

n



PRZEGLĄD WZAJEMNY POLSKA 2016



Funded by
European Union
Civil Protection

PRZEGLĄD WZAJEMNY

POLSKA

2016

Program wzajemnych przeglądów w ramach unijnej współpracy w zakresie ochrony ludności i zarządzania zagrożeniem klęskami i katastrofami na lata 2015-2016



Funded by
European Union
Civil Protection



Falck

veiligheidsregio
ZHZ

Wyłączenie odpowiedzialności

Informacje i opinie przedstawione w niniejszej publikacji stanowią informacje i opinie autorów i nie muszą odzwierciedlać urzędowego stanowiska Komisji Europejskiej lub macierzystych organizacji autorów. Komisja Europejska ani żadna osoba działająca w jej imieniu nie odpowiada za użytek, jaki może zostać zrobiony z informacji zawartych w niniejszym dokumencie.

Kopiowanie jest dozwolone z zastrzeżeniem podania źródła.

Podziękowania

Raport powstał dzięki czasowi poświęconemu przez ekspertów oraz ich wiedzy. Zespół dokonujący przeglądu składał się z czworga ekspertów:

- **John Agius**, Dyrekcja ds. Ochrony Infrastruktury Krytycznej (OIKD), Kancelaria Prezesa Rady Ministrów (OPM), Malta
- **Omar Harrami**, Sekcja ds. Ochrony Infrastruktury Krytycznej (OIK) oraz Ochrony Krytycznej Infrastruktury Informatycznej, Agencja ds. Bezpieczeństwa Ludności, Szwecja
- **Lyubomira Raeva**, Dyrekcja Generalna ds. Ochrony Przeciwpożarowej i Ochrony Ludności, Ministerstwo Spraw Wewnętrznych, Bułgaria
- **Çiğdem Tetik Bicer**, Dyrekcja ds. Zarządzania Ryzykiem Klęsk Żywiolowych i Sytuacji Awaryjnych, Kancelaria Prezesa Rady Ministrów, Turcja

Komisję Europejską podczas misji reprezentował Andrew Bower z Dyrekcji Generalnej ds. Pomocy Humanitarnej i Ochrony Ludności. Laura Schmidt z Dyrekcji Generalnej ds. Pomocy Humanitarnej i Ochrony Ludności służyła radą i wsparciem z Brukseli. Konsorcjum, na czele którego stanęła firma Falck B.V., pomagało Komisji w przeprowadzeniu programu przeglądu wzajemnego. W skład zespołu projektowego zajmującego się Polską, w imieniu partnera konsorcjum, Regionu Bezpieczeństwa Holandia Południowa-Południe, weszli Nico van Os i Ruud Houdijk oraz Jens Poul Madsen, reprezentujący firmę Falck. W misji uczestniczył również Jack Radish z OECD.

*Przegląd wzajemny został istotnie wzbogacony dzięki zaangażowaniu wszystkich podmiotów, które podlegały przeglądowi oraz ich współpracy w zakresie zbierania danych i informacji na potrzeby niniejszego projektu. Nie byłoby to możliwe bez pełnego zaangażowania Pani **Doroty Leduchowskiej** oraz Pani **Beaty Janowczyk** z Rządowego Centrum Bezpieczeństwa.*

Przegląd wzajemny został sfinansowany przez Komisję Europejską, m.in. poprzez jej wkład finansowy w Forum Wysokiego Szczegółu OECD w sprawie ryzyka.

Spis treści

Wprowadzenie.....	11
Proces przeglądu	11
Zakres przeglądu	12
Najważniejsze wnioski i rekomendacje	13
1. Ramy, koordynacja i zaangażowanie zainteresowanych stron	16
1.1 Ramy.....	16
1.2 Koordynacja	19
1.3 Zaangażowanie innych zainteresowanych stron.....	22
2. Metodologia	24
3. Informowanie i komunikacja	30
3.1 Wymiana informacji.....	30
3.2 Infrastruktura teleinformatyczna	33
3.3 Komunikacja ryzyka	34
4. Wiedza ekspercka	38
5. Finansowanie	40
6. Styk z obszarem zarządzania ryzykiem.....	42
6.1 Styk z szeroko pojętym obszarem zarządzania ryzykiem	42
6.2 Styk z dziedziną ochrony infrastruktury krytycznej	44
6.3 Styk z obszarem adaptacji do zmian klimatu	47
Załącznik I Terminologia i skróty	50
Załącznik II Przegląd zainteresowanych stron.....	53
Załącznik III Dokumentacja	54
Załącznik IV Tematyczne ramy przeglądu	56

Wprowadzenie

Przegląd wzajemny jest narzędziem zarządczym polegającym na ocenie systemów zarządzania ryzykiem klęsk i katastrof jednego kraju („kraj podlegający ocenie”) przez ekspertów z innych krajów. Unijny program wzajemnych przeglądów w dziedzinie ochrony ludności i zarządzania ryzykiem klęsk i katastrof został wprowadzony po dwóch udanych pilotażowych przeglądach w Wielkiej Brytanii (2012) i Finlandii (2013), zrealizowanych wspólnie z Organizacją Współpracy Gospodarczej i Rozwoju (OECD) oraz funkcjonującym w ramach ONZ Sekretariatem Międzynarodowej Strategii ds. Redukcji Zagrożeń Naturalnych (UNISDR).

Celem unijnego programu przeglądów wzajemnych jest umożliwienie wymiany dobrych praktyk oraz wydanie rekomendacji w zakresie poprawy polityki zarządzania ryzykiem klęsk lub katastrof, jak również działań w krajach podlegających ocenie. Program sprzyja wymianie dobrych praktyk i wzajemnemu zrozumieniu oraz umożliwia prowadzenie dialogu zarówno wewnątrz państw, jak i między nimi oraz wśród ekspertów.

Polska zgłosiła Komisji Europejskiej zainteresowanie uczestnictwem w tematycznym przeglądzie wzajemnym dotyczącym **oceny ryzyka**. Poprosiła o przeprowadzenie analizy zdolności dokonywania oceny ryzyka w świetle wytycznych¹ UE w zakresie oceny zdolności zarządzania ryzykiem oraz unijnego ustawodawstwa w obszarze ochrony ludności (art. 6, 1313/2013/UE²).

Proces przeglądu

Po potwierdzeniu udziału Polski w tematycznym przeglądzie w zakresie oceny ryzyka, w krajach uczestniczących w Unijnym Mechanizmie Ochrony Ludności oraz współpracujących państwach sąsiednich ogłoszono nabór ekspertów. W przeglądzie wzięło udział 4 specjalistów z: Bułgarii, Malty, Szwecji i Turcji, wspieranych przez Komisję Europejską i zespół projektowy.

Misja przeglądu wzajemnego w Polsce trwała 5 dni (25-29 stycznia 2016 r.)³. Przeprowadzono rozmowy z ponad 50 zainteresowanymi stronami z różnych organizacji, w tym instytucji szczebla centralnego, regionalnego i lokalnego, organizacji pozarządowych (NGO) oraz środowisk naukowych.

Rozmowy odbywały się w następujących miejscach:

- Rządowe Centrum Bezpieczeństwa (RCB);
- Urząd Miasta Stołecznego Warszawy;
- Państwowa Agencja Atomistyki (PAA);
- Komenda Główna Państwowej Straży Pożarnej;
- Szkoła Główna Służby Pożarniczej;
- Polskie Sieci Elektroenergetyczne S.A. (PSE S.A.);

¹ [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015XC0808\(01\)](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015XC0808(01))

² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0924:0947:EN:PDF>

³ Raport zawiera wyniki eksperckiej analizy sytuacji w Polsce w styczniu 2016 r. Zmiany, które ewentualnie nastąpiły od tego czasu, nie były brane pod uwagę.

- Mazowiecki Urząd Wojewódzki;
- Urząd Miasta Płock;
- Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy;
- Krajowy Zarząd Gospodarki Wodnej (KZGW).

Jednym z punktów programu była wizja terenowa osuwiska zlokalizowanego na skarpie wiślanej w Płocku oraz wizyta w Miejskim Centrum Zarządzania Kryzysowego Miasta Płocka oraz w siedzibie PKN Orlen S.A.

Dzięki spotkaniom przedstawicieli wielu środowisk posiadających wiedzę z rozmaitych dziedzin i różny zakres odpowiedzialności, sesje przeglądu wzajemnego pomogły w wymianie informacji w zakresie oceny ryzyka i sprzyjały współpracy między zainteresowanymi stronami.

Zakres przeglądu

Przegląd koncentrował się na zdolności oceny ryzyka i przebiegał zgodnie z *Wytycznymi oceny zdolności zarządzania ryzykiem* Komisji Europejskiej. Eksperci skupili się na zagadnieniach dotyczących przepisów i rozwiązań w zakresie zarządzania oraz stosowanych metodologii z uwzględnieniem międzysektorowego ujęcia oceny ryzyka w Polsce. Szczególną uwagę poświęcono zdolności oceny ryzyka w świetle wybranych istotnych zagrożeń występujących w Polsce oraz zakresu wiedzy instytucji uczestniczących w spotkaniach dotyczących ochrony infrastruktury krytycznej (OIK), adaptacji do zmian klimatu (CCA), powodzi, ekstremalnych zjawisk pogodowych oraz osuwisk⁴.

Niniejszy raport wyszczególnia zarówno stosowane w Polsce dobre praktyki, jak i obszary wymagające udoskonalenia, zawiera także szereg rekomendacji. W gestii polskiego Rządu oraz zainteresowanych instytucji pozostaje rozważenie sposobu wykorzystania rekomendacji w celu wzmocnienia odporności społeczeństwa na zagrożenia oraz budowania zrównoważonego dialogu na temat polityki krajowej w zakresie oceny ryzyka.

Część najważniejszych dokumentów dotyczących krajowej oceny ryzyka (KOR) oraz OIK w Polsce, ze względu na wrażliwą zawartość, ma charakter niejawnny. W konsekwencji, misja przeglądu wzajemnego w dużej mierze bazowała na streszczeniach i wnioskach z tych dokumentów oraz informacjach przekazanych podczas prowadzonych dyskusji.

Niniejszy raport posługuje się definicjami zawartymi w unijnych wytycznych odnośnie do oceny i tworzenia map ryzyka w zakresie zarządzania klęskami lub katastrofami⁵ (zob. Załącznik I). Koncepcja oceny zagrożeń, którą posługuje się Polska, odnosi się do oceny ryzyka. Raporty cząstkowe należy rozumieć jako sektorowe i regionalne raporty oceny ryzyka, które stanowią podstawę w procesie tworzenia Raportu o zagrożeniach bezpieczeństwa narodowego (RoZBN).

⁴ Misja oceny wzajemnej zastosowała w procesie przeglądu podejście obejmujące wszystkie rodzaje ryzyka, ale niektóre konkretne zagrożenia zostały omówione w sposób bardziej szczegółowy.

⁵ https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

Najważniejsze wnioski i rekomendacje

Polska wdrożyła wiele dobrych praktyk w zakresie prowadzenia oceny ryzyka:

- Polska posiada odpowiednie ramy prawne, właściwą koordynację i współpracę międzysektorową. Mechanizm raportów częściowych do Raportu o zagrożeniach bezpieczeństwa narodowego pomaga identyfikować główne ryzyka, a także związane z nimi oddziaływania oraz zapewnia zaangażowanie różnych podmiotów w ocenę ryzyka. Dwukierunkowo prowadzony proces oceny: od poziomu lokalnego, poprzez wojewódzki, do krajowego (KOR) sprzyja wymaganej współpracy pomiędzy wszystkimi szczeblami administracji. Za koordynację opracowania KOR odpowiada jedna główna organizacja (RCB) posiadająca wiedzę na temat zagrożeń zidentyfikowanych na poziomie krajowym. W proces oceny ryzyka zaangażowany jest ponadto sektor prywatny, uczelnie oraz organizacje pozarządowe.
- Polska stworzyła własną metodologię KOR, która jest zgodna ze standardami unijnymi. RCB wydaje wskazówki dotyczące opracowania oceny ryzyka przeznaczone także dla szczebla regionalnego ale dostosowuje ocenę do poziomu krajowego.
- Polska posiada wysokiej jakości dane i analizy, które są wykorzystywane do opracowania KOR. Dysponuje także oprogramowaniem na potrzeby KOR.
- RCB prowadzi stronę internetową, na której znajdują się informacje dla opinii publicznej dotyczące porad na temat zachowywania się w sytuacjach zagrożeń.
- Mapy ryzyka powodziowego dostępne są w internecie oraz realizowany jest program edukacji w zakresie zagrożenia powodziowego.
- Polscy eksperci i pracownicy wszystkich szczebli administracji zajmujący się tematyką oceny ryzyka posiadają fachową wiedzę w tym zakresie. Problematyka ta znajduje się w programie studiów m. in. Szkoły Głównej Służby Pożarniczej. Istnieje także program e-learningu podnoszący poziom wiedzy osób zawodowo zaangażowanych w tę dziedzinę.
- Tworzy się powiązania z zarządzaniem ryzykiem. Obowiązuje bardzo jasny podział zadań oraz odpowiedzialności za rodzaje ryzyka (dla wszystkich czterech faz zarządzania kryzysowego). Istnieje bezpośrednie powiązanie pomiędzy planami na poziomie lokalnym, regionalnym i krajowym.
- W ochronie infrastruktury krytycznej zastosowano podejście obejmujące wszystkie rodzaje zagrożeń („all-hazard”). W Narodowym Programie Ochrony Infrastruktury Krytycznej (NPOIK) odzwierciedlone zostały zasady: współodpowiedzialności, współpracy i zaufania. OIK obejmuje planowanie ciągłości działania.
- Polska promuje czynne uczestnictwo obywateli w zagadnieniach dotyczących adaptacji do zmian klimatu.

Wyróżniono 5 głównych rekomendacji, które szczegółowo zostaną przedstawione w dalszej części raportu:

- Zapewnić czytelne relacje pomiędzy KOR oraz wszystkimi czterema fazami zarządzania kryzysowego.

- Zachęcać do sporządzania oceny ryzyka na szczeblu lokalnym w celu wsparcia pracy i planowania samorządów.
- Wykorzystać dwukierunkowy proces aby koordynować strategie zapobiegania sytuacjom kryzysowym na wszystkich szczeblach administracji.

Usprawnić proces konsultacji z zainteresowanymi stronami:

- Poprawić międzysektorową współpracę i koordynację poprzez organizację wspólnych spotkań (warsztatów).
 - Rozszerzyć dialog z sąsiednimi krajami dotyczący współpracy międzynarodowej i transgranicznej.
 - W większym stopniu wykorzystywać wiedzę i doświadczenie sektora prywatnego.
 - W procesie KOR rozważyć zwiększenie aktywności podmiotów zajmujących się problematyką adaptacji do zmian klimatu (climate change adaptation – CCA).
- Wdrożyć oprogramowanie, np. ARMOR, wspierające proces oceny ryzyka.
- Rozwijać polską metodologię oceny ryzyka na podstawie prowadzonych ewaluacji oraz informacji zwrotnych od podmiotów z niej korzystających. Zachęcać do korzystania ze wspólnej metodologii na wszystkich szczeblach administracji w celu zapewnienia monitorowania także ryzyk, które nie stanowią problemu ogólnokrajowego. Wyjaśnić, jakie są powiązania między metodologią KOR a innymi sektorowymi.
- Zwrócić się do Wspólnego Centrum Badawczego Komisji Europejskiej (JRC) w celu porównania polskiej metodologii z metodologiami innych państw członkowskich.
- Stworzyć wspólny zakres danych wykorzystywanych w ocenie ryzyka oraz zbadać możliwość wdrożenia mapowania ryzyka obejmującego wiele zagrożeń w oparciu o standardy wymiany danych oraz GIS.
- Na bazie KOR stworzyć ogólną strategię komunikacji ryzyka. RCB powinno odgrywać centralną rolę koordynacyjną w strategii, zapewniając jej spójność oraz zgodność informacji. Udoskonalić wymianę wrażliwych informacji w zakresie OIK i stworzyć ogólną strategię komunikacji w obszarze CCA.
- Podnosić poziom wiedzy fachowej poprzez:
 - stworzenie możliwości wymiany doświadczeń pomiędzy ekspertami pracującymi nad krajową metodologią oceny ryzyka;
 - zbadanie możliwości przygotowania przez RCB we współpracy z jednostkami naukowo-badawczymi (np. Szkołą Główną Służby Pożarniczej) wspólnej strategii dalszego rozwoju zdolności administracyjnych;
 - promowanie interdyscyplinarnego dialogu akademickiego w zakresie metodologii oceny ryzyka w różnych sektorach;
 - stworzenie krajowej strategii koordynacji badań i rozwoju w zakresie oceny ryzyka i zarządzania nim.

