AKADEMIA MARYNARKI WOJENNEJ
im. BOHATERÓW WESTERPLATTE

ROCZNIK BEZPIECZEŃSTWA MORSKIEGO

kmdr dr Grzegorz KRASNODĘBSKI

Modelowanie systemu zarządzania bezpieczeństwem infrastruktury krytycznej państwa

Rozprawa habilitacyjna

GDYNIA 2013

ŻEGLUGA MORSKA
BEZPIECZEŃSTWO MORSKIE AMW
ROCZNIK pol.

Zasadniczym celem „Rocznika Bezpieczeństwa Morskiego" jest stworzenie szerokiego, interdyscyplinarnego forum dyskusyjnego, zarówno dla środowiska naukowego jak również przedstawicieli podmiotów gospodarczych związanych z szeroko rozumianą gospodarką morską, możliwości wymiany doświadczeń i osiągnięć naukowych związanych z problematyką bezpieczeństwa morskiego.

„Rocznik Bezpieczeństwa Morskiego" jest ponadto próbą zwiększenia zainteresowania szerokiego grona decydentów oraz opinii publicznej poruszanymi zagadnieniami, jak również swoistą promocją „Polski Morskiej". Mamy nadzieję, że spotka się on z przychylnym zainteresowaniem tych wszystkich, którym bliska jest problematyka morska.

ISSN 1898-3189

W skład Rady Naukowej „Rocznika Bezpieczeństwa Morskiego” wchodzą:

SPIS TREŚCI

WYKAZ SKRÓTÓW

ABW	Agencja Bezpieczeństwa Wewnętrznego
BPMN	Notacja Modelowania Procesów Biznesowych
CPR	Centrum Powiadamiania Ratunkowego
EIK	Europejska Infrastruktura Krytyczna
EPOIK	Europejski Program Ochrony Infrastruktury Krytycznej
GZZK	Gminny Zespół Zarządzania Kryzysowego
IK	Infrastruktura Krytyczna
KPZK	Krajowy Plan Zarządzania Kryzysowego
KW POLICJI	Komenda Wojewódzka Policji
KW PSP	Komenda Wojewódzka Państwowej Straży Pożarnej
MAiC	Ministerstwo Administracji i Cyfryzacji
MEN	Ministerstwo Edukacji Narodowej
MF	Ministerstwo Finansów
MG	Ministerstwo Gospodarki
MNiSW	Ministerstwa Nauki i Szkolnictwa Wyższego
MON	Ministerstwo Obrony Narodowej
MOSG	Morski Oddział Straży Granicznej
MPiPS	Ministerstwo Pracy i Polityki Społecznej
MRiRW	Ministerstwo Rolnictwa i Rozwoju Wsi
MRR	Ministerstwo Rozwoju Regionalnego
MSPiR	Morska Służba Poszukiwania i Ratownictwa
MSW	Ministerstwo Spraw Wewnętrznych
MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji
MSZ	Ministerstwo Spraw Zagranicznych
MŚ	Ministerstwo Środowiska
MTBiGM	Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej
MW RP	Marynarka Wojenna Rzeczypospolitej Polskiej
MZ	Ministerstwo Zdrowia
NATO	Organizacja Traktatu Północnoatlantyckiego
NPOIK	Narodowy Program Ochrony Infrastruktury Krytycznej

NSPK	Narodowy System Pogotowia Kryzysowego
OC	Obrona Cywilna
OIK	Ochrona Infrastruktury Krytycznej
PRM	Państwowe Ratownictwo Medyczne
PUW	Pomorski Urząd Wojewódzki
RCB	Rządowe Centrum Bezpieczeństwa
RDLP	Regionalna Dyrekcja Lasów Państwowych
RM	Rada Ministrów
RWPG	Rada Wzajemnej Pomocy Gospodarczej
RZGW	Regionalny Zarząd Gospodarki Wodnej
RZZK	Rządowy Zespół Zarządzania Kryzysowego
SBP	System Bezpieczeństwa Państwa
SOZIK	Sieć Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej
SZBIK	Systemu Zarządzania Bezpieczeństwem Infrastruktury Krytycznej
UE	Unia Europejska
UEFA	Unia Europejskich Związków Piłkarskich
UM	Urząd Marszałkowski
WBiZK	Wydział Bezpieczeństwa i Zarządzania Kryzysowego
WCPR	Wojewódzkie Centrum Powiadamiania Ratunkowego
WCZK	Wojewódzkie Centrum Zarządzania Kryzysowego
WINB	Wojewódzki Inspektorat Nadzoru Budowlanego
WIOŚ	Wojewódzki Inspektorat Ochrony Środowiska
WPZK	Wojewódzki Plan Zarządzania Kryzysowego
WSSE	Wojewódzka Stacja Sanitarno-Epidemiologiczna
WSzW	Wojewódzki Sztab Wojskowy
WZZK	Wojewódzki Zespół Zarządzania Kryzysowego

WSTĘP

"Those who cannot remember the
past are condemned to repeat it"

George Santayana[1],
The Life of Reason, 1905-1906.

Ci, którzy nie pamiętają przeszłości, skazani są na jej powtarzanie – cytat ten doskonale wkomponowuje się w zasady funkcjonowania systemu zarządzania kryzysowego, a tym samym w proces ochrony infrastruktury krytycznej, gdzie doświadczenia zdobyte podczas reagowania na sytuacje kryzysowe, powinny być utrwalane i wykorzystywane na potrzeby budowania skutecznych mechanizmów podnoszących bezpieczeństwo każdej istoty ludzkiej, każdej celowo zorganizowanej struktury oraz każdego społeczeństwa.

„Bezpieczeństwo" to wolność od lęku i niepewności. Wolność od zagrożeń i możliwość zaspokojenia podstawowych potrzeb człowieka, za które uznaje się istnienie, przetrwanie, tożsamość, niezależność, spokój, posiadanie czy pewność rozwoju[2]. Świadczy o tym wszystkim, ulokowanie bezpieczeństwa na II poziomie piramidy potrzeb Maslova, bezpośrednio za potrzebami fizjologicznymi człowieka.

Bezpieczeństwo odgrywa ogromną rolę w rozwoju osobniczym, społecznym i cywilizacyjnym ludzkości[3]. Dualność jego charakteru powoduje, że jest ono postrzegane, jako stan oraz jako losowy proces, którym niezwykle trudno zarządzać w nieprzychylnym otoczeniu zewnętrznym oraz trudnym środowisku wewnętrznym. Bezpieczeństwo to stan, który nie jest dany raz na zawsze.

Zmienny w czasie i ciągle rosnący zbiór współczesnych zagrożeń bezpieczeństwa powoduje, że problem skutecznego przeciwdziałania nim jest najważniejszym przedsięwzięciem realizowanym zarówno

[1] George Santayana (ur. 16 grudnia 1863 r. w Madrycie, zm. 26 września 1952 r. w Rzymie), amerykański pisarz i filozof.
[2] T. Szubrycht (red.), *Leksykon bezpieczeństwa morskiego*, AMW, Gdynia 2008, s. 17.
[3] K. Ficoń, *Bezpieczeństwo jako systemowa kategoria ontologiczna*, BELLONA, 2012, s. 6.

w wymiarze lokalnym, regionalnym jak i globalnym. Zarządzanie bezpieczeństwem odgrywa wyjątkową rolę w społeczeństwach demokratycznych, o czym świadczą między innymi działania podejmowane przez Unię Europejską na arenie międzynarodowej. Wyrazem tych tendencji jest budowany europejski system bezpieczeństwa, ukierunkowany również na realizację zadań z zakresu identyfikacji i ochrony infrastruktury krytycznej.

Organa władzy publicznej w Polsce[4] jak również w innych państwach demokratycznych mają konstytucyjny obowiązek kształtowania wielowymiarowego bezpieczeństwa zewnętrznego, wewnętrznego i globalnego na maksymalnym poziomie, zgodnie ze światowymi standardami i zasadami prawno-międzynarodowymi.

XXI wiek od samego początku charakteryzuje się intensywnym rozwojem nowoczesnych technologii oraz procesów globalizacji. Towarzyszy temu również szereg zagrożeń niosących ze sobą skutki w skali całego świata. Należą do nich: zagrożenia demograficzne, żywnościowe, ekologiczne, wyczerpywanie się surowców energetycznych, a także zagrożenia wynikające z dysproporcji rozwojowych poszczególnych rejonów świata i coraz częściej akcentowane zagrożenia informacyjne, zagrożenia płynące z cyberprzestrzeni, która staje się polem działania przestępczości oraz najbardziej zaawansowanych technologicznie armii świata[5].

Skuteczne przeciwdziałanie zidentyfikowanym zagrożeniom wymaga budowy efektywnego systemu zarządzania kryzysowego, działającego w strukturach nadrzędnego systemu bezpieczeństwa narodowego. Systemu, który zapewniłby odpowiedni poziomu bezpieczeństwa wewnętrznego, akceptowanego przez wszystkich obywateli.

Doświadczenia pokazują, że system zarządzania kryzysowego wymaga jasnego podziału kompetencji oraz bezwzględnej współpracy administracji publicznej wszystkich szczebli oraz podmiotów spoza tego

[4] Mówi o tym art. 5 Konstytucji RP z dnia 2 kwietnia 1997 r.: *Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju*, Dz. U. z 1997 r. Nr 78, poz. 483, ze zm.

[5] G. Krasnodębski, *Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego*, [w:] *Problemy zapewnienia bezpieczeństwa regionalnego*, Olsztyn 2008.

obszaru. Budowa systemu zarządzania kryzysowego to proces długotrwały, wymagający lat pracy oraz dużych środków finansowych. Należy podkreślić, że w Polsce uczyniono w tym zakresie już bardzo wiele. Stworzono podstawy formalno-prawne oraz zdefiniowano podstawowe pojęcia takie jak: sytuacja kryzysowa, zarządzanie kryzysowe czy też infrastruktura krytyczna. *Ustawa o zarządzaniu kryzysowym* definiuje również hierarchiczną strukturę tego systemu oraz zakres zadań dla poszczególnych jego elementów[6].

Kolejne lata zdobywanych doświadczeń powodują, że zapobieganie i przygotowanie do sytuacji kryzysowych jest coraz doskonalsze. Taki stan nie gwarantuje jednak stuprocentowej pewności, że nadciągający żywioł zostanie opanowany, a konsekwencje społeczne i ekonomiczne będą znikome.

Poważne awarie techniczne, anomalie klimatyczne, wzrost zagrożenia atakami terrorystycznymi oraz wroga działalność w cyberprzestrzeni powodują, że bardzo istotnym zadaniem realizowanym przez system bezpieczeństwa narodowego, a w szczególności przez system zarządzania kryzysowego jest ochrona infrastruktury krytycznej.

Pojęcie infrastruktury krytycznej już na stałe zagościło w problematyce bezpieczeństwa i przez cały czas ewoluuje. Mimo, że ochrona najważniejszych obiektów czy instalacji prowadzona była już od dawna podczas trwania konfliktów zbrojnych to pod koniec XX i na początku XXI wieku proces ten nabrał szczególnego znaczenia. Okazało się bowiem, że podczas pokoju również należy chronić systemy sektora militarnego, społecznego oraz gospodarczego tak, aby nie dopuścić do przerwania ciągłości ich pracy. Przyczyniły się do tego poważne awarie sieci energetycznych w USA i Kanadzie, ataki terrorystyczne przeprowadzone na World Trade Center i Pentagon w USA, zamachy w Madrycie, zamachy w Londynie oraz liczne klęski żywiołowe. Ostatnie lata pokazują również, że zaawansowane technologicznie społeczeństwa mogą ponosić dotkliwe straty spowodowane atakami z cyberprzestrzeni.

Pierwsze inicjatywy związane z ochroną infrastruktury krytycznej zostały podjęte w 1996 r. przez prezydenta Billa Clintona, który utworzył specjalną komisję do zbadania podatności infrastruktury

[6] R. Sulęta, G. Krasnodębski, *Podstawy prawne zarządzania kryzysowego w Polsce*, [w:] *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, WSAiB, Gdynia 2011.

krytycznej Stanów Zjednoczonych na zagrożenia. W skład komisji weszli przedstawiciele rządu, przedstawiciele organizacji pozarządowych oraz właściciele infrastruktury krytycznej z sektora prywatnego[7].

Opierając się na doświadczeniach Stanów Zjednoczonych, również i inne państwa rozpoczęły projekty dotyczące ochrony infrastruktury krytycznej, w tym również Polska. Bardzo duży wpływ na kształtowanie się procesu ochrony infrastruktury krytycznej w Polsce mają akty normatywne NATO oraz Unii Europejskiej.

Prace nad stworzeniem mechanizmów ochrony infrastruktury krytycznej w Unii Europejskiej rozpoczęto po ataku terrorystycznym z 11 września 2001 roku na World Trade Center w USA, jednak ich faktyczna intensyfikacja miała miejsce dopiero w 2004 roku po atakach terrorystycznych w Madrycie, czyli w momencie, kiedy zagrożenia bezpośrednio dotknęły „organizm" Unii Europejskiej. Rada Europejska w czerwcu 2004 r. zgłosiła postulat, aby opracować ogólną strategię zwiększenia ochrony infrastruktury krytycznej. W odpowiedzi na ten postulat już w październiku 2004 roku Komisja Wspólnot Europejskich wydała komunikat dotyczący ochrony infrastruktury krytycznej w walce z terroryzmem[8], który zapoczątkował kolejne prace nad tym problemem.

Niewątpliwie najważniejszym obecnie dokumentem z zakresu ochrony infrastruktury krytycznej jest Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania Europejskiej Infrastruktury Krytycznej (EIK) oraz oceny potrzeb w zakresie poprawy jej ochrony, której celem jest stworzenie procedury rozpoznawania i wyznaczania Europejskiej Infrastruktury Krytycznej oraz opracowanie wspólnego podejścia do oceny potrzeb w zakresie poprawy jej ochrony.

Polska, jako członek Unii Europejskiej jest zobligowana do stworzenia mechanizmów ochrony infrastruktury krytycznej oraz prowadzenia współpracy w tym zakresie na poziomie Wspólnoty. W wyniku tych działań przygotowano już odpowiednie regulacje formalno-prawne dające podstawy do budowy systemu ochrony infrastruktury krytycznej.

---

[7] *Critical Infrastructure Threats and Terrorism*, DCSINT Handbook No. 1.02, 2006, s 1, (http://www.fas.org/irp/threat/terrorism/sup2.pdf).

[8] *Communication from the Commission to the Council and the European Parliament, Critical Infrastructure Protection in the fight against terrorism*, Brussels, 20.10.2004, COM(2004) 702 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= COM: 2004:0702:FIN:EN:PDF).

Podjęcie przez autora badań z zakresu modelowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej państwa wpisuje się w proces budowy oprzyrządowania do prowadzenia wielokryterialnych analiz, dotyczących utrzymania ciągłości działania w sytuacjach kryzysowych przez obiekty, instalacje, urządzenia, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorstw.

Zainteresowania autora problematyką ochrony infrastruktury krytycznej wynikają głównie ze zdobytego doświadczenia zawodowego podczas wykonywania obowiązków służbowych w Zakładzie Zarządzania Kryzysowego Akademii Marynarki Wojennej i kierowania studiami podyplomowymi *Zarządzanie Kryzysowe*. Prowadzenie zajęć dydaktycznych, uczestniczenie w pracach naukowych oraz ścisła współpraca z Wydziałem Bezpieczeństwa i Zarządzania Kryzysowego Pomorskiego Urzędu Wojewódzkiego zaowocowała wypracowaniem koncepcji budowy modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej, przydatnego na poziomie regionalnym oraz rządowym. Bardzo użyteczne okazały się również doświadczenia zdobyte na stanowisku projektanta i analityka zautomatyzowanych systemów dowodzenia w Zespole Informatyki Marynarki Wojennej.

Obszar prowadzonych badań i analiz naukowych obejmuje problematykę budowy i funkcjonowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej na szczeblu państwa i regionu, wspomagającego pracę etatowych organów władzy publicznej odpowiedzialnych za utrzymanie określonego poziomu ochrony kluczowych dla państwa zasobów i struktur.

Włączenie się w proces budowy skutecznych mechanizmów ochrony infrastruktury krytycznej, jako istotnego elementu systemu zarządzania kryzysowego spowodowało, że **przedmiotem badań** stał się *system infrastruktury krytycznej* natomiast głównym **celem badań** było *opracowania modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej*. Systemu należącego do grupy systemów prakseologicznych wykorzystywanych do diagnozowania, prognozowania i kształtowania bezpieczeństwa.

Osiągniecie głównego celu badań było możliwe poprzez realizację następujących **celów szczegółowych**:

