – weryfikacja i ocena ryzyka, w tym również środków przeznaczonych do jego utrzymania pod kontrolą,
4. postępowanie z ryzykiem – zdefiniowanie działań niezbędnych wobec ryzyka nieakceptowanego,
5. określenie właścicieli ryzyk – wskazanie osób odpowiedzialnych za podjęcie działań zaradczych i wyznaczanie stosownych terminów dla tych działań,
6. monitorowanie – bieżący przegląd i sprawozdawczość⁵⁸⁵.

Za powyższe działania w pewnym stopniu odpowiadają wszyscy uczestnicy systemu zarządzania ryzykiem. Wyznaczeni właściciele ryzyk odpowiadają w szczególności za bieżącą identyfikację i analizę ryzyk oraz projektowanie mechanizmów kontrolnych w zakresie swojego obszaru działalności⁵⁸⁶.

Na potrzebę etapów identyfikacji i analizy ryzyka autorzy przygotowali wykaz czynników ryzyka, nie stanowi on jednak katalogu zamkniętego⁵⁸⁷. Czynniki ryzyka podlegają ocenie pod kątem istotności dla realizacji celów⁵⁸⁸. Do oszacowania prawdopodobieństwa i skutków potencjalnych zdarzeń stosowana jest

⁵⁸³ § 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*.

⁵⁸⁴ Tamże, § 2.

⁵⁸⁵ Tamże, § 8.

⁵⁸⁶ Tamże, § 13.

⁵⁸⁷ Tamże, § 15.

⁵⁸⁸ Tamże, § 16.

skala ocen w opracowanych tabelach punktowych: prawdopodobieństwa wystąpienia ryzyka i oddziaływania ryzyka. Określenie istotności ryzyka prowadzi do uporządkowania ryzyk i hierarchizacji mechanizmów kontrolnych⁵⁸⁹.

Ewaluacja ryzyka jest oparta na czterech poziomach istotności ryzyka, do których zostaną przyporządkowane ryzyka po ich identyfikacji i analizie⁵⁹⁰. Do poziomu ryzyka niskiego zakwalifikowano ryzyko akceptowalne, które należy monitorować i sprawdzać prawidłowość jego kontroli. Ryzyko średnie może mieć znaczny wpływ na działalność, więc istnieje potrzeba jego monitorowania i rozważenia podjęcia działań zaradczych. Dla ryzyka wysokiego wymagane jest wprowadzenie mechanizmów kontrolnych, w celu jego ograniczenia. Poważnym zagrożeniem może okazać się ryzyko bardzo wysokie, w związku z czym niezbędne są natychmiastowe działania mające na celu zniwelowanie jego skutków, gdyż jego występowanie nie może być tolerowane. Ryzyko bardzo wysokie podlega stałemu monitoringowi⁵⁹¹. Stanowi ono istotny czynnik mogący wpłynąć na osiągnięte cele, stąd wymagane jest wykorzystanie dostępnych lub opracowanie nowych, skutecznych środków bądź mechanizmów kontroli, które pozwolą obniżyć albo utrzymać poziom ryzyka na stałym poziomie.

W polityce zarządzania ryzykiem przewidziano następujące sposoby postępowania z ryzykiem: przeniesienie, tolerowanie lub przeciwdziałanie ryzyku, a także odroczenie działań o wysokim poziomie ryzyka⁵⁹². Można zauważyć, że działania te stanowią odpowiedniki opcji przywołanych 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 mechanizmy kontrolne⁵⁹³. Monitorowanie oraz raportowanie o zidentyfikowanych zagrożeniach odbywa się na

⁵⁸⁹ § 17 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*.

⁵⁹⁰ Tamże.

⁵⁹¹ Tamże, § 20.

⁵⁹² Tamże, § 21.

⁵⁹³ Tamże, § 22.

każdym szczeblu zarządzania⁵⁹⁴. Weryfikacja systemu i procedur następuje raz do roku w celu jego aktualizacji⁵⁹⁵.

W województwach na potrzeby analizy ryzyka wykorzystywane są m.in. arkusze identyfikacji bądź identyfikacji i oceny ryzyka⁵⁹⁶. Kolejnym podstawowym dokumentem stosowanym w ramach kontroli zarządczej są rejestry ryzyka. Przykłady takich narzędzi służących do dokumentowania zarządzania ryzykiem w województwach załączono poniżej.

Tabela 71. Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku⁵⁹⁷

Ryzyko						Przeciwdziałanie ryzyku
Lp.	Cel – zadanie	Ryzyko (wraz z podaniem kategorii)	Wpływ	Prawdopodobieństwo	Istotność ryzyka	Planowana metoda przeciwdziałania ryzyku
1	2	3	4	5	6	7
1.						
2.						

⁵⁹⁴ Tamże, § 24 i § 26.

⁵⁹⁵ Tamże, § 29.

⁵⁹⁶ W tabelach 71 i 72 przedstawiono formularze wykorzystywane w jednostkach podczas analizy ryzyka do zbadania możliwości wystąpienia i konsekwencji danego zdarzenia.

⁵⁹⁷ Źródło: załącznik nr 5 do zarządzenia nr 115/10 wojewody podlaskiego z dnia 29 października 2010 r. w sprawie kontroli zarządczej w Podlaskim Urzędzie Wojewódzkim w Białymstoku.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

Tabela 72. Tabela zbiorcza identyfikacji i oceny ryzyka w WZFE⁵⁹⁸

Lp.	Cel	Miernik osiągnięcia celu	Zidentyfikowane ryzyko		Prawdopodobieństwo wystąpienia ryzyka ⁵⁹⁹	Zidentyfikowane ryzyko	Mechanizm zapobiegania zagrożeniu
			przyczyna	skutek			
1	2	3	4	5	6	7	8

Tabela 73. Wydziałowy rejestr ryzyk⁶⁰⁰

Nr identyfikacyjny ryzyka	Nazwa i opis ryzyka	Kategoria ryzyka	Wpływ	Prawdopodobieństwo	Istotność	Metody przeciwdziałania ryzyku	Właściciel ryzyka	Termin realizacji metod przeciwdziałania ryzyku

Tabela 74. Rejestr ryzyka⁶⁰¹

1. Nr ryzyka:	2. Właściciel ryzyka:
3. Cel:	
4. Nazwa ryzyka:	

⁵⁹⁸ Źródło: załącznik nr 2 do zarządzenia nr 8 dyrektora generalnego LUW z dnia 29 stycznia 2010 r.

⁵⁹⁹ Należy zauważyć, że sformułowanie w dokumencie zawiera błąd logiczny, ponieważ definicja ryzyka obejmuje kombinację prawdopodobieństwa i konsekwencji.

⁶⁰⁰ Źródło: załącznik nr 5 do zarządzenia nr 115/10 wojewody podlaskiego z dnia 29 października 2010 r. w sprawie kontroli zarządczej w Podlaskim Urzędzie Wojewódzkim w Białymstoku.

⁶⁰¹ Źródło: załącznik nr 2 do zarządzenia nr 8 dyrektora generalnego LUW z dnia 29 stycznia 2010 r.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

5. Przyczyny ryzyka:	6. Skutki ryzyka:
7. Prawdopodobieństwo wystąpienia (skala 1-5):	8. Potencjalne skutki/straty (skala 1-5):
9. Punktowa ocena ryzyka (pkt 7 x pkt 8):	
10. Funkcjonujące działania – mechanizmy kontrolne:	
11. Wymagane działania – mechanizmy kontrolne:	
12. Odpowiedzialność za wykonanie działań:	13. Termin wykonania działań:
14. Data ostatniego przeglądu:	
15. Data następnego przeglądu:	

Szczegół powiatowy

Ramy działania systemu zarządzania ryzykiem w Warszawie prezydent ustanowił zarządzeniem⁶⁰², które przedstawia przede wszystkim terminologię, zakres zadań i obowiązków uczestników systemu, zasady identyfikowania ryzyka oraz dokonywania oceny ryzyka, zasady określania reakcji na ryzyko, zasady identyfikowania i raportowania incydentów, zakres i sposób monitorowania oraz raportowania ryzyka⁶⁰³.

⁶⁰² Zarządzenie nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.

⁶⁰³ D. Wróblewski (red. nauk.), *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 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 kontroli⁶⁰⁴. 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 skutków oddziaływania. Iloczyn tych czynników stanowi o poziomie danego ryzyka, uzyskane wyniki po uwzględnieniu hierarchizacji odnotowuje się w rejestrze ryzyka⁶⁰⁵.

Tabela 75. Rejestr ryzyka⁶⁰⁶

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.
L.p.	Cele/procesy	Rodzaj celu (np.: zadaniowy, główny, pozostaly)	Symbol procesu z SZJ	Miernik (nazwa)	Planowany poziom miernika	Wykonany poziom miernika	Opis ryzyka	Właściciel ryzyka	Prawdopodobieństwo ryzyka ⁶⁰⁷ (od 1 do 5)	Oddziaływanie ryzyka ⁶⁰⁸ (od 1 do 5)	Poziom ryzyka (iloczyn oddziaływania i prawdopodobieństwa.)	Reakcja na ryzyko
1.												
2.												

⁶⁰⁴ § 12 zarządzenia nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.

⁶⁰⁵ § 14 zarządzenia nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.

⁶⁰⁶ Załącznik nr 1 do zarządzenia prezydenta miasta stołecznego Warszawy nr 3666/2012 z dnia 18 grudnia 2012 r.

⁶⁰⁷ Termin zastosowany w dokumencie nadmiernie wykorzystuje słowo „ryzyko”.

⁶⁰⁸ W ten sposób w dokumencie określono skutki.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.
L.p.	Cele/procesy	Rodzaj celu (np.: zadaniowy, główny, pozostaty)	Symbol procesu z SZJ	Miernik (nazwa)	Planowany poziom miernika	Wykonany poziom miernika	Opis ryzyka	Właściciel ryzyka	Prawdopodobieństwo ryzyka ⁶⁰⁷ (od 1 do 5)	Oddziaływanie ryzyka ⁶⁰⁸ (od 1 do 5)	Poziom ryzyka (ilożycyn oddziaływania i prawdopodobieństwa.)	Reakcja na ryzyko
3.												
4.												
5.												

Właściciele ryzyk po ich przeanalizowaniu są zobowiązani określić sposób reakcji na dane ryzyko. Przewidziano następujące działania: akceptację, dzielenie 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 ryzyka⁶⁰⁹. Należy w tym celu wykorzystać także matrycę ryzyka (rys. 59), która prezentuje akceptowalny oraz nieakceptowalny poziom ryzyka. Czterostopniowa skala oznaczona na mapie kolorami wskazuje działania do podjęcia dla każdego z nich.

⁶⁰⁹ § 15 zarządzenia nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.

**SKUTKI
ODDZIAŁY-
WANIA**

KATASTROFALNE	5	10	15	20	25	PRAWDOPODO- BIENSTWO WYSTĄPIENIA
POWAŻNE	4	8	12	16	20	
ŚREDNIE	3	6	9	12	15	
MAŁE	2	4	6	8	10	
NIEZNACZNE	1	2	3	4	5	
	ZNI- KO- ME	NI- SKIE	ŚRED- NIE	WY- SOKIE	BAR- DZO WY- SOKIE	

Rys. 59. Matryca ryzyka⁶¹⁰

Legenda⁶¹¹:

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.
4. Poziom bardzo wysoki (kolor czerwony) – nieakceptowalny poziom ry-

⁶¹⁰ Załącznik nr 4 do zarządzenia prezydenta miasta stołecznego Warszawy nr 3666/2012 z dnia 18 grudnia 2012 r.

⁶¹¹ § 15 zarządzenia nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.

zyka, konieczność wycofania się lub opracowania i wdrożenia planu działań sprowadzających ryzyko do akceptowanego poziomu w terminie uzgodnionym z bezpośrednim przełożonym. Właściciel ryzyka zobowiązany jest do monitorowania poziomu ryzyka i skuteczności przyjętych działań. Realizacja celów/procesów obciążonych ryzykiem bardzo wysokim wymaga akceptacji bezpośredniego przełożonego oraz zaraportowania do pełnomocnika ds. ryzyka.

Szczebel gminny

W gminie Legionowo zarządzeniem⁶¹² prezydenta miasta wprowadzone zostały zasady zarządzania ryzykiem. Odpowiedzialność za właściwą realizację postanowień dokumentu ponoszą wszyscy pracownicy z prezydentem Legionowa na czele. Objaśnione zostały również podstawowe pojęcia niezbędne do prawidłowego zastosowania opisanej metodyki zarządzania ryzykiem.

Zgodnie z ustaloną procedurą zarządzania ryzykiem poszczególne kroki są następujące:

1. identyfikacja ryzyka,
2. analiza i ocena ryzyka⁶¹³,
3. reakcja na ryzyko⁶¹⁴.

W ramach identyfikacji ryzyka wskazywane są zdarzenia, które mogą zagrozić osiągnięciu celów jednostki⁶¹⁵. Zidentyfikowane zagrożenia podlegają analizie oraz ocenie punktowej. Na tym etapie określona zostaje wartość prawdopodobieństwa wystąpienia ryzyka, jego skutków⁶¹⁶ oraz współczynnik niewykania zdarzenia w skali od 1 do 3. Iloczyn tych czynników przedstawia istotność danego ryzyka.

⁶¹² Zarządzenie nr 204/2012 prezydenta miasta Legionowa z dnia 15 października 2012 r. w sprawie zasad zarządzania ryzykiem w Urzędzie Miasta Legionowa.

⁶¹³ Dokument wprowadza dwa pojęcia w jednym kroku, definiując przy tym jedynie ocenę ryzyka jako punktowe określenie prawdopodobieństwa i wpływu. Faktycznie etap ten obejmuje zgodnie z rozumieniem normy ISO 31000: analizę i ewaluację ryzyka.

⁶¹⁴ Należy rozumieć jako postępowanie z ryzykiem według normy ISO 31000.

⁶¹⁵ § 6 zarządzenia nr 204/2012 prezydenta miasta Legionowa z dnia 15 października 2012 r. w sprawie zasad zarządzania ryzykiem w Urzędzie Miasta Legionowa.

⁶¹⁶ Dokument tworzy nowe pojęcia: prawdopodobieństwo wystąpienia/prawdopodobieństwo skutków – niezgodnie ze sztuką, terminy te powinny zostać ujęte jako prawdopodobieństwo i skutki (konsekwencje), gdyż takie znaczenie wnoszą w proces oceny ryzyka.

Tabela 76. Analiza i ocena istotności ryzyka⁶¹⁷

Liczba ryzyka	Określenie ryzyka	Prawdopodobieństwo wystąpienia (Pw)	Prawdopodobieństwo skutków (Ps)	Współczynnik niewykrycia (Pn)
1	2	3	4	5
1	niskie	mało realne, incydentalne	małe zagrożenie	niski
2	średnie	prawdopodobne, zdarza się	skutki zauważalne, akceptowalne	średni (możliwość niewykrycia)
3	wysokie	bardzo prawdopodobne	skutki nie do zaakceptowania	wysoki

Istotność ryzyka (R) stanowi iloczyn prawdopodobieństwa wystąpienia (Pw), prawdopodobieństwa skutków (Ps), współczynnika niewykrycia (Pn):

$$R = Pw \times Ps \times Pn$$

Tabela 77. Skala punktowa istotności ryzyka⁶¹⁸

Określenie ryzyka	Skala punktowa
ryzyko niskie	1-3
ryzyko średnie	4-12
ryzyko wysokie	18-27

Uzyskany wynik determinuje dalsze działania, które kryją się pod zwrotem „reakcja na ryzyko”. W ramach tego kroku stosuje się: akceptację ryzyka, zmniejszenie wpływu lub prawdopodobieństwa wystąpienia, przeniesienie ryzyka, tolerowanie ryzyka, wycofanie z działań lub ich brak⁶¹⁹. W porównaniu z działaniami określonymi na szczeblu województwa i powiatu na poziomie gminnym w największym stopniu wykorzystano wachlarz kroków dostępnych dla etapu postępowania z ryzykiem. Analiza i ocena ryzyka dokonywana jest w ramach załączonego do zarządzenia „Arkusza zarządzania ryzykiem”, który przedstawia tabela 78. Za bieżące monitorowanie zarządzania ryzykiem odpowiadają wszyscy pracownicy.

⁶¹⁷ Załącznik nr 1 do zarządzenia nr 204/2012 prezydenta miasta Legionowa z dnia 15 października 2012 r. w sprawie zasad zarządzania ryzykiem w Urzędzie Miasta Legionowa.

⁶¹⁸ Tamże.

⁶¹⁹ § 8 zarządzenia nr 204/2012 prezydenta miasta Legionowa z dnia 15 października 2012 r. w sprawie zasad zarządzania ryzykiem w Urzędzie Miasta Legionowa.

Tabela 78. Arkusz zarządzania ryzykiem⁶²⁰

Data:		Proces:								
Element procesu	Zagrożenie	Prawdopodobieństwo wystąpienia	Pw	Następstwo zdarzenia ⁶²¹	Ps	Prawdopodobieństwo niewykrycia ⁶²²	Pn	R	Wskaźnik realizacji celu ⁶²³	Działania doskonalące
Podpis przewodniczącego zespołu ds. zarządzania ryzykiem:				Zatwierdził:			Data:			R = Pw x Ps x Pn
				Podpis:						

⁶²⁰ Załącznik nr 2 do zarządzenia nr 204/2012 prezydenta miasta Legionowa z dnia 15 października 2012 r. w sprawie zasad zarządzania ryzykiem w Urzędzie Miasta Legionowa.

⁶²¹ To kolejny przykład niezgodności terminologicznej – w jednym dokumencie wprowadzono drugie pojęcie dla tego samego przykładu, a należy je rozumieć jako skutki (konsekwencje).

⁶²² Dokument wprowadza oszacowanie możliwości niewykrycia danego ryzyka, również wprowadzając drugie pojęcie dla jednego przykładu.

⁶²³ Dokument wprowadza wskaźnik będący wyznacznikiem realizacji celu procesu lub jego elementu, dla którego zidentyfikowano ryzyko.

5. METODYKA DIAGNOZOWANIA SYSTEMÓW REAGOWANIA POMRISC – ELEMENTY ZARZĄDZANIA RYZYKIEM

W latach 2008-2009 CNBOP na zlecenie władz Samorządu Województwa Pomorskiego 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 województwa pomorskiego na lata 2007-2013⁶²⁴.

Celem głównym realizacji tematu było przedstawienie podstaw funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa na terenie województwa pomorskiego na podstawie oceny funkcjonującego systemu ratownictwa, które pozwoliłyby na kompleksową diagnozę stanu bezpieczeństwa oraz podniesienie jego poziomu, zwłaszcza w tych elementach, które ujawniono 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 zewnętrznego otoczenia. W zależności od środowiska działania organizacji i podmiotów w nich osadzonych organizowany jest proces planowania, kierowania i kontroli działalności w organizacji, mający zmniejszyć wpływ ryzyka na wyniki organizacji. Ze względu na niebywałą 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 projektowego⁶²⁵ 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

⁶²⁴ D. Wróblewski (red. nauk.), *Koncepcja regionalnego zintegrowanego systemu ratownictwa województwa pomorskiego*, s. 23.

⁶²⁵ Zespół autorski w składzie: kierownik projektu: D. Wróblewski, zespół: E. W. Roguski, A. Kołodziej-Saramak, D. Kwiatkowski, J. Prasła, T. Sowa, T. Wilczyński, R. Zakrzewski.

projektowego w zakresie zarządzania ryzykiem, w wyniku czego powstała unikatowa w Polsce metodyka oceny ryzyk i ich interpretacji: PomRisc⁶²⁶. 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/2008.

5.1. Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego

Dla prawidłowego, 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 ryzyka⁶²⁷, jednakże brakowało odpowiednio dopasowanej dla potrzeb zdiagnozowania stanu elementów systemu ratownictwa województwa pomorskiego. Narzędziem, które wspomogło identyfikację obszarów ryzyka⁶²⁸ – zarówno zagrożeń, jak i szans, była wypracowana w ramach realizacji projektu, relatywnie obiektywna metodyka PomRisc⁶²⁹. Warunkiem realizacji projektu „Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego” było objęcie systemu analizą obejmującą wszystkie podmioty w nim uczestniczące i aspekty jego funkcjonowania.

Przedmiot badań zespołu projektowego stanowiły następujące zagadnienia:

1. analiza ryzyka⁶³⁰, przeprowadzona według odpowiedniej metodologii badawczej,

⁶²⁶ Rozwinięcie skrótu PomRisc – Pomorska Regionalna Integracja Systemów Cywilnych, RZSR WP.

⁶²⁷ Patrz: definicja na s. 29.

⁶²⁸ Patrz: definicja na s. 46.

⁶²⁹ 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. 3.

⁶³⁰ Patrz: definicja na s. 31.

2. diagnoza obecnego stanu elementów w systemie ratownictwa (np. zasoby, infrastruktura, wyposażenie, lokalizacja placówek),
3. analiza słabych ogniw systemu (brakujące lokalizacje, deficyty infrastruktury i wyposażenia, wyposażenie, zasady integracji) – w świetle analizy ryzyka oraz diagnozy,
4. docelowa (całościowa) wizja zintegrowanego systemu ratownictwa w województwie pomorskim – sieć placówek, standardy wyposażenia, narzędzia, zasady integracji itp.
5. rekomendacje w sprawie priorytetowych potrzeb inwestycyjnych wskazanych do współfinansowania z RPO WP, uporządkowanych rankingowo według takich kryteriów, jak np.:
 - a. stopień pilności przedsięwzięcia,
 - b. kluczowe znaczenie dla funkcjonowania systemu jako całości,
 - c. waga finansowa (koszty przekraczające bieżące możliwości zainteresowanej jednostki organizacyjnej),
 - d. 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 wykorzystania w pełni środków (ocena wykonalności), celowość inwestycji w kontekście RZSR WP oraz zdolność do obniżania potencjalnych ryzyk na danym terenie (ocena strategiczna)⁶³¹.

⁶³¹ D. Wróblewski (red. nauk.), *Koncepcja regionalnego zintegrowanego systemu ratownictwa województwa pomorskiego*, s. 23.

5.2. Metody badawcze wykorzystane na potrzeby analizy oceny ryzyka PomRisc⁶³²

Podstawą do opracowania eksperckiej metodyki PomRisc była szeroka analiza literatury krajowej i zagranicznej oraz norm i metod między innymi: Australian/New Zealand Standard *Risk Management AS/NZS 4360:2004*⁶³³ oraz Handbook *Risk Management Guidelines* HB 436:2004 i *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, „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*⁶³⁴ – ISO 31000⁶³⁵.

Realizacja zadania oparta została na zbiorze ankiet, zawierających pytania dotyczące elementów technicznych, funkcjonalnych, powiązań między podmiotami i ich zakresie 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 Pomorskiego⁶³⁶.

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:

⁶³² Patrz szerzej: PN-ISO 31000:2012 *Zarządzanie ryzykiem. Zasady i wytyczne*.

⁶³³ Patrz: AS/NZS 4360 *Zarządzanie ryzykiem* (ostatnie zmiany dokonane w 2004 r.), po raz pierwszy opublikowana w 1995 r.

⁶³⁴ ISO 31000:2009 *Risk Management – Principles and Guidelines*, zastępuje AS/NZS 4360:2004.

⁶³⁵ Międzynarodowy Komitet Normalizacyjny (International Organization for Standardization) 13 listopada 2009 r. opublikował standard ISO 31000:2009 *Risk Management – Principles and Guidelines*.

⁶³⁶ 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. 2.

1. gotowości do realizacji inwestycji oraz wykorzystania w pełni środków (ocena wykonalności),
2. celowości inwestycji w kontekście RZSR WP,
3. zdolności do obniżania potencjalnie istniejących ryzyk na danym terenie (ocena strategiczna)⁶³⁷,
4. oceny systemów reagowania,
5. szacowania ryzyka⁶³⁸ poprzez tworzenie aktualnych matryc ryzyka i powiązania informacji zarówno z procedurami w powiązaniu z bazami infrastrukturalno-sprzętowymi oraz kapitałem ludzkim,
6. procedur operacyjno-logistycznych podmiotów,
7. 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, a następnie uszeregowano je od najważniejszych do mniej ważnych z punktu widzenia własnego podmiotu, polityki gminy, powiatu, województwa. Zespół projektowy, kwalifikując ryzyka, w dużej mierze oparł się na własnej wiedzy (w tym bazach danych) i wiedzy pozyskanej od podmiotów. Wskazane ryzyka ograniczono do zdarzeń destrukcyjnych wywołujących straty i uszeregowano według rodzaju:

1. wypadki i katastrofy w komunikacji i transporcie,
2. awarie infrastruktury technicznej (wodno-kanalizacyjnej, energetycznej, gazowej itd.),
3. pożary według rodzajów,
4. klęski i zagrożenia naturalne (powodzie, pożary lasów, gradobicia, silne wiatry, nadmierne opady atmosferyczne, oblodzenia, silne mrozy i susze itp.),

⁶³⁷ D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 23.

⁶³⁸ Patrz: definicja na s. 39.

5. awarie i katastrofy budowlane, w tym dotyczące budowli hydrotechnicznych,
6. awarie i katastrofy chemiczne,
7. awarie i katastrofy ekologiczne oraz radiacyjne,
8. zagrożenia biologiczne (epidemie, epizootie, epifitozy),
9. 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 uwzględniała najbardziej niekorzystne zdarzenie i wszystkie kategorie (zdrowie i bezpieczeństwo, straty materialne, środowisko naturalne, społeczne/dziedzictwo kulturowe, społeczność/rząd/reputacja/mass media, kategoria cywilnoprawna)⁶³⁹.

Wykonawcy badań zidentyfikowali 17 rodzajów zagrożeń, biorąc pod uwagę miejsce danego zagrożenia w hierarchii i uwzględniając liczbę wskazań (dot. danego zagrożenia w powiecie) oraz wartość punktową wielkości strat i częstości zdarzenia z matrycy⁶⁴⁰.

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

Jedną z najlepszych metod oceny stanu bezpieczeństwa jest identyfikacja⁶⁴¹, analiza i ewaluacja ryzyka⁶⁴². Przed przystąpieniem do wykonania procedury

⁶³⁹ E. W. Roguski, D. Wróblewski, *Diagnostyczna metoda oceny ryzyk i systemów reagowania PomRisc jako narzędzie programowania zmian doskonalących systemu bezpieczeństwa i ich monitorowania*, BiTP Issue 4, 2008, s. 5.

⁶⁴⁰ Patrz szerzej: D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 25.

⁶⁴¹ Patrz: definicja na s. 27.

⁶⁴² Patrz: definicja na s. 37.

oceny ryzyka należy zebrać informacje dotyczące omawianego terenu, czyli dokonać identyfikacji zagrożeń, a następnie identyfikacji ryzyka⁶⁴³.

Skuteczność w zapewnieniu bezpieczeństwa mieszkańcom uzależniona jest w dużym stopniu od sposobu zarządzania bezpieczeństwem poprzez zarządzanie ryzykiem i zarządzanie 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 administracyjnym⁶⁴⁴.

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 zespolenia⁶⁴⁵.

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 potrzebujących.

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, definiują tworzony RZSR WP⁶⁴⁶.

⁶⁴³ D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 1.

⁶⁴⁴ Tamże.

⁶⁴⁵ Tamże, s. 6.

⁶⁴⁶ Patrz szerzej: D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 7.

Zakres prac obejmował:

1. analizę ryzyka, przeprowadzona według odpowiedniej metodologii badawczej;
2. diagnozę obecnego stanu elementów systemu ratownictwa, a w szczególności:
 - a. zasobów,
 - b. infrastruktury,
 - c. wyposażenia,
 - d. lokalizację placówek;
3. analizę słabych ogniw systemu, a w szczególności:
 - a. brakujących lokalizacji,
 - b. deficytów infrastruktury i wyposażenia,
 - c. poziomu wykszolenia,
 - d. w świetle analizy ryzyka i diagnozy;
4. ocenę propozycji (przedstawionych przez podmioty), wraz z uzasadnieniem, zasad funkcjonowania każdego z podmiotów ratowniczych w Regionalnym Zintegrowanym Systemie Ratownictwa Województwa Pomorskiego (RZSR WP), 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) wizja RZSR WP, w szczególności na podstawie wniosków i propozycji w zakresie:
 - a. sieci placówek,
 - b. standardów wyposażenia,
 - c. narzędzi i zasad integracji,
 - d. poziomu wykszolenia, 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.:
- stopień pilności przedsięwzięcia,
 - kluczowe znaczenie dla funkcjonowania systemu jako całości,
 - waga finansowa (koszty przekraczające bieżące możliwości zainteresowanego podmiotu)⁶⁴⁷.

5.2.2. Diagnoza stanu bezpieczeństwa w województwie pomorskim⁶⁴⁸

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, opracowanie procedur zarządzania bezpieczeństwem podmiotu i optymalizacji jego procesów informacyjno-decyzyjnych⁶⁴⁹.

Zespół projektowy wykorzystał dane historyczne, czyli dane o awariach, wypadkach i innych zdarzeniach destrukcyjnych, które miały miejsce na omawianym terenie⁶⁵⁰. Zakres danych obejmował zagadnienia dotyczące ogólnej wiedzy na temat omawianego obszaru (charakterystyka terenu, charakterystyka aktualnej sytuacji, substancji niebezpiecznych, warunków hydrologiczno-meteorologicznych, struktury społecznej i demograficznej, zagospodarowania przestrzennego, podmiotów tworzących system bezpieczeństwa itp.).

⁶⁴⁷ Patrz szerzej: D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 23-24.

⁶⁴⁸ Opracowanie na podstawie: 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. 3-8.

⁶⁴⁹ Patrz szerzej: część I, rozdział 1 *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, podrozdział 1.4. *Proces zarządzania ryzykiem*.

⁶⁵⁰ Patrz: PN-ISO 31000. Identyfikacja ryzyka może obejmować dane historyczne, analizy teoretyczne, pozyskane opinie, opinie ekspertów oraz potrzeby interesariuszy.

Otrzymane informacje umożliwiają przegląd dotychczas zaistniałych sytuacji – **ryzyk kinetycznych**⁶⁵¹. 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**⁶⁵².

Informacje dotyczące identyfikacji i analizy ryzyk, oszacowanie ich wielkości, hierarchizacja⁶⁵³ mogą mieć wpływ na podejmowanie wszelkich decyzji związanych z ochroną ludności oraz tworzenie lokalnej polityki bezpieczeństwa⁶⁵⁴. Aby zapewnić prawidłowość oceny ryzyk, poza działaniami analitycznymi i probabilistycznymi prowadzono dialog z władzami różnych szczebli podziału administracyjnego, służbami i podmiotami świadczącymi usługi dla ludności w zakresie ratownictwa, środowiskami ekspertów a społeczeństwem. Takie podejście do problemu dało szansę wyboru optymalnej drogi poprawy bezpieczeństwa mieszkańców poprzez wybór 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 ryzyka⁶⁵⁵ 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 sys-

⁶⁵¹ Ryzyko kinetyczne – źródło bądź miejsce uwolnienia zagrożenia o określonych skutkach. Źródło: na podstawie 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. 4.

⁶⁵² Ryzyko potencjalne – źródło bądź miejsce najbardziej narażone na zagrożenie o określonych skutkach. Źródło: na podstawie 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. 4.

⁶⁵³ Patrz: definicja na s. 84.

⁶⁵⁴ 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 zagrożenia i doskonalenie systemu ochrony ludności”, Józefów 2011.

⁶⁵⁵ Patrz: definicja na s. 39 (poziom ryzyka).

temu bezpieczeństwa oraz planowania szkoleń doskonalących. Po zakończeniu procesu identyfikacji ryzyk należy dokonać ich wstępnej hierarchizacji i zdecydować o kierunku działań skierowanych na każde z nich⁶⁵⁶.

Szacowanie ryzyka⁶⁵⁷, zgodnie z definicją przywołaną w części I, polega na określeniu wielkości ryzyka, z uwzględnieniem prawdopodobieństwa jego wystąpienia, strat i innych konsekwencji przez nie wywołanych oraz skutków społecznych, społeczno-ekonomicznych i środowiskowych⁶⁵⁸. W praktyce stosujemy dwie metody szacowania ryzyka: jakościową i ilościową.

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 niezbędne są do przeprowadzenia kolejnych kroków:

1. tworzenia planów ratowniczych,

⁶⁵⁶ Patrz szerzej: część I, rozdział 1 *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, podrozdział 1.4 *Proces zarządzania ryzykiem*.

⁶⁵⁷ E. W. Roguski, D. Wróblewski, *Diagnostyczna metoda oceny ryzyk i systemów reagowania PomRisc jako narzędzie programowania zmian doskonalących systemu bezpieczeństwa i ich monitorowania*, BiTP Issue 4, 2008, s. 3.

⁶⁵⁸ Patrz szerzej: część I, rozdział 1 *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, podrozdział 1.4. *Proces zarządzania ryzykiem*.

2. wyboru dróg do przewożenia substancji niebezpiecznych,
3. tworzenia procedur informowania, ostrzegania i alarmowania,
4. tworzenia planów obrony cywilnej i zarządzania kryzysowego,
5. doskonalenia powiązań organizacyjnych,
6. planowania inwestycji i zakupów inwestycyjnych dla elementów systemu bezpieczeństwa,
7. planowania szkoleń doskonalących⁶⁵⁹.

Korzystając z metodyki PomRisc, zidentyfikowano 17 ryzyk istotnych w kontekście powiatów:

1. ataki terrorystyczne,
2. skażenia radiacyjne,
3. gradobicia,
4. niewypały,
5. mrozy, śnieżyce, oblodzenia,
6. susze,
7. naruszenia porządku publicznego,
8. utonięcia,
9. wichury,
10. powódzie i podtopienia,
11. skażenia chemiczne,
12. katastrofy ekologiczne,
13. awarie,
14. katastrofy budowlane,
15. pożary,
16. zakażenia masowe,
17. 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 punk-

⁶⁵⁹ Na podstawie: 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. 8.

towym 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 tworzą, wykorzystując dane z poziomu powiatowego i 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 ryzyka na terenie województwa i tym samym trafniej sformułować rekomendację działań zapobiegawczych, korygujących lub doskonalących system reagowania, autorzy stworzyli zespół matryc zbiorczych, które podlegały przekształceniom⁶⁶⁰.

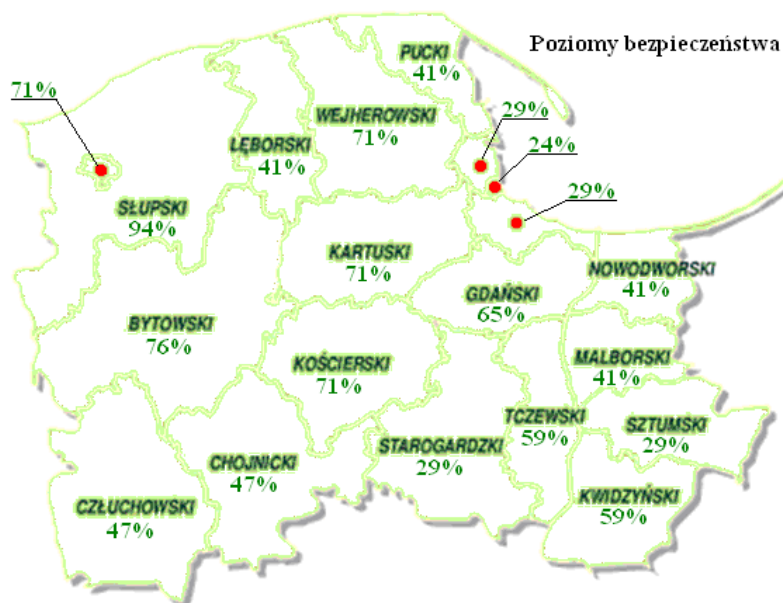
Do sformułowania rekomendacji niezbędna była wizualizacja względna wielkości ryzyka w kontekście powiatów i województwa, które budowały relacyjną przestrzeń ryzyka. Cel tych przekształceń stanowiło powstanie matryc rekomendacji działań z perspektywy powiatów oraz województw. Warto dodać, że w metodyce 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 operacyjnym⁶⁶¹.

Mapę administracyjną ryzyka województwa wykonano na podstawie analizy matryc wypełnionych przez podmioty deklarujące udział w RZSR WP. Uzupeł-

⁶⁶⁰ E. W. Roguski, D. Wróblewski, *Diagnostyczna metoda oceny ryzyka i systemów reagowania PomRisc jako narzędzie programowania zmian doskonalących systemy bezpieczeństwa i ich monitorowania*, BiTP Issue 4, 2008, s. 24.

⁶⁶¹ Tamże, s. 24-25.

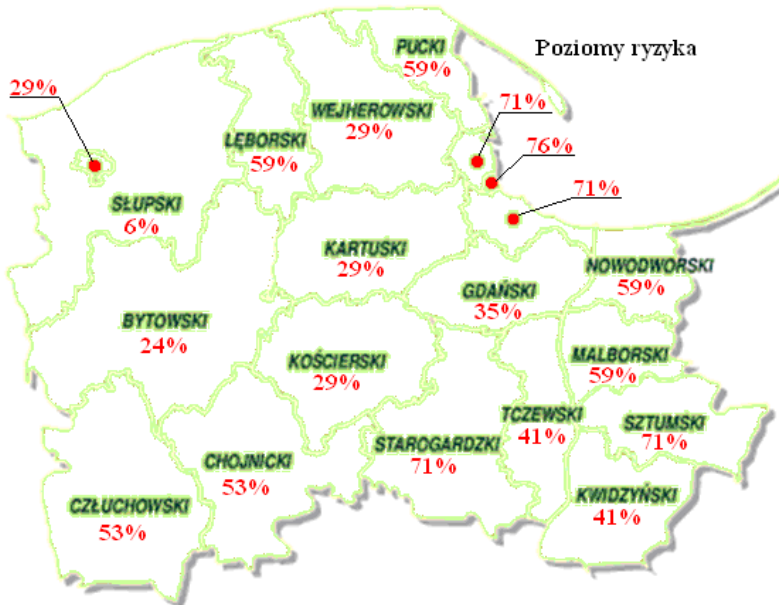
nieniem mapy administracyjnej ryzyk województwa pomorskiego są graficzne wizualizacje w postaci „poziomów bezpieczeństwa”.



Rys. 60. Mapa terytorialnego rozkładu poziomu bezpieczeństwa⁶⁶² województwa pomorskiego

W celu uzyskania porównywalności ryzyk w powiatach z perspektywy województwa stworzono mapę terytorialnego rozkładu ryzyk obszarowych, którą przedstawia rys. 61.

⁶⁶² Mapa terytorialnego rozkładu poziomu bezpieczeństwa województwa – mapa przygotowana na podstawie matryc bazujących na danych z poziomu powiatowego, przedstawiająca poziom zsumowanego ryzyka pomijalnego i akceptowalnego. Źródło: na podstawie D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 3.

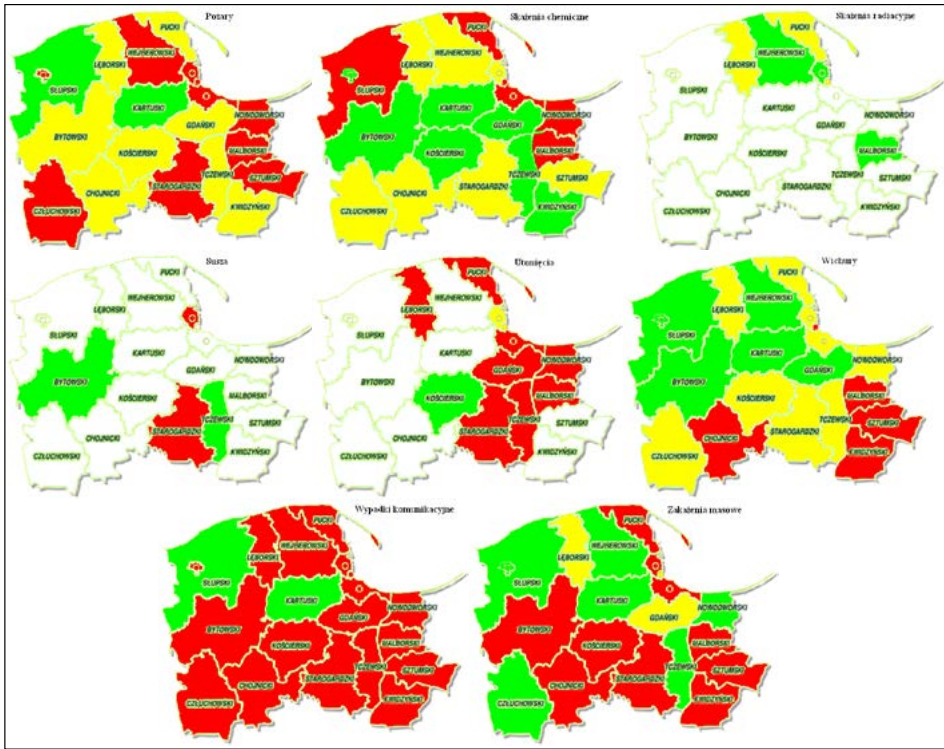


Rys. 61. Mapa terytorialnego rozkładu ryzyk obszarowych⁶⁶³ województwa pomorskiego⁶⁶⁴

⁶⁶³ Mapa terytorialnego rozkładu ryzyk obszarowych województwa – mapa przygotowana na podstawie matryc bazujących na danych z poziomu powiatowego, przedstawiająca poziom zsumowanego ryzyka tolerowanego i nietolerowanego. Źródło: na podstawie D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 3.

⁶⁶⁴ Patrz szerzej: D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 53.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP



Rys. 62. Mapy terytorialnego rozkładu ryzyk cząstkowych⁶⁶⁵ województwa pomorskiego⁶⁶⁶

⁶⁶⁵ Mapy terytorialnego rozkładu ryzyk cząstkowych województwa – mapy przygotowane w oparciu o matryce bazujące na danych uzyskanych z poziomu powiatowego, przedstawiające poziomy ryzyka w rozbiciu na zidentyfikowane ryzyka. Źródło: na podstawie D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 3.

⁶⁶⁶ D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 5.

Poniżej w celach poglądowych przedstawiono matryce ryzyk powiatu kwidzyńskiego.

Tabela 79. Matryca ryzyk – pow. kwidzyński (przykład)⁶⁶⁷

Wielkość strat Częstość		1	2	3	4	5
		nieistotne	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 ko- munikacyjne zakażenia ma- sowe	
D	bardzo częste		pożary	awarie		
E	ustawiczne (per- manentne)					

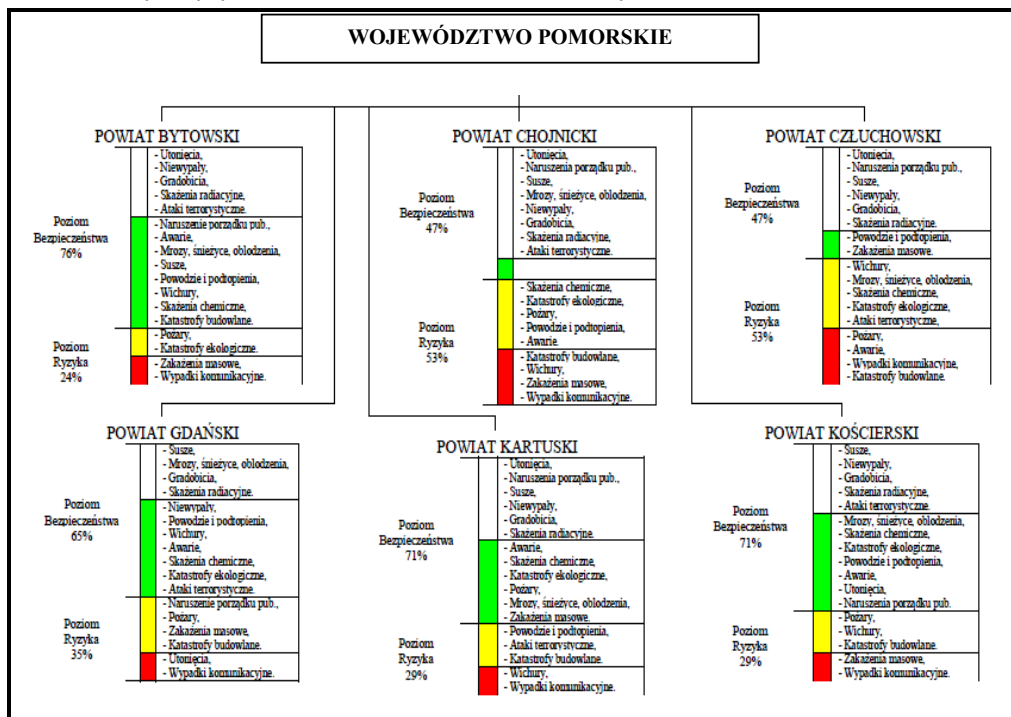
	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

Kolejnym etapem było sporządzenie mapy administracyjnej ryzyk województwa⁶⁶⁸ pomorskiego. Na mapie tej zaznaczono procentowe poziomy ryzyka i bezpieczeństwa w danym powiecie.

⁶⁶⁷ Tamże, s. 66.

⁶⁶⁸ 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. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 30.

W skład poziomu bezpieczeństwa wchodziły ryzyka pomijalne (kolor biały) i akceptowalne (kolor zielony), w skład poziomu ryzyka – ryzyka tolerowalne (kolor żółty) i ryzyka nietolerowane (kolor czerwony).



Rys. 63. Mapa administracyjna ryzyk województwa pomorskiego (cz. 1/4)⁶⁶⁹

Następnie sporządzono hierarchiczną tablicę ryzyk⁶⁷⁰ oraz hierarchiczną tablicę rekomendacji działań podnoszących poziom bezpieczeństwa⁶⁷¹. Tablice te po-

⁶⁶⁹ Patrz szerzej: D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 49.

⁶⁷⁰ Hierarchiczna tablica ryzyk – narzędzie priorytetyzujące działania w zależności od hierarchii ryzyk, przedstawiające procentowy rozkład poziomu zidentyfikowanego ryzyka dla poszczególnych powiatów. Źródło: na podstawie D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 17-18.

⁶⁷¹ Hierarchiczna tablica rekomendacji działań podnoszących poziom bezpieczeństwa – narzędzie priorytetyzujące działania w zależności od hierarchii ryzyk, przedstawiające rekomendowane działania techniczne i nietechniczne względem zidentyfikowanych ryzyk dla poszczególnych powiatów. Źródło: na podstawie D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 17-18.

służyły jako instrument pomocniczy podczas wyboru rekomendowanych inwestycji⁶⁷².

Ataki terrorystyczne			6,3	23,3	21,1			15,8	8,4	11,6			2,1	7,4					2,1	
Skazenia radiacyjne								35,9	5,1	30,8				17,9			5,1		5,1	
Grudobicia							100													
Niewypały				46,9						29,7			12,5			7,8	3,1			
Mrozy, śnieżyce, oblodzenia	2,9		2,6		4,5	1,6	10,6	10,6		10,3		41,3	1,6	6,4	3,2		2,9	0,6	0,6	
Susze,	25												19,4		5,6			20		
Narusz. porządku publ.	2,3			11,9		10,8		0,6					16,5	14,8		10,8	9,1	18,3	5,1	
Utonięcia				9,8		2,2		19	3,8	27,2	7,1		4,1		9,2		11,1	8,7	1,9	
Wichury	4,2	5,9	5,7	2,9	6	4,8	3,5	12,3	4,2	4	3,6	14,3	4,4	6	1,6	1,3	2,1	5,9	5,9	
Powodnie i podtopienia	3,6	4,3	3,9	5,1	4,5	6,8	4,6	3,7	6	7,3	5,8	6,6	5,3	5,2	3,8	3	3,1	1,7	6,5	
Skazenia chemiczne	3,2	3,8	5,2	2,5	6,3	2	5,5	3,7	3,6	6	5,4	12,3	9,2	4,7	2,9	2,6	4,1	2,9	4,3	
Katastrofy ekologiczne	8,6	5,5	7,4	2,9	8,2	2,6	8,1	1,9	4,8	2,4	4,2		6,8	6,5	3,1	0,7	5,8	6,4	7,5	
Awarie	2,9	4,9	5,9	4,3	5,1	1,9	7,4	3,4	8,9	3,4	1,3	1	4,7	7,2	3,5	2,5	7,6	7,7	8,9	
Katastrofy budowlane	3,8	4,4	7,3	3,5	8,3	6,2	4,9	2,7	2,5	3,3	3,2		4,2	5,3	14,7	1,6	5,3	8,1	5,1	
Pozary	5	4,8	5,8	6,1	4,4	7,3	3,9	5,1	4	5,1	5,3	2,6	4,7	4,1	2,2	8,1	6,5	3,6	5,3	
Zakażenia masowe	18,2	13,7	1,7	4,6	1,6	5,3	5,7	3	8,3	3,8	4	3,1	3,8	3,5	0,8	1,2	3	11,6	0,7	
Wypadki komunikacyjne	3,4	4,3	5,2	3,9	4,6	5	4,1	4,1	5,3	4	6,6	1	4,1	4,1	9,4	10,7	4,6	4,5	4,6	
	p. bytowski	p. chojnicki	p. człuchowski	p. gdański	p. kartuski	p. kościerski	p. kwidziński	p. lęborski	p. malborski	p. nowodworski	p. pucki	p. sępolski	p. starogardzki	p. sztumski	p. tczewski	p. wejherowski	Gdańsk	Gdynia	Słupsk	Sopot

Rys. 64. Hierarchiczna tablica ryzyk (perspektywa wojewódzka) [%]⁶⁷³

Ataki terrorystyczne			-	+	+			+	-		+				-					-
Skazenia radiacyjne								+			+				-					-
Grudobicia								-												-
Niewypały			+								+			-						-
Mrozy, śnieżyce, oblodzenia	-		-					+	+		+			-						-
Susze,	-																			-
Narusz. porządku publicznego	-			+																-
Utonięcia	-																			-
Wichury	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Powodnie i podtopienia	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Skazenia chemiczne	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Katastrofy ekologiczne	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Awarie	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Katastrofy budowlane	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Pozary	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Zakażenia masowe	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Wypadki komunikacyjne	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
	p. bytowski	p. chojnicki	p. człuchowski	p. gdański	p. kartuski	p. kościerski	p. kwidziński	p. lęborski	p. malborski	p. nowodworski	p. pucki	p. sępolski	p. starogardzki	p. sztumski	p. tczewski	p. wejherowski	Gdańsk	Gdynia	Słupsk	Sopot

+ A1: rekomendowane działania techniczne i niotechniczne
 - A2: rekomendowane działania techniczne
 + A1: rekomendowane działania techniczne i niotechniczne
 - A3: rekomendowane działania niotechniczne
 + A2: rekomendowane działania techniczne
 - A4: rekomendowane działania niotechniczne, o charakterze zapobiegawczym, w szczególności edukacyjne, uświadamiające

Rys. 65. Hierarchiczna tablica rekomendacji działań podnoszących poziom bezpieczeństwa (perspektywa wojewódzka) – translator⁶⁷⁴

⁶⁷² Patrz szerzej: D. Wróblewski (red. nauk.), *Koncepcja Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 393.

⁶⁷³ Patrz szerzej: tamże, s. 55.

⁶⁷⁴ Tamże, s. 56.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

			wichury skażenia chemiczne			
D	bardzo częste					
E	ustawiczne (permanentne)			wypadki ko- munikacyjne		

	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

Hierarchizacja zagrożeń pod względem częstotliwości wskazania:

1. zakażenia masowe,
2. pożary,
3. wypadki komunikacyjne,
4. katastrofy ekologiczne,
5. powodzie i podtopienia,
6. wichury,
7. katastrofy budowlane,
8. skażenia chemiczne,
9. awarie,
10. mrozy, śnieżyce, oblodzenia,
11. susze,
12. naruszenia porządku publicznego.

Tabela 81. Matryca ryzyk – Sopot, miasto na prawach powiatu (przykład)⁶⁷⁸

Wielkość strat		1	2	3	4	5
		nie- stotne	ograniczo- ne	poważne	bardzo po- ważne	katastrofalne
A	sporadyczne					skażenia ra- diacyjne, ataki terrory- styczne

⁶⁷⁸ Tamże, s. 79.

CZĘŚĆ IV
ZARZĄDZANIE RYZYKIEM W RP

B	rzadkie				katastrofy budowlane, utonięcia	wichury, skażenia chemiczne, katastrofy ekologiczne
C	częste			awarie, zakażenia masowe, naruszenia porządku pub	powodzie i podtopienia, pożary, wypadki komunikacyjne	
D	bardzo częste					
E	ustawiczne (permanentne)					

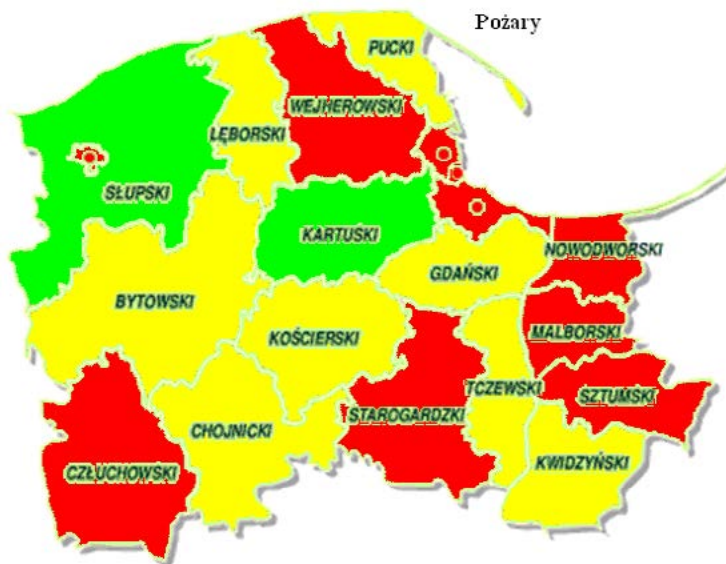
	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

Hierarchizacja zagrożeń pod względem częstotliwości wskazania:

1. powodzie i podtopienia,
2. pożary,
3. wypadki komunikacyjne,
4. awarie,
5. wichury,
6. katastrofy budowlane,
7. katastrofy ekologiczne,
8. skażenia chemiczne,
9. zakażenia masowe,
10. naruszenie porządku publicznego,
11. utonięcia,
12. skażenia radiacyjne,
13. ataki terrorystyczne.

Mapy ryzyk⁶⁷⁹

Na podstawie matryc ryzyk realizatorzy projektu opracowali mapy ryzyk. Poniżej podano dwie przykładowe mapy zagrożeń dla pożarów oraz wypadków komunikacyjnych.

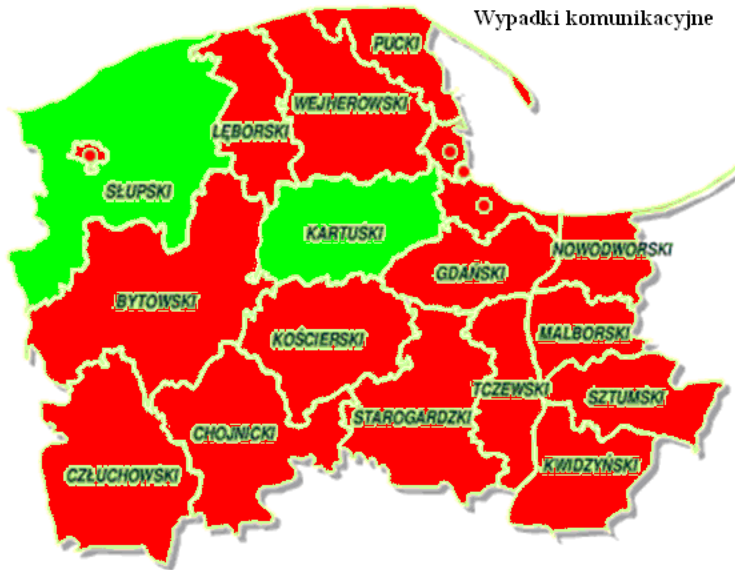


Rys. 67. Mapa terytorialnego rozkładu ryzyk częściowych województwa pomorskiego – pożary⁶⁸⁰

	ryzyko pomijalne
	ryzyko akceptowalne
	ryzyko tolerowalne
	ryzyko nietolerowalne

⁶⁷⁹ Patrz szerzej: tamże, s. 81-90.

⁶⁸⁰ Tamże, s. 90.



Rys. 68. Mapa terytorialnego rozkładu ryzyk częściowych województwa pomorskiego – wypadki komunikacyjne⁶⁸¹

	ryzyko pomijalne
■	ryzyko akceptowalne
■	ryzyko tolerowalne
■	ryzyko nietolerowalne

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:

⁶⁸¹ Patrz szerzej: tamże, s. 81-90.

1. Państwowa Straż Pożarna,
2. ochotnicze straże pożarne,
3. Policja,
4. Morska Służba Poszukiwania i Ratownictwa SAR,
5. pogotowie ratunkowe, szpitale oraz SOR,
6. straże miejskie oraz gminne,
7. Straż Graniczna,
8. inspektoraty ochrony środowiska,
9. inspektoraty nadzoru budowlanego,
10. inspektoraty weterynarii,
11. stacje sanitarno-epidemiologiczne,
12. Wodne Ochotnicze Pogotowie Ratunkowe,
13. centra zarządzania kryzysowego.

Każdy z wymienionych podmiotów działa we własnym otoczeniu prawnym, tj. najczęściej na podstawie ustaw, rozporządzeń, zarządzeń lub innych regulacji formalno-prawnych.

W związku z szybkim rozwojem naszego kraju regulacje te tworzone były i są 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 podmiotów⁶⁸².

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.

⁶⁸² 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.

Podejmowane próby diagnozowania wybranych elementów wspólnego działania w toku ograniczały się do wspólnych ćwiczeń i manewrów, doskonaląc 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 zgodności⁶⁸³.

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 wzmacniać⁶⁸⁴.

Należy podjąć działania zmierzające do minimalizacji ryzyka w rozumieniu systemu bezpieczeństwa funkcjonującego na danym terenie, doskonaląc zabezpieczenia techniczne i nietechniczne zmniejszające prawdopodobieństwo wystąpienia 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 efektywnościowe⁶⁸⁵.

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 kluczo-

⁶⁸³ 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. 13-14.

⁶⁸⁴ Tamże, s. 17.

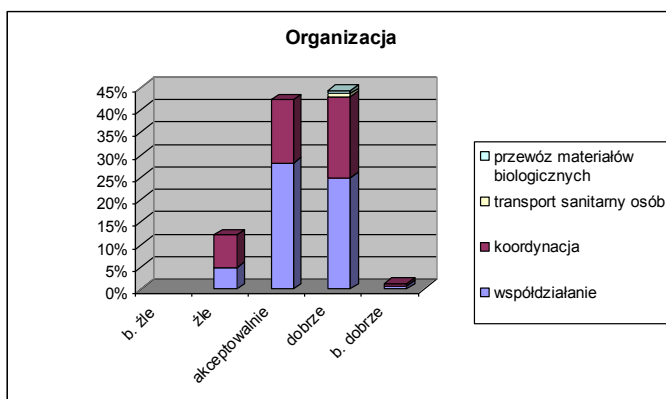
⁶⁸⁵ Tamże, s. 13.

wych 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 edukacja⁶⁸⁶.

Organizacja

Rys. 69 przedstawia sumaryczny rozkład takich elementów organizacji, jak przewóz materiałów biologicznych, transport sanitarny, koordynacja i współdziałanie.



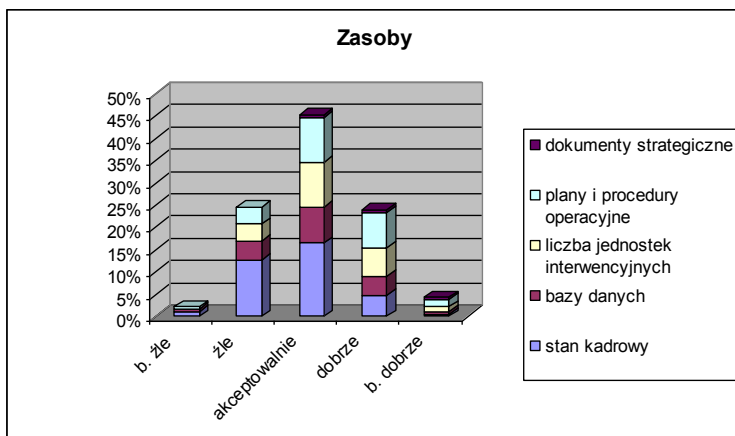
Rys. 69. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – organizacja⁶⁸⁷

Zasoby

Rys. 7 obrazuje sumaryczny rozkład zasobów, takich jak dokumenty strategiczne, plany i procedury operacyjne, liczba jednostek interwencyjnych, bazy danych oraz stan kadrowy.

⁶⁸⁶ Tamże, s. 17.

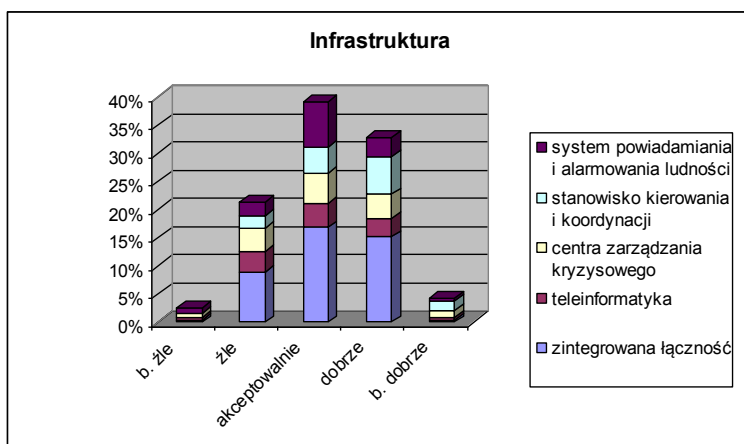
⁶⁸⁷ D. Wróblewski (red. nauk.), *Koncepcja Funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 13.



Rys. 70. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – zasoby⁶⁸⁸

Infrastruktura

Na rys. 71 przedstawiono sumaryczny rozkład elementów infrastruktury, takich jak system powiadamiania i alarmowania ludności, stanowiska kierowania i koordynacji, centra zarządzania kryzysowego, teleinformatyka oraz zintegrowana łączność.

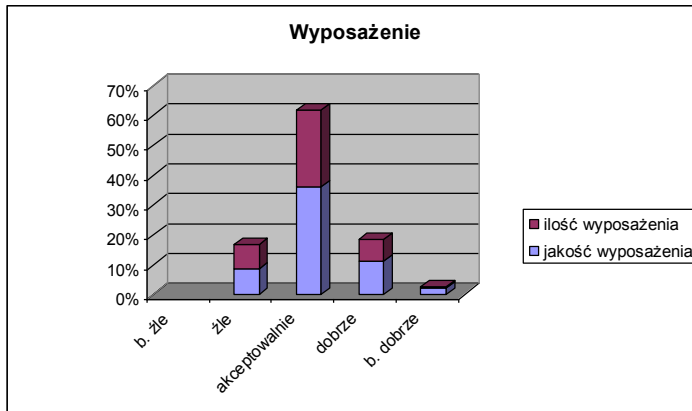


Rys. 71. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – infrastruktura⁶⁸⁹

⁶⁸⁸ Tamże, s. 8.

Wyposażenie

Rys. 72 przedstawia sumaryczny rozkład cech wyposażenia: jego ilości i jakości.



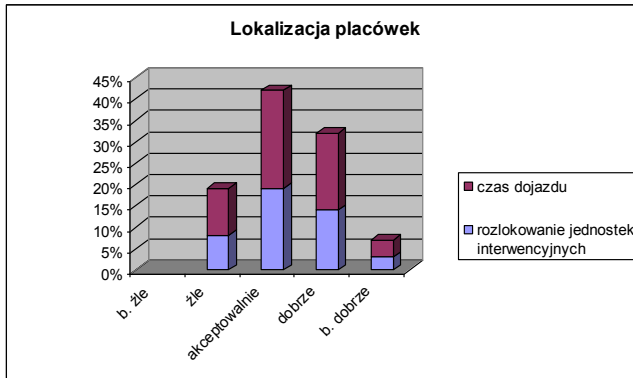
Rys. 72. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – wyposażenie⁶⁹⁰

Lokalizacja placówek

Na rys. 71 zobrazowany został sumaryczny rozkład elementów systemu określających lokalizację, czas dojazdu i rozlokowanie jednostek interwencyjnych.

⁶⁸⁹ Tamże, s. 9.

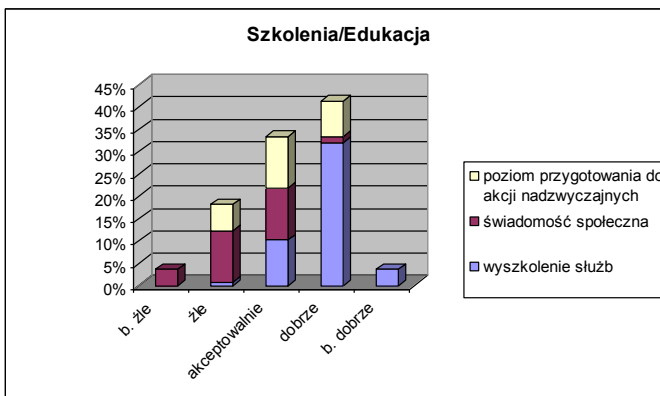
⁶⁹⁰ Tamże, s. 11.



Rys. 73. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – lokalizacja placówek⁶⁹¹

Szkolenie i edukacja

Rys. 74 pokazuje sumaryczny rozkład kolejnych elementów systemu, czyli cech szkolenia/edukacji.



Rys. 74. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – szkolenia/edukacja⁶⁹²

⁶⁹¹ Tamże, s. 12.

⁶⁹² Tamże, s. 14.

5.4.2. Analiza systemu

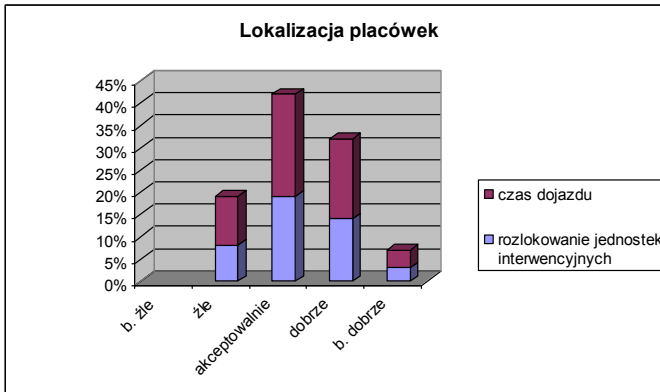
Zespół projektowy dokonał analizy, opierając się na materiałach (formularzach) nadesłanych przez wybrane podmioty zaangażowane w tworzenie RZSR WP.

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:

1. podmioty prowadzące działalność w skali województwa,
2. podmioty prowadzące działalność w skali powiatów,
3. podmioty prowadzące działalność w skali miast na prawach powiatu.

Z analizy wynika, że do słabych ogniw systemu należy zaliczyć brakujące lokalizacje, najwięcej potrzeb w tym zakresie zgłosiły podmioty zajmujące się ratownictwem medycznym, Państwowa Straż Pożarna, ochotnicze straże pożarne oraz Policja. Deficyty infrastrukturalnych potrzeb poszczególnych podmiotów dotyczą głównie prac remontowych i modernizacyjnych i innych działań mających na celu poprawę sytuacji w tym dużych potrzeby 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 wydają się być w pełni racjonalne⁶⁹³.

⁶⁹³ Tamże, s. 135-165.



Rys. 75. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – lokalizacja placówek⁶⁹⁴

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 obrazu systemu reagowania do osiągnięcia. 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, jak również efektu dopasowania do potrzeb użytkownika końcowego. Warto dodać, że promowanie zorganizowanego i systemowego myślenia o bezpieczeństwie może prowadzić do wytworzenia się kultury bezpieczeństwa⁶⁹⁵, definiowanej w organizacji i zarządzaniu jako zestaw wartości i norm, które wytyczają określony sposób myślenia, mówienia i działania związanego z bezpieczeństwem⁶⁹⁶.

W ramach badań dotyczących kapitału technicznego badaniu poddano elementy mające wpływ na:

⁶⁹⁴ Tamże, s. 107.

⁶⁹⁵ Patrz: definicja na s. 121.

⁶⁹⁶ 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. 17.

1. sprawne zarządzanie informacją oraz siłami i środkami systemu reagowania (stanowiska kierowania i koordynacji, centra zarządzania kryzysowego, teleinformatyka i zintegrowana łączność),
2. poziom i jakość nasycenia systemu siłami i środkami (liczba jednostek ratowniczych oraz prawidłowość ich rozlokowania, ilość i jakość wyposażenia),
3. 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, 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.

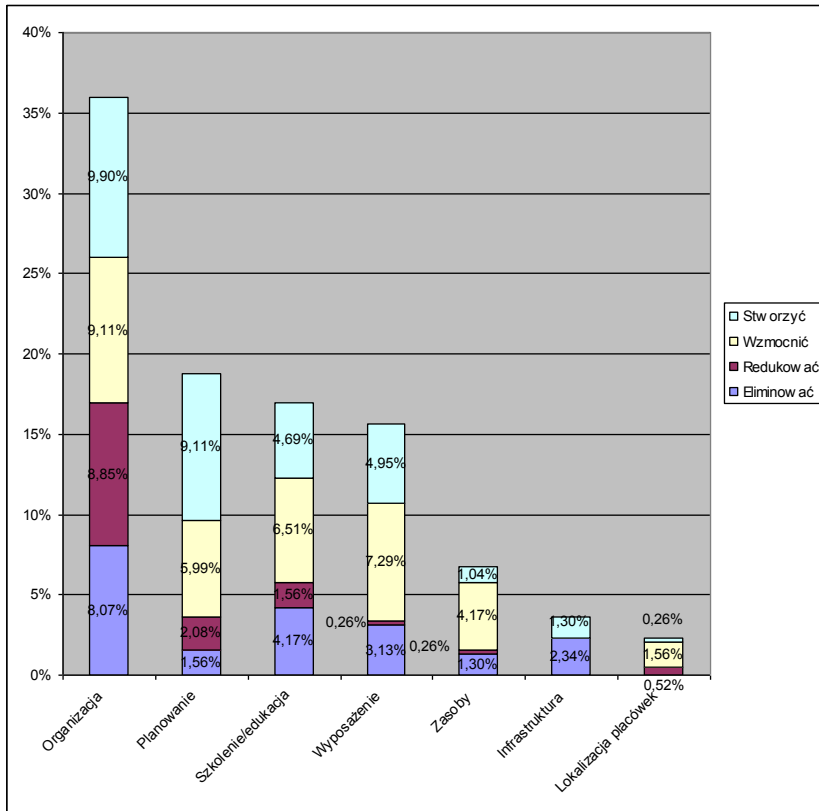
W odniesieniu do kapitału ludzkiego analizowane były dokumenty dotyczące stanu kadrowego, wyszkolenia służb i świadomości społecznej. Największe znaczenie w ocenie partnerstwa i komplementarności miały podmioty wchodzące w skład powiatów oraz funkcje, jakie mogą pełnić w razie wystąpienia określonych 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 wprowadzenia⁶⁹⁷.

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 lokaliza-

⁶⁹⁷ D. Wróblewski (red. nauk.), *Koncepcja Funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 188-190.

cja placówek. Graficzne przedstawienie zmian sugerowanych przez podmioty systemu przedstawia rys. 76⁶⁹⁸:



Rys. 76. Wskaźnik oczekiwanej potrzeby zmian sugerowanych przez podmioty systemu⁶⁹⁹

⁶⁹⁸ Tamże, s. 273.

⁶⁹⁹ D. Wróblewski (red. nauk.), *Koncepcja Funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, s. 273.

Rekomendacje w kontekście potrzeb zarządzania ryzykiem na rozpatrywanym terenie⁷⁰⁰

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 stworzyć (rozbudowywać) system reagowania, jak np.:

1. administracja rządowa,
2. administracja samorządowa,
3. organizacje pozarządowe,
4. jednostki sektora finansów publicznych,
5. przedsiębiorcy,
6. związki i stowarzyszenia,
7. Państwowa Straż Pożarna,
8. ochotnicze straże pożarne,
9. Policja,
10. Morska Służba Poszukiwania i Ratownictwa SAR,
11. pogotowie ratunkowe, szpitale oraz SOR;
12. straże miejskie i gminne,
13. Straż Graniczna,
14. inspektoraty ochrony środowiska,
15. inspektoraty nadzoru budowlanego,
16. inspektoraty weterynarii,
17. stacje sanitarno-epidemiologiczne,
18. Wodne Ochotnicze Pogotowie Ratunkowe,
19. centra zarządzania kryzysowego.

⁷⁰⁰ 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.

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.
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 strategicznej⁷⁰¹.

Podział na rekomendacje techniczne i nietechniczne powstał z uwagi na fakt, że z rekomendowanymi działaniami wiążą się wymierne koszty finansowe.

⁷⁰¹ Patrz szerzej: tamże, s. 23.

„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)”⁷⁰².

System monitorowania skuteczności zmian

Kolejnym etapem po wdrożeniu rekomendacji działań powinno być monitorowanie efektów działań i porównywanie ich z wcześniej przyjętymi założeniami. Zarówno monitorowanie⁷⁰³, jak i przegląd⁷⁰⁴ powinny być planowaną częścią procesu zarządzania ryzykiem i obejmować regularne weryfikowanie lub nadzór procesy monitorowania i przeglądu w organizacji obejmowały wszystkie aspekty procesu zarządzania ryzykiem. Rezultaty monitorowania i przeglądu powinny być dokumentowane oraz raportowane na zewnątrz i wewnątrz, jeśli jest to uzasadnione, oraz zaleca się, aby były używane również jako dane wejściowe do przeglądu struktury ramowej zarządzania ryzykiem⁷⁰⁵.

Z tego względu warto ustalić zestaw wskaźników w kontekście sformułowanych celów i oczekiwanych efektów oraz rozważyć, kto będzie tego dokonywał, co i kiedy będzie podlegało monitorowaniu, w tym wskaźniki nowe i wcześniej niemonitorowane. Najczęściej każdy z podmiotów uczestniczący 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 województwa⁷⁰⁶.

Jeżeli przyjmujemy założenie, że systemy reagowania oraz systemy bezpieczeństwa powszechnego pełnią funkcję usługową, należy rozważyć wykorzysta-

⁷⁰² Patrz: część I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 1 *Zarządzanie ryzykiem według normy ISO 31000*, podrozdział 1.4 *Proces zarządzania ryzykiem*.

⁷⁰³ Patrz: definicja na s. 37.

⁷⁰⁴ Patrz: definicja na s. 37.

⁷⁰⁵ Patrz: definicja na s. 26.

⁷⁰⁶ 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.

nie do wdrożenia strategii poprawy bezpieczeństwa narzędzia zwanego strategiczną kartą wyników. Strategiczna karta wyników jest narzędziem 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 publicznej⁷⁰⁷.

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.

⁷⁰⁷ Tamże.

6. DOCHODZENIE W SPRAWACH O POŻARY JAKO ELEMENT ZARZĄDZANIA RYZYKIEM POŻAROWYM W POLSCE

W Polsce problemy z niską jakością dochodzeń popożarowych oraz brakiem wykorzystania możliwości prewencyjnych tkwiących w poprawie standardu ustalania przyczyn pożarów były podnoszone wielokrotnie, m.in. podczas poznańskich konferencji *Research into the casues of fire*⁷⁰⁸. Były również prezentowane na posiedzeniu komisji sejmowej MSWiA⁷⁰⁹, jednak nie przyniosły one 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 NCBR⁷¹⁰, którego celem jest 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 jest Komenda Główna Państwowej Straży Pożarnej. Główne zadania zaplanowane do realizacji w projekcie to:

1. Analiza ekonomiczno-funkcjonalna dochodzeń popożarowych w Polsce obejmująca:

⁷⁰⁸ P. Guzewski (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z III Międzynarodowej Konferencji, Izba Rzecznawców SITP, Poznań 2003*; P. Guzewski (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z II Międzynarodowej Konferencji, Izba Rzecznawców SITP, Poznań 2005*; P. Guzewski (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z II Międzynarodowej Konferencji, Izba Rzecznawców SITP, Poznań 2007*.

⁷⁰⁹ <http://orka.sejm.gov.pl/Biuletyn.nsf/0/2B93F0D31874C31FC125788C0047B43B>, dostęp: marzec 2015 oraz

http://www.ptedp.pl/index.php?option=com_content&view=article&id=132&Itemid=153, dostęp: marzec 2015.

⁷¹⁰ Projekt nr DOBR-BIO4/050/13009/2013, metryka wniosku nr 13009 w ramach konkursu BIO 4 finansowanego przez Narodowe Centrum Badań i Rozwoju „Opracowanie systemowych rozwiązań wspomagających prowadzenie dochodzeń popożarowych wykorzystujących nowoczesne technologie, w tym narzędzia techniczne i informatyczne”.

- 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 popożarowych 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 popożarowych, w tym w szczególności:
 - a. stworzenie prostej w obsłudze aplikacji na urządzenia przenośne usprawniające odwzorowanie pogorzelniska, 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 (*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 pogorzeliisku (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 jest w okresie od grudnia 2013 r. do grudnia 2016 r. przez konsorcjum w składzie:

1. Szkoła Główna Służby Pożarniczej,
2. Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tułuskowskiego – Państwowy Instytut Badawczy,
3. Centralne Laboratorium Kryminalistyczne Policji – Instytut Badawczy,
4. Szkoła Aspirantów Państwowej Straży Pożarnej w Poznaniu,
5. przedsiębiorstwo CYBID Sp. j. w Krakowie.

6.1. 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 obrażenia⁷¹¹. 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

⁷¹¹ N. Brushlinsky, S. Sokolov, P. Wagner, J. R. Hall, *World Fire Statistics – Report № 10*, 2nd edition, Center of Fire Statistics of CTIF, 2005, s. 150.

Ziemi) wyniósł przeciętnie 0,3% PKB, a kolejne 0,7% PKB pochłaniały wydatki na utrzymanie jednostek straży pożarnych, techniczne środki zabezpieczeń przeciwpożarowych, ubezpieczenia oraz edukację i szkolenia, rozwój badań naukowych w tym obszarze⁷¹². 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% PKB⁷¹³. Główne problemy związane z zagrożeniami pożarowymi dzięki osiągnięciom nauki będą mogły być skutecznie rozwiązane dopiero w kolejnych stuleciach⁷¹⁴.

W Polsce w latach w 2003-2012 rejestrowano około 150-180 tys. pożarów rocznie (rys. 80)⁷¹⁵. 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 obiektów⁷¹⁶, ok. 20% pożarów – w obiektach mieszkalnych, kolejne 20%

⁷¹² Tamże, s. 151.

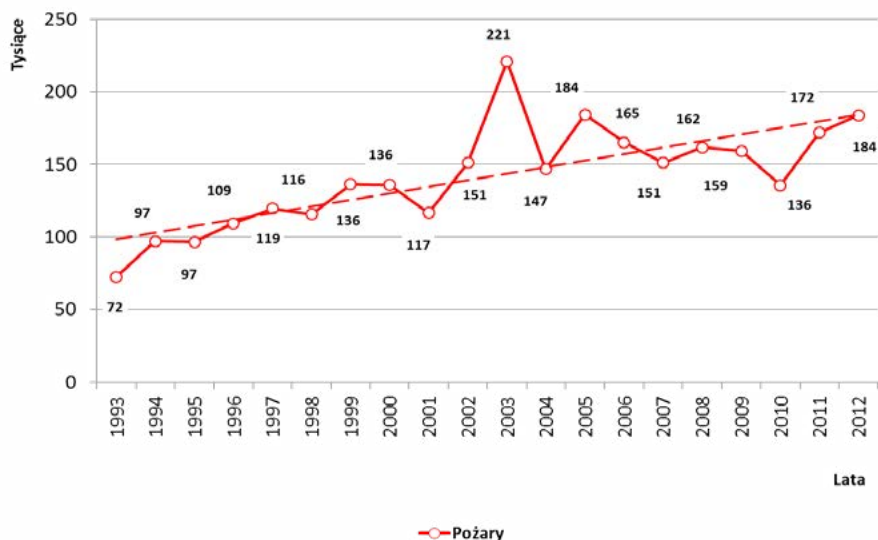
⁷¹³ Tamże, s. 152.

⁷¹⁴ N. Bruschlinsky, S. Sokolov, P. Wagner, *Ryzyko pożarowe i zapobieganie pożarom dzisiaj i prognozy na przyszłość*, w: P. Guzewski, D. Wróblewski, D. Małozieć (red.), *Czerwona księga pożarów*, CNBOP-PIB, Józefów 2014, s. 977-1034.

⁷¹⁵ Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 1993-2011*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 1994-2012.

⁷¹⁶ Inne obiekty to: śmietniki wolnostojące, wysypiska śmieci; zsypy, pomieszczenia zsypane, śmietniki wewnątrz budynków; kanały wentylacyjne, dymowe, dylatacje, palne elewacje lub okładziny ścian zewnętrznych; garaże, warsztaty samochodowe poza budynkami, w tym kompleksy garażowe; garaże, warsztaty samochodowe wewnątrz budynków mieszkalnych; garaże, warsztaty samochodowe wewnątrz pozostałych budynków lub ich części, zaliczonych do kategorii zagrożenia ludzi; garaże, warsztaty samochodowe wewnątrz budynków magazynowych i produkcyjnych; zabytki kultury materialnej niebędące budynkami; obiekty lub grupa obiektów przyrody naturalnej (pojedyncze drzewa, minerały, jaskinie, inne); obiekty hydrotechniczne; rozlewiska, wycieki, zanieczyszczenia powstałe na zbiornikach, ciekach i akwenach wodnych; inne zdarzenia powstałe na zbiornikach, ciekach i akwenach wodnych; obiekty wojskowe; obiekty użytkowane przez konsulaty, ambasady (eksterytorialne); pobocza dróg i szlaków komunikacyjnych (ale bez zdarzeń z udziałem środków transportu, bez pożarów traw na poboczach; płyty manewrowe i pasy lotnisk, szlaki kolejowe i manewrowe, drogi i ulice (ale bez zdarzeń z udziałem środków transportu, bez pożarów traw); trawy, trawniki na terenach nierolniczych, poboczach dróg i szlaków, ulic; zdarzenia występujące na dużych obszarach mieszkalnych lub gospodarczych na terenach gmin, miast i osiedli (np. poszukiwania ludzi i zwierząt na tere-

– 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% pożarów⁷¹⁷.



Rys. 77. Pożary w Polsce ogółem w latach 1993-2012⁷¹⁸

Wartość mienia, które uległo spaleniowi w pożarach w tym samym okresie (tzw. straty bezpośrednie), mieściła się w przedziale od ok. 1 do 1,4 mld zł rocznie (rys. 78)⁷¹⁹, ze średnią stratą przypadającą na jeden pożar wynoszącą ok. 6 tys. zł.⁷²⁰

nach wiejskich, miejskich, lasów, udział w ewakuacji z tych obszarów, pomoc w działaniach innych służb obejmujących te obszary; inne nietypowe obiekty, budynki, instalacje.

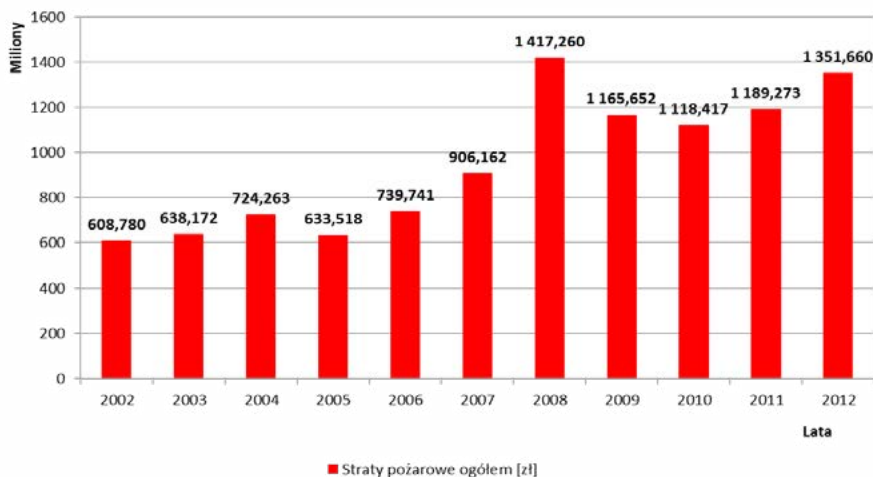
⁷¹⁷ Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2003-2012*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2004-2013.

⁷¹⁸ Źródło: opracowanie własne na podstawie: praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 1993-2012*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 1994-2013.

⁷¹⁹ Źródło: Komenda Główna Państwowej Straży Pożarnej, dane pozyskane z Informacji ze zdarzeń zawartych w programie do ewidencjonowania działań ratowniczych podejmowanych przez jednostki Krajowego Systemu Ratowniczo-Gaśniczego EWID.

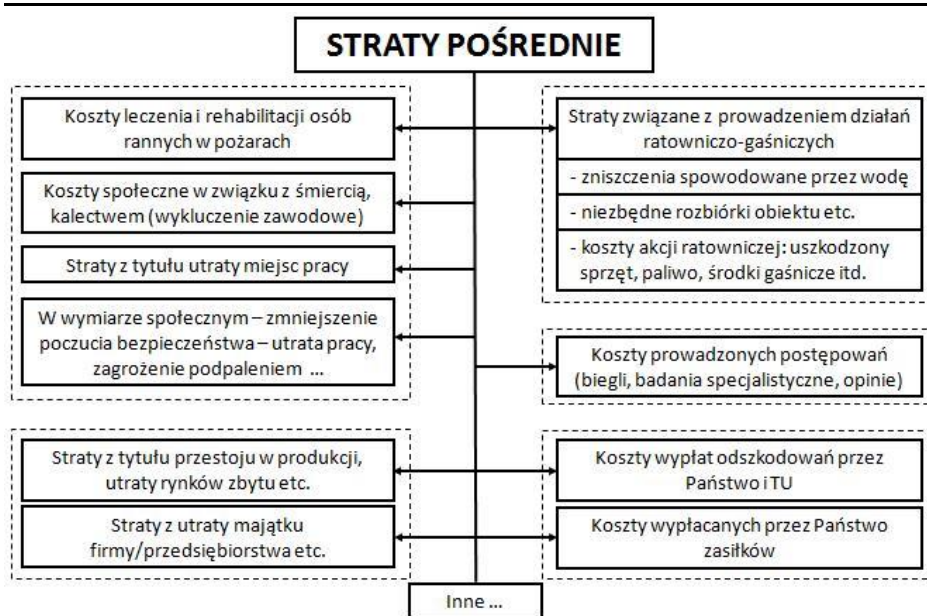
⁷²⁰ Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej. Roczniki*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2009-2013.

Straty pośrednie (rys. 79), nieobjęte ewidencją, nie są znane. Ocenia się, że mogą one stanowić wielokrotność strat bezpośrednich, zwłaszcza w grupie pożarów średnich, dużych i bardzo dużych.



Rys. 78. Straty bezpośrednie w pożarach w latach 2002-2012⁷²¹

⁷²¹ Opracowanie własne na podstawie: Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2002-2012*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2003-2013.



Rys. 79. Straty pośrednie w pożarach⁷²²

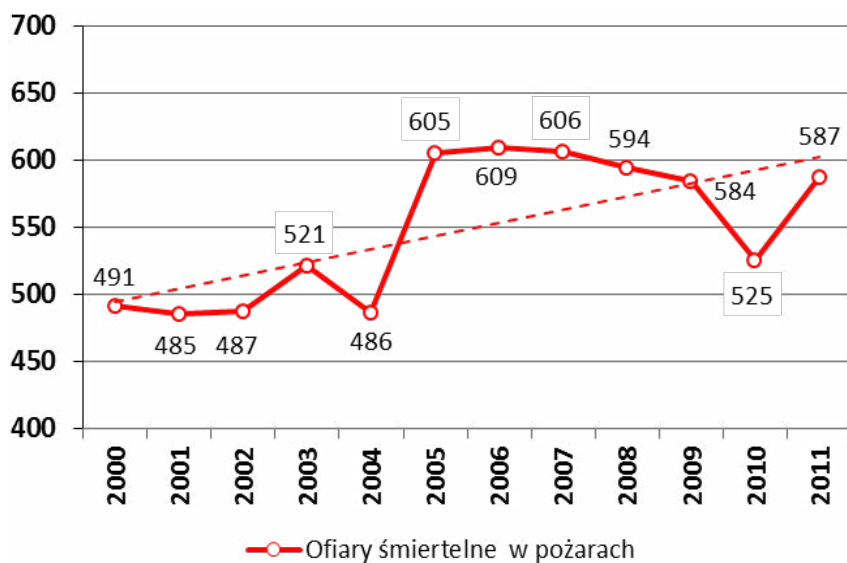
W Polsce w ostatnich latach w pożarach ginie każdego roku przeciętnie 540-580 osób (rys. 80), a ok. 4,0-4,3 tys. odnosi obrażenia (rys. 81)⁷²³. Koszty ponoszone przez państwo w związku ze śmiercią człowieka oszacowano na kwotę ok. 1 mln euro⁷²⁴. Koszty leczenia osób rannych w pożarach nie zostały jak 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

⁷²² Źródło: opracowanie własne.

⁷²³ Praca zbiorowa: *Biuletyn Informacyjny...*, wyd. cyt.

⁷²⁴ M. Giergiczny, *Wycena wartości statystycznego życia ludzkiego (VSL)*, w: P. Guzewski, D. Wróblewski, D. Małozieć (red.), *Czerwona księga pożarów*, publikacja opracowana w ramach projektu nr DOBR-BIO4/050/13009/2013 finansowanego przez NCBR, CNBOP-PIB, Józefów 2014, s. 639.

średni koszt leczenia pacjentów oparzonych to ok. 31 tys. zł.⁷²⁵, natomiast rzeczywiste koszty oscylują w przedziale od 4 do 100 tys. zł.⁷²⁶

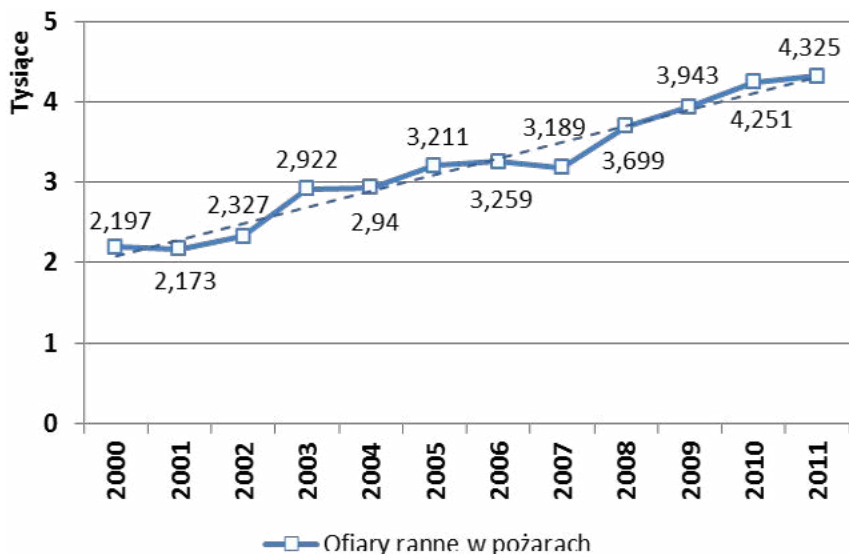


Rys. 80. Liczba ofiar śmiertelnych w pożarach w latach 2000-2011 (w tym ratownicy)⁷²⁷

⁷²⁵ M. Nowak, M. Kawecki, J. Skotnicka, G. Kniefel, I. Ryszkiewicz, *Wybrane aspekty medyczne i psychologiczne leczenia ofiar pożarów – organizacja leczenia oparzeń*, w: P. Guzowski, D. Wróblewski, D. Małozieć (red.), *Czerwona księga pożarów*, CNBOP-PIB, Józefów 2014, s. 567.

⁷²⁶ Tamże, s. 543.

⁷²⁷ Opracowanie własne na podstawie: praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2000-2011*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2001-2012.



Rys. 81. Liczba ofiar rannych w pożarach w latach 2000-2011 (w tym ratownicy)⁷²⁸

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)⁷²⁹. Wskaźnik ofiar śmiertelnych jest jednym z najwyższych w grupie 63 państw analizowanych przez *Centre of Fire Statistics* w okresie 1993-2002⁷³⁰ oraz w 2006 r. w grupie 30 analizowanych państwa świata⁷³¹. Podobnie wygląda sytuacja w odniesieniu do ofiar rannych.

⁷²⁸ Opracowanie własne na podstawie: praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2000-2011*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2001-2012.

⁷²⁹ Praca zbiorowa: *Biuletyn Informacyjny Państwowej Straży Pożarnej. Roczniki*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 1993-2013.

⁷³⁰ N. Brushlinsky, S. Sokolov, P. Wagner, J. R. Hall, *World Fire Statistics – Report № 10, ...*, wyd. cyt., s. 34.

⁷³¹ N. Brushlinsky, S. Sokolov, P. Wagner, J. R. Hall, *World Fire Statistics – Report № 13*, wyd. II, Center of Fire Statistics of CTIF, 2008, s. 32.

6.2. Zarządzanie ryzykiem pożarowym w aspekcie teoretycznym i praktycznym

Ryzyko pożarowe to *kombinacja prawdopodobieństwa wystąpienia pożaru oraz jego skutków*⁷³². Ryzyko jest codziennym elementem życia człowieka i podejmowanych przez niego wyborów. Identyfikacja ryzyka⁷³³ pożarowego, analiza⁷³⁴ prawdopodobieństwa jego wystąpienia, ewaluacja ryzyka⁷³⁵ stanowią podstawowe kroki w procesie zarządzania ryzykiem⁷³⁶, którego efektem jest planowanie przedsięwzięć ukierunkowanych na obniżenie ryzyka do akceptowalnego poziomu (rys. 82).



Rys. 82. Zarządzanie ryzykiem pożarowym⁷³⁷

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. 83). Scenariusze zdarzeń pożarowych oraz ich wpływ na funkcjonowanie firmy uwzględniane są w planach zapewnie-

⁷³² Należy tu zwrócić uwagę na zgodność z jedną z definicji ryzyka w normie ISO Guide 73:2009.

⁷³³ Patrz: definicja na s. 27.

⁷³⁴ Patrz: definicja na s. 31.

⁷³⁵ Patrz: definicja na s. 37.

⁷³⁶ Proces zarządzania ryzykiem pożarowym zawiera wybrane kroki procesu oceny ryzyka scharakteryzowanego w części I *Zagadnienia ogólne z zakresu zarządzania ryzykiem*, rozdział 1 *Zarządzanie ryzykiem według normy ISO 31000*, podrozdział 1.4 *Proces zarządzania ryzykiem*.

⁷³⁷ Źródło: opracowanie własne.

nia ciągłości funkcjonowania firmy – *Business Continuity Planning* (BCP) oraz analizach wpływu na efekt finansowy – *Business Impact Analysis* (BIA).

OCENA RYZYKA POŻAROWEGO

OBIEKT	PROCESY	CZŁOWIEK	UWARUNKOWANIA ZEW.
<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. 83. Obszary oceny ryzyka pożarowego⁷³⁸

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 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

⁷³⁸ Źródło: opracowanie własne.

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^{739, 740}.

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 etc. Służy to bezpośrednio zarządzaniu ryzykiem ubezpieczenia 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 etc.) czy też podczas posługiwania się ogniem otwartym 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 Hołyst⁷⁴¹. 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

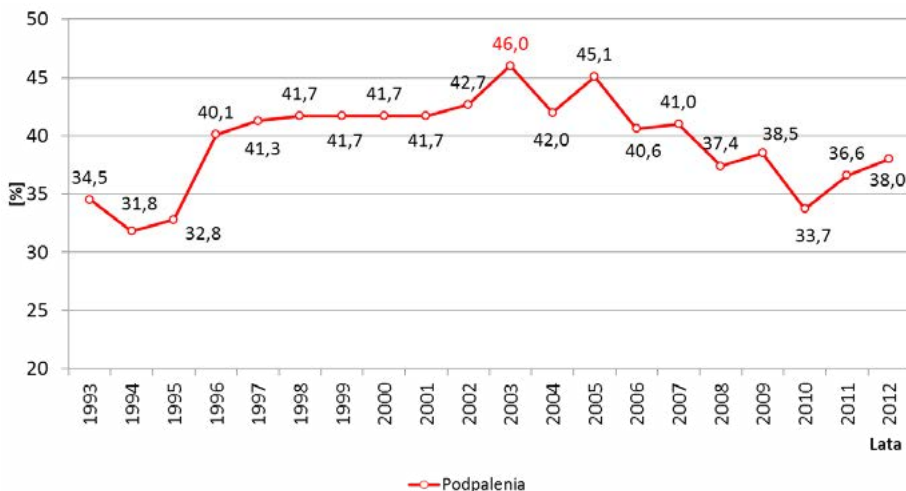
⁷³⁹ P. Guzewski, D. Wróblewski, D. Małozieć (red.), *Czerwona księga pożarów*, CNBOP-PIB, Józefów 2014.

⁷⁴⁰ Praca zbiorowa, *Safer Communities: Towards Effective Arson. The Report of the Arson Scoping Study*, Home Office, London 1999.

⁷⁴¹ B. Hołyst, *Kryminalistyczna problematyka pożarów*, Wydawnictwo Zakładu Kryminalistyki Komendy Głównej MO, Warszawa 1962, s. 22.

w Polsce, ale również w wielu państwach UE i świata⁷⁴². 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, co wynika 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. 84).

⁷⁴² B. Albinson, U. Erlandson, *Fire investigation methods and lessons learned from fires and other relevant incidents – Final Report*, Swedish Rescue Services Agency – Emergency Prevention Department, Karlstad 2005.



Rys. 84. Podpalenia w latach 1993-2012⁷⁴³

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 etc.

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,

⁷⁴³ Opracowanie własne na podstawie: praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 1993-2012*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 1994-2013.

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%⁷⁴⁴, 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 podpażeń, 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 1997⁷⁴⁵ do 18% w roku 2011⁷⁴⁶. 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.

⁷⁴⁴ D. Myers, *Ograniczenie liczby podpażeń poprzez zastosowanie podejścia partnerskiego do dochodzeń popożarowych w Wielkiej Brytanii*, w: P. Guzowski (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z II Międzynarodowej Konferencji*, Izba Rzecznawców SITP, Poznań 2005, s. 136.

⁷⁴⁵ D. Myers, *Ograniczenie liczby podpażeń...*, wyd. cyt., s. 135.

⁷⁴⁶ Praca zbiorowa, *Fire Statistics, Great Britain 2010-2011*, Department for Communities and Local Government, London November 2011, s. 10.

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:

1. *wiemy, że wiemy (known knowns),*
2. *wiemy, że nie wiemy (known unknowns),*
3. *nie wiemy, że nie wiemy (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)⁷⁴⁷.

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.

⁷⁴⁷ Z. W. Kundzewicz, P. Matczak, Z. Sadowski, *Wprowadzenie do raportu o zagrożeniach*, Nauka 4/2010 PAN, s. 12.

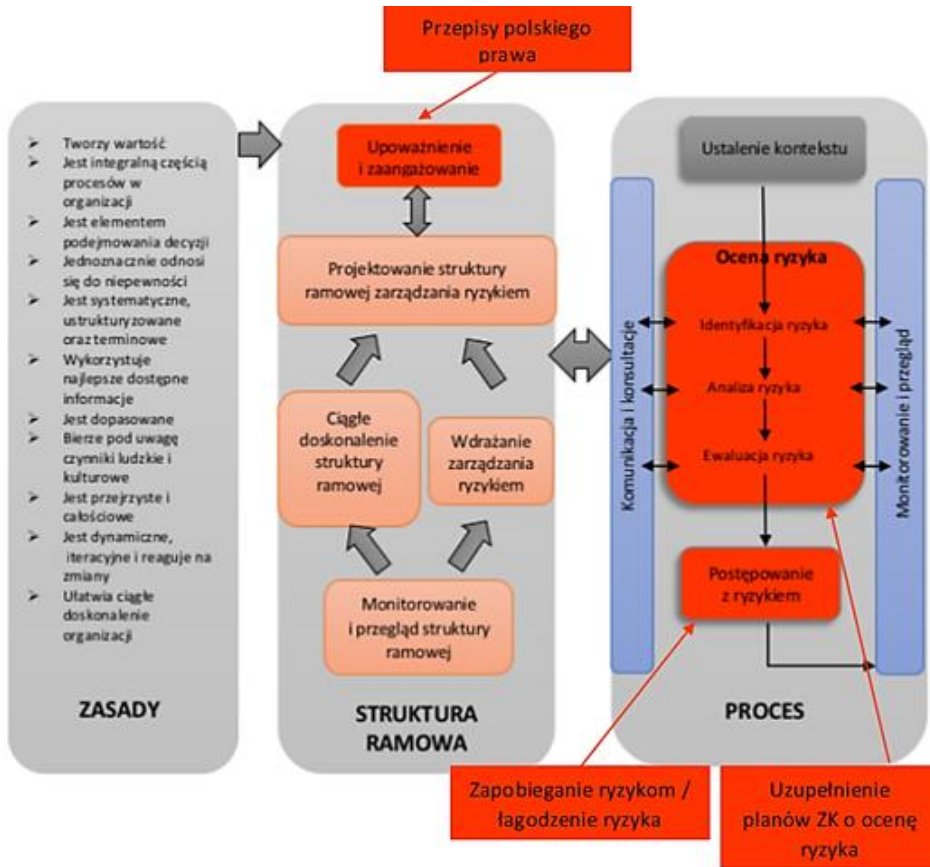
Można więc wskazać, że zarządzanie ryzykiem to proces, w wyniku którego organizacja (a więc i państwo) zdobywa zdolność łagodzenia ryzyka, a w konsekwencji ograniczania skutków zagrożeń. Refleksja nad tymi możliwościami (a także obowiązkiem państwa) w konsekwencji prowadzi do sformalizowania wymagań w postaci dedykowanych rozwiązań prawnych.

Biorąc pod uwagę analizę przepisów ustawy o zarządzaniu kryzysowym wraz towarzyszącymi jej rozporządzeniami, poprzez ich uogólnienie, można określić generalne grupy wymogów w zakresie zarządzania ryzykiem, które dla systemu zarządzania kryzysowego wskazał ustawodawca. Wymagania te to:

1. rozszerzenie planów zarządzania kryzysowego o **ocenę ryzyka** oraz **mapy ryzyka**,
2. **zapobieganie ryzykom** (łagodzenie ryzyka) funkcjonalności i ciągłości działań oraz integralności infrastruktury krytycznej,
3. uwzględnienie w ocenie ryzyka **podatności** obiektów IK,
4. wykorzystanie przy ocenie ryzyka **metody scenariuszowej**.

Biorąc pod uwagę powyższe warunki⁷⁴⁸ oraz wskazane propozycje organizacji ISO, można skazać graficznie (rys. 85) obszary zaleceń ISO, które mogą zostać wykorzystane (przy obecnie obowiązujących normach prawnych) przez system zarządzania kryzysowego.

⁷⁴⁸ Wymogi te należy traktować jako spełnienie zaleceń wynikających z norm ISO odwołujących się również do zewnętrznych warunków formalnych, z uwzględnieniem przepisów obowiązującego prawa oraz przedsięwzięć realizowanych podczas etapu *upoważnienia*.



Rys. 85. Proces zarządzaniem ryzykiem a potrzeby systemu zarządzania kryzysowego⁷⁴⁹

Ujęte na rys. 85 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, że⁷⁵⁰:

⁷⁴⁹ Źródło: opracowanie własne.

⁷⁵⁰ Wymienione zasady (wskazane w dalszej części rozdziału poprzez zastosowanie *kursywy*) wskazuje norma PN-ISO 31000:2012 w części: Zasady, s. 27-29.

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 *ciągłe doskonalenie organizacji i ułatwia proces doskonalenia organizacji*⁷⁵¹.
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*⁷⁵².
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*.

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 *rozumienia kontekstu* z pewnością wypełniany jest poprzez konieczność ujmowania w procesie planowania zagrożeń wraz z ich charakterystyką. Działanie to odnosi się do szeroko rozumianego zewnątrz systemu (sytuacje kryzysowe czy zagrożenia polityczno-militarne), ale i ukazania własnego potencjału (czyli wnętrza).

⁷⁵¹ Zapewnia również zaangażowanie w proces zarządzania ryzykiem decydentów (wymóg procesu projektowania struktury ramowej)

⁷⁵² Kolejne aktualizacje uzupełniają dokument o nowe zagrożenia/ryzyka i wskazują sposoby postępowania z nimi.

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, których działanie 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 i konsultacji czy monitorowania i przeglądu*.

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 towarzyszące 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 dysfunkcyjny, 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.

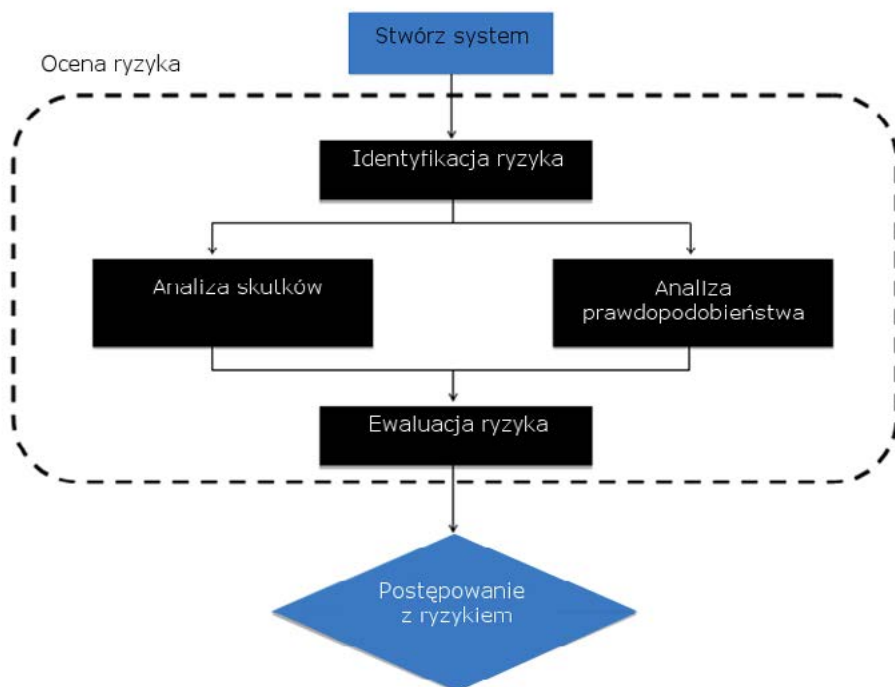
Porównanie norm z przepisami prawa wykazało jeszcze jeden problem uniemożliwiający pełną ich implementację. Ocena ryzyka na potrzeby zarządzania kryzysowego wychodzi od oceny wystąpienia zagrożeń (w tym dla zdrowia, życia, mienia i środowiska). W tej sytuacji to zagrożenie staje się podstawową kategorią 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 służą-

cych 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. 88 obszarów:

1. *upoważnienia i zaangażowania,*
2. *oceny ryzyka,*
3. *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 IV. Przy dokonywaniu *oceny ryzyka* i określaniu sposobów *postępowania z nim* można zastosować rozwiązania wykorzystywane w standardzie BSI. Sposób ten przedstawia rys. 86.



Rys. 86. Proces oceny ryzyka⁷⁵³

Jak wynika z rys. 86, 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 metody⁷⁵⁴:

1. SWIFT – „co, jeśli?”,
2. metodę scenariuszową,
3. metodę drzewa błędów,

⁷⁵³ Źródło: opracowanie własne na podstawie materiału szkoleniowego BSI: PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym.

⁷⁵⁴ 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 matrycy ryzyka:

Tabela 82. Przykładowa matryca ryzyka 6 x 6⁷⁵⁵

X	Prawdopodobieństwo					
Skutki						

Matryce stosowane obecnie przez system zarządzania kryzysowego są matrycami nieparzystymi 5 x 5⁷⁵⁶. W opinii autorów (po dokonaniu analizy raportów cząstkowych) należy wskazać, że w projektowanej metodzie powinno się zastosować matryce o liczbie parzystej (np. 4 x 4 lub 6 x 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 kryzysowego⁷⁵⁷. 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 ryzykiem⁷⁵⁸ do wypełnionej matrycy można zastosować poniżej

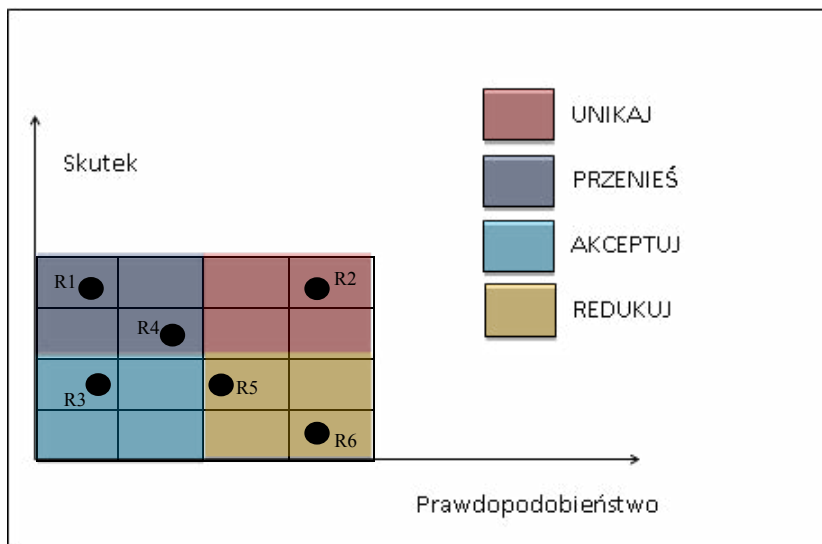
⁷⁵⁵ Opracowanie własne na podstawie: ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*.

⁷⁵⁶ Takie matryce 5 x 5 stosuje się między innymi podczas sporządzania raportów cząstkowych i *Raportu o zagrożeniach bezpieczeństwa narodowego*.

⁷⁵⁷ Dyrektywy wskazują jako nazwę dokumentu przypisanego do tego działania: *Plan postępowania z ryzykiem*.

⁷⁵⁸ K. Gawęcki, *PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym*, materiał szkoleniowy BSI, Warszawa 2012.

przedstawiony zabieg. Matryce dzielimy na cztery części, tak by stworzone w ten sposób pola determinowały dalsze sposoby postępowania.



Rys. 87. Zasady wyboru opcji postępowania na przykładzie matrycy ryzyka⁷⁵⁹

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 przez system zarządzania kryzysowego metod zarządzania ryzykiem należy dążyć do jego rozszerzenia.

Analiza przedstawiona w niniejszej części wskazuje, że postulat ten może zostać spełniony z wykorzystaniem norm ISO. Potwierdza ona również postawioną w części IV hipotezę, że:

Zalecenia i dyrektywy ISO można wykorzystać w procesie planowania cywilnego w zakresie ujednoczenia nazewnictwa wykorzystywanego przez system ZK oraz przygotowania procesu oceny ryzyka i procedur postępowania z ryzykiem.

⁷⁵⁹ Źródło: opracowanie własne na podstawie: ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*.

Tak więc pozytywna odpowiedź na problem badawczy, który brzmiał: *czy narzędzie, jakim są normy ISO (w zakresie zarządzania ryzykiem), można efektywnie wykorzystać w procesie planowania cywilnego?*

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 IV 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. System zarządzania kryzysowego ma zdolności do wdrożenia pełnego procesu zarządzania ryzykiem, jednak możliwe to będzie dopiero po zmianie obowiązującego prawa.
3. Wiele norm podejmuje problematykę zarządzania czy oceny ryzyka, niemniej jednak na potrzeby planowania cywilnego wystarczające jest oparcie się na: 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 – ujednolicenia 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, mający na celu zwalczanie 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 zaleceń 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 spójne w zadowalającym stopniu 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 ryzyk 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 oraz wskazanie optymalnych kierunków działań doskonalących. Istota metody zawiera się w powiązaniu systemowym wyników analizy ryzyka z jednoznacznym wskazaniem przyczyn, kierunków eliminacji i redukcji ryzyk oraz optymalnych kierunków rozbudowy i doskonalenia systemu reagowania (ratownictwa) czy innego systemu bezpieczeństwa. PomRisc stanowić może doskonałe 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. 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.

SUMMARY AND CONCLUSIONS

The needs connected with a system-based approach to risk management are today more valid than ever for emergency management. Since introducing the elements of risk management in 2009, its importance has been continuously growing. It is therefore recommended to use recognised guidelines for risk management, which unify the terminology, offer universal principles, a flexible framework structure, appropriately matched processes, including tools supporting risk assessment and risk management evidencing. The legal framework in force does not support currently a possibility of implementing best practices in risk management in this scope, hence it is important to discuss the matter of amending legislation in this field.

Donald Rumsfeld delivered a speech in 2002 a part of which is frequently quoted. Rumsfeld distinguished three categories of knowledge by referring to the notion of a threat. He pointed that these are situations in which there exist:

1. *known knowns*;
2. *known unknowns*;
3. *unknown unknowns*.

The first two refer to a situation where we have cognitive control. Dangers in the third case are not taken into account at specific time. It may be that we do not realise we do not know something, at all. Rumsfeld failed to mention one more category though, necessary for combinatoric completeness – when we pretend we do not know, while consciously ignoring the knowledge (unknown knowns)⁷⁶⁰.

Insofar ignorance is a category which cannot be subject to a rational discourse, nonetheless the other categories (indicated as the first three categories) assume that behaviours are rational, and when analysing such behaviours, to make them as useful as possible, only such notions as *uncertainty*, *consequences* or *risk* should be taken into consideration. It is the risk assessment that enables an organisation to identify and describe threats and manage them regardless it can take control over them at the start of the process or not. It can thus

⁷⁶⁰ Z. W. Kundzewicz, P. Matczak, Z. Sadowski, *Introduction to the Report on Threats*, Nauka 4/2010, PAN, p. 12.

be pointed out that risk management is a process as a result of which an organisation (so also the state) acquires a capability to mitigate a risk, and consequently to reduce the effects of threats. By reflecting over such possibilities (and also the state's obligation), requirements are consequently formulated in the form of dedicated legal solutions.

If we take into account an analysis of the provisions of the emergency planning act with its accompanying ordinances, general groups of requirements for risk management indicated by the regulator for the emergency management system can be determined by generalising them. The requirements include:

1. to expand emergency management plans to incorporate **risk assessment** and **risk maps**;
2. **risk prevention (risk mitigation)** for functionality, continuous operation and integrity of critical infrastructure;
3. to consider **vulnerability** of IK objects in risk assessment;
4. to use **a scenario-based method** for risk assessment.

Having regard to the above conditions⁷⁶¹ and the indicated proposals of ISO organisation, the areas of ISO recommendations can be shown on the image shown (fig. 85), which can be used (for the currently valid legal standards) by the emergency management system.

⁷⁶¹ The requirements should be viewed as the fulfilment of recommendations resulting from ISO standards referring also to external formal conditions in accordance with valid laws and projects carried out at the *empowerment stage*.

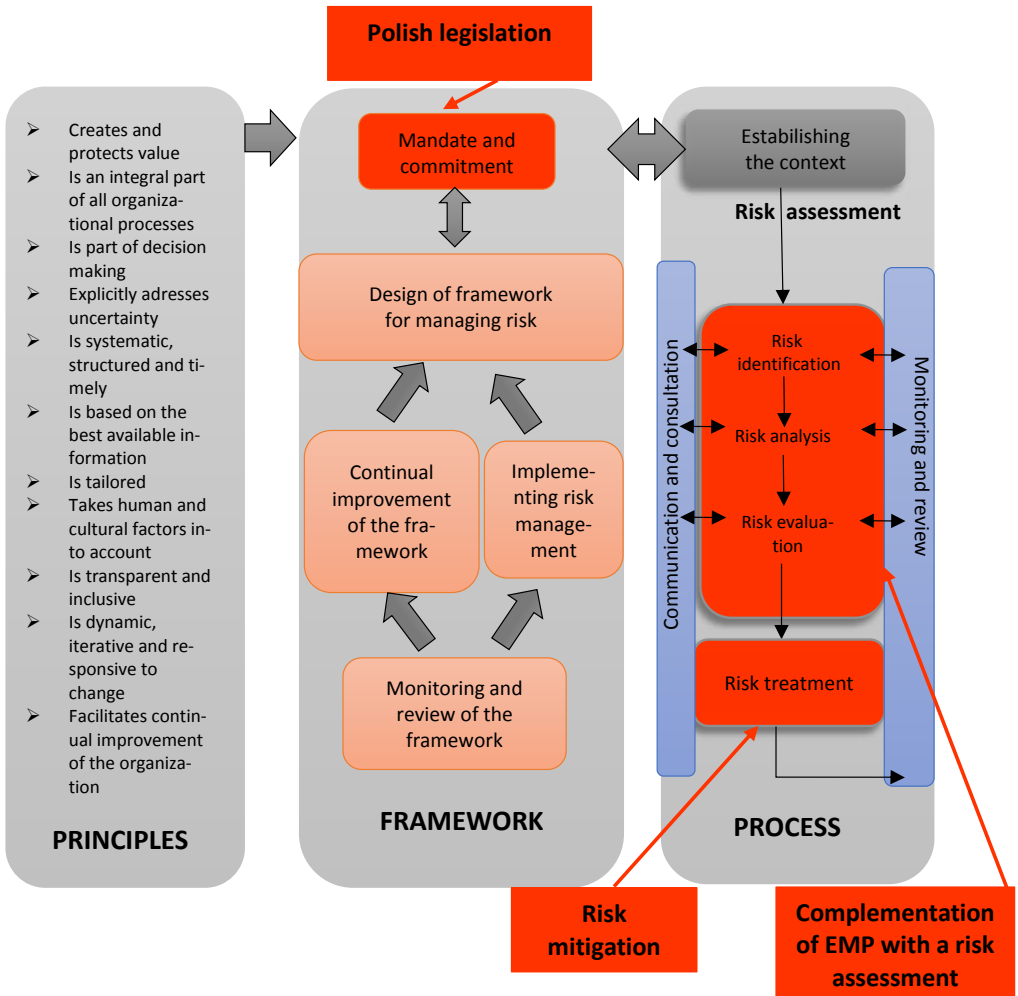


Fig. 85. Risk management process and the needs of the emergency management system⁷⁶²

The emergency management system requirements shown in the figure above are direct requirements and result literally from the law. It should nevertheless be noted that other indirect legal regulations exist referring indirectly to the rules of ISO standards.

⁷⁶² Reference: an own study.

It can be stated when comparing risk management *principles* with requirements of the provisions of the act delegated for its ordinances that⁷⁶³:

1. A principle of *integrity of risk management with processes relevant to the organisation* would be fulfilled by introducing a risk assessment requirement into a civilian emergency planning process.
2. It can be pointed out considering the process of preparing, approving and the structure of interim reports and the *Report on threats to state security* (public administration's requirements, necessity to consider conclusions from reports in emergency management plans or the adoption of the *Report* by the Council of Ministers) that it is an *element of decision-making* influencing *constant improvement of organisation and it facilitates the organisation improvement process*⁷⁶⁴.
3. *Is systematised, structured and timely* as legal regulations specify the structure of not only documents but also of the process and the dates of the next document updates. At the same time, the obligatory biannual update makes it *dynamic, iterated and responsive to changes*⁷⁶⁵.
4. Through its objectives, it *creates, but first of all protects values* (human life, environment, state interests) and in the process, as all relevant entities participate (ministries, heads of central and voivodeship offices), *uses the best available information*.

It is naturally debatable to what extent the imposition itself of obligations in scope of civilian emergency planning (including risk assessment) on governmental bodies, so on the structure of the state, can be regarded as the fulfilment of a recommendation concerning framework structure preparation. Certainly some of the framework structure's elements are materialised by the general principles of the ZK system. The requirement of *understanding the context* is surely met by the necessity to include threats in the planning process

⁷⁶³ The principles mentioned (indicated further in the chapter by *italicisation*) are indicated in PN-ISO 31000:2012 in the part: principles, p. 27-29.

⁷⁶⁴ It also ensures that decision-makers are engaged in the risk management process (a requirement of the framework structure designing process)

⁷⁶⁵ The next updates are adding new threats/risks to the document and indicate handling methods.

together with describing such threats. This activity refers to a widely understood exterior of the system (crisis situations or political and military threats), but also to showing an own potential (i.e. interior).

It should also be noted that some elements of the framework structure, i.e. *determination of internal and external communication and reporting are available* (tools which can fulfil this function are available) to the emergency management system, however, they are not used in a literally understood risk management process. The operating emergency management centres, whose activities could be considered as entities fulfilling such recommendations, are not involved in the process described. An issue of *constant improvement, monitoring and review of framework structure, communication and consultation or dunning and review* can be approached likewise.

Given the complexity of the system and diverse processes executed therein, a theoretical emergency management system model can be built, in which each element indicated in the standards can be ascribed to the existing bodies, persons or institutions. Such considerations would be purely postulatory though, at least for two reasons:

1. The system is based on formal legal solutions, consequently, for its individual elements to fulfil the allocated roles in the risk management process, the valid law must be changed.
2. Solely elements of the risk management process have been introduced to the emergency management system as a result of amending the emergency management act of 2009 and its accompanying ordinances. Risk assessment was an item on which the main focus was placed, without introducing the full risk management process. Such situation is dysfunctional as even for a correctly assessed risk there is no legal obligation to manage it properly.

In such circumstances we face a situation where the lack of pertinent legal regulations hinders to implement and use fully the ISO standards.

Additionally, one more problem preventing their full implementation has been identified by comparing the standards with legal regulations. Risk assessment for the purpose of emergency management begins with the estimation of existing threats (including health, life, property, environment). In this situation the threat becomes the basic category and a starting point for the entire pro-

cess is to define it appropriately. A process is the principal category for the risk management described in the standards. A risk is identified in this case for processes serving to achieve the set objectives within an organisation and they are the basic category to which all further activities relate.

The divergences addressed above are therefore conditional for the way of solving the research problem. The areas shown in fig. 88 have to be discussed at the current stage of considerations, i.e.:

1. *empowerment and involvement*;
2. *risk assessment*;
3. *risk handling*.

As *empowerment* and *involvement* is an outcome of legal regulations in scope of emergency management and general legal norms governing the functioning of public administration in Poland, they are not discussed more broadly in the considerations in part IV. When performing *risk assessment* and determining the methods of *risk handling*, the solutions used in a BSI (*British Standards Institutions*) standard can be applied. This method is shown in fig. 86.

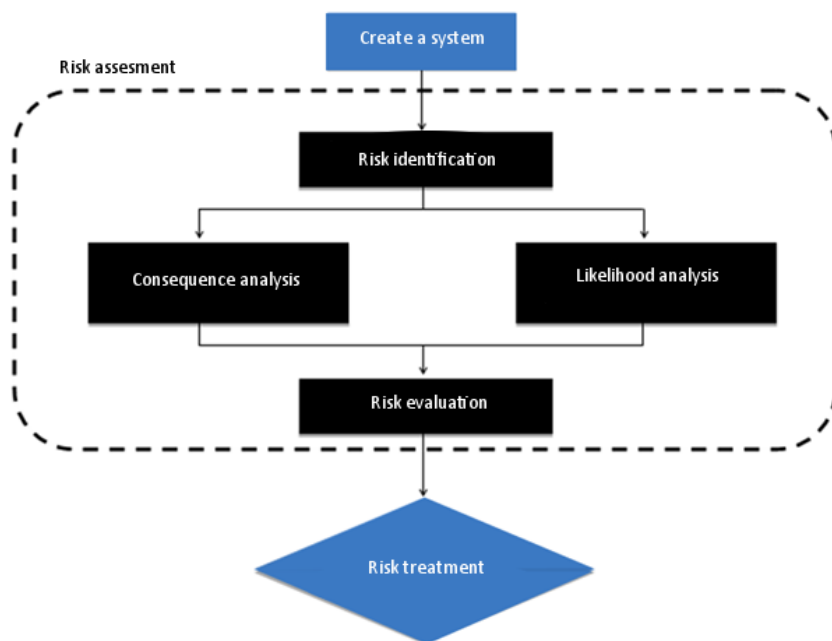


Fig. 86. Risk assessment process⁷⁶⁶

The figure above reveals that *risk identification, analysis of consequences and likelihood* is necessary for risk assessment.

After analysing the *methods* indicated in table 3 and the needs of the project for which the studies have been pursued, it can be asserted that the following method can be employed to make a risk assessment (apart from risk identification)⁷⁶⁷:

1. SWIFT – *what if?*.
2. Scenario method.
3. Fault tree.
4. Event tree.
5. Bow tie.

⁷⁶⁶ Reference: an own study according to training material BSI: PN-ISO 31000:2012 – guidelines in scope of corporate risk management.

⁷⁶⁷ K. Gawęcki, Training material: PN-ISO 31000:2012 – guidelines in scope of corporate risk management, BSI training material, Warsaw, 2012.

Regardless the method selected, it is desired to present the results of the above analyses on a risk matrix to determine the next element:

Table 82. Example of 6x6 risk matrix⁷⁶⁸

X	Likelihood					
Consequences						

The matrices currently used by the emergency management system are non-parity 5x5 matrices⁷⁶⁹. It is the author's opinion (after analysing interim reports) that parity matrices should be used in the planned method (e.g. 4x4 or 6x6). This solution will eliminate a common procedure of averaging the results of likelihood and consequences.

Matrices are created to determine the context to establish a further risk handling procedure to be subsequently incorporated into emergency management plans⁷⁷⁰. Before an organisation starts to prepare procedures (relevant to the civilian planning process), the standards indicate general directions of the next actions. The adopted risk handling practice⁷⁷¹ provides that the procedure presented below can be used for a completed matrix. The matrix is divided into four parts so that the fields created determine further actions.

⁷⁶⁸ Reference: an own paper based on: ISO/IEC 31010 *Risk Management – Risk Assessment Techniques*.

⁷⁶⁹ Such 5x5 matrices are used mainly when preparing interim reports and the Report on threats to state security.

⁷⁷⁰ The directive indicate as a name of a document dedicated to such measure – *risk handling plan*.

⁷⁷¹ K. Gawecki, *Training material: PN-ISO 31000:2012 – guidelines in scope of corporate risk management*, BSI training material, Warsaw, 2012.

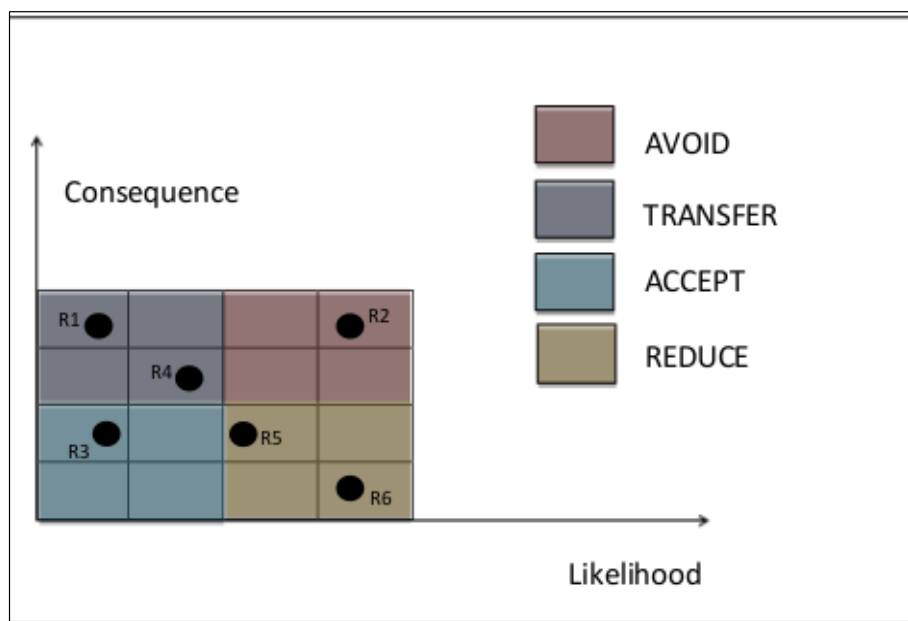


Fig. 87. Selection principles of actions with the example of risk matrix⁷⁷²

The aspect of risk assessment was adopted in the Polish legal order over five years ago. The emergency management system has introduced such principles in the meanwhile and now we can see how far the approach proposed by the law has fulfilled its task. A general argument can be proposed based on the experience gathered by the system in the meanwhile:

Due to a limited scope of the risk management methods used by the system, an attempt should be made to expand the system.

An analysis presented in this part shows that the argument can be fulfilled using ISO standards. It also confirms the hypothesis presented in part IV that:

The ISO recommendations and directives can be used in the civilian emergency planning process to harmonise a terminology used by the EM system and prepare the risk assessment process and risk management procedures.

Therefore, a positive answer to the following research problem, i.e.,

⁷⁷² Reference: an own paper based on: ISO/IEC 31010 *Risk Management — Risk Assessment Techniques*.

can tools such as ISO standards (for risk management) be effectively used in the civil emergency planning process?

has allowed to determine which of the processes, guidelines and methods recommended by the ISO can be used for complying with the valid emergency management law (chapter VI of the act).

Part IV presents a diagnosis of the current status (valid law, methodologies used) enabling to indicate the desired and effective solutions aimed at improving the civilian emergency planning process as far as it uses the notion of risk.

The following conclusions should be stated given the above:

1. The risk management methods currently implemented by the emergency management system (conditioned by the legal order) are insufficient for the full application of ISO standards.
2. The emergency management system is capable of implementing a full risk management process, however, it will only be possible after changing the valid law.
3. Numerous standards concentrate on risk management or risk assessment, nonetheless, it is sufficient to rely on PN-ISO 31000:2012 *Risk management. Principles and guidelines*, PKN-ISO Guide 73:2012 *Risk Management – Terminology* and ISO/IEC 31010 *Risk Management – Risk Assessment Techniques* for the purpose of civilian emergency planning.
4. The standards highlighted in item three of the standard can be used in scope of:
 - a. PKN-ISO Guide 73:2012 *Risk Management – Terminology* – harmonisation of vocabulary;
 - b. PN-ISO 31000:2012 *Risk Management. Principles and guidelines* – identification of processes;
 - c. ISO/IEC 31010 *Risk Management – Risk Assessment Techniques* – to use the methods and research tools stated there.
5. The research results presented show that the standards (despite a different approach to risk) should be taken into account when preparing a risk assessment methodology.
6. Flood risk management is conditioned by a sectoral and strategic dimension of such solution whose purpose is to combat this force that has not been harnessed by man so far. The method mentioned is not applicable to

- other risk management areas. Space for improvement can be found in its structure, though, in terms of international recommendations of ISO risk management standards.
7. All the risk assessment methodologies collected in the regulations of the national ministry-specific law contain joint elements such as the basic risk management phases, including notably: risk identification, risk analysis, risk evaluation, risk management or monitoring of the undertaken measures. Uncomplicated qualitative descriptions are used to assess a risk. Risk matrices and simple graphical representations in the form of risk maps are also used. A reference document in most of the cases is the information included in announcements of the Minister of Finance concerning detailed guidelines for a public finance sector in scope of risk planning and management.
 8. The risk management documents existing in the ministry-specific law show satisfactory consistency with the guidelines of ISO 31000:2009. It is important though that the analysis was only based on those ministries and central offices which have prepared full risk assessment documents. In this case it appears necessary to create uniform guidelines (e.g. based on ISO 31000), on the basis of which ministries would establish their risk management methods.
 9. The state administration documents analysed reveal that risk management should be a continuous, active and systematic process aimed at understanding the risk, manage it and inform about it. Risk management at a central level should facilitate strategic decision-making contributing to the achievement of objectives.
 10. Risk management in the national local law exists to a limited extent. Risk assessment methodologies are mainly used for governance control focusing most of all on balanced management of finance and other resources. A fact is also broadly perceived that it is worth developing the solutions elaborated in this field and use them for the purpose of safety – including emergency management. It should be noted that responsibilities associated with risk exist and are used at all levels of state administration. It would be substantiated and important to extend them across the whole institu-

tion and integrate within a uniform risk management system in public administration.

11. It should be considered to use ready and proven solutions for risk assessment and proper risk interpretation – especially where an expert analysis seems justified. The PomRisc method was created in 2009 based on literature and Australian methods, including a draft of the prepared ISO 31000 standard. A unique method discovering unexplored areas of risk assessment were then created. The PomRisc methodology enables to diagnose the condition and indicate optimum directions of improvement actions. The essence of the method consists of system linkages between the risk analysis results and clear indication of causes, directions of risk elimination and reduction and optimum directions of expansion and improvement of the response (rescue) system or another safety system. ‘PomRisc’ may be an excellent tool to be used in plans, proceedings of an emergency management team, containing elements useful for paving new directions in safety development and works of research teams and practitioners.
12. Actions are necessary leading to full implementation and improvement of the fire risk management process in Poland – also for the application of recommendations of international ISO standards laying down methods of designing a risk management architecture and its formal launch.

LITERATURA

Wydawnictwa zwarte i czasopiśmiennicze

1. Albinson B., Erlandson U., *Fire investigation methods and lessons learned from fires and other relevant incidents – Final Report*, Swedish Rescue Services Agency – Emergency Prevention Department, Karlstad 2005.
2. Bruszlinsky N., Sokolov S., Wagner P., *Ryzyko pożarowe i zapobieganie pożarom dzisiaj i prognozy na przyszłość*, w: Guzewski P., Wróblewski D., Małozieć D. (red.), *Czerwona księga pożarów*, CNBOP-PIB, Józefów 2014.
3. Brushlinsky N., Sokolov S., Wagner P., Hall J. R., *World Fire Statistics – Report № 10, Second Edition*, Center of Fire Statistics of CTIF, 2005.
4. Brushlinsky N., Sokolov S., Wagner P., Hall J. R., *World Fire Statistics – Report № 13, Second Edition*, Center of Fire Statistics of CTIF, 2008.
5. Giergiczny M., *Wycena wartości statystycznego życia ludzkiego (VSL)*, w: Guzewski P., Wróblewski D., Małozieć D. (red.), *Czerwona księga pożarów*, CNBOP-PIB, Józefów 2014.
6. Guzewski P. (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z III Międzynarodowej Konferencji*, Izba Rzecznawców SITP, Poznań 2003; P. Guzewski (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z II Międzynarodowej Konferencji*, Izba Rzecznawców SITP, Poznań 2005.
7. Guzewski P. (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z II Międzynarodowej Konferencji*, Izba Rzecznawców SITP, Poznań 2007.
8. Guzewski P., Wróblewski D., Małozieć D. (red.), *Czerwona księga pożarów*, CNBOP-PIB, Józefów 2014.
9. Hołyst B., *Kryminalistyczna problematyka pożarów*, Wydawnictwo Zakładu Kryminalistyki Komendy Głównej MO, Warszawa 1962.
10. Kundzewicz Z. W., Matczak P., Sadowski Z., *Wprowadzenie do raportu o zagrożeniach*, Nauka 4/2010, PAN.
11. Majda T., Wałydowski P., Adamczyk J., Grygoruk M., *Typologia terenów narażonych na niebezpieczeństwo powodzi*, TUP, Warszawa 2012.

12. Myers D., *Ograniczenie liczby podpałek poprzez zastosowanie podejścia partnerskiego do dochodzeń popożarowych w Wielkiej Brytanii*, w: Guzewski P. (red.), *Badanie przyczyn powstawania pożarów – zbiór referatów z II Międzynarodowej Konferencji*, Izba Rzecznawców SITP, Poznań 2005.
13. Nowak M., Kawecki M., Skotnicka J., Knefel G., Ryszkiewicz I., *Wybrane aspekty medyczne i psychologiczne leczenia ofiar pożarów – organizacja leczenia oparzeń*, w: Guzewski P., Wróblewski D., Małozieć D. (red.), *Czerwona księga pożarów*, CNBOP-PIB, Józefów 2014.
14. Pilch T., *Zasady badań pedagogicznych*, wyd. Żak, Warszawa 1995.
15. Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za rok 1993-2011*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 1994-2012.
16. Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2000-2011*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2001-2012.
17. Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2003-2012*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2004-2013.
18. Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej za lata 2002-2012*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2003-2013.
19. Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej. Roczniki*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2009-2013.
20. Praca zbiorowa, *Biuletyn Informacyjny Państwowej Straży Pożarnej. Roczniki*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 1993-2013.
21. Praca zbiorowa, *Fire Statistics, Great Britain 2010-2011*, Department for Communities and Local Government, Londyn, listopad 2011.
22. Praca zbiorowa, *Safer Communities: Towards Effective Arson. The Report of the Arson Scoping Study*, Home Office, Londyn 1999.
23. Roguski E. W., Wróblewski D., *Diagnostyczna metoda oceny ryzyk i systemów reagowania PomRisc jako narzędzie programowania zmian*

- doskonalących systemy bezpieczeństwa i ich monitorowania*, BiTP Issue 4, 2008.
24. Wróblewski D. (red. nauk.), *Koncepcja funkcjonowania Regionalnego Zintegrowanego Systemu Ratownictwa Województwa Pomorskiego*, Józefów 2009.
25. Wróblewski D. (red. nauk.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, CNBOP-PIB, Józefów 2014.
26. Wróblewski D. (red. nauk.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego*, CNBOP-PIB, Józefów 2014.
27. Wróblewski D., Połec B., *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: D. Majchrzak (red.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa 2014.
28. *Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce*, wyd. Bentley Dennison, Warszawa 2007.

Akty prawne

1. Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r.
2. Ustawa z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. nr 115, poz. 1229).
3. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590, z późn. zm.).
4. Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.
5. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. nr 157, poz. 1240, z późn. zm.).
6. Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz.U. nr 179, poz. 1485, z późn. zm.).
7. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. nr 91, poz. 578, z późn. zm.).
8. Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz.U. nr 95, poz. 425, z późn. zm.).

9. 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. nr 0, poz. 104).
10. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. nr 83, poz. 542).
11. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. nr 83, poz. 541).
12. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie *Raportu o zagrożeniach bezpieczeństwa narodowego* (Dz.U. nr 83, poz. 540).
13. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie *Raportu o zagrożeniach bezpieczeństwa narodowego*.
14. Rozporządzenie Rady nr 1466/97/WE z dnia 7 lipca 1997 r. w sprawie wzmocnienia nadzoru pozycji budżetowych oraz nadzoru i koordynacji polityk gospodarczych.
15. Zarządzenie nr 115/10 wojewody podlaskiego z dnia 29 października 2010 r. w sprawie kontroli zarządczej w Podlaskim Urzędzie Wojewódzkim w Białymstoku.
16. Zarządzenie nr 1 ministra administracji i cyfryzacji z dnia 15 stycznia 2013 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Administracji i Cyfryzacji (Dz.Urz. MAiC nr 1).
17. 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 nr 24).
18. Zarządzenie nr 204/2012 prezydenta miasta Legionowa z dnia 15 października 2012 r. w sprawie zasad zarządzania ryzykiem w Urzędzie Miasta Legionowa.
19. Zarządzenie nr 25 ministra administracji i cyfryzacji z dnia 31 grudnia 2014 r. w sprawie wprowadzenia *Polityki zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.

20. Zarządzenie nr 3666/2012 prezydenta miasta stołecznego Warszawy z dnia 18 grudnia 2012 r. w sprawie systemu zarządzania ryzykiem w m. st. Warszawie.
21. 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 nr 4).
22. Zarządzenie nr 42 ministra spraw zagranicznych z dnia 15 grudnia 2011 r. w sprawie zasad zarządzania ryzykiem w działach administracji rządowej kierowanych przez ministra spraw zagranicznych (Dz.Urz. MSZ nr 9, poz. 72).
23. Zarządzenie nr 59 ministra spraw wewnętrznych z dnia 6 września 2012 r. w sprawie systemu kontroli zarządczej w dziale administracji rządowej – sprawy wewnętrzne.
24. Zarządzenie nr 8 dyrektora Generalnego LUW z dnia 29 stycznia 2010 r.
25. Zarządzenie nr 80 wojewody mazowieckiego z dnia 9 lutego 2011 r. w sprawie ustalenia *Polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie*.
26. 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).
27. *Polityka zarządzania ryzykiem w Ministerstwie Administracji i Cyfryzacji*.
28. Procedura opracowania raportu cząstkowego do *Raportu o zagrożeniach bezpieczeństwa narodowego*.

Normy i standardy

1. AS/NZS 4360:1999 *Risk Management*.
2. ISO/IEC 31010:2010 *Risk Management – Risk Assessment Techniques*.
3. PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.
4. PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*.
5. PN-EN ISO 9000:2006 *Systemy zarządzania jakością – Podstawy i terminologia*.

Dokumenty elektroniczne, strony internetowe i inne

1. *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 24 lutego 2015].
2. Gawecki K., *PN-ISO 31000:2012 – wytyczne w zakresie zarządzania ryzykiem korporacyjnym*, materiał szkoleniowy BSI, Warszawa 2012.
3. <http://geoforum.pl>.
4. <http://orka.sejm.gov.pl>.
5. <http://www.isok.gov.pl>.
6. <http://www.kzgw.gov.pl>.
7. <http://www.ptedp.pl>.
8. *Metodyka opracowania planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych*, KZGW, Warszawa 2013.
9. *National Security Programme – National Risk Assessment Method Guide 2008*.
10. *Raport z opracowania wstępnej oceny ryzyka powodziowego*, KZGW, Warszawa 2011.
11. Wniosek nr 13009 na projekt nr DOBR-BIO4/050/13009/2013 pt. „Opracowanie systemowych rozwiązań wspomagających prowadzenie dochodzeń popożarowych wykorzystujących nowoczesne technologie, w tym narzędzia techniczne i informatyczne”, finansowany przez Narodowe Centrum Badań i Rozwoju w ramach 4. konkursu z zakresu bezpieczeństwa i obronności.
12. 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.

INDEKS POJĘĆ

A

Agregacja ryzyka 46

Akceptacja ryzyka 346

Akceptowany poziom ryzyka 43

Analiza kosztów i korzyści 156

Analiza ryzyka 31

Awaria 62

C

Cel strategiczny 26

Cele taktyczne i operacyjne 26

Czynnik ryzyka 244

D

Działania korygujące 343

Działania zapobiegawcze 343

E

Efekt domina 44

Ewaluacja ryzyka 37

F

Finansowanie ryzyka 252

G

Gotowość kryzysowa państwa 171

H

Hierarchiczna tablica rekomendacji działań podnoszących poziom bezpieczeństwa 392

Hierarchiczna tablica ryzyk 392

Hierarchizacja ryzyka 87

I

Identyfikacja ryzyka 27

Interesariusz 42

Interoperacyjność 130

K

Katalog zdarzeń 234

Katastrofa naturalna 243

Katastrofy kaskadowe 119

Kategoria 240

Klasyfikacja ryzyka 87

Kompetencje 43

Komunikacja i konsultacje 40

Konsekwencje 29

Kryteria ryzyka 40

Kultura bezpieczeństwa 121

Kultura organizacyjna 26

Kultura zarządzania ryzykiem 37

Ł

Ład organizacyjny 36

M

Mapa administracyjna ryzyk województwa 391

Mapy ryzyka powodziowego 325

Mapa terytorialnego rozkładu poziomu bezpieczeństwa województwa 387

Mapy terytorialnego rozkładu ryzyk częściowych województwa 390

Mapa terytorialnego rozkładu ryzyk obszarowych województwa 388

Mapy zagrożenia powodziowego 324

Metoda postępowania z ryzykiem 46

Modyfikacja ryzyka 165

Monitorowanie 37

N

Natężenie 195

Niepewność 226

O

Obszar ryzyka 45

Obszary, na których wystąpienie powodzi jest prawdopodobne 323

Ocena ryzyka 29

Odporność 39

Ograniczanie ryzyka 157

P

Percepcja ryzyka 39

Podatność wystąpienia zdarzenia w czasie 136

Polityka 33

Postępowanie z ryzykiem 28

Poziom podatności 130

Poziom ryzyka 39

Prawdopodobieństwo 43

Profil ryzyka 222

Przegląd 37

R

Rejestr ryzyk 48

Ryzyko 28

Ryzyko akceptowalne 38

Ryzyko całkowite 68

Ryzyko kinetyczne 383

Ryzyko potencjalne 383

Ryzyko reliktowe (rezydualne, szczątkowe) 22

S

Strategia 33

Strategia postępowania z ryzykiem 46

Struktura ramowa zarządzania ryzykiem 32

Sytuacja nadzwyczajna 243

Szacowanie ryzyka 39

Szkoda 243

U

Ustalenie kontekstu 31

W

Właściciel ryzyka 32

Wrażliwość ekspozycji 39

Z

Zarządzanie ryzykiem 26

Zdarzenie 49

Zdarzenie inicjujące 73

Zdarzenie niekorzystne 67

Znaczące ryzyko powodziowe 323

Ź

Źródło ryzyka 45

SPIS RYSUNKÓW

Rys. 1. Relacje między zasadami, strukturą ramową i procesem zarządzania ryzykiem	30
Rys. 2. Relacje pomiędzy elementami struktury ramowej	34
Rys. 3. Proces zarządzania ryzykiem.....	41
Rys. 4. Koncepcja reagowania na ryzyko.....	49
Rys. 5. Przykład analizy przyczyn i konsekwencji	63
Rys. 6. Model diagramu Ishikawy.....	64
Rys. 7. Przykład analizy przyczynowo-skutkowej	65
Rys. 8. Przykład analizy warstw ochrony – LOPA	68
Rys. 9. Przykład analizy drzewa decyzji	70
Rys. 10. Przykład analizy drzewa błędów	72
Rys. 11. Przykładowe drzewo logiczne wykorzystywane w analizie drzewa błędów	73
Rys. 12. Przykład analizy drzewa zdarzeń.....	74
Rys. 13. Przykład oceny niezawodności człowieka.....	75
Rys. 14. Przykład analizy muchy	79
Rys. 15. Przykład metody konserwacji ukierunkowanej na niezawodność – RCM ...	80
Rys. 16. Diagram stref rozmieszczenia ryzyka (pozytywnego i negatywnego)	90
Rys. 17. Analiza ryzyka w ramach CIRAM.....	131
Rys. 18. Zarządzanie ryzykiem: zasady, struktura i procesy	161
Rys. 19. Struktura ramowa zarządzania ryzykiem	163
Rys. 20. Ogólny schemat procesu zarządzania ryzykiem	163
Rys. 21. Metodyka oceny ryzyka wystąpienia zdarzeń niekorzystnych	168
Rys. 22. Zasada ALARP.....	178
Rys. 23. Schemat działalności w „punkcie decyzyjnym”	181
Rys. 24. Schemat procesu oceny ryzyka.....	182
Rys. 25. Strefy matrycy ryzyka.....	185
Rys. 26. Narodowa matryca ryzyka – zagrożenia naturalne	191
Rys. 27. Narodowa matryca ryzyka – zagrożenia w transporcie	192
Rys. 28. Narodowa matryca ryzyka – zagrożenia technologiczne.....	192
Rys. 29. Narodowa matryca ryzyka – zagrożenia cywilne	193
Rys. 30. Narodowa matryca ryzyka – wszystkie zagrożenia.....	194
Rys. 31. Matryca ryzyka wykorzystywana przez niemieckie Federalne Biuro Ochrony Ludności.....	197
Rys. 32. Przykładowe zestawienie porównawcze różnorodnych zagrożeń w macierzy	204
Rys. 33. Analiza ryzyka jako centralny element zarządzania ryzykiem (w oparciu o ISO 31000)	205
Rys. 34. Proces zarządzania ryzykiem.....	210
Rys. 35. Graficzny opis obiegu informacji na temat analizy ryzyka.....	211
Rys. 36. Przykładowe matryce ryzyka	219

Rys. 37. Metoda MVA.....	220
Rys. 38. Metoda ROSA.....	223
Rys. 39. Zależność pomiędzy skalą ryzyka a rodzajami zdarzeń.....	224
Rys. 40. Matryca ryzyka analizowanych scenariuszy w <i>Narodowej ocenie ryzyka 2012</i>	227
Rys. 41. Sześć kroków oceny ryzyka	233
Rys. 42. Zagrożenia umieszczone na wykresie w kontekście prawdopodobieństwa i wpływu	240
Rys. 43. Podstawowe zagrożenia, na jakie narażona jest Wielka Brytania	242
Rys. 44. Przykładowy rozkład czynników ryzyka	245
Rys. 45. Proces zarządzania ryzykiem.....	247
Rys. 46. Matryca ryzyka na potrzeby <i>Raportu (...)</i>	294
Rys. 47. Proces oceny ryzyka	300
Rys. 48. Prezentacja obszarów badawczych w oparciu o wnioski z poprzedniego etapu badań	301
Rys. 49. Schemat metody ilościowej	307
Rys. 50. Proces wprowadzania wymogów dyrektywy powodziowej	322
Rys. 51. Wstępna ocena ryzyka powodziowego. Mapa obszarów narażonych na niebezpieczeństwo powodzi	324
Rys. 52. Algorytm opracowania wstępnej oceny ryzyka powodziowego.....	326
Rys. 53. Schemat blokowy lokalizacji i identyfikacji obszarów potencjalnie zagrożonych powodzią	328
Rys. 54. Przykładowa mapa zagrożenia powodziowego – Podolsze	329
Rys. 55. Fragment mapy ryzyka powodziowego – negatywne konsekwencje dla ludności i wartość potencjalnych strat powodziowych.....	330
Rys. 56. Fragment mapy ryzyka powodziowego – negatywne konsekwencje dla środowiska, dziedzictwa kulturowego i działalności gospodarczej.....	332
Rys. 57. Schemat procesu planowania w zarządzaniu ryzykiem powodziowym	334
Rys. 58. Struktura działań ograniczających ryzyko powodziowe	336
Rys. 59. Matryca ryzyka	370
Rys. 60. Mapa terytorialnego rozkładu poziomu bezpieczeństwa województwa pomorskiego.....	387
Rys. 61. Mapa terytorialnego rozkładu ryzyk obszarowych województwa pomorskiego	388
Rys. 62. Mapy terytorialnego rozkładu ryzyk cząstkowych województwa pomorskiego.....	390
Rys. 63. Mapa administracyjna ryzyk województwa pomorskiego (cz. 1/4).....	392
Rys. 64. Hierarchiczna tablica ryzyk (perspektywa wojewódzka) [%]	393
Rys. 65. Hierarchiczna tablica rekomendacji działań podnoszących poziom bezpieczeństwa (perspektywa województwa) – translator	393
Rys. 66. Hierarchiczna tablica ryzyk (perspektywa powiatowa) [%]	394

Rys. 67. Mapa terytorialnego rozkładu ryzyk cząstkowych województwa pomorskiego – pożary	397
Rys. 68. Mapa terytorialnego rozkładu ryzyk cząstkowych województwa pomorskiego – wypadki komunikacyjne	398
Rys. 69. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – organizacja.....	401
Rys. 70. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – zasoby.....	402
Rys. 71. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – infrastruktura	402
Rys. 72. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – wyposażenie	403
Rys. 73. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – lokalizacja placówek.....	404
Rys. 74. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – szkolenia/edukacja	404
Rys. 75. Diagnoza obecnego stanu elementów systemu ratownictwa województwa pomorskiego – lokalizacja placówek.....	406
Rys. 76. Wskaźnik oczekiwanej potrzeby zmian sugerowanych przez podmioty systemu	408
Rys. 77. Pożary w Polsce ogółem w latach 1993-2012.....	418
Rys. 78. Straty bezpośrednie w pożarach w latach 2002-2012	419
Rys. 79. Straty pośrednie w pożarach	420
Rys. 80. Liczba ofiar śmiertelnych w pożarach w latach 2000-2011 (w tym ratownicy).....	421
Rys. 81. Liczba ofiar rannych w pożarach w latach 2000-2011 (w tym ratownicy).....	422
Rys. 82. Zarządzanie ryzykiem pożarowym.....	423
Rys. 83. Obszary oceny ryzyka pożarowego.....	424
Rys. 84. Podpalenia w latach 1993-2012.....	427
Rys. 85. Proces zarządzaniem ryzykiem a potrzeby systemu zarządzania kryzysowego.....	431
Rys. 86. Proces oceny ryzyka.....	435
Rys. 87. Zasady wyboru opcji postępowania na przykładzie matrycy ryzyka	437

SPIS TABEL

Tabela 1. Rejestr ryzyka.....	53
Tabela 2. Rejestr ryzyka.....	54
Tabela 3. Możliwe metody do zastosowania przy ocenie ryzyka.....	58
Tabela 4. Przykład analizy wpływu na działalność – BIA	86
Tabela 5. Określenie prawdopodobieństwa wystąpienia zdarzenia	87
Tabela 6. Ocena poziomu ryzyka	88
Tabela 7. Szablon do sporządzania listy priorytetów dla każdego ryzyka.....	89
Tabela 8. Przykładowa maczyca prognozowania konsekwencji pozytywnych i negatywnych	89
Tabela 9. Rejestr ryzyka (przykład).....	174
Tabela 10. Tabela prawdopodobieństwa	175
Tabela 11. Procentowy rozkład prawdopodobieństwa nasilenia w latach przy szansie 1%	176
Tabela 12. Maczyca ryzyka.....	177
Tabela 13. Ewaluacja ryzyka – wysoki poziom wiarygodności	178
Tabela 14. Ewaluacja ryzyka – średni poziom wiarygodności	179
Tabela 15. Ewaluacja ryzyka – niski poziom wiarygodności.....	179
Tabela 16. Klasyfikacja prawdopodobieństwa	187
Tabela 17. Klasyfikacja wpływu	188
Tabela 18. Parametry i centralne pytania do opisu scenariusza	198
Tabela 19. Przykładowy model klasyfikacji prawdopodobieństwa	199
Tabela 20. Przykładowe parametry charakteryzujące miejsce	199
Tabela 21. Przykładowe parametry charakteryzujące zdarzenie	200
Tabela 22. Model klasyfikacji kategorii Ludność	203
Tabela 23. Opis jakościowy z pomocą skali	217
Tabela 24. Wyniki ilościowej analizy ryzyka	217
Tabela 25. Skala prawdopodobieństwa	228
Tabela 26. Skala konsekwencji	228
Tabela 27. Skala niepewności.....	229
Tabela 28. Wskaźniki dla wartości narodowych podlegających ochronie	236
Tabela 29. Opis ryzyka (przykład).....	249
Tabela 30. Pomiar skutków	250
Tabela 31. Prawdopodobieństwo wystąpienia zagrożenia	251
Tabela 32. Identyfikacja ryzyka (zagrożeń) w metodykach oceny ryzyka wybranych państw	259
Tabela 33. Analiza ryzyka w metodykach oceny ryzyka wybranych państw.....	260
Tabela 34. Porównanie poszczególnych metodyk oceny ryzyka z uwzględnieniem etapu oceny ryzyka.....	262
Tabela 35. Skala prawdopodobieństwa na potrzeby <i>Raportu (...)</i>	292

Tabela 36. Skala konsekwencji na potrzeby <i>Raportu (...)</i>	293
Tabela 37. Metody rekomendowane dla planowania cywilnego przy ocenie ryzyka	303
Tabela 38. Częstotliwość	308
Tabela 39. Gwałtowność	308
Tabela 40. Wzburzenie	309
Tabela 41. Skala	310
Tabela 42. Ranni	310
Tabela 43. Ofiary śmiertelne	311
Tabela 44. Ewakuacja	311
Tabela 45. Pogorszenie warunków bytowych	312
Tabela 46. Poziom oddziaływania ekonomicznego dla jednostek dysponujących budżetem własnym (samorząd terytorialny)	312
Tabela 47. Poziom oddziaływania ekonomicznego dla jednostek administracji rządowej (objętych regulacjami ustawy budżetowej)	314
Tabela 48. Straty środowiskowe	314
Tabela 49. Straty wizerunkowe	315
Tabela 50. Szacowanie wartości poziomu ryzyka	316
Tabela 51. Wykaz instytucji dysponującymi danymi wyjściowymi	317
Tabela 52. Analiza SWOT	319
Tabela 53. Szacowanie wartości poziomu ryzyka	320
Tabela 54. Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałania ryzykom związanym z osiągnięciem celów	345
Tabela 55. Wykaz ryzyk i działań zapobiegawczych do <i>planu działalności ministra spraw zagranicznych</i> na rok	346
Tabela 56. Arkusz oceny	347
Tabela 57. Matryca istotności ryzyka	348
Tabela 58. Ocena następstw ryzyka	349
Tabela 59. Ocena prawdopodobieństwa ryzyka	350
Tabela 60. Poziom ryzyka wyrażony jest w postaci kombinacji następstw oraz ich prawdopodobieństwa	350
Tabela 61. Prawdopodobieństwo wystąpienia zagrożenia	351
Tabela 62. Skutek związany z danym zagrożeniem	351
Tabela 63. Istotność ryzyka	352
Tabela 64. Graficzne przedstawienie analizy ryzyka	352
Tabela 65. Rejestr ryzyk	353
Tabela 66. Ewaluacja ryzyka	354
Tabela 67. Postępowanie z ryzykiem	356
Tabela 68. Plan postępowania z ryzykiem	356
Tabela 69. Rejestr ryzyk	357
Tabela 70. Informacja na temat procesu zarządzania ryzykiem w roku	358

Tabela 71. Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku	365
Tabela 72. Tabela zbiorcza identyfikacji i oceny ryzyka w WZFE	366
Tabela 73. Wydziałowy rejestr ryzyk	366
Tabela 74. Rejestr ryzyka	366
Tabela 75. Rejestr ryzyka	368
Tabela 76. Analiza i ocena istotności ryzyka	372
Tabela 77. Skala punktowa istotności ryzyka	372
Tabela 78. Arkusz zarządzania ryzykiem	373
Tabela 79. Matryca ryzyk – pow. kwidzyński (przykład)	391
Tabela 80. Matryca ryzyk – pow. bytowski (przykład)	394
Tabela 81. Matryca ryzyk – Sopot, miasto na prawach powiatu (przykład)	395
Tabela 82. Przykładowa matryca ryzyka 6 x 6	436

NOTKI BIOGRAFICZNE AUTORÓW I RECENZENTÓW**dr Grzegorz Abgarowicz**

Doktor nauk społecznych w zakresie nauk o bezpieczeństwie. Adiunkt Zakładu Polityki Bezpieczeństwa w Instytucie Politologii Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, pracownik Rządowego Centrum Bezpieczeństwa. Zajmuje się problematyką bezpieczeństwa powszechnego, zarządzania kryzysowego, ochrony ludności oraz Kaukazu. Autor licznych publikacji naukowych, promotor i recenzent prac naukowych, uczestnik projektów badawczych m.in. z zakresu ochrony ludności (*Anvil – Analysis of civil security systems in Europe*), metodyki oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP, zintegrowanych systemów budowy planów zarządzania kryzysowego opartych na nowoczesnych technologiach informatycznych. Członek Krakowskiego Oddziału Polskiego Towarzystwa Ludoznawczego, armenolog.

**mgr Inga Abgarowicz**

Absolwentka Wydziału Prawa i Administracji Wyższej Szkoły Menedżerskiej w Warszawie oraz Wydziału Bezpieczeństwo Narodowe Akademii Obrony Narodowej. Kierownik Działu Ochrony Ludności w Centrum Naukowo-Badawczym Ochrony Przeciwpowodziowej – Państwowym Instytucie Badawczym. Jako kierownik zespołu ze strony konsorcjanta prowadzi projekt pt. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP”. Jest zastępcą kierownika w projekcie „Emergency Management in Social Media Generation” po stronie CNBOP-PIB. Autorka wystąpień i publikacji z zakresu ochrony ludności, zarządzania kryzysowego i zarządzania ryzykiem. Uczestniczy w projektach naukowych finansowanych przez instytucje krajowe oraz europejskie.

**mgr inż. Anna Banulska**

Absolwentka studiów I stopnia na Wydziale Inżynierii Bezpieczeństwa Cywilnego Szkoły Głównej Służby Pożarnej w Warszawie oraz studiów II stopnia na Wydziale Bezpieczeń-

stwa Narodowego w Akademii Obrony Narodowej. Specjalista do spraw certyfikacji i dopuszczeń w Jednostce Certyfikującej CNBOP-PIB. Wykonawca projektów badawczo-rozwojowych realizowanych przez CNBOP-PIB we współpracy z innymi instytucjami.



dr Jan Gołębiewski

Absolwent Akademii Sztabu Generalnego. Od 1987 r. przez 11 lat pracował w instytucjach centralnych (Komisja Planowania przy Radzie Ministrów, Centralny Urząd Planowania, Biuro Bezpieczeństwa Narodowego i Urząd Szefa Obrony Cywilnej Kraju), gdzie zajmował się sprawami ochrony ludności. W latach 90. ukończył kursy w ramach programu Partnerstwa dla Pokoju, organizowane w Polsce, ośrodku NATO w Oberammergau, w Kanadzie i innych ośrodkach. Od listopada 1998 r. na emeryturze zajmuje się zarządzaniem kryzysowym, cywilnym planowaniem kryzysowym i bezpieczeństwem. Prowadzi zajęcia ze studentami kilku uczelni. Autor ponad 150 artykułów z zakresu zarządzania kryzysowego, systemu obronnego, cywilnego planowania zarządzania kryzysowego, gotowości cywilnej i dziedzin pokrewnych. Doktorat uzyskał w 2010 r. w Akademii Marynarki Wojennej w Gdyni. Temat rozprawy: „Model zarządzania kryzysowego wobec współczesnych zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej”. Autor kilku publikacji zwartych, m.in.: „Podręcznika menedżera programów kryzysowych”, „Vademecum zarządzania kryzysowego” oraz „Zarządzania kryzysowego w świetle wymogów bezpieczeństwa”.



dr inż. Piotr Guzowski

Absolwent Szkoły Głównej Służby Pożarniczej w Warszawie (1988) i Uniwersytetu Ekonomicznego w Poznaniu (2003). Główny specjalista w Centrum Naukowo-Badawczym Ochrony Przeciwpożarowej – Państwowym Instytucie Badawczym w Józefowie. Od ponad 20 lat ekspert ds. badań przyczyn pożarów. Pomyślny i organizator cyklu międzynarodowych konferencji „Research into the causes of fire” oraz warsztatów z dochodzeń popożarowych. Autor programów szkoleniowych oraz licznych opracowań z obszaru dochodzeń popo-

zarowych i metodyki ustalania przyczyn pożarów. Ukończył kursy specjalistyczne: „Fire Science and Fire Investigation” (Uniwersytet w Edynburgu, Edynburg 2005), „Fire Investigator Course” (Fire Service College, Centrex NTC, Moreton-in-Marsh 2006), „The Principles of Electrical Fires Short Course” (Interscience Communication Ltd, San Francisco 2009). Współzałożyciel i prezes Polskiego Towarzystwa Ekspertów Dochodzeń Popożarowych. W 2014 r. obronił na Wydziale Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego rozprawę doktorską pt. „Prawnokryminalistyczne aspekty ustalania przyczyn pożarów”.



Maria Kędzierska

Wieloletni pracownik CNBOP-PIB, obecnie pełni funkcję głównego specjalisty ds. promocji i współpracy. Współorganizatorka licznych sympozjów i konferencji o zasięgu ogólnokrajowym i międzynarodowym. Autorka wielu publikacji z zakresu bezpieczeństwa oraz działalności CNBOP-PIB w prasie branżowej, krajowej i zagranicznej oraz kwartalniku „Bezpieczeństwo i Technika Pożarnicza”. Współtwórcza projektów badawczo-rozwojowych realizowanych przez instytut we współpracy z innymi instytucjami. Współautorka założeń merytorycznych do programu komputerowego wspomagającego tworzenie planów zarządzania kryzysowego Elikzir.



mł. bryg. mgr inż. Daniel Małozieć

Absolwent Szkoły Głównej Służby Pożarniczej w Warszawie (1999). Obecnie pełni funkcję kierownika w Zespole Laboratoriów Procesów Spalania i Wybuchowości w CNBOP-PIB. Autor lub współautor licznych artykułów o tematyce bezpieczeństwa pożarowego, właściwości palnych materiałów budowlanych oraz wielu ekspertyz związanych z ustalaniem przyczyn pożarów. W CNBOP-PIB zajmuje się przede wszystkim tematyką związaną z badaniami w zakresie reakcji na ogień wyrobów budowlanych oraz ustalaniem przyczyn pożarów.



mgr inż. Maciej Napiórkowski

Absolwent Wydziału Inżynierii Środowiska na Politechnice Warszawskiej. Obecnie doktorant w Zakładzie Informatyki i Badań Jakości Środowiska macierzystego wydziału PW. Pracownik Działu Ochrony Ludności w CNBOP-PIB. Wykonawca zadań w projektach naukowo-badawczych realizowanych przez CNBOP-PIB we współpracy z innymi instytucjami.



mgr Bartłomiej Połec

Absolwent studiów II stopnia na Wydziale Bezpieczeństwa Narodowego w Akademii Obrony Narodowej. Pracownik CNBOP-PIB. Autor licznych publikacji z zakresu bezpieczeństwa i zarządzania kryzysowego. Współtwórca projektów badawczo-rozwojowych realizowanych przez CNBOP-PIB we współpracy z innymi instytucjami.



mgr inż. Ewa Sobór

Absolwentka studiów I i II stopnia na Wydziale Inżynierii Bezpieczeństwa Cywilnego w Szkole Głównej Służby Pożarnej w Warszawie (2001-2007). Od 2005 r. pracownik Jednostki Certyfikującej CNBOP-PIB, obecnie zastępca kierownika. Autorka publikacji z zakresu bezpieczeństwa.

mgr inż. Tomasz Sowa

Absolwent Wydziału Inżynierii Bezpieczeństwa Pożarowego Szkoły Głównej Służby Pożarnej w Warszawie. Obecnie pracownik Zespołu Laboratoriów Systemów Sygnalizacji Pożarowej i Automatyki Pożarnej w Centrum Naukowo-Badawczym Ochrony Przeciwpożarowej – Państwowym Instytucie Badawczym. Specjalizuje się w badaniach głośników przeznaczonych do użytku w dźwiękowych systemach ostrzegawczych.



dr inż. Witold Skomra

Doradca w Rządowym Centrum Bezpieczeństwa. Jest specjalistą w zakresie bezpieczeństwa narodowego, zarządzania kryzysowego, analizy ryzyka i ochrony infrastruktury krytycznej. W RCB odpowiada za obszar ochrony IK, ocenę ryzyka na poziomie krajowym oraz planowanie cywilne. Kierownik projektu badawczo-rozwojowego pt. „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP”. Jest także wykładowcą akademickim w Wyższej Szkole Informatyki i Zarządzania w Rzeszowie.



Paweł Stępień

Kierownik Zespołu Laboratoriów Sygnalizacji Alarmu Pożaru i Automatyki Pożarniczej w CNBOP-PIB. Mechanik, elektronik, elektroakustyk. Koordynator ze strony polskiej projektu “The Cell Broadcast for Public Warning project – sharing knowledge and experiences and identification and standardisation of (technical) requirements”, który uzyskał aprobatę Komisji Europejskiej

mgr Małgorzata Trzcńska

Pracownik Biura Współpracy Międzynarodowej Komendy Głównej Państwowej Straży Pożarnej. W 2011 r. oddelegowana do Stałego Przedstawicielstwa RP przy UE w związku ze sprawowaniem przez RP prezydencji w Radzie UE. Była przewodniczącą Grupy Przyjaciół Prezydencji i w ramach konsultacji z Sekretariatem Generalnym Rady UE, Europejską Służbą Działań Zewnętrznych oraz Komisją Europejską prowadziła prace nad zagadnieniem *Crisis Coordination Arrangements*, obecnie *EU Integrated Political Crisis Response Arrangements*.



bryg. dr inż. Dariusz Wróblewski – absolwent Szkoły Głównej Służby Pożarniczej (1994), doktorat o specjalności bezpieczeństwo państwa uzyskany w Akademii Obrony Narodowej w Warszawie (2001). Ukończone programy dla wyższej kadry menedżerskiej, a także kursy dla kadry kierowniczej PSP oraz administracji publicznej. Służbę rozpoczął w SGSP, w pionie

liniowym w 1994 r., stanowiska kierownicze zajmował od 2002 r. w Centrum Edukacji Bezpieczeństwa Powszechnego SGSP, a następnie podjął pracę na stanowisku zastępcy dyrektora ds. naukowo-badawczych CNBOP. Od 2009 r. do 2014 r. dyrektor CNBOP-PIB. Od maja do grudnia 2014 r. doradca komendanta głównego PSP. 1 stycznia 2015 r. powołany na II kadencję na stanowisko dyrektora CNBOP-PIB. W dorobku naukowo-dydaktycznym ma 40 projektów naukowo-badawczych, jest autorem lub współautorem ponad 90 publikacji zwartych i artykułów w pismach branżowych. Prelegent na konferencjach krajowych i zagranicznych, a także wykładowca podczas ćwiczeń oraz warsztatów i treningów na szkoleniach i kursach.



st. bryg. dr inż. Paweł Janik

Absolwent Szkoły Głównej Służby Pożarniczej (1993), doktorat w zakresie ubezpieczeń uzyskany w Akademii Ekonomicznej w Poznaniu (2000). Służbę pełnił w Komendzie Rejonowej Państwowej Straży Pożarnej w Koninie – jako oficer ds. operacyjnych (1993-1995), Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Koninie – oficer ds. kontrolno-rozpoznawczych (1995). W 1995 r. rozpoczął służbę w Komendzie Głównej Państwowej Straży Pożarnej (od 2007 r. dyrektor Biura Rozpoznawania Zagrożeń). Specjalizuje się w tematyce związanej z ochroną przeciwpożarową, rozpoznawaniem zagrożeń, analizą i oceną ryzyka, oceną dokumentacji bezpieczeństwa, zarządzaniem kryzysowym. Autor kilkudziesięciu publikacji dotyczących ochrony przeciwpożarowej, rozpoznawania, analizowania, oceny i zapobiegania zagrożeniom.



mł. bryg. dr inż. Paweł Kęпка

Kierownik Katedry Badań Bezpieczeństwa Szkoły Głównej Służby Pożarniczej w Warszawie, specjalista z zakresu ochrony ludności i zarządzania kryzysowego, absolwent SGSP, były kierownik Zakładu Zarządzania Kryzysowego, prodziekan Wydziału Inżynierii Bezpieczeństwa Cywilnego Szkoły Głównej Służby Pożarniczej, ekspert NATO (*Ad-hoc Group on Risk and Vulnerabilities Analysis*), główny specjalista w Wydziale Planowania Rządowego Centrum Bezpieczeń-

stwa, wykładowca zarządzania kryzysowego, systemów informacji przestrzennych i projektowania systemów bezpieczeństwa. Autor książki „Bioteroryzm. Polska wobec użycia broni biologicznej” (2007) oraz kilkudziesięciu artykułów.



dr hab. inż. Bogdan Kosowski

Profesor WSZOP. Oficer pożarnictwa – st. bryg. w stanie spoczynku. Absolwent Politechniki Krakowskiej, Szkoły Głównej Służby Pożarniczej oraz Akademii Górniczo-Hutniczej. W 2013 r. na Wydziale Bezpieczeństwa Narodowego Akademii Obrony Narodowej obronił rozprawę habilitacyjną na temat „Współdziałanie instytucjonalne na rzecz zapewnienia bezpieczeństwa ludności w Polsce”. Wiedzę z zakresu nauk organizacji i zarządzania integruje z naukami o bezpieczeństwie. Specjalizuje się w problematyce systemu zarządzania bezpieczeństwem w podmiotach gospodarczych, w instytucjach oraz jednostkach administracji publicznej. Obecnie zatrudniony w Wyższej Szkole Zarządzania Ochroną Pracy w Katowicach. Wiedzę teoretyczną konfrontuje z wiedzą praktyczną. Jest autorem wielu opracowań na temat systemu zarządzania, zwłaszcza zarządzania bezpieczeństwem. W 2007 r. otrzymał nagrodę ministra za całokształt dorobku oraz publikacje naukowe mające istotny wpływ na stan wiedzy i kierunki dalszych badań.



st. bryg. mgr inż. Dariusz Marczyński

Dyrektor Krajowego Centrum Koordynacji Ratownictwa i Ochrony Ludności Komendy Głównej Państwowej Straży Pożarnej w Warszawie, które nadzoruje operacyjnie krajowy system ratowniczo-gaśniczy oraz pełni rolę międzynarodowego punktu kontaktowego w sprawie pomocy ratowniczej, a ponadto wypełnia zadania CZK KG PSP i CZK MSW. Absolwent Szkoły Głównej Służby Pożarniczej (1988). Autor wielu referatów i publikacji. Znanca ratownictwa i planowania operacyjnego. Dowódca i uczestnik wielu akcji ratowniczych, jak również szef lub zastępca szefa sztabu KG PSP. Członek OSP.

Wybrane zagadnienia z zakresu planowania cywilnego w systemie zarządzania kryzysowego RP

Redakcja naukowa: Dariusz Wróblewski

Wydawnictwo prezentuje problematykę poruszoną podczas konferencji „Planowanie cywilne w systemie zarządzania kryzysowego”, w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne” finansowanego przez NCBR. W publikacji omówiono m.in. takie zagadnienia jak system zarządzania kryzysowego w Polsce, planowanie cywilne w zarządzaniu kryzysowym czy technologia i metody wykorzystywane przy opracowywaniu planów zarządzania kryzysowego.



Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem

Redakcja naukowa: Dariusz Wróblewski

Publikacja jest wydawnictwem prezentującym problematykę poruszoną w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne” finansowanego przez NCBR. Autorzy zidentyfikowali i przeanalizowali dokumenty (normy, standardy, przepisy prawa międzynarodowego oraz krajowego z uwzględnieniem prawa miejscowego). Na potrzeby opracowania leksykonu dokonano analizy wybranych pozycji literaturowych.

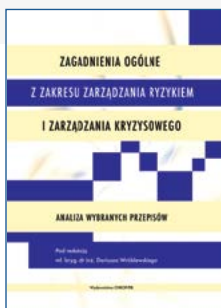


Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego. Analiza wybranych przepisów

Redakcja naukowa: Dariusz Wróblewski

Wydawnictwo swoim zakresem obejmuje identyfikację i przegląd wybranych przepisów prawnych obowiązujących w Polsce oraz Unii Europejskiej związanych z zarządzaniem kryzysowym i zarządzaniem ryzykiem.

Przy doborze treści do niniejszej publikacji kierowano się kryterium oceny użyteczności dla realizowanego projektu oraz użyteczności dla czytelnika. Publikacja została wydana w ramach projektu nr O ROB 0016 03 002 finansowanego ze środków NCBR.



Publikację rekomenduję osobom, które ze względu na pełnione funkcje zajmują się bezpieczeństwem lub działają na jego rzecz. Wielu liderów i menadżerów znajdzie w tym opracowaniu zarówno praktyczne wskazówki do poszukiwań, jak i rozwiązania, które mogą zostać wykorzystane w celu usprawnienia mechanizmu bezpieczeństwa lub instytucji działającej na rzecz dobra publicznego w ramach działań dla bezpieczeństwa: ludności, środowiska lub mienia, bezpieczeństwa gminy, powiatu, województwa i kraju.

*Z recenzji st. bryg. mgr. inż. Dariusza Marczyńskiego
Dyrektora Krajowego Centrum Koordynacji
Ratownictwa i Ochrony Ludności*

ISBN 978-83-61520-18-4

DOI: 10.17381/2015.1

Wydawnictwo CNBOP-PIB

www.cnbop.pl