- Pracować nad czytelnymi procedurami dotyczącymi finansowania. Stworzyć politykę alokacji środków finansowych w celu prowadzenia oceny ryzyka na wszystkich szczeblach i sektorach administracji. Finansowanie przedsięwzięć z zakresu zapobiegania, przygotowania, reagowania i usuwania skutków powinno opierać się na identyfikacji i ocenie ryzyk. Należy zapewnić ciągłość realizacji ważnych projektów związanych z zapobieganiem i monitorowaniem, finansowanych z programów UE lub innych źródeł.
- Inwestować w powiązanie oceny ryzyka z zarządzaniem nim. Należy stworzyć krajową strategię ograniczenia ryzyka katastrof (DRR), zgodnie z Ramowym Programem Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof z Sendai. Zalecenia RoZBN powinny zostać włączone w plany działania DRR. Rozważyć przyznanie jednemu podmiotowi odpowiednich kompetencji do koordynowania przygotowania i wdrażania strategii DRR, w ścisłym powiązaniu z KOR. Zapewnić gminom wsparcie techniczne aby mogły stworzyć własne programy ograniczenia ryzyka.
- Zapewnić aby NPOIK nie odnosił się wyłącznie do obiektów IK lecz do systemów IK oraz współzależności między nimi. Dokonać przeglądu systemu zachęt dla operatorów IK. Dokonać wyraźnego rozróżnienia pomiędzy posiedzeniami forum OIK, warsztatami i konferencjami dotyczącymi IK.
- Stworzyć bezpośrednie korelacje pomiędzy KOR a strategiami CCA. Nadać priorytet wszystkim skutkom krótko- i długoterminowym związanym ze zmianą klimatu z punktu widzenia bezpieczeństwa narodowego.

1. Ramy, koordynacja i zaangażowanie zainteresowanych stron

1.1 Ramy

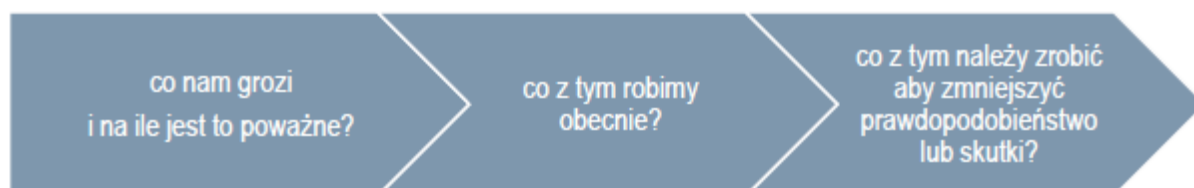
Cel: ocena ryzyka jest prowadzona na podstawie czytelnych ram prawnych i/lub proceduralnych, zaś rola oceny ryzyka w ogólnym zarządzaniu ryzykiem klęsk i katastrof jest określana na odpowiednim szczeblu krajowym i/lub niższym.

Najważniejszą ustawą w RP dotyczącą oceny ryzyka jest **ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym**. Polskie prawodawstwo definiuje „zarządzanie kryzysowe” jako kompleksowy proces obejmujący zapobieganie, przygotowanie, reagowanie i usuwanie skutków. Proces oceny ryzyka uważa się za część m.in. fazy zapobiegania wpływający na kolejne fazy. Ustawa opisuje cykl planowania w zakresie zarządzania kryzysowego jako „okresowe realizowanie etapów: analizowania, programowania, opracowywania planu lub programu, jego wdrażanie, testowanie i uruchamianie”. Jednak Rządowe Centrum Bezpieczeństwa (RCB) przyznaje, że definicje znajdujące się w ustawie będą musiały zostać dostosowane do terminologii Unijnego Mechanizmu Ochrony Ludności.

Ustawa o zarządzaniu kryzysowym nakłada obowiązek sporządzenia **Krajowego Planu Zarządzania Kryzysowego (KPZK)**, przygotowanego na wypadek zdarzeń o zasięgu ogólnokrajowym lub wyczerpania zasobów i możliwości reagowania na szczeblu wojewódzkim. **KPZK** identyfikuje 20 zagrożeń istotnych dla bezpieczeństwa państwa.

Ustawa reguluje ocenę zagrożeń i ryzyka. Na potrzeby KPZK ministrowie kierujący działami administracji, kierownicy urzędów centralnych i wojewodowie zobowiązani są opracować wkład do **Raportu o zagrożeniach bezpieczeństwa narodowego (RoZBN)** w formie raportów częściowych. Dyrektor RCB zapewnia koordynację przygotowania RoZBN, natomiast Szef Agencji Bezpieczeństwa Wewnętrznego odpowiada za koordynację i przygotowanie części dotyczącej zagrożeń o charakterze terrorystycznym. Ze względów bezpieczeństwa RoZBN jest dokumentem niejawnym.

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego określa tryb i terminy jego sporządzenia. Raport musi odpowiadać na następujące pytania:



Rysunek 1: Pytania znajdujące się w Raporcie

Rozporządzenie definiuje typy zagrożeń dla bezpieczeństwa narodowego w następujący sposób:

- a) mające istotny wpływ na funkcjonowanie i możliwości rozwoju państwa, a w szczególności zagrożenia mogące mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego;
- b) których skutki mogą:
 - godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, a w szczególności suwerenność, niepodległość i nienaruszalność terytorium;
 - zagrażać życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach;
 - oddziaływać także na inne państwa;
 - dotyczyć terytorium RP lub jej obywateli, mimo możliwego wystąpienia w innym państwie;
- c) występujące w rejonach napięć, konfliktów oraz kryzysów międzynarodowych i mające wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych;
- d) zagrożenia o charakterze terrorystycznym mogące doprowadzić do sytuacji kryzysowej.



Rysunek 2: Proces akceptacji ryzyka na szczeblu krajowym

Ocena ryzyka jest procesem dwukierunkowym. Najpierw oceny ryzyka są przekazywane przez gminy i powiaty do województw, a następnie przez województwa na poziom krajowy. RCB pełni funkcję instytucji koordynującej przygotowanie krajowej oceny ryzyka. Wojewodowie mają obowiązek opracowywać raporty częściowe i przekazywać je do RCB. Zwrotnie otrzymują informacje w postaci uwag i sugestii. Raporty te stanowią podstawę do opracowania RoZBN. Jednostki niższego szczebla wykorzystują opracowane przez RCB wytyczne dotyczące opracowania raportów częściowych.

Województwa biorą pod uwagę oceny ryzyka prowadzone na szczeblu powiatów i gmin. Jednak problematyka procesu oceny ryzyka nie ma niewystarczającej podstawy prawnej. Ustawa o zarządzaniu kryzysowym nie mówi bowiem wprost o obowiązku sporządzania oceny na poziomie powiatów i gmin. Istnieje ogólne zalecenie dotyczące oceny ryzyka, która powinna uwzględniać prawdopodobieństwo wystąpienia, skutki, skalę i oddziaływania. Jednostki niższego szczebla administracji uwzględniają szerszy zakres zagrożeń niż ujęte na poziomie krajowym.

Mimo że RoZBN nakreśla „cele strategiczne” w zakresie zarządzania ryzykiem, bezpośrednie powiązanie legislacyjne pomiędzy KOR a KPZK sprawia wrażenie, że bardziej koncentruje się na przygotowaniu niż na zapobieganiu (zob. również rozdział 6).

Podsumowując można stwierdzić, że proces KOR jest jasny i funkcjonuje prawidłowo, a ramy prawne do jego przygotowania są wystarczające.

Dobre praktyki:

- Mechanizm opracowywania raportów cząstkowych pozwala identyfikować główne rodzaje ryzyka i związane z nimi oddziaływanie oraz zapewnia zaangażowanie różnych podmiotów w proces oceny ryzyka. W konsekwencji, RoZBN umożliwia udział przedstawicieli różnych środowisk (i uwzględnienie wszystkich możliwych zagrożeń).
- Dwukierunkowy proces oceny ryzyka: od poziomu lokalnego, poprzez wojewódzki, do KOR (oraz pętla informacji zwrotnej od szczebla krajowego do wojewódzkiego), spełnia wymóg współpracy pomiędzy wszystkimi uczestnikami procesu. Spójność i ścisła koordynacja są widoczne na wszystkich etapach planowania zarządzania kryzysowego. Proces ten tworzy również podstawę do koordynacji strategii zapobiegania zagrożeniom. Możliwe jest jednak udoskonalenie współpracy (zob. rekomendacje).

Rekomendacje:

- Zapewnić czytelne relacje pomiędzy KOR a wszystkimi czterema fazami zarządzania kryzysowego (zapobieganie, przygotowanie, reagowanie i usuwanie skutków).
- Aby wspomóc proces planowania samorządów (plany zarządzania kryzysowego, ograniczanie ryzyka wystąpienia klęsk żywiołowych i katastrof, planowanie przestrzenne) należy wspierać prowadzenie procesu oceny ryzyka na szczeblu lokalnym poprzez wprowadzenie prawnego obowiązku (dla powiatów) i/lub zintensyfikować udzielanie przez instytucje centralne pomocy przy tworzeniu ocen i planów na szczeblu lokalnym, co umożliwi zapewnienie spójności podejścia i metodologii.
- Wykorzystać dobrze funkcjonujący proces dwukierunkowy oraz pętlę informacji zwrotnych do koordynacji stworzenia ogólnokrajowej struktury spójnych strategii zapobiegania ryzykom na wszystkich szczeblach administracji.
- Dostosować polską terminologię prawną do obowiązującego prawodawstwa unijnego.

1.2 Koordynacja

Cel: istnieje czytelny podział obowiązków i ról/funkcji przypisanych do podmiotów uczestniczących w ocenie ryzyka.

Ustawa o zarządzaniu kryzysowym określa obowiązki wszystkich szczebli administracji, ogólne zasady zarządzania kryzysowego oraz zasady finansowania zadań w tym zakresie. Najwyższym szczeblem odpowiedzialnym za zarządzanie kryzysowe jest Rada Ministrów. W przypadku wystąpienia sytuacji kryzysowej zbiera się Rządowy Zespół Zarządzania Kryzysowego (RZZK), na którego czele stoi Prezes Rady Ministrów. RZZK obsługiwany jest przez RCB, które jest państwową jednostką budżetową podległą Prezesowi Rady Ministrów i pełni również funkcję krajowego centrum zarządzania kryzysowego. Jego dyrektor jest powoływany przez Prezesa Rady Ministrów i jest sekretarzem RZZK.

Krajowy Plan Zarządzania Kryzysowego obejmuje wszystkie 4 fazy zarządzania kryzysowego tj. zapobieganie, przygotowanie, reagowanie i usuwanie skutków. Wybór zagrożeń wynika z analizy ryzyka przeprowadzonej w RoZBN. W KPZK wymieniono podmioty odpowiedzialne za zarządzanie kryzysowe oraz podano obowiązującą podstawę prawną. W formie siatki bezpieczeństwa w sposób szczegółowy opisano zadania, kompetencje oraz określono podmioty wiodące oraz współpracujące z nimi dla każdego z 20 zidentyfikowanych zagrożeń w każdej z faz zarządzania kryzysowego (z uwzględnieniem szczebla krajowego i regionalnego, a także lokalnego). Siatka bezpieczeństwa nie odzwierciedla jednak wszystkich zagrożeń z uwzględnieniem efektów kaskadowych oraz następstw długoterminowych, które powinny być przedmiotem zainteresowania Rządu. Jeżeli zagrożenie nie ma jednego podmiotu wiodącego, RCB proponuje przypisanie go do wskazanego podmiotu w celu zagwarantowania, że za każde ryzyko będzie odpowiadała konkretna instytucja.

RCB:

1. przygotowuje procedury (wytyczne) sporządzania raportów cząstkowych⁶, tak aby wszystkie zaangażowane jednostki posługiwały się jednolitą metodą;
2. organizuje szkolenia i warsztaty, podczas których prezentowana jest metodologia w zakresie oceny ryzyka w celu podniesienia poziomu wiedzy;
3. sporządza i redaguje projekt RoZBN;
4. prowadzi proces uzgadniania RoZBN oraz przygotowuje uchwałę Rady Ministrów w sprawie jego przyjęcia.

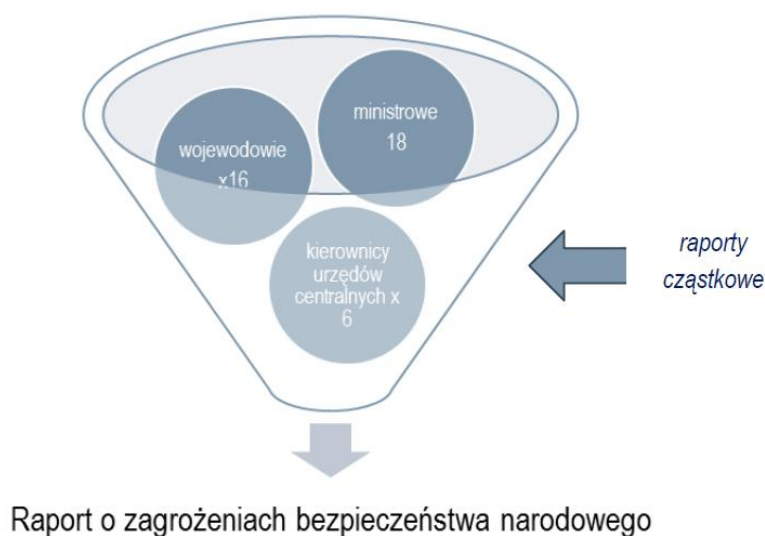
RCB jest jednostką koordynującą przygotowanie RoZBN. Współpracuje w tym zakresie ze wszystkimi istotnymi instytucjami publicznymi. Wiedza fachowa pozwalająca prowadzić proces oceny ryzyka leży w gestii odpowiednich zainteresowanych stron a nie RCB, które wydaje niezbędne wytyczne do przygotowania raportów cząstkowych oraz sprawdza projekty pod kątem spójności i ewentualnych błędów. W proces zaangażowane są ministerstwa, urzędy centralne oraz województwa. Wszystkie zainteresowane strony uznają koordynacyjną rolę RCB w zakresie przygotowania RoZBN.

⁶ Zob. wstęp do uwag dotyczących stosowanej terminologii.

Ministerstwa, urzędy centralne i województwa odpowiadają za sporządzanie raportów częściowych⁷. Jak dotąd powstało 40 takich raportów. Także Agencja Bezpieczeństwa Wewnętrznego sporządza 2 rodzaje raportów częściowych:

- standardowy raport częściowy, odpowiednik raportów innych ministerstw/urzędów, koncentrujący się na intencjonalnej szkodliwej działalności człowieka (sabotaż, przekupstwo, szpiegostwo itd.);
- raport stanowiący część składową RoZBN, skupiający się na zagrożeniach związanych z aktami terroryzmu, które mogą prowadzić do sytuacji kryzysowej. Pod tym względem rolą Agencji jest zebranie częściowych raportów ministerstw, kierowników urzędów centralnych oraz województw, dotyczących zagrożeń terrorystycznych oraz innych powiązanych informacji/zagrożeń.

RCB nie wykonuje własnej oceny ryzyka poszczególnych zagrożeń ale bazuje na informacjach przekazywanych przez instytucje, które odpowiadają za ich identyfikację i analizę. Rola Centrum polega na zestawieniu raportów częściowych w kompleksowy RoZBN.



*Rysunek 3: Raporty częściowe
do Raportu o zagrożeniach bezpieczeństwa narodowego*

RCB prowadzi również analizy krzyżowe raportów częściowych w celu zidentyfikowania problemów o charakterze przekrojowym. Dyrektor RCB przekazuje informacje zwrotne co do stopnia szczegółowości, zakresu i formy raportów częściowych oraz w stosownych przypadkach zaleca ich aktualizację. Jeżeli RCB uzna, że istnieje taka potrzeba, zaleca koordynację między różnymi instytucjami, zaś raporty są aktualizowane na podstawie informacji zwrotnych zebranych od różnych instytucji i zainteresowanych stron.

Po ukończeniu opracowywania RoZBN przez RCB, dokument zostaje przesłany do ministerstw i urzędów centralnych oraz województw z prośbą o uwagi. Po dokonaniu korekt, projekt Raportu jest przedkładany Radzie Ministrów. Przyjęcie RoZBN uchwałą Rady Ministrów zapewnia wysoki poziom odpowiedzialności za decyzje dotyczące

⁷ W przypadku ministerstw i urzędów centralnych raporty częściowe pojmowane są jako raporty sektorowe.

akceptacji ryzyka. Po zatwierdzeniu RoZBN, RCB rozsyła dokument do wszystkich podmiotów uczestniczących w procesie jego opracowywania.

Podmioty odpowiadające za raporty częściowe biorą również pod uwagę transgraniczny charakter zagrożeń (w sytuacjach tego wymagających). Polska zawarła umowy ze wszystkimi sąsiednimi państwami, jak również Węgrami, Chorwacją i Słowenią, dotyczące współpracy i wzajemnej pomocy w przypadku klęski lub katastrofy. Polska wdrożyła Konwencję w sprawie transgranicznych skutków awarii przemysłowych (UNECE). Jest członkiem Międzynarodowej Komisji Ochrony Odry przed Zanieczyszczeniem, a także uczestniczy w międzynarodowym projekcie flagowym w ramach Strategii UE dla regionu Morza Bałtyckiego (From GAPS to CAPS 2015-2016) oraz projekcie BaltPrevResilience.

Dobre praktyki:

- Zadania wszystkich urzędów publicznych uczestniczących w systemie zarządzania kryzysowego od szczebla lokalnego do centralnego regulują zapisy ustawy (ustawa o zarządzaniu kryzysowym).
- Siatka bezpieczeństwa przypisuje do każdego rodzaju zagrożenia instytucję wiodącą i współpracującą w każdej fazie zarządzania kryzysowego. Tworzy to czytelny podział odpowiedzialności. W przypadkach gdy nie sprecyzowano podmiotu odpowiedzialnego za określone ryzyko, RCB sugeruje przypisanie konkretnego „właściciela”.
- Jedna główna organizacja (RCB) odpowiada za koordynację procesu KOR i posiada wiedzę na temat zagrożeń zidentyfikowanych na poziomie krajowym. Ponadto zapewnia wsparcie w prowadzeniu oceny ryzyka przez ministerstwa, urzędy centralne i województwa.
- Analiza krzyżowa raportów częściowych prowadzona przez RCB, jako część pętli informacji zwrotnej, umożliwia wielosektorowe ujęcie zagadnienia. Stanowi to podstawę udoskonalania współpracy i koordynacji międzysektorowej (zob. zalecenia).
- Przyjęcie Raportu uchwałą Rady Ministrów nadaje właściwy status końcowemu wynikowi procesu oceny ryzyka oraz zapewnia wysoki poziom odpowiedzialności za zidentyfikowane rodzaje ryzyk na politycznym poziomie decyzyjnym.
- Polska współpracuje z sąsiednimi państwami i bierze pod uwagę potencjalne transgraniczne skutki różnych scenariuszy zagrożeń (po obu stronach granicy).

Rekomendacje:

- Poprawić międzysektorową współpracę i koordynację poprzez organizację wspólnych spotkań (warsztatów), podczas których przedstawiciele instytucji odpowiedzialnych za opracowanie raportów częściowych będą mogli prowadzić międzysektorową analizę współzależności pomiędzy raportami. Taki rodzaj dialogu i wspólnej oceny mógłby poprawić pętlę informacji zwrotnej, co może polepszyć sposób uzupełniania raportów częściowych i pomóc w identyfikacji współzależności oraz niewystarczających sił i środków, jak również zapewnić lepszą analizę ryzyk. Wspólna ocena sprzyja także zrozumieniu podziału odpowiedzialności między poszczególnymi podmiotami.

- Rozszerzyć dialog z sąsiednimi państwami w sprawie współpracy międzynarodowej i transgranicznej. Może to obejmować wymianę informacji w sprawie krajowych procesów i metodologii oceny ryzyka (zwłaszcza w odniesieniu do zagrożeń naturalnych, technicznych i nieintencjonalnych), wymianę danych dotyczących transgranicznych zagrożeń i podatności, jak również wymianę wiedzy i doświadczeń dotyczących KOR. Rozważyć zainicjowanie konkretnych projektów w zakresie oceny ryzyka, zapobiegania i przygotowania dotyczących zagrożeń transgranicznych w wybranych obszarach przygranicznych, z udziałem zarówno jednostek centralnych, jak i samorządów.⁸

1.3 Zaangażowanie innych zainteresowanych stron

Cele: podmioty prowadzące ocenę ryzyka współpracują z szerokim spektrum zainteresowanych stron, w tym z sektorem prywatnym, uczelniami oraz innymi instytucjami rządowymi i samorządowymi niezaangażowanymi bezpośrednio w proces oceny.

Raporty cząstkowe do RoZBN są głównym źródłem informacji zasilającym krajowy proces oceny ryzyka. W trakcie przygotowywania tych dokumentów istotne są wymiany poglądów i myśli, a także tworzenie scenariuszy zagrożeń z udziałem szerokiego gremium ekspertów. Podczas opracowywania raportów cząstkowych/sektorowych, urzędnicy współpracują ze sobą oraz z podmiotami sektora prywatnego (np. właścicielami/operatorami infrastruktury krytycznej), naukowcami i organizacjami pozarządowymi. Zaangażowani są również eksperci, średnie kadry zarządcze oraz decydenci, jako członkowie zespołów zarządzania kryzysowego. Przykładem współpracy z podmiotami pozarządowymi jest projekt mający na celu udoskonalenie metodyki oceny ryzyka realizowany przez konsorcjum składające się ze Szkoły Głównej Służby Pożarniczej, Politechniki Warszawskiej, Centrum Naukowo-Badawczego Ochrony Przeciwpowodzi, Akademii Obrony Narodowej oraz firmy informatycznej Medcore.

OIK stanowi jeden z głównych obszarów RoZBN. Istnieje bezpośrednie powiązanie pomiędzy KOR oraz OIK, ponieważ z mocy prawa w NPOIK uwzględnia się wnioski z RoZBN. Z drugiej strony wojewódzkie wykazy IK wchodzą bezpośrednio do planów zarządzania kryzysowego.

Na szczeblu krajowym za integralność systemu IK odpowiada ministerstwo właściwe dla danego sektora (wskazane w NPOIK). Wszyscy właściciele/operatorzy IK są zobowiązani do współpracy z administracją rządową. Współpraca w zakresie OIK przebiega na trzech poziomach: strategicznym, operacyjnym i zarządczym. Na poziomie *strategicznym* istnieją trzy fora: krajowe forum OIK, forum systemów OIK oraz regionalne fora OIK. Na poziomie *operacyjnym* wymianę informacji zapewnia mechanizm OIK, w tym forum internetowe służące wymianie informacji (jawnych). Na poziomie *zarządczym* organizowane są konferencje i publikowane newslettery. Zostały także wydane cztery podręczniki (dotyczące materiałów wybuchowych, biometrii,

⁸ Biorąc pod uwagę m.in. Konwencję UNECE w sprawie transgranicznych skutków awarii przemysłowych (<http://www.unece.org/env/teia.html>) oraz Konwencję o ochronie i użytkowaniu cieków transgranicznych i jezior międzynarodowych (<http://www.unece.org/env/water>).

oceny niezawodności i wytyczne na temat włączania OIK w plany zarządzania kryzysowego). Dobre praktyki i zalecenia w sprawie OIK znajdują się w załączniku do NPOIK.

Utworzono także grupy robocze, w tym m.in. ds. standardów ochrony teleinformatycznej. Polska stale rozwija możliwości lepszego wykorzystywania forum IK. RCB dokłada wszelkich starań by pomóc podmiotom efektywnie z nich korzystać. W przeszłości fora były organizowane w formie konferencji dla różnych zainteresowanych stron. Fora regionalne i resortowe są obecnie uważane za mniej użyteczne.

Właściciele/operatorzy IK są również włączeni w etapy identyfikacji i analizy ryzyka we wstępnej ocenie ryzyka powodziowego, za które odpowiada KZGW. Na szczeblu krajowym KZGW współpracuje z RCB. Na szczeblu regionalnym dyrektorzy regionalnych zarządów gospodarki wodnej (RZGW) współpracują z wojewodami.

Partnerstwo publiczno-prywatne w Polsce opiera się na zapisach ustawowych i dotyczy m.in. wspólnych (publiczno-prywatnych) inwestycji w projekty infrastrukturalne. Zaangażowane podmioty oraz RCB efektywnie współpracują z sektorem prywatnym.

Dobre praktyki:

- Sektor prywatny, uczelnie i organizacje pozarządowe są zaangażowane w proces oceny ryzyka co najmniej sektorowo w zakresie różnych raportów częściowych.
- Polski rząd dąży do współpracy z sektorem prywatnym i uczelniami w celu rozwinięcia swojej metodyki oceny ryzyka.

Rekomendacje:

- Bardziej konkretnie i pod kierunkiem jednostki centralnej (RCB) korzystać z wiedzy teoretycznej i praktycznej sektora prywatnego (uczelnie, instytuty naukowo-badawcze, organizacje pozarządowe, IK, przedsiębiorstwa) jako uzupełnienie określonych, zdefiniowanych części raportów częściowych oraz przekrojowych zagrożeń i tematów.
- Rozważyć większe zaangażowanie w proces KOR podmiotów realizujących działających na rzecz adaptacji do zmian klimatu.

2. Metodologia

Cel: opracowanie metodologii oceny ryzyka. Oczekiwany wpływ zidentyfikowanego ryzyka jest oceniany zgodnie z przyjętą metodologią, odpowiednio zhierarchizowane są rodzaje ryzyk.

Metoda prowadzenia oceny ryzyka w Polsce została określona w *Procedurze opracowywania raportu częściowego*, przygotowanej przez RCB w celu umożliwienia przeprowadzenia procesu analizy ryzyka i ustandaryzowania informacji przekazywanych przez zainteresowane strony. W procedurze „ryzyko” zostało zdefiniowane jako kombinacja prawdopodobieństwa wystąpienia zagrożenia oraz jego skutków. Aby ocenić prawdopodobieństwo, należy skorzystać ze wszystkich dostępnych danych historycznych i statystycznych.

Ministerstwa opracowują własne raporty częściowe. Mogą one się różnić, jednak zachowują ujednolicone podejście i metody. Metodologia oceny ryzyka opiera się bezpośrednio na Wytycznych Komisji Europejskiej dotyczących oceny ryzyka i planowania w zarządzaniu katastrofami⁹ oraz raporcie Wspólnego Centrum Badawczego pt. Ryzyko, zagrożenie i narażenie ludzi na zagrożenia naturalne, przegląd definicji, koncepcji i danych¹⁰, jak również doświadczeniach zebranych w Szwecji, Holandii i Norwegii. Opis metodologii, która została opracowana na polskie potrzeby, znajduje się w podręczniku, który uzupełnia szablon w programie Excel (zob. rozdział 3).

Podstawą metodologii jest systematyczny proces oceny ryzyka. Brane są pod uwagę wszystkie dostępne informacje (dane historyczne) i opinie (ekspertów). System jest otwarty na dodawanie nowych informacji, np. danych statystycznych. Metodologia ma zastosowanie do wszystkich czterech szczebli administracji, a korzystanie z niej nie jest skomplikowane. Metoda polega na analizowaniu i ocenie ponad 20 zidentyfikowanych zagrożeń. Klasyfikacja ryzyka/zagrożeń, określona w wytycznych opracowywania raportów częściowych, identyfikuje zagrożenia pierwotne, klęski żywiołowe lub katastrofy, zagrożenia wobec ludności cywilnej, zagrożenia wynikające z celowej działalności człowieka, zagrożenia terrorystyczne, polityczne i wojskowe. Rejestr zagrożeń zawiera 164 pozycje należące do ww. kategorii.

Zgodnie z procedurą określoną w wytycznych, powoływany jest zespół ekspertów zajmujący się analizą zidentyfikowanych zagrożeń. Najpierw dokonuje się analizy kontekstu: identyfikacji i zdefiniowania problemów, zaangażowania właściwych zainteresowanych stron (np. gmin, organizacji, właścicieli nieruchomości, populacji itd.), opisu obowiązujących przepisów i dokumentów strategicznych, uwarunkowań politycznych i ekonomicznych oraz kwestii społecznych i kulturowych. Rzeczywista analiza ryzyka rozpoczyna się od opisu scenariusza potencjalnego zagrożenia (uwzględniającego prawdopodobieństwo wystąpienia) i jego skutków. Scenariusze opisują co może się wydarzyć i wymieniają potencjalne oddziaływania/następstwa. By zrozumieć prawdopodobieństwo wystąpienia scenariusza, stosuje się analizę drzewa błędów. Inne metody analizy prawdopodobieństwa obejmują: drzewo zdarzeń

⁹ https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

¹⁰ JRC EUR 21410 (2004).

(częściowe prawdopodobieństwo określonych ścieżek następstw), dane statystyczne, dane historyczne, analizę niezawodności i niepewności oraz opinie eksperckie.

Po dokonaniu oceny wystąpienia zagrożenia, konieczny jest opis jego następstw za pomocą analizy drzewa zdarzeń. W odniesieniu do każdego scenariusza badany jest jego możliwy wpływ na ludność, gospodarkę, mienie, infrastrukturę i środowisko. W każdej z tych kategorii wskazywane są zarówno oddziaływania bezpośrednie, jak i pośrednie. Zgodnie z unijnymi wytycznymi oceny i tworzenia map ryzyka bierze się pod uwagę wpływ na ludzi, gospodarkę, środowisko, a także kwestie społeczno-polityczne (ostatnie stanowią podpunkt wpływu na ludzi).

Wpływ na ludzi

W ramach analizy wpływu danego scenariusza na ludzi, metodologia przyjęta w Polsce bierze pod uwagę następujące czynniki:

- potencjalna liczba ofiar śmiertelnych;
- potencjalna liczba osób hospitalizowanych (rannych lub chorych);
- potencjalna liczba osób ewakuowanych.

W drugiej fazie wskazuje się potencjalny wpływ na życie codzienne. Brane są również pod uwagę pośrednie skutki społeczne (np. wzrost bezrobocia oraz trwała niezdolność do pracy) i negatywne skutki psychologiczne. Ponadto uwzględnia się ochronę grup społecznych najbardziej narażonych na zagrożenia, np. osób starszych i dzieci.

Wpływ na gospodarkę/mienie/infrastrukturę

Bierze się pod uwagę potencjalne straty w mieniu i infrastrukturze, jak również koszty bezpośrednie i pośrednie (np. bezpośredni koszt odbudowy zniszczonego budynku, pośredni koszt przerwy w działalności gospodarczej wynikający ze zniszczenia siedziby).

Wpływ na środowisko

Opisuje się potencjalne szkody dla flory i fauny, powietrza, gleby i wody. Należy wskazać, czy negatywny wpływ danego zdarzenia jest odwracalny czy nie (tzn. powoduje trwałą lub długookresową degradację środowiska).

Średnia ocena tych kryteriów oddziaływania opiera się na wcześniej ustalonych kryteriach. Waga każdego z nich jest obliczana na podstawie poziomu prawdopodobieństwa. Metoda ta stanowi połączenie podejścia ilościowego i jakościowego.

Wszystkie rodzaje ryzyka wyszczególnione w RoZBN prezentowane są w postaci matrycy ryzyka będącej odzwierciedleniem prawdopodobieństwa wystąpienia ryzyka i jego skutków. Dla każdego zagrożenia wymienionego w raporcie przygotowuje się oddzielną matrycę ryzyka 5x5.

Wartości ryzyka oznaczono kolorami:

SKUTKI	5					
	4					
	3					
	2					
	1					
		A	B	C	D	E
		PRAWDOPODOBIENSTWO				

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

Końcowym etapem jest określenie poziomu akceptacji ryzyka w odniesieniu do każdego scenariusza. Istnieją cztery kategorie akceptacji ryzyka:

- akceptowane (A) – nie są wymagane żadne dodatkowe środki bezpieczeństwa. Aktualne rozwiązania i przypisane im siły i zasoby są wystarczające. Oprócz środków monitorujących nie jest wymagane działanie;
- tolerowane (T) – należy dokonać oceny alternatyw odpowiadając na pytanie: czy wprowadzenie niewielkich zmian organizacyjnych (prawnych bądź funkcjonalnych) nie przyczyni się do poprawy bezpieczeństwa lub jego poczucia;
- warunkowo tolerowane (WT) – należy wprowadzić dodatkowe środki bezpieczeństwa w terminie 6 miesięcy oraz polepszyć stosowane rozwiązania;
- nieakceptowane (N) – należy podjąć natychmiastowe działania w celu zwiększenia bezpieczeństwa, wprowadzić dodatkowe/nowe rozwiązania.

RoZBN zawiera poziom akceptacji ryzyka dla szczebla centralnego i wojewódzkiego w odniesieniu do każdego scenariusza. Poziomy akceptacji mogą się różnić w zależności od percepcji ryzyka na poziomie krajowym i regionalnym. Podczas gdy szczebel centralny uważa, że system zarządzania kryzysowego jest przygotowany na wystąpienie zagrożenia, postrzeganie władz województwa nie obejmuje obszaru całego kraju lecz terytorium, za które odpowiada. W związku z tym ryzyko, które może zostać zaakceptowane na poziomie jednego województwa, w kombinacji ze skutkami w innym województwie, może nie być do zaakceptowania dla szczebla centralnego. Z drugiej strony, ryzyko, które jest akceptowane na poziomie krajowym, może być niemożliwe do zaakceptowania na poziomie konkretnego województwa. RCB obiektywnie ocenia poziom ryzyka i przekazuje swoją decyzję odpowiednim zainteresowanym stronom.

Inny element analizy polega na określeniu kompetencji poszczególnych instytucji zaangażowanych w scenariusze (podmioty wiodące, koordynujące czy współpracujące). Ta część analizy powinna być podparta wszystkimi dostępnymi danymi, tj. graficznymi i tabelarycznymi, schematami, programami, mapami, wykresami, diagramami lub innymi danymi pochodzącymi z programów symulacyjnych, na podstawie których opisany został dany scenariusz. W odniesieniu do każdego scenariusza należy podjąć decyzję czy powinien on zostać włączony do KPZK. W zakresie rozwoju zdolności i gotowości RCB nie koncentruje się na określonym zagrożeniu ale na modułach działań i zasobów, do których trzeba się odwołać podczas przygotowywania KPZK. Niektóre działania i zasoby mogłyby być takie same w odniesieniu do różnych typów ryzyka, zatem należy zapewnić, że podczas tworzenia KPZK wszystkie zagrożenia oraz odpowiednie działania zostaną uwzględnione.

W realizowanym projekcie dotyczącym metodyki oceny ryzyka zaprojektowano oprogramowanie ARMOR (zob. ppkt 3.2).

Metodologia oceny ryzyka dla infrastruktury krytycznej

RoZBN odnosi się do zagrożeń, podatności i skutków w zakresie IK, jak również współzależności. Współzależności tworzą zagrożenia wpływające na działanie systemu (zagrożenia bezpośrednie) oraz wynikające z działań/operacji mających wpływ na użytkownika końcowego/podmioty zależne. Podczas analizowania negatywnego oddziaływania danego scenariusza należy stwierdzić czy może w nim ucierpieć IK. W szablonie krajowej oceny zagrożeń sporządzonym w programie Excel (zob. punkt 3.2) należy zdefiniować i szczegółowo opisać, w jakim zakresie istotne systemy IK mogą ucierpieć.

Ocena IK opiera się na podejściu obejmującym wszystkie zagrożenia i nie stosuje się oddzielnego rozróżnienia pomiędzy przyczynami technicznymi i aktami sabotażu. OIK rozumie się jako zapewnienie ochrony: fizycznej, technicznej, osobowej, teleinformatycznej (IT/OT) i prawnej oraz zarządzania ciągłością działalności, a także przywrócenia sprawności. Jak dotąd operatorów IK obowiązuje swoboda wyboru własnej metodologii, niemniej jednak RCB wydaje wytyczne oraz zalecenia dotyczące oceny ryzyka i włączania OIK w plany zarządzania kryzysowego. RCB promuje zarządzanie ciągłością działania. Obecnie jedna z grup roboczych pracuje nad identyfikacją wspólnej metodyki oceny ryzyka oraz włączeniem kwestii OIK w plany zarządzania kryzysowego. Generalnie, RCB zaleca właścicielom/operatorom IK stosowanie norm ISO.

RCB dokonuje przeglądu oceny ryzyka sporządzonej przez właścicieli/operatorów IK w planach OIK i w razie potrzeby formułuje zalecenia (przegląd zidentyfikowanych zagrożeń, kontrola współzależności oraz zalecenie ćwiczeń). W sytuacji gdy jakość wykonanej oceny ryzyka jest przez RCB kwestionowana, właściciele/operatorzy IK zapraszani są na spotkania w formule 1:1 (RCB – organizacja) w celu przedyskutowania różnic. W przypadku gdy wszystkie zagrożenia nie zostały wzięte pod uwagę lub brakuje niektórych oddziaływań/następstw, RCB prosi o wyjaśnienie. Dodatkowo, jeżeli nie zgadza się z oceną właścicieli/operatorów IK stara się zidentyfikować powody/uzasadnienie/wyjaśnienia. RCB jak dotąd nie ma prawa dokonywania kontroli operatorów IK. W celu podniesienia jakości oceny ryzyka prowadzone są ćwiczenia.

Metodologia oceny zagrożeń związanych ze zmianami klimatu

W ramach oceny scenariuszy związanych ze zmianami klimatu bierze się pod uwagę wszystkie aspekty wpływu i podatności (np. społeczne, gospodarcze itd).

KZGW koordynuje implementację Dyrektywy Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim, potocznie zwanej Dyrektywą Powodziową (2007/60/WE¹¹). Wszystkie obowiązki unijne zostały implementowane do przepisów polskich. Tworzone są wstępne oceny ryzyka powodziowego, które dają ogólny ogłęd ryzyka powodziowego oraz analizy GIS. Zgodnie z dyrektywą sporządzono mapy ryzyka powodziowego. Ocena obejmuje

¹¹ <http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:32007L0060>

gromadzenie danych, tworzenie bazy danych, identyfikację istotnych ryzyk oraz wybór obszarów potencjalnego znaczącego ryzyka powodziowego (APSFR). Kryteria oddziaływania ryzyka wystąpienia powodzi uwzględniają następujące czynniki:

1. oddziaływanie bezpośrednie;
2. oddziaływanie gospodarcze;
3. skuteczność istniejących środków ochrony przeciwpowodziowej;
4. oddziaływanie zagospodarowania przestrzennego.

Podczas oceny podatności na wystąpienie ryzyka brane są pod uwagę takie czynniki jak: życie i zdrowie ludzi, środowisko, dziedzictwo kulturowe i działalność gospodarcza. Istnieje mechanizm mający na celu ustalenie priorytetów inwestycji.

Metodologia oceny ryzyka teleinformatycznego

Ocena zagrożeń teleinformatycznych opiera się na normach ISO 31000 oraz ISO 27005. Przy obliczeniu poziomu zagrożenia bierze się pod uwagę kombinację prawdopodobieństwa wystąpienia oraz wartość strat. Jeżeli jest niższy niż 20% wartości maksymalnej, zostaje automatycznie zaakceptowany. Jeżeli jest wyższy niż 20%, rozpoczyna się kolejna faza oceny ryzyka, podczas której wprowadzane są środki kontroli, a następnie poziom zagrożenia oblicza się i ocenia ponownie. Jeżeli nowy poziom jest niższy niż 20%, dane zagrożenie zostaje zaakceptowane ale pozostaje pod nadzorem właściciela w celu monitorowania. Zagrożenia na poziomie pomiędzy 20% a 80% podlegają zatwierdzeniu zgodnie z zasadami określonymi przez jednostkę lub podlegają ponownej ocenie. Zagrożenia na poziomie ponad 80% są przedkładane do zatwierdzenia najwyższymi kadrami zarządczymi jednostki. Co roku jednostki publiczne muszą zgłaszać wyniki analizy ryzyka do ministerstwa właściwego do spraw wdrażania rozwiązań informatycznych.

Dobre praktyki:

- Polska stworzyła własną metodologię krajowej oceny ryzyka, która jest zgodna ze standardami UE (np. odzwierciedla wszystkie aspekty podatności – społeczne, fizyczne, gospodarcze i polityczne). Bierze pod uwagę rozwiązania stosowane w innych państwach, które dostosowuje do polskich potrzeb. Szczególnie godne uwagi są elementy takie jak: proces dwukierunkowy, pętla informacji zwrotnych, cząstkowe raporty sektorowe, kombinacja metod jakościowych, ilościowych i półilościowych czy kwestionariusz, z którego mogą korzystać osoby niebędące ekspertami.
- RCB opracowuje ocenę ryzyka na szczeblu krajowym na podstawie raportów cząstkowych ministerstw, urzędów centralnych i województw, dla których wydaje wytyczne w tym zakresie. W przypadku rozbieżności pomiędzy poziomami akceptacji ryzyka na szczeblu centralnym i regionalnym wykorzystuje się dwukierunkową procedurę, w ramach której prowadzone są dyskusje i wypracowywany kompromis.
- Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy (PIG) monitoruje miejsca zagrożone osuwiskami w Polsce; w celu oszacowania ryzyka posługuje się podejściem jakościowym oraz metodologią korzystającą z dobrej jakości danych.
- RCB zaleca operatorom/właścicielom IK stosowanie norm ISO.

Rekomendacje:

- Wdrożyć oprogramowanie, np. ARMOR, oraz dokonać odpowiednich korekt w metodzie oceny w sposób usystematyzowany.¹²
- Kontynuować rozwijanie polskiej metodologii oceny ryzyka na podstawie ewaluacji i informacji zwrotnych pochodzących od zainteresowanych stron.
- Aktywnie podjąć współpracę z Wspólnym Centrum Badawczym Komisji Europejskiej aby porównać polską metodologię z metodologiami innych państw członkowskich w celu zbadania możliwości wykorzystania jej innowacyjnych elementów dla poprawy jakości metodologii oceny ryzyka stosowanej aktualnie w UE.
- Przeprowadzić symulację wykorzystania wspólnej metodologii oceny ryzyka na wszystkich poziomach, aby zagwarantować, że monitorowane będą również te zagrożenia, które nie są istotne z perspektywy bezpieczeństwa całego kraju.
- Rozważyć dostosowanie metodologii krajowej do zastosowania na szczeblu lokalnym (gminy i powiaty).
- Rozważyć, w jaki sposób ocena lokalnych i regionalnych podatności oraz zdolności mogłaby znaleźć odzwierciedlenie w metodologii, ponieważ może to być istotne w sytuacji gdy zasoby pozostające w dyspozycji szczebla niższego są niewystarczające w danej sytuacji kryzysowej (wywołując potrzebę zaangażowania poziomu krajowego).¹³
- Wyjaśnić, jakie są wzajemne powiązania między metodologią KOR oraz kilkoma metodami sektorowymi, np. OIK, CCA, ocena ryzyka powodziowego itd. Rozważyć opracowanie poradnika zawierającego informacje na temat wykorzystania RoZBN do prowadzenia sektorowych ocen ryzyka.
- Rozważyć zwrócenie w metodologii większej uwagi na kwestie zagrożeń międzynarodowych i transgranicznych w celu wzmocnienia dialogu z sąsiednimi państwami (zob. ppkt 1.2).
- Stosować ustandaryzowane definicje (EU, ISO, UNISDR) w odniesieniu do wszystkich istotnych pojęć.

¹² Polska spodziewa się, że oprogramowanie ARMOR zostanie wdrożone do połowy 2017 r.

¹³ Szkoła Główna Służby Pożarniczej pracuje obecnie (połowa 2016 r.) nad zidentyfikowaniem barier systemowych, w tym zdolności lokalnych i regionalnych oraz bada możliwości ich ilościowego ujęcia.

3. Informowanie i komunikacja

3.1 Wymiana informacji

Cel: dostępna jest infrastruktura i odpowiednie informacje do prowadzenia procesu oceny ryzyka.

Procedura sporządzania raportu cząstkowego określa następujące sposoby pozyskiwania danych:

- analiza danych statystycznych;
- analiza danych historycznych;
- szacowanie eksperckie;
- badania terenowe;
- ocena sytuacji międzynarodowej;
- modelowanie matematyczne;
- analiza danych z systemu monitorowania zagrożeń;
- analiza trendów;
- badanie przypadków („case study”);
- ocena środowiskowa itd.

RoZBN scala i analizuje wszystkie dane w jednolity sposób. Część danych jest niejawna, dlatego nie jest udostępniana wszystkim zainteresowanym stronom (ani opinii publicznej).

W 2011 r. wprowadzono procedurę dotyczącą wykorzystywania danych historycznych na potrzeby oceny ryzyka ale wydaje się, że nie osiągnięto jednolitego poziomu ich jakości.

Niedawno kilka ministerstw podjęło inicjatywę stworzenia zgodnej z wytycznymi unijnymi metodologii pozyskiwania danych dotyczących strat. Dane historyczne z różnych sektorów nie są porównywalne i zależą od podmiotów oraz regionów. W celu oceny strat spowodowanych przez klęski żywiołowe, departament zajmujący się tą problematyką w Ministerstwie Spraw Wewnętrznych i Administracji stara się ujednolicić zakres zbieranych informacji.

Ochrona infrastruktury krytycznej

Regulacje zobowiązują właścicieli/operatorów IK do dzielenia się informacjami z administracją rządową. Mają obowiązek zgłaszać i przekazywać władzom informacje, gdy zdarzenie ma wpływ na świadczone usługi oraz na populację. NPOIK zobowiązuje do utworzenia punktów kontaktowych IK dla wyznaczonej IK. RCB jest pierwszym punktem kontaktowym dla właścicieli i operatorów wyznaczonej IK, spełniającym funkcję koordynacyjną. Wytyczne RCB zawierają wskazówki na temat przekazywania informacji właścicielom i operatorom IK oraz między nimi, szczególnie w kwestiach dotyczących współzależności. Punkty kontaktowe służą jako kanał wymiany informacji i wiedzy pomiędzy właścicielami i operatorami IK, władzami lokalnymi i RCB. RCB stanowi pierwszy poziom kontaktu w sytuacji awaryjnej. Na poziomie operacyjnym istnieje platforma internetowa, będąca narzędziem OIK do wymiany ogólnych i jawnych informacji.

RCB dzieli się wszelkimi informacjami mającymi znaczenia dla OIK z władzami województw oraz właścicielami/operatorami IK. Operatorzy IK mogą dzielić się informacjami niejawnymi z RCB, ministerstwami i władzami województw. Agencja Bezpieczeństwa Wewnętrznego bezpośrednio dzieli się z operatorami IK informacjami dotyczącymi zagrożenia aktami terrorystycznymi. Mimo że wymiana informacji jest obowiązkowa, właściciele/operatorzy IK decydują, którymi informacjami się dzielą. RCB nie ma gwarancji, że przekazują 100% informacji. Operatorzy IK niechętnie dzielą się wszystkimi informacjami twierdząc, że wrażliwe informacje dotyczące kwestii rynkowych i handlowych mogą zostać wykorzystane przez konkurencję. Rolą RCB jest ocena kompletności otrzymanych informacji i poprawa systemu wymiany informacji pomiędzy właścicielami/operatorami IK a władzami centralnymi. Mimo faktu, że w Polsce system OIK nie przewiduje sankcji, operatorzy na ogół rzetelnie traktują swoją odpowiedzialność za OIK.

Funkcjonuje także specjalna procedura wymiany informacji pomiędzy właścicielami/operatorami IK, samorządami lokalnymi oraz RCB dotycząca zagrożeń osuwiskami i innymi klęskami żywiołowymi. RCB stara się zapewnić, aby wszystkie zainteresowane strony przestrzegały tej procedury.

Dostosowanie do zmian klimatycznych

Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy współpracuje z RCB, Państwową Strażą Pożarną itd. Jednym z najważniejszych działań jest wydawanie ostrzeżeń o zagrożeniach mogących potencjalnie wystąpić w niedługim czasie. Poza tym prowadzi badania i przygotowuje długookresowe prognozy potencjalnych zagrożeń. Podstawowym ograniczeniem jest przedział czasu dotyczący prognozowanych zdarzeń. Prognoza na okres dłuższy niż 10 dni nie jest miarodajna. Instytut nie ma wyposażenia pozwalającego zapewnić wiarygodne prognozy długoterminowe. Konieczne są dalsze inwestycje w badania aby takie prognozy mogły być przygotowywane. Doskonaleniu wiedzy służy także prowadzony proces oceny i prognozowania ryzyka. Instytut nie posiada regulacji dotyczących oceny ryzyka suszy i zarządzania nim ale stara się to zmienić.

Instytut blisko współpracuje z RCB, które w opracowywanych ocenach zagrożeń uwzględnia informacje dotyczące m.in. wpływu potencjalnych ekstremalnych zdarzeń pogodowych na obywateli, gospodarkę oraz bezpieczeństwo państwa. Stosuje się wiele różnorodnych narzędzi przekazywania informacji instytucjom państwowym oraz opinii publicznej. Instytut zbiera i ocenia dane związane z zagrożeniami oraz przekazuje je do dalszej analizy instytucjom w celu identyfikacji potencjalnego ryzyka i dokonania rozróżnienia pomiędzy niebezpieczeństwem, zagrożeniem i ryzykiem.

Dokument strategiczny dotyczący zarządzania ryzykiem powodziowym jest na ostatnich etapach akceptacji. Instytut śledzi zmiany następujące w innych państwach i wykorzystuje ich dobre praktyki. KZGW posiada rejestry powodzi odnotowanych w XX w. Baza danych nie uwzględnia wprowadzie strat, jednak KZGW zbiera informacje umożliwiające zarządzanie nimi. Komisja Europejska współpracuje z Polską w zakresie poprawy ewidencjonowania strat związanych z powodziami.

Osuwiska

Jedną z głównych przyczyn osuwisk w Polsce jest szkodliwa działalność inwestycyjna. Najważniejszymi czynnikami aktywującymi osuwiska jest spływ wód deszczowych i roztopowych, których oddziaływanie potęgowane jest przez niewłaściwą działalność człowieka. Podejście do oceny ryzyka w przypadku osuwisk jest jakościowe. W ramach realizowanego przez PIG projektu System Osłony Przeciwsuwiskowej (SOPO) przeprowadzono inwentaryzację osuwisk oraz sporządzono mapy osuwisk i terenów potencjalnie zagrożonych ruchami masowymi w Polsce, które przekazano administracji lokalnej. Władze powiatów mają obowiązek prowadzenia rejestru terenów zagrożonych.

Dobre praktyki:

- Polska dysponuje wysokiej jakości danymi i korzysta z analiz naukowych do celów KOR, jak również wykorzystuje inne dane statystyczne dotyczące różnych zagrożeń.
- Organizowane są warsztaty i konferencje na specjalistyczne tematy związane z IK, np. niezawodność techniczna, biometria, materiały wybuchowe itd. Opracowywane są także newslettery poświęcone tej problematyce.

Rekomendacje:

- Stworzyć wspólny standard danych wykorzystywanych w ocenie ryzyka.
- W procesie opracowania metodologii tworzenia baz danych o stratach mogłyby pomóc wytyczne Komisji Europejskiej dotyczące ewidencjonowania danych na temat katastrof, zniszczeń i strat.
- Należy podjąć starania, aby udoskonalić wymianę wrażliwych informacji dotyczących tematów związanych z OIK. Kwestie rynkowe i konkurencyjne stanowią przeszkody, którymi należy zarządzać metodą perswazji oraz budowania zaufania ale również wyraźnego „modus operandi” wymiany informacji wrażliwych (zob. również zalecenia w ppkt. 6.2).
- Budować zaufanie pomiędzy prywatnymi operatorami a sektorem publicznym w procesie wymiany informacji biorąc pod uwagę ekonomiczną wartość ryzyka ponoszoną przez poszczególnych operatorów. Ocena ryzyka mogłaby zawierać oszacowanie potencjalnych strat ekonomicznych, jakie poniósłby operator w przypadku zakłócenia jego działalności. Z informacji tych można korzystać przy określaniu priorytetów wspierania podmiotów prywatnych przez sektor publiczny w zakresie zarządzania ciągłością działania.
- Zachęcać władze (powiatów i gmin) do wdrożenia projektu SOPO oraz jego wyników na wszystkich obszarach narażonych na osuwanie się ziemi.
- Zwracać większą uwagę na działalność człowieka jako główny czynnik utraty stateczności skarp i zboczy podczas lokalnej oceny ryzyka osuwisk.

3.2 Infrastruktura teleinformatyczna

Cel: na potrzeby oceny ryzyka dostępny jest skuteczny system teleinformatyczny.

Szablon w programie Excel na potrzeby oceny ryzyka

W celu ułatwienia opracowania KOR stworzony został specjalny szablon/formularz w programie Excel.

W szablonie muszą znaleźć się następujące informacje:

- „zagrożenia” – gdzie wskazywane są zagrożenia/ryzyka, dla których opracowywane są scenariusze i wykonywana ocena ryzyka;
- „zapobieganie” – gdzie określone są cele strategiczne wraz ze szczegółowymi działaniami oraz wskazane siły i środki niezbędne do ich realizacji;
- „przygotowanie” – gdzie wymienione są programy mające na celu poprawę bezpieczeństwa wraz z informacją o czasie ich trwania, źródłach finansowania i instytucjach je realizujących;
- „reagowanie” – gdzie opisuje się priorytety oraz zasady reagowania;
- „dane historyczne” – gdzie opisane są występujące w przeszłości zagrożenia z uwzględnieniem m.in. daty lub przedziału czasowego, miejsca/obszaru, konsekwencji/strat.
- „wnioski” – gdzie znajdują się dodatkowe informacje, spostrzeżenia i wnioski.

Dokument metodologiczny obejmuje płytę CD, na której w szablonie w programie Excel znajduje się leksykon obejmujący 795 scenariuszy.

ARMOR

ARMOR jest programem, który został stworzony do wparcia przygotowania oceny ryzyka na różnych szczeblach administracji. Znajduje się w początkowej fazie testów. Wymaga uzupełnienia o elementy związane z identyfikacją poszczególnych ryzyk oraz wprowadzenia zestawu parametrów, które są zróżnicowane w zależności od zagrożeń wymienionych w rejestrze. Wprowadzane parametry opierają się na kwestionariuszu zawierającym pytania, na które należy udzielić odpowiedzi tak lub nie (w fazie identyfikacji ryzyka) oraz pytania otwarte dotyczące m.in. liczby osób czy danych geograficznych.

Pytania w kwestionariuszu są z góry ustalone, a oprogramowanie AMOR interpretuje odpowiedzi, które system zapisuje i nie pyta o nie ponownie. Wynik jest prezentowany bezpośrednio w macierzy ryzyka. Scenariusze mogą zostać przedstawione na mapie i udostępnione wszystkim szczeblom administracji państwowej. Każde województwo może zobaczyć wszystkie scenariusze dla swoich powiatów i gmin, natomiast informacje dotyczące innych województw widoczne są w formie zbiorczej.

Poziomy akceptacji ryzyka są ustalane przez podmioty odpowiedzialne za dane ryzyko (właścicieli ryzyka). Użytkownicy programu ARMOR mogą zgłaszać sugestie dotyczące jego dalszego rozwoju lub bezpośrednio wprowadzać informacje do systemu.

W aktualnej wersji program ARMOR jest narzędziem informatycznym, przygotowanym dla centralnych instytucji państwowych. Docelowo ma być dostępny dla niższych szczebli administracji (województw, powiatów i gmin). Może być również wykorzystywany w OIK. Zakłada się, że program będzie użytkowany przez ekspertów

i pracowników z instytucji zajmujących się oceną ryzyka. Osoby niebędące ekspertami mogą zadawać pytania ekspertom i uzyskiwać odpowiedzi (Q&A). Decyzja o tym kogo uwzględnić, zależy od zaangażowanych instytucji, natomiast zalecane jest włączenie podmiotów na wszystkich szczeblach administracji. System stosuje zastrzeżone środki bezpieczeństwa. Narzędzie znajduje się jeszcze w fazie testów (nie zostało uruchomione).

ISOK

Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy pracuje nad kilkoma systemami, w tym systemem ISOK (Informatyczny System Ochrony Kraju przed Nadzwyczajnymi Zagrożeniami), który jest realizowany w ramach unijnego projektu przez konsorcjum, na którego czele stoi KZGW. ISOK jest systemem informatycznym, stworzonym w celu ochrony społeczeństwa, gospodarki i środowiska przed ekstremalnymi zagrożeniami oraz wsparcia procesu podejmowania decyzji w razie ich wystąpienia. Znajduje się obecnie w piątej (końcowej) fazie wdrażania. Zawiera lokalne mapy zagrożeń. Stanowi element Infrastruktury Informacji Przestrzennej i wykorzystuje dane referencyjne udostępniane przez Główny Urząd Geodezji i Kartografii (GUGiK). Jego elementem są portale prezentujące informacje i dane przestrzenne (mapy) z różnych źródeł (tworzonych w systemie lub ze źródeł zewnętrznych).

System ISOK prezentuje m.in. wstępną ocenę ryzyka powodziowego, mapy zagrożenia powodziowego i ryzyka powodziowego oraz dane geoprzestrzenne, związane z wybranymi zagrożeniami meteorologicznymi. Dzięki dodatkowym danym znajdującym się w systemie (ostrzeżenia Państwowej Służby Hydrologiczno-Meteorologicznej, komunikaty, dane tabelaryczne, wykresy itp.) możliwa jest szybka identyfikacja skali oraz zasięgu zagrożenia, co pozwala przygotować się do potencjalnego zagrożenia oraz podjąć odpowiednie działania w sytuacji jego wystąpienia.

Dobre praktyki:

- Na potrzeby KOR opracowano specjalne, zindywidualizowane oprogramowanie: zbiorczy arkusz kalkulacyjny (tabela w programie Excel zawierająca stopnie ryzyka) oraz oprogramowanie ARMOR z kwestionariuszem przeznaczonym także dla osób niebędących ekspertami.

Rekomendacje:

- Zbadać możliwość wprowadzenia mapowania wszystkich rodzajów ryzyka w oparciu o standardy wymiany danych oraz GIS, co pozwoliłoby na integrację istniejących map opracowanych w różnych skalach¹⁴, tak aby wyniki oceny ryzyka mogły zostać implementowane do jednolitego systemu informacji przestrzennej lub tworzyć spójny zestaw systemów.

3.3 Komunikacja ryzyka

Cel: dostępne są zdolności administracyjne konieczne, aby komunikować opinii publicznej wyniki oceny ryzyka.

¹⁴ Zob. również: Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE); <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007L0002>

RoZBN jest dokumentem niejawnym, natomiast KPZK jest ogólnodostępny. W przyszłości planuje się publikowanie KPZK na stronie internetowej w postaci dokumentu z aktywnymi łączami pomiędzy poszczególnymi jego częściami. Jednak byłaby ona przeznaczona dla osób zawodowo zajmujących się tymi zagadnieniami lub zainteresowanych tą tematyką, a nie dla obywateli. Polska stara się stworzyć stronę internetową angażującą społeczeństwo w proces zarządzania kryzysowego. Obecnie RCB na stronie internetowej publikuje porady na temat zachowania się w sytuacji zagrożeń. Wykorzystuje w tym celu także media społecznościowe (Facebook i Twitter).

RCB zachęca instytucje rządowe do publikowania planów zarządzania kryzysowego. Co do zasady, plany, za wyjątkiem fragmentów niejawnych dotyczących IK, stanowią informację publiczną. Jeżeli chodzi o IK, większość informacji nie jest publikowana. Podczas misji przeglądu wzajemnego przedstawiono kilka dobrych przykładów informowania opinii publicznej (np. przez PAA, IMGW i KZGW) o wynikach oceny ryzyka aby ludność zamieszkująca tereny zalewowe mogła podjąć środki zapobiegawcze i przygotować się na nadejście powodzi. Także Mazowiecki Urząd Wojewódzki, Urząd Miasta Stołecznego Warszawy oraz Urząd Miasta Płock dysponują systemami alarmowymi i procedurami powiadamiania obywateli o zidentyfikowanych i poddanych ocenie rodzajach ryzyka. Publicznie dostępne są różnorodne informacje o zagrożeniach (w tym mapy). Zazwyczaj pochodzą one z lokalnych ocen ryzyka oraz raportów cząstkowych nie zaś z RoZBN. W celu podnoszenia poziomu świadomości społeczeństwa o zagrożeniach lepszą metodą są ćwiczenia niż plany. Polska włącza w ćwiczenia zainteresowane organizacje ale nie ogół społeczeństwa.

IMI GW przekazuje informacje, które wykorzystywane są w bezpłatnej aplikacji mobilnej ostrzegającej przez zjawiskami pogodowymi oraz innymi zagrożeniami. Regionalny System Ostrzegania jest wykorzystywany przez wojewodów do informowania opinii publicznej. Zawiera on także porady dla ludności na temat zachowania się w sytuacjach różnych zagrożeń.

Centrum Bezpieczeństwa m.st. Warszawy¹⁵ dostarcza opinii publicznej ogólne informacje o zdarzeniach mających istotne znaczenie dla społeczeństwa. Ludność może się skontaktować z Centrum przez Internet. Jego strona internetowa jest przeznaczona do przekazywania ludności powiadomień i zawiera wiele informacji, które mogą być interesujące i ważne dla obywateli. Dostępna jest darmowa aplikacja mobilna, którą można ściągnąć na telefon komórkowy informująca o „problematycznych wydarzeniach”. Centrum wysyła również ludności ostrzeżenia o sytuacjach kryzysowych. Zawarto umowy z mediami (stacjami telewizyjnymi itd.) umożliwiające przekazywanie komunikatów do ludności za pośrednictwem środków masowego przekazu.

W przypadku zdarzeń radiacyjnych komunikację społeczną zapewnia PAA, które także udziela wsparcia eksperckiego decydentom (Minister Spraw Wewnętrznych i Administracji, wojewodowie). Agencja stworzyła i wdrożyła strategię komunikacji oraz utrzymuje kontakty z mediami w celu wyjaśniania informacji dotyczących bezpieczeństwa jądrowego i ochrony radiologicznej w przypadku kryzysu.

¹⁵ Podczas misji przeglądu wzajemnego miała miejsce wizyta w Centrum, którego dotyczą zawarte w Raporcie opinie, natomiast nie opisano innych miast i podobnych jednostek, których misja nie dotyczyła.

W ramach przygotowania do ewentualnej sytuacji kryzysowej PAA wspiera uczelnie w rozpowszechnianiu wśród studentów wiedzy na temat zakresu odpowiedzialności i zadań młodych ludzi oraz istniejących procedur przygotowania na sytuacje awaryjne oraz reagowania na awarie jądrowe i zagrożenia radiologiczne.

Krajowa polityka miejska ma na celu przede wszystkim zapewnienie bezpieczeństwa obywatelom. Zakłada informowanie różnych grup społecznych (w tym dzieci i osób starszych) jak zachowywać się w sytuacji zagrożenia by zagwarantować, że plany rządu będą użyteczne i zgodne z potrzebami ludności oraz sprawdzić czy informacje są wystarczająco zrozumiałe dla obywateli.

W odniesieniu do zagrożeń osuwiskami, społeczeństwo ma dostęp do informacji zebranych przez PIG w bazie SOPO. W przypadku przewidywanych inwestycji publicznych, informacje o terenach narażonych na osuwanie się ziemi można uzyskać za pośrednictwem jednostek samorządowych i potwierdzić w PIG. Przed rozpoczęciem budowy na obszarach zagrożonych osuwiskami, obywatele są zachęceni aby zwrócić się do samorządu. Władze powiatów mają obowiązek monitorowania obszarów/lokalizacji osuwisk tam gdzie występuje zagrożenie dla życia ludzi lub zapewnienia podstawowych potrzeb społeczeństwa oraz transportu. Zobowiązane są także do informowania o zagrożeniach opinii publicznej.

Ochrona infrastruktury krytycznej

Większość informacji na temat OIK jest niejawną. Uważa się to za przeszkodę w uzyskaniu wystarczającego poziomu przejrzystości komunikacji ze społeczeństwem. Jednym ze sposobów zwiększenia świadomości ryzyka wśród ludności bez ujawniania informacji niejawnych jest zaangażowanie zainteresowanych stron w proces zarządzania skutkami zdarzeń.

Dostosowanie do zmian klimatu

Mapy oceny ryzyka powodziowego są dostępne w Internecie. W konsultacjach społecznych planów zarządzania ryzykiem powodzi, za pośrednictwem Krajowego Forum Wodnego, wzięło udział ok. 3 tys. osób m.in. ze środowisk samorządowych, naukowych oraz obywateli zamieszkujących zagrożone tereny. KZGW sporządził 12 projektów planów zarządzania ryzykiem powodzi. Opracowuje programy edukacji o ryzyku powodzi: materiały promocyjne (np. film pt. „Mnie to nie dotyczy”), jak również materiały reklamowe.

Biuro Infrastruktury m.st. Warszawy wykorzystuje grę planszową, za pomocą której przekazuje młodzieży informacje o zmianach klimatu. Do programów nauki szkolnej na poziomie podstawowym dodano również specjalne lekcje dotyczące tej tematyki. Organizowane są różnorodne przedsięwzięcia i gry przeznaczone dla różnych grup wiekowych oraz wiele kampanii edukacyjnych. Publikowane są także broszury edukacyjne dla dzieci. Polska zaczęła dopiero podejmować działania w tej dziedzinie i wciąż rozwija metody przekazywania informacji na temat zmian klimatu szerokiej opinii publicznej.

Dobre praktyki:

- RCB na stronie internetowej publikuje broszury i porady na temat zachowania się w sytuacji zagrożeń.
- Mapy ryzyka powodziowego dostępne są w Internecie, istnieje również program edukacji w tym zakresie. Dostępność informacji prowadzi do zwiększenia udziału różnych zainteresowanych stron oraz społeczeństwa w zarządzaniu ryzykiem powodzi.
- Mapy ryzyka ISOK mają być dostępne dla wszystkich obywateli.
- Istnieje bezpłatna aplikacja ostrzegająca przed zjawiskami pogodowymi i innymi zagrożeniami.

Rekomendacje:

- Na bazie KOR stworzyć strategię komunikacji ryzyka (uwzględniającą IK) mającą na celu podniesienie poziomu wiedzy i świadomości obywateli oraz zwiększenie ich udziału w działaniach dotyczących prewencji, przygotowania, reagowania i usuwania skutków zagrożeń. Powinna ona wskazywać podmioty odpowiedzialne za komunikowanie (w oparciu o siatkę bezpieczeństwa), jak również zapewniać spójność i integrację działań komunikacyjnych ministerstw, instytucji krajowych oraz innych jednostek administracji państwowej na wszystkich szczeblach i we wszystkich sektorach gospodarki (np. ogólnopolska strona internetowa, biuletyny, kampanie informacyjne itd.).
- RCB powinno pełnić koordynacyjną rolę w strategii, zapewniając jej spójność i zgodność informacji. Opracowane przez RCB poradniki na temat zachowania się w sytuacjach zagrożeń mogłyby zostać włączone do jej zapisów. Publikacja dodatkowych broszur i informacji na podstawie RoZBN powinna zostać potraktowana priorytetowo.
- Opracować (jako część komunikacji ryzyka lub przynajmniej w bezpośredniej korelacji z nią) strategię komunikacji CCA, łącząc działania komunikacyjne Ministerstwa Edukacji Narodowej, Ministerstwa Środowiska, RCB itd.

4. Wiedza ekspercka

Cel: eksperci prowadzący krajową ocenę ryzyka posiadają niezbędne kompetencje i wyznaczone zadania oraz otrzymali odpowiednie przeszkolenie w zakresie prowadzenia oceny ryzyka.

RCB koordynuje opracowywanie metodologii KOR. Wydało również wytyczne dotyczące procedury opracowywania raportów częściowych. Rola RCB polega także na organizowaniu szkoleń i warsztatów dla podmiotów zaangażowanych w ten proces. Celem jest przedstawienie przyjętej metodyki oceny ryzyka i zwiększanie świadomości wśród ekspertów z zakresu zarządzania kryzysowego.

Oprogramowanie ARMOR służące do wykonania KOR jest przyjazne dla użytkownika. Zadaje proste pytania, a osoby na nie odpowiadające nie muszą posiadać specjalistycznego wykształcenia w zakresie metodologii badań (program może być wykorzystywany na wszystkich szczeblach administracji przez użytkowników nieposiadających wiedzy technicznej, a jednocześnie spełniać swój cel). Użytkownicy mogą mieć przygotowanie eksperckie i fachową wiedzę w zakresie oceny ryzyka albo być administratorami, zbierając dane na podstawie rejestrów statystycznych bez potrzeby posiadania specjalistycznego wykształcenia. Przeszkolony urzędnik będzie zadawał pytania wskazane przez program ARMOR, a lokalni eksperci muszą udzielić odpowiedzi, które po wprowadzeniu do systemu zostaną automatycznie zinterpretowane. W złożonych scenariuszach parametry są przedstawiane w sposób zrozumiały dla laika, co pozwala administratorowi nieposiadającemu wiedzy technicznej/naukowej zadawać pytania zainteresowanym stronom, gromadzić konieczne dane wejściowe, czego wynikiem jest automatyczna interpretacja odpowiedzi.

W polskim środowisku naukowym istnieje wiele uczelni, które szkolą i wspierają podmioty rządowe w prowadzeniu ocen ryzyka (Szkoła Główna Służby Pożarniczej, Politechnika Warszawska, Akademia Obrony Narodowej itd.). Nie istnieje formalny program szkolenia wszystkich osób zawodowo zajmujących się oceną ryzyka w sektorze administracji państwowej. Dostępne są natomiast kursy umożliwiające podnoszenia kwalifikacji zawodowych, m.in. w ramach studiów oraz studia podyplomowe oferowane przez Szkołę Główną Służby Pożarniczej.

SGSP jest uczelnią wyższą nadzorowaną przez MSWiA, przygotowującą kadry ochrony przeciwpożarowej oraz ochrony ludności. Posiada dwustronne umowy ze swoimi odpowiednikami w innych państwach. Prowadzi również specjalne kursy dla pracowników innych sektorów służby publicznej. Studenci SGSP obecnie szkoleni są z posługiwania się przyjętą metodą KOR. Opracowano również program e-learningowy dla administratorów (rysko.e.ucz.pl), którego celem jest poprawa poziomu wiedzy kadr zajmujących się oceną ryzyka i zarządzaniem nim w instytucjach publicznych. Ponadto SGSP tworzy obecnie pełny program kształcenia z metody KOR. W ten sposób rozwija zdolności administracji w zakresie wykonywania oceny ryzyka, ale podejście jest bardziej ukierunkowane na systemy niż na politykę i w dużym stopniu zależy od indywidualnych możliwości.

W Polsce prowadzone są liczne projekty związane z oceną ryzyka i zarządzania nim, pomagające uzyskać wysoki poziom wiedzy teoretycznej i praktycznej kadry zajmującej się tą tematyką.

Dobre praktyki:

- Szkoła Główna Służby Pożarniczej oferuje studia w zakresie inżynierii bezpieczeństwa pożarowego, inżynierii bezpieczeństwa cywilnego i bezpieczeństwa wewnętrznego. Program każdego z tych kierunków obejmuje problematykę oceny ryzyka, w tym metodykę ilościową i jakościową.
- Wśród instytucji zaangażowanych w proces oceny ryzyka występuje odpowiedni poziom wiedzy. Na wszystkich szczeblach administracji zatrudnione są osoby posiadające specjalistyczną wiedzę.
- Istnieje program e-learningowy, którego celem jest poprawa poziomu wiedzy pracowników administracji rządowej w zakresie oceny ryzyka.

Rekomendacje:

- Oprócz prowadzenia edukacji, zagwarantować możliwości wymiany doświadczeń między osobami zawodowo zajmującymi się krajową metodologią oceny ryzyka.
- Zbadać możliwość przygotowania przez RCB we współpracy z jednostkami naukowo-badawczymi (np. Szkołą Główną Służby Pożarniczej) wspólnej strategii dalszego rozwoju zdolności administracyjnych do prowadzenia oceny ryzyka na wszystkich szczeblach administracji. Zamiast polegać na pracownikach indywidualnie zapisujących się na kursy lub studentach podejmujących specjalistyczne studia, stworzyć celowościowe podejście pozwalające identyfikować i wzmacniać słabe punkty w administracji.
- Jako część powyższego programu można wykorzystać istniejące materiały e-learningowe. Można również zorganizować szkolenia w zakresie oceny ryzyka i podejmowania decyzji na wszystkich poziomach administracji, ukierunkowane na standaryzację metodologii oceny ryzyka w całym kraju.
- Promować interdyscyplinarny dialog akademicki na temat metodologii oceny ryzyka w różnych sektorach, aby w przyszłości udoskonalać metodologię.
- Rozważyć opracowanie krajowej strategii badań i rozwoju w zakresie oceny ryzyka (i zarządzania ryzykiem) jako podstawy wspólnych działań realizowanych z uczelniami, organizacjami pozarządowymi i sektorem prywatnym, w ramach których badania dotyczące problematyki oceny ryzyka i zarządzania nim byłyby udostępniane, przekazywane i wykorzystywane przez wszystkie zainteresowane strony w kraju.

5. Finansowanie

Cel: finansowanie obejmuje identyfikację, szacowanie kosztów i rezerwowanie środków wymaganych do prowadzenia i aktualizacji oceny ryzyka.

Finansowanie działań z zakresu zarządzania klęskami żywiołowymi i katastrofami stanowi złożony obszar. Zgodnie z ustawą o zarządzaniu kryzysowym, budżet państwa zapewnia finansowanie zadań z zakresu zarządzania kryzysowego na szczeblu krajowym, w tym część środków znajduje się w dyspozycji wojewodów. Gminy, powiaty i województwa muszą finansować zadania z zakresu zarządzania kryzysowego z własnego budżetu, mogą jednak otrzymać dotacje z budżetu państwa. Budżet państwa przewiduje roczną rezerwę na zapobieganie i usuwanie skutków klęsk żywiołowych w wysokości ok. 1 mld PLN (230 mln EUR).

W 2016 r. Polska planuje wykorzystać ok. 50% tej kwoty na zapobieganie klęskom żywiołowym i katastrofom. Rezerwa jest również wykorzystywana na cele odbudowy infrastruktury przeciwpowodziowej, bezpośrednią pomoc dla ludności oraz ochronę przed osuwiskami. Art. 26 ust. 4 ustawy o zarządzaniu kryzysowym nakazuje jednostkom samorządu terytorialnego tworzenie rezerwy na zapobieganie i usuwanie skutków sytuacji kryzysowych w wysokości 0,5% budżetu.

Ministerstwo Spraw Wewnętrznych i Administracji zarządza następującymi projektami przeciwpowodziowymi:

1. Projekt Ochrony Przeciwpowodziowej Dorzecza Odry (całkowity koszt: 712 mln EUR), który obejmuje budowę suchego zbiornika przeciwpowodziowego w Raciborzu oraz modernizację Wrocławskiego Węzła Wodnego. Realizacja projektu bezpośrednio poprawi ochronę przeciwpowodziową ok. 2,5 mln ludzi;
2. Projekt Ochrony Przeciwpowodziowej Dorzecza Odry i Wisły (całkowity koszt: 1,2 mld EUR), który obejmuje budowę nowych zbiorników i modernizację wałów przeciwpowodziowych wzdłuż Odry Dolnej i Środkowej, w Kotlinie Kłodzkiej oraz wzdłuż Górnej Wisły. Realizacja projektu bezpośrednio poprawi ochronę przeciwpowodziową ok. 5,2 mln ludzi.

Oba projekty są finansowane z budżetu państwa, Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej, pożyczek na projekty w zakresie gospodarki wodnej udzielanych przez Europejski Bank Odbudowy i Rozwoju oraz Bank Rozwoju Rady Europy oraz z funduszy europejskich.

Rząd wspiera realizację projektów na szczeblu regionalnym i lokalnym ale istnieje potrzeba zintegrowanego instrumentu oceny finansowej (np. by ocenić, czy uzasadniony jest zakup szczepionki przeciw grypie). Nie istnieje jak dotąd jasna procedura wyznaczania priorytetów finansowania w zakresie działań prewencyjnych oraz powiązania ich z oceną ryzyka w RoZBN. RCB opracowało metodologię oceny zasobów finansowych w celu obniżenia poziomu ryzyka. Ostatecznie będzie ona musiała zostać wykorzystana jako część dokumentu strategicznego dotyczącego kwestii zarządzania ryzykiem i powinna zostać zatwierdzona przez Radę Ministrów.

Co więcej, nie dokonano alokacji środków na osiągnięcie zdolności oceny ryzyka. Jednak RCB posiada własny budżet na realizację swoich zadań, w tym koordynację RoZBN.

Departament Ochrony Ludności i Zarządzania Kryzysowego (dawniej Departament ds. Usuwania Skutków Klęsk Żywiolowych) w Ministerstwie Spraw Wewnętrznych i Administracji zajmuje się prowadzeniem spraw związanych z uruchamianiem środków z rezerwy celowej budżetu państwa na przeciwdziałanie i usuwanie skutków klęsk żywiołowych na potrzeby administracji rządowej, jednostek samorządu terytorialnego i obywateli. W ostatnim przypadku, pomoc finansowa jest przyznawana na podstawie ustawy o pomocy społecznej w drodze decyzji administracyjnej przez samorząd (podlegającej zaskarżeniu).

Dobre praktyki:

- Korzystanie ze specjalnej rezerwy do finansowania modernizacji infrastruktury technicznej jednostek samorządowych oraz infrastruktury ochrony przeciwpowodziowej. Jednostki samorządu terytorialnego muszą spełnić określone kryteria aby otrzymać fundusze. Muszą zostać przedstawione plany obrazujące sposób przywrócenia stanu początkowego przy uwzględnieniu zmian pozwalających uniknąć ponownych szkód spowodowanych przez zagrożenie o podobnej skali.

Rekomendacje:

- Stworzyć politykę alokacji środków finansowych w celu prowadzenia oceny ryzyka na wszystkich szczeblach i w sektorach administracji. Ponieważ „rozumienie ryzyka” stanowi kluczowy priorytet w Ramowym Programie Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof z Sendai, logiczne wydaje się przyznanie określonego budżetu w krajowej strategii DRR (zob. ppkt 6.1) w celu poprawy zdolności oceny ryzyka.
- Finansowanie przedsięwzięć z zakresu zapobiegania, przygotowania, reagowania i usuwania skutków powinno opierać się na identyfikacji i ocenie ryzyk, tzn. bazować na KOR lub konkretnej (sektorowej) ocenie.
- W przypadku finansowania projektów ze środków unijnych wymagane jest posiadanie oceny ryzyka wskazującej istotność i stopień priorytetowego traktowania proponowanego przedsięwzięcia.
- Należy zapewnić ciągłość realizacji ważnych projektów związanych z zapobieganiem i monitorowaniem, finansowanych z programów UE lub innych źródeł.
- Musi istnieć silniejsze powiązanie pomiędzy istotnymi projektami krajowymi i regionalnymi oraz budżetem państwa aby uniknąć podwójnego finansowania podobnych działań lub priorytetów.
- Należy zachęcać instytucje wszystkich szczebli administracji do sprawdzenia możliwości pozyskiwania i wykorzystywania finansowania unijnego lub krajowego w celu zarządzania ryzykiem lub planowania działań w zakresie zapobiegania/reagowania.

6. Styk z obszarem zarządzania ryzykiem

Cel: po opracowaniu krajowej oceny ryzyka i map ryzyka zaangażowane instytucje powinny poszukać miejsc styku z elementami znajdującymi się na dalszych etapach zarządzania ryzykiem.

6.1 Styk z szeroko pojętym obszarem zarządzania ryzykiem

Ustawodawstwo definiuje „zarządzanie kryzysowe” jako kompleksową koncepcję obejmującą zapobieganie, przygotowanie, reagowanie i usuwanie skutków sytuacji kryzysowej. RoZBN stanowi podstawę planowania kryzysowego i ochrony cywilnej oraz strategicznych polityk DRR. Wszystkie dokumenty RCB (KPZK, NPOIK) bazują na Krajowej Ocenie Ryzyka.

Wnioski z RoZBN nie tylko są częścią KPZK, ale zawarte są również we wszystkich innych planach zarządzania kryzysowego na wszystkich szczeblach administracji. Każde ministerstwo i instytucja publiczna spośród wymienionych w ustawie o zarządzaniu kryzysowym musi opracować swój własny sektorowy plan zarządzania kryzysowego uwzględniający wnioski z RoZBN. W niektórych przypadkach szczegółowe wymagania dotyczące przygotowania na sytuacje kryzysowe oraz reagowania na określone zagrożenia są również zawarte w aktach prawnych, np. Rozporządzeniu w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych.¹⁶ Zgodnie z ustawą, wszystkie szczeble administracji muszą stworzyć własne plany zarządzania kryzysowego, które muszą zawierać „charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym zagrożeń dla IK, mapy ryzyka i zagrożenia”. Aby powiązać ze sobą centralne i lokalne procesy planowania, plany zarządzania kryzysowego (oraz oceny ryzyka, na którym one się opierają) muszą zostać zatwierdzone na wyższym poziomie administracji (w przypadku powiatów przez województwo, w przypadku województw przez władze centralne).

Chodzi o to, by nie powstało zbyt wiele szczegółowych planów zarządzania kryzysowego. Planowanie dzieli się więc na moduły i skupia na przygotowanych ogólnych zdolnościach reagowania oraz kompetencjach pracowników (podnoszonych poprzez szkolenia i ćwiczenia). RCB skupia się na procesie przygotowania KPZK, nie na samym planie. Dlatego główny nacisk położony jest na szkolenie i przygotowanie oraz krajowe i międzynarodowe ćwiczenia, podczas których procedury sprawdzane są na wszystkich szczeblach administracji.

RoZBN określa „strategiczne cele” zarządzania ryzykiem. Zdolności zarządzania ryzykiem są zdefiniowane jako środki mające na celu ograniczenie ryzyka, dostosowanie do niego lub łagodzenie jego skutków. Cele przewidują działania, które mają zminimalizować prawdopodobieństwo wystąpienia potencjalnego zagrożenia lub

¹⁶PAA jest centralnym organem administracji rządowej do spraw bezpieczeństwa jądrowego i ochrony radiologicznej (organem regulacyjnym). Jej działalność reguluje ustawa *Prawo atomowe* z 29 listopada 2000 r. (Dz. U. z 2004 r. poz. 1512). Aby umożliwić wczesne powiadamianie o awariach jądrowych i zagrożeniach radiologicznych, Polska podpisała umowy bilateralne z 10 państwami, w tym wszystkimi państwami sąsiednimi. Plany postępowania awaryjnego w przypadku zdarzeń radiacyjnych są tworzone i aktualizowane na szczeblu wojewódzkim oraz krajowym i stanowią załącznik do planów zarządzania kryzysowego (na szczeblu wojewódzkim i centralnym).

złagodzić jego negatywne następstwa. Wymagane jest wskazanie zarówno zasobów, jak i zdolności niezbędnych do osiągnięcia wszystkich celów strategicznych. Kolejnym krokiem jest nakreślenie szczegółowych działań.

RoZBN powinien obejmować programy, których celem jest poprawa ochrony i bezpieczeństwa na poziomie krajowym, regionalnym i lokalnym. Powinien wskazywać podmioty odpowiedzialne za każdy z programów oraz harmonogramy ich realizacji. Umożliwia to wskazanie podejmowanych działań zapobiegawczych i zapewniających przygotowanie na wystąpienie zagrożeń. Pozwala identyfikować braki lub powielanie przedsięwzięć oraz informuje decydentów o wysokości środków finansowych przeznaczanych na zarządzanie ryzykiem oraz inwestycji niezbędnych do jego zmniejszenia.

Określono konkretne wskaźniki pozwalające monitorować wdrażanie działań z zakresu DRR. W najbliższej przyszłości przewiduje się stworzenie tabeli wyników zawierającej bardziej szczegółowe informacje.

Polska opracowała Krajową strategię rozwoju regionalnego do 2023 r., jednak wydaje się, że nie jest ona związana z polityką zarządzania ryzykiem.

Cykl zarządzania ryzykiem kończy ewaluacja. Faza usuwania skutków nie polega jedynie na odbudowie ale również ewaluacji na potrzeby nowego cyklu planowania oraz ponownej oceny ryzyka: jeżeli coś zawiodło, konieczne jest zapewnienie alternatywy.

Dobre praktyki:

- Istnieje klarowny podział odpowiedzialności za różne rodzaje ryzyka (dla wszystkich czterech faz zarządzania kryzysowego) oparty na siatce bezpieczeństwa przygotowywanej przez RCB.
- Istnieje bezpośrednie powiązanie pomiędzy planami na poziomie lokalnym, regionalnym i krajowym.
- Wszystkimi projektami DRR związanymi z ryzykiem powodziowym zarządza KZGW. Zaangażowane są wszystkie władze regionalne, na które oddziałują ww. projekty.

Rekomendacje:

- Zapewnić, aby KOR była brana pod uwagę we wszystkich czterech fazach zarządzania kryzysowego: zapobieganie, przygotowanie, reagowanie i usuwanie skutków. Należy stworzyć krajową strategię ograniczenia ryzyka katastrof (DRR), zgodnie z Ramowym Programem Działania na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof z Sendai. Zalecenia zawarte w RoZBN powinny zostać włączone w plany działania DRR.
- Rozważyć przyznanie jednemu podmiotowi odpowiednich kompetencji do koordynowania przygotowania i wdrażania strategii DRR, w ścisłym powiązaniu z KOR.
- Zapewnić gminom wsparcie techniczne, by mogły opracować własne programy dotyczące ograniczenia ryzyka, łagodzenia skutków, zbieranie i wymiany informacji oraz podnoszenia świadomości zagrożeń. Można stworzyć różne scenariusze dla decydentów i społeczeństwa umożliwiające im stosowanie

właściwych środków zapobiegawczych w zakresie ochrony ludności i infrastruktury miejskiej.

- Dokonać analizy istniejących dokumentów planistycznych oraz raportów instytucji publicznych i prywatnych pod kątem przeglądu i udoskonalenia zarządzania ryzykiem.
- Stworzyć bezpośrednie powiązanie pomiędzy zarządzaniem ryzykiem, planowaniem urbanistycznym i zagospodarowaniem przestrzennym oraz korzystać z dostępnych map ryzyka przy planowaniu miejskim. Równie ważne jest zaplanowanie skutecznego programu ograniczenia i/lub minimalizacji ryzyka poprzez lepsze wykorzystanie planowania przestrzennego.
- Zaangażować obywateli w ćwiczenia na wypadek sytuacji kryzysowych (a nie tylko informować).

6.2 Styk z dziedziną ochrony infrastruktury krytycznej

Ustawa o zarządzaniu kryzysowym definiuje IK jako „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”.

IK składa się z następujących systemów (sektorów):

- zaopatrzenia w energię, paliwa i surowce energetyczne;
- łączności;
- sieci teleinformatycznych;
- finansowe;
- zaopatrzenia w żywność;
- zaopatrzenia w wodę;
- ochrony zdrowia;
- transportowe i komunikacyjne;
- ratownicze;
- zapewniające ciągłość działania administracji publicznej;
- produkcji, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Scenariusze zakłóceń określa się pod kątem kosztów, ofiar itd. OIK bazuje na cyklu Deminga¹⁷. System OIK nie przewiduje sankcji ale opiera się na współodpowiedzialności, współpracy i zaufaniu.

Ustalane są kryteria wyznaczania IK w każdym systemie. Wyznaczanie IK jest procesem trzyetapowym:

- wstępna selekcja IK na podstawie ustalonych kryteriów sektorowych;
- ocena, czy wskazana IK ma zasadnicze znaczenie dla funkcjonowania społeczeństwa;

¹⁷ „Planuj, zrób, sprawdzaj, działaj”.

- ocena IK jest dokonywana na podstawie przekrojowych kryteriów biorących pod uwagę ofiary, skutki gospodarcze, potrzebę ewakuacji, utratę usług, czas usuwania skutków, skutki międzynarodowe i unikalność. Aby zakwalifikować system do IK, musi on spełniać co najmniej dwa spośród podanych kryteriów.

Kryteria oraz lista wyznaczonej IK są niejawne. Województwa włączają wykaz IK znajdującej się na ich terytorium w swoje plany zarządzania kryzysowego. Niektóre systemy i zasoby należące do samorządów są uznawane za IK.

Nie ma żadnych szczególnych procedur czy przepisów dotyczących IK, będących własnością podmiotów zagranicznych. Każdy podmiot będący właścicielem IK musi być zarejestrowany w Polsce i ma obowiązek przestrzegać polskie prawa.

Art. 2 dyrektywy w sprawie OIK¹⁸ definiuje „europejską infrastrukturę krytyczną” (EIK) jako krytyczne systemy, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz którego zakłócenie lub zniszczenie miałyby istotny wpływ na co najmniej dwa państwa członkowskie. Dyrektor RCB rozróżnia pomiędzy EIK znajdującą się na polskim terytorium oraz znajdującą się na terytorium innych państw członkowskich, która mogłaby mieć istotny wpływ na Polskę. W celu identyfikacji EIK bierze się pod uwagę progi stosowane przez Komisję Europejską oraz państwa członkowskie, określające charakterystyczne parametry lub funkcje obiektów, urządzeń i instalacji. Informacje dotyczące IK oraz EIK są niejawne zgodnie z art. 9 dyrektywy.

Stwierdzono, że Polska jest uzależniona od pewnej liczby IK znajdującej się w innych krajach. Polska uwzględnia tą problematykę w planach zarządzania kryzysowego.

Uchwałą Rada Ministrów przyjęty został NPOIK, którego celem jest stworzenie warunków poprawy ochrony infrastruktury krytycznej, w szczególności poprzez:

- 1) zapobieganie awariom IK;
- 2) przygotowanie na sytuacje kryzysowe, które mogłyby negatywnie wpłynąć na IK;
- 3) reagowanie w przypadku zniszczenia lub zakłócenia funkcjonowania IK;
- 4) odbudowę IK.

NPOIK skupia się na krajowej IK (lokalna lub regionalna IK włączona jest w odpowiednie plany zarządzania kryzysowego).

NPOIK określa:

- 1) krajowe priorytety, cele, wymagania i standardy, aby zapewnić płynne funkcjonowanie IK;
- 2) ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych odpowiedzialnych za systemy;
- 3) szczegółowe kryteria identyfikacji obiektów, instalacji, urządzeń i usług stanowiących część systemów IK, z uwzględnieniem ich znaczenia dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.

¹⁸ 2008/114/WE.

NPOIK został przygotowany przez dyrektora RCB we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy oraz operatorami IK. We współpracy z właściwymi ministrami dyrektor sporządza wykaz obiektów, instalacji, urządzeń i usług wyznaczonych jako IK.

Ocena osiągnięcia celów NPOIK dokonywana jest poprzez audyty wewnętrzne, zmiany strukturalne i budżetowe oraz ćwiczenia. Ćwiczenia dotyczące bezpieczeństwa teleinformatycznego przeprowadzane są co roku (od 2012 r.)¹⁹ w różnych sektorach. Zgodnie z ustawą z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, pełnomocnicy ds. OIK sporządzają co trzy miesiące raport o stanie OIK, który jest przekazywany do wiadomości Ministra Skarbu Państwa (obecnie Ministra Energii) oraz dyrektora RCB.

OIK stanowi obowiązek jej właściciela/operatora, zaś RCB działa jako podmiot koordynujący. Od operatorów IK (publiczni i prywatni) wymaga się przygotowania planu OIK opartego na ocenie ryzyka. Plany, które podlegają ocenie i zatwierdzeniu przez dyrektora RCB, obejmują:

1. charakterystykę IK;
2. ocenę ryzyka;
3. reakcję (procedury);
4. współpracę z administracją.

Wskazane w rozporządzeniu organy, posiadające specjalistyczną wiedzę (np. KZGW itd.) są zaangażowane w proces uzgadniania planów OIK.

Opracowane zostały wytyczne włączania informacji dotyczących OIK w odpowiednie plany zarządzania kryzysowego.

Praktycznym przykładem jest prywatny koncern naftowy PKN ORLEN w Płocku, uważany za zakład wysokiego ryzyka poważnej awarii przemysłowej. PKN ORLEN współpracuje z RCB w procesie przygotowywania planów zarządzania kryzysowego. Straż pożarna miasta Płock uczestniczy we wspólnych ćwiczeniach razem z PKN ORLEN, a urząd miasta informuje obywateli o ćwiczeniach. PKN ORLEN posiada własny lokalny system wczesnego ostrzegania, który jest testowany dwa razy w roku.

Dobra praktyka:

- Jeżeli chodzi o OIK, funkcjonuje podejście obejmujące wszystkie zagrożenia. NPOIK ściśle odzwierciedla reguły współodpowiedzialności, współpracy i zaufania. OIK obejmuje planowanie ciągłości działania.
- Proces wyznaczania krajowej IK obejmuje trzy wyraźne etapy i kieruje się dobrze zdefiniowanymi kryteriami.
- Stworzenie forum OIK na poziomie krajowym, regionalnym oraz poszczególnych systemów zapewnia konieczną reprezentację różnych zainteresowanych stron.

¹⁹ Ćwiczenia Cyber-EXE™ Polska organizuje Fundacja Bezpieczna Cyberprzestrzeń i RCB.

- Mechanizm OIK na poziomie operacyjnym umożliwia wymianę informacji i obejmuje platformę internetową dzielenia się informacjami na różne tematy związane z IK.
- Wszyscy operatorzy IK przygotowują plany OIK, które zatwierdza dyrektor RCB.
- RCB zaleca i zachęca do prowadzenia ćwiczeń na podstawie zidentyfikowanych scenariuszy zarówno w sektorze publicznym, jak i prywatnym.

Zalecenia:

- Zapewnić, by NPOIK nie odnosił się wyłącznie do obiektów IK lecz do systemów IK oraz współzależności między nimi. Przedkładanie RCB planów poszczególnych operatorów IK stanowi znakomitą bazę pozwalającą zapobiegać zakłóceniom, które mogą wpływać na kraj jako całość i planować na wypadek ich wystąpienia (identyfikacja potencjalnego efektu domina).
- Rozważyć wprowadzenie zachęt związanych z OIK. Aktualne zasady współodpowiedzialności, współpracy i zaufania stanowią znakomitą podstawę, ale w pewnych przypadkach mogą nie spełnić oczekiwanych efektów. W niektórych okolicznościach warto rozważyć zastosowanie dodatkowych zachęt, np. finansowania, korzyści podatkowych, dotyczących wymagań wobec OIK w zamówieniach publicznych, a wreszcie również sankcji.
- Należy zapewnić, by właściciele/operatorzy IK dzielili się informacjami istotnymi w procesie KOR. Jeżeli chodzi o informacje niejawne, nie powinno być (zauważalnych) przeszkód w dzieleniu się informacjami z organem regulacyjnym (tj. z RCB w przypadku Polski).
- Wprowadzić wyraźne rozróżnienie pomiędzy posiedzeniami forum OIK, warsztatami i konferencjami IK. Najlepiej by fora skupiały się na wymianie dobrych praktyk oraz networkingu pomiędzy punktami kontaktowymi zainteresowanych stron na poziomie sektorowym i międzysektorowym (aby identyfikować współzależności) i budowaniu zaufania pomiędzy różnymi właścicielami i operatorami IK. Warsztaty i konferencje powinny się skupiać na wymianie informacji i networkingu pomiędzy przedstawicielami zainteresowanych stron.

6.3 Styk z obszarem adaptacji do zmian klimatu

Polska realizuje, spójną ze strategią UE, krajową politykę adaptacji do zmian klimatu, której cele określone są w Strategicznym planie adaptacji dla sektorów i obszarów wrażliwych na zmiany klimatu do roku 2020 z perspektywą do roku 2030 (SPA). Dokument wyznacza kierunki działań i rozwoju w odniesieniu do prognozowanych zmian klimatu z uwzględnieniem wszystkich szczebli administracji. Bierze pod uwagę aspekty DRR oraz obejmuje cele krótko- i długoterminowe. Pierwsze są związane przede wszystkim z reagowaniem (na sytuacje kryzysowe spowodowane zjawiskami klimatycznymi), co stanowi element poprawy zdolności radzenia sobie z zagrożeniem. Natomiast w ramach działań długoterminowych priorytetem jest dostosowanie infrastruktury do zmian klimatu, w tym np. zabezpieczenie budowli. Jeżeli chodzi o finansowanie, Polska rozważa udział w projektach UE z tego zakresu.

Strategia obejmuje zestaw wskaźników do monitorowania postępów jej wdrażania (wykorzystując dane statystyczne i inne informacje) ale nie istnieje mechanizm ani system raportowania. Niemniej jednak Polska dąży do opracowania szczegółowego kwestionariusza, mającego na celu rejestrowanie postępów jej wdrażania. W zakresie oceny ryzyka związanego ze zmianami klimatu Polska opracowała poradnik przygotowania inwestycji z uwzględnieniem łagodzenia zmian klimatu i przystosowania do nich oraz budowania odporności na klęski żywiołowe. Jego celem jest określenie wskazówek i metodologii obliczeń uwzględniających zagadnienia klimatyczne w procesie przygotowania inwestycji (przedsięwzięć oraz projektów) na wszystkich jego etapach od strategii, poprzez studium wykonalności, ocenę oddziaływania na środowisko, wdrażanie aż po rozbiórkę.

Przez ostatnie 10 lat Polska była zaangażowana w aktualizowanie, dostosowanie prawodawstwa i transponowanie unijnych regulacji dotyczących gospodarowania zasobami wodnymi. Wszystkie dyrektywy unijne zostały implementowane, zaś przyszłe plany będą opracowywane analogicznie do rozwoju sytuacji w UE.

KZGW odpowiada za ocenę ryzyka powodziowego. Na szczeblu krajowym współpracuje z RCB. Na szczeblu regionalnym funkcjonują regionalne zarządy gospodarki wodnej (jednostki administracji rządowej niezespoliczonej), które współpracują z wojewodami i powołują grupy planistyczne odpowiadające za przygotowanie planów zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych.

Podczas opracowywania wstępnej oceny ryzyka powodziowego nie jest brany pod uwagę wpływ na zagospodarowanie przestrzenne.

Jednak plany zagospodarowania przestrzennego uwzględniają efekty oceny ryzyka, a dyrektorzy RZGW uzgadniają plany zagospodarowania przestrzennego w zakresie obszarów narażonych na niebezpieczeństwo powodzi.

Dobre praktyki:

- Stworzenie nieformalnej grupy roboczej w celu wdrożenia SPA i zapewnienia wsparcia dla miast powyżej 100 tys. mieszkańców.
- Promowanie aktywnego udziału obywateli w zagadnieniach dotyczących CCA. Publikowane są poradniki na temat zachowania się poszczególnych grup społecznych np. dzieci, osób starszych w sytuacji wystąpienia poszczególnych zagrożeń (np. fale upałów).

Rekomendacje:

- Stworzyć bezpośrednie powiązanie pomiędzy KOR i strategiami CCA. SPA oraz regionalne strategie rozwoju powinny być bardziej skorelowane z RoZBN w kwestiach strategii inwestycyjnej oraz rozwojowej.
- Zapewnić aby kryteria dotyczące inwestycji w rozwój i zwiększenia zdolności adaptacji do zmian klimatu uwzględniały KOR.
- Wyróżnić w ocenie ryzyka zagrożenia i podatności mogące mieć wpływ na zmiany klimatu.

- Wyznaczyć jako priorytetowe działania przeciwdziałające wszystkim krótko- i długoterminowym skutkom zmian klimatu z punktu widzenia bezpieczeństwa narodowego. Jednocześnie ustalić relację między okresem planowania zawartym w KOR a okresami planowania w strategiach CCA. Ponieważ CCA wymaga długoterminowej strategii, działania powinny obejmować szereg różnych przedziałów czasowych (np. krótko-, średnio- i długookresowych) zawierających określone cele.
- Rozwijać uczestnictwo w kampanii „odporne miasta” prowadzonej przez UNISDR oraz prowadzić kampanię poprzez zwiększanie poziomu zainteresowania i świadomości DRR, skupiając się na zagrożeniach dla miast.
- Jeżeli chodzi o implementację SPA, ważne jest zwrócenie się do zainteresowanych stron z prośbą o wybranie odpowiednich wskaźników oraz stworzenie rocznych raportów dotyczących ich implementacji w celu poprawy monitorowania postępów realizacji celów krótko- i długoterminowych.

Załącznik I Terminologia i skróty

Poniższe definicje są roboczym opracowaniem wyłącznie do celów przeglądu wzajemnego. W dużej mierze bazują na prawodawstwie i wytycznych UE. W przypadkach gdy definicje unijne nie były dostępne, posłużono się definicjami UNISDR²⁰.

Definicje

Planowanie kryzysowe – element procesu zarządzania analizujący konkretne potencjalne zagrożenia lub sytuacje, które mogą zagrozić społeczeństwu lub środowisku naturalnemu, wprowadzający procedury umożliwiające skuteczne oraz odpowiednie reagowanie na zdarzenia i sytuacje we właściwym czasie.

Klęska lub katastrofa odnosi się do jakiegokolwiek sytuacji, która ma lub może mieć poważny wpływ na ludzi, środowisko naturalne lub mienie oraz dziedzictwo kulturowe.

Niebezpieczeństwo jest to groźne zjawisko, substancja, działalność ludzka lub zdarzenie, które mogą spowodować utratę życia, uszkodzenie ciała lub inny uszczerbek na zdrowiu, zniszczenie mienia, utratę źródeł utrzymania i usług, konflikty społeczne i ekonomiczne bądź szkody w środowisku naturalnym.

Służby ratownicze oznacza zbiór specjalistycznych podmiotów posiadających określone zakresy odpowiedzialności i cele związane ze służbą ludziom oraz ochroną ludzi i mienia w sytuacjach kryzysowych.

Raporty cząstkowe dotyczą sektorowych i wojewódzkich raportów oceny ryzyka, stanowiących podstawę RoZBN.

Przegląd wzajemny stanowi instrument zarządczy, za pomocą którego osiągnięcia danego państwa w konkretnej dziedzinie (w tym przypadku zarządzanie ryzykiem/ochrona ludności) są badane przez ekspertów z innych krajów.

Przygotowanie jest to stan przygotowania oraz osiągnięcia zdolności zasobów ludzkich i materialnych, struktur, społeczności i organizacji, pozwalający zapewnić skuteczną, szybką reakcję na klęski i katastrofy, uzyskany dzięki wcześniej przygotowanym działaniom.

Zapobieganie jest działaniem ukierunkowanym na ograniczenie ryzyka lub łagodzenie niekorzystnych następstw klęski lub katastrofy dla ludzi, środowiska naturalnego i mienia oraz dziedzictwa kulturowego.

Ryzyko jest kombinacją następstw zdarzenia (zagrożenia) oraz związanym z nim prawdopodobieństwem jego wystąpienia.

Odporność jest zdolnością systemu, społeczności lub społeczeństwa narażonego na zagrożenie poprzez stawienie oporu zagrożeniu, przyjęcie nad nim kontroli, dostosowanie się do niego lub usunięcie jego skutków w sposób skuteczny i we

²⁰<http://www.unisdr.org/we/inform/terminology>

właściwym czasie, m.in. poprzez zachowanie i odbudowę zasadniczych struktur i funkcji.

Reagowanie stanowi działanie podjęte na szczeblu krajowym lub niższym w przypadku nadchodzącej klęski lub katastrofy bądź podczas niej albo po niej, odnoszące się do jej bezpośrednich niekorzystnych następstw.

Zdolność zarządzania ryzykiem jest to umiejętność państwa członkowskiego lub jego regionów do ograniczenia ryzyka, adaptacji do niego lub łagodzenia jego skutków (oddziaływanie i prawdopodobieństwo klęski żywiołowej lub katastrofy). Identyfikowane jest w procesie w ocenie ryzyka i obniżane do poziomów akceptowanych przez państwo członkowskie. Zdolność oceniana jest pod względem potencjału technicznego, finansowego i administracyjnego pozwalającego na prowadzenie:

- (a) odpowiedniej oceny ryzyka;
- (b) odpowiedniego planowania zarządzania ryzykiem w zakresie zapobiegania i gotowości;
- (c) odpowiednich działań w zakresie zapobiegania ryzyku i gotowości.

Zainteresowane strony są to grupy społeczne zainteresowane kwestiami zarządzania kryzysowego obejmujące m.in. środowiska naukowe (w tym w dziedziny: inżynieria, geografia, nauki społeczne, nauki o zdrowiu, gospodarka i środowisko naturalne), praktyków, przedsiębiorców, decydentów politycznych, władze centralne, regionalne lub lokalne oraz społeczeństwo;

Poziom niższy odnosi się do regionalnego, powiatowego lub lokalnego szczebla władzy, które realizują działania z zakresu zarządzania kryzysowego;

Zagrożenie jest to potencjalnie destrukcyjne zdarzenie fizyczne, zjawisko lub działalność o charakterze intencjonalnym/sabotażu.

Ocena zagrożeń (w przypadku Polski) odnosi się do oceny ryzyka.

Skróty

Skrót	Definicja
APSFR	Obszar potencjalnego znacznego ryzyka powodziowego
CCA	Adaptacja do zmian klimatu
IK	Infrastruktura krytyczna
OIK	Ochrona Infrastruktury Krytycznej
DRR	Ograniczanie ryzyka klęsk żywiołowych i katastrof
EIK	Europejska infrastruktura krytyczna
RZZK	Rządowy Zespół Zarządzania Kryzysowego
GIS	Systemy informacji geograficznej
GUGiK	Główny Urząd Geodezji i Kartografii
RCB	Rządowe Centrum Bezpieczeństwa
ISOK	Informatyczny System Osłony Kraju przed nadzwyczajnymi zagrożeniami
JRC	Wspólne Centrum Badawcze Komisji Europejskiej
SPA	Strategiczny plan adaptacji dla sektorów i obszarów wrażliwych na zmiany klimatu do roku 2020 z perspektywą do roku 2030
NPOIK	Narodowy Program Ochrony Infrastruktury Krytycznej
KPZK	Krajowy Plan Zarządzania Kryzysowego
KOR	Krajowa Ocena Ryzyka
KZGW	Krajowy Zarząd Gospodarki Wodnej
PAA	Państwowa Agencja Atomistyki
PIG	Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy
PSE S.A.	Polskie Sieci Elektroenergetyczne S.A.
RoZBN	Raport o zagrożeniach bezpieczeństwa narodowego
RZGW	Regionalny Zarząd Gospodarki Wodnej
SOP	System Osłony Przeciwośmiskowej
UNISDR	Międzynarodowa Strategia Redukcji Zagrożeń Naturalnych ONZ

Załącznik II Przegląd zainteresowanych stron

W przegląd wzajemny zaangażowani byli przedstawiciele następujących instytucji:

- Główny Inspektorat Ochrony Środowiska
- Urząd Miasta Płock i Miejskie Centrum Zarządzania Kryzysowego
- Urząd Miasta Stołecznego Warszawy – Biuro Bezpieczeństwa i Zarządzania Kryzysowego oraz Biuro Infrastruktury
- Rządowe Centrum Bezpieczeństwa
- Główny Urząd Geodezji i Kartografii
- Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy
- Instytut Telekomunikacji
- Agencja Bezpieczeństwa Wewnętrznego
- Szkoła Główna Służby Pożarniczej
- Mazowiecki Urząd Wojewódzki
- Ministerstwo Spraw Wewnętrznych i Administracji
- Ministerstwo Rozwoju
- Ministerstwo Cyfryzacji
- Ministerstwo Energii
- Ministerstwo Środowiska
- Ministerstwo Finansów
- Ministerstwo Infrastruktury i Budownictwa
- Ministerstwo Edukacji Narodowej
- Państwowa Agencja Atomistyki
- Akademia Obrony Narodowej
- Komenda Główna Państwowej Straży Pożarnej
- Biuro Bezpieczeństwa Narodowego
- Krajowy Zarząd Gospodarki Wodnej
- PKN ORLEN S.A.
- Państwowy Instytut Geologiczny – Państwowy Instytut Badawczy
- Polskie Sieci Elektroenergetyczne S.A.
- Centrum Naukowo-Badawcze Ochrony Przeciwpowodziowej
- Politechnika Warszawska

Załącznik III Dokumentacja

Do przygotowania oceny wykorzystano następujące dokumenty:

Lp.	Typ dokumentu	Tytuł	Wersja
1	Ustawa/rozporządzenie	Ustawa o zarządzaniu kryzysowym	2007
2	Ustawa/rozporządzenie	Rozporządzenie w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego	2010
3	Ustawa/rozporządzenie	Prawo atomowe	2015 (ostatnia zmiana)
4	Ustawa/rozporządzenie	Rozporządzenie w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych	2007 (ostatnia zmiana)
5	Procedura	Procedura opracowania raportu częściowego do RoZBN	2010
6	Raport	Krajowa Ocena Ryzyka – RoZBN	2013
7	Artykuł	Streszczenie projektu System Osłony Przeciwośmiskowej SOPO oraz jego powiązanie z celami ograniczenia ryzyka	2008
8	Broszura	Powódź? Mnie to nie dotyczy. Sprawdź, czy jesteś w grupie ryzyka	
9	Broszura	Plany zarządzania ryzykiem powodziowym dla obszarów dorzeczy i regionów wodnych	
10	Prezentacja	Implementacja dyrektywy powodziowej w Polsce	
11	Arkusze informacyjny	Informacje o projekcie KLIMAT	2015
12	Raport	Strategiczny Plan Adaptacji dla sektorów i obszarów wrażliwych na zmiany klimatu do roku 2020 z perspektywą do roku 2030 (SPA2020)	2013
13	Artykuł	Oparty na klimatologii system ostrzegania przed zagrożeniami meteorologicznymi i skrajnymi zjawiskami pogodowymi: Polska (Climatologically based warning system against meteorological hazards and weather extremes: Poland)	2014
14	Raport	Wzmocnienie prawnych i politycznych ram reagowania na klęski żywiołowe i katastrofy na szczeblu międzynarodowym	2014

15	Prezentacja	Informatyczny System Oslony Kraju przed nadzwyczajnymi zagrozeniami (ISOK)	2014
15a	Mapy	ISOK – mapy innych zagrozeń	2014
15b	Mapy	ISOK – mapy innych zagrozeń (krótka charakterystyka)	2014
15c	Mapy	ISOK – zagrożenia meteorologiczne (system wizualizacji na potrzeby ochrony kraju przed niezwykleymi zagrożeniami)	2014
15d	Mapy	ISOK – mapy ostrzegające przed niezwykleymi zagrożeniami meteorologicznymi	2014

Załącznik IV Tematyczne ramy przeglądu

Przeglądy wzajemne są prowadzone przez ekspertów z wykorzystaniem wzorca ułatwiającego pozyskiwanie informacji oraz analizowanie struktur zarządzania ryzykiem klęsk i katastrof, a także sposobu realizacji działań w tym zakresie w kraju podlegającym ocenie. Wzorzec opisuje cele, wymagania i wskaźniki dotyczące różnych obszarów zarządzania ryzykiem. Przykładowe pytania w nim zawarte mogą zostać wykorzystane jako wskazówki dla zespołu dokonującego przeglądu zarówno w czasie przygotowań do wizyty, jak i podczas jej trwania. Zespoły mogą także opracowywać dodatkowe pytania.

Na potrzeby misji w Polsce, wzorzec został dostosowany do zgłoszonego tematu przeglądu dotyczącego zdolności prowadzenia procesu oceny ryzyka. Konstrukcja wzorca i raportu opiera się na unijnych Wytycznych oceny zdolności zarządzania ryzykiem chociaż niektóre tematy zostały połączone w jeden rozdział (1 i 3), a w rozdziale 6 dodano problematykę styku oceny ryzyka z zarządzaniem nim.

Każdy rozdział i punkt rozpoczyna się od wymienienia celu, zgodnie z poniższą tabelą. Pytania z kwestionariusza samooceny, odnoszące się do wytycznych unijnych, zostały wykorzystane do przekształcenia każdego z celów w konkretne wymagania podlegające ocenie. Z początkowego wzorca wybrano kilka kluczowych wskaźników jako podstawę pytań zadawanych podczas misji. Są one ściśle związane z celami, szczególnie tam, gdzie otrzymane wstępne informacje nie były wystarczająco czytelne lub kompletne. Wskaźniki obejmują szeroki zakres tematów odnosząc się do strategii, narzędzi oraz metodologii i mogą być pomocne dla ekspertów we wskazaniu przykładów dobrych praktyk, obszarów wymagających udoskonalenia lub ewentualnych luk. Wskaźniki nie stanowią „listy kontrolnej”, na podstawie której prowadzona byłaby formalna ocena danego państwa.

1.1	Ramy: Ocena ryzyka pasuje do ogólnych ram
P1.	Ocena ryzyka jest prowadzona na podstawie czytelnych ram prawnych i/lub proceduralnych. Rola oceny ryzyka w całości procesu zarządzania ryzykiem klęsk i katastrof jest określona w odpowiednim szczeblu krajowym i/lub niższym
1.2	Koordynacja: Struktura zarządzania ryzykiem przypisuje jasne zakresy odpowiedzialności wszystkim podmiotom zaangażowanym w ocenę ryzyka, tak że można uniknąć powielania zadań lub niedostosowania pomiędzy zakresami odpowiedzialności i zdolnościami
P2.	Zakresy odpowiedzialności oraz role/funkcje są jasno zdefiniowane i przypisane do odpowiednich podmiotów uczestniczących w ocenie ryzyka
	Na początku procesu KOR jedna instytucja musi otrzymać zadanie koordynowania prac
	Określa się kryteria ryzyka (politycznego), by ustalić, czy ryzyko i/lub jego rozmiar mogą zostać zaakceptowane lub być tolerowane
	Podejmowana jest decyzja polityczna na temat akceptacji ryzyka oraz ustalenia priorytetów w zakresie zapobiegania ryzyku i przygotowań
P3.	Zakresy odpowiedzialności za ocenę poszczególnych rodzajów ryzyka są przydzielone odpowiednim podmiotom
P4.	Międzysektorowy wymiar ryzyka został włączony w ocenę ryzyka

	Oceny ryzyka są powiązane ze strategiami CCA
	Oceny ryzyka na innych szczeblach administracji rządowej i w różnych sektorach są brane pod uwagę w KOR
	Rząd zachęca i stymuluje inne szczeble administracji rządowej i różne sektory do prowadzenia oceny ryzyka
P5. Podział zakresów odpowiedzialności za ocenę ryzyka jest regularnie weryfikowany	
1.3	Inne zainteresowane strony: Podmioty prowadzące oceny ryzyka współpracują z szeregiem zainteresowanych stron, w tym z sektora prywatnego, środowisk akademickich oraz innych podmiotów rządowych niezaangażowanych bezpośrednio w proces oceny
P7. Odpowiednie zainteresowane strony są zaangażowane w proces oceny ryzyka	
	Metoda oceny ryzyka jest tworzona we współpracy z odpowiednimi autorytetami takimi jak społeczności naukowe, w tym w dziedzinach nauk społecznych, ekonomicznych, o zdrowiu i środowisku, z praktykami, przedsiębiorcami, osobami narażonymi na zagrożenia oraz decydentami politycznymi
	Oceny zainteresowanych stron dokonuje się przed rozpoczęciem procesu oceny ryzyka i aktualizacji (MiSRaR – łagodzenie skutków ryzyka związanego z zagospodarowaniem przestrzeni w europejskich regionach i miastach) [Zainteresowane strony (publiczne, prywatne oraz na różnych szczeblach administracji rządowej), które mają być zaangażowane w ocenę, są definiowane i zapraszane do udziału]
	Istnieje współpraca z sektorem prywatnym, tam gdzie oceny ryzyka uzupełniają wysiłki władz publicznych
	Ocena ryzyka jest publikowana i ogłaszana zainteresowanym stronom do konsultacji
	Zainteresowane strony informuje się o szczegółowym ryzyku, które ich dotyczy
	Zainteresowane strony biorą udział w procesie konsultacji planów zarządzania ryzykiem powodzi w zależności od skali oddziaływania
	Mapy i plany powodziowe są udostępniane publicznie
2.	Metodologia: Opracowuje się metodologię prowadzenia oceny ryzyka. Oczekiwany wpływ zidentyfikowanych rodzajów ryzyka jest oceniany za pomocą opracowanej metodologii, wśród rodzajów ryzyka wyznacza się priorytety
P11. Podmiot krajowy lub niższego poziomu opracował metodologię oceny ryzyka	
	Koncepcje „ryzyka” oraz główne czynniki ryzyka, które muszą być brane pod uwagę w ocenie ryzyka, są definiowane i akceptowane
	Zakres lub szerokość oceny ryzyka (oraz uzasadnienie włączenia lub wykluczenia określonych rodzajów ryzyka) są definiowane i akceptowane
	Klasyfikacja rodzajów ryzyka jest zdefiniowana i akceptowana
	Kryteria punktacji w ocenie ryzyka są definiowane i akceptowane
	Metody stosowane w ocenie ryzyka są definiowane i akceptowane
	Protokół stosowany w opiniach ekspertów jest definiowany i akceptowany
	Niepewność metod jest uzasadniana
	Istnieje wykaz oddzielnych rodzajów ryzyka i związanych z nimi scenariuszy wraz z ich opisem
	Do każdego rodzaju ryzyka istnieje oddzielną mapę ryzyka, obrazującą przestrzenny rozkład zagrożenia i podatności
	Analiza ryzyka zawiera ocenę prawdopodobieństwa i skutków, jak również analizę podatności

	Analiza oddziaływania ryzyka uwzględnia skutki dla ludzi, gospodarki, środowiska, polityki oraz społeczeństwa
	Oddzielna punktacja wpływu każdego rodzaju ryzyka jest zapisywana i uzasadniana z zastosowaniem jasno zdefiniowanych i popartych faktami założeń
	Wynik analizy ryzyka może zostać zaprezentowany na siatce ryzyka obejmującej wpływ i prawdopodobieństwo
P12. Transgraniczny wymiar różnych rodzajów ryzyka został włączony w oceny ryzyka	
	Istnieje krajowa/międzynarodowa sieć współpracy w celu stworzenia analizy ryzyka na poziomie makroregionów. Sąsiednie państwa są angażowane w kompilowanie analiz ryzyka, a ich analizy ryzyka są brane pod uwagę
P13. Ocena ryzyka bierze pod uwagę IK	
3.1	Informacje i komunikacja: Na potrzeby oceny ryzyka dostępny jest skuteczny system informacyjno-komunikacyjny
P9. Niezbędne zdolności administracyjne są dostępne na szczeblu krajowym i/lub odpowiednim niższym, aby wewnątrz komunikować wyniki oceny ryzyka, w tym scenariusze, lekcje itd.	
3.2	Infrastruktura teleinformatyczna: Do przeprowadzenia oceny ryzyka dostępna jest odpowiednia infrastruktura i informacje
P14. Do przeprowadzenia oceny ryzyka dostępna jest infrastruktura teleinformatyczna	
P15. Do przeprowadzenia oceny ryzyka dostępne są odpowiednie informacje i dane (w tym dane historyczne)	
3.3	Komunikacja ryzyka: Dostępne są konieczne zdolności administracyjne, aby komunikować opinii publicznej wyniki oceny ryzyka
P8. Dostępne są niezbędne zdolności administracyjne, aby komunikować opinii publicznej wyniki oceny ryzyka	
P10. Wyniki oceny ryzyka włącza się w strategię komunikacji ryzyka	
	Ocena ryzyka oraz zawarte w niej scenariusze są jawne i publikowane
	Dostarcza się konkretne informacje o poszczególnych rodzajach ryzyka zagrażających określonej ludności (na pewnych obszarach)
	Publikacja oceny ryzyka obejmuje przegląd środków przygotowawczych rządu
	Publikacja oceny ryzyka obejmuje informacje na temat możliwości lepszego przygotowania się ludności
	Właściwy podmiot publiczny zdecydował, które informacje w KOR są wrażliwe i dlatego nie zostaną opublikowane
4.	Wiedza ekspercka: Eksperti prowadzący ocenę ryzyka posiadają odpowiednie kompetencje i zakresy odpowiedzialności oraz otrzymali odpowiednie przeszkolenie
P6. Eksperti odpowiedzialni za przeprowadzenie oceny ryzyka zostali odpowiednio poinformowani, przeszkoleni i mają doświadczenie w tym zakresie	
5.	Finansowanie: Finansowanie obejmuje identyfikowanie i szacowanie wysokości kosztów oraz rezerwowanie funduszy wymaganych do prowadzenia i aktualizowania ocen ryzyka
P16. Dostępne są odpowiednie możliwości finansowe, by prowadzić i aktualizować oceny ryzyka	
6.	Styk z zarządzaniem ryzykiem: po opracowaniu KOR i map ryzyka, właściwe władze powinny starać się zapewnić odpowiedni styk z kolejnym etapem zarządzania ryzykiem

	Istnieje plan lub program prowadzenia analizy zdolności oraz rozwoju planowania zdolności na podstawie krajowej oceny ryzyka
	Efektem procesu oceny ryzyka są konkretne zalecenia dla powiązanych obszarów strategicznych
	Dokonyje się uzgodnienia planu lub programu wdrożenia
	Istnieją powiązania pomiędzy planami krajowymi, zdecentralizowanymi i sektorowymi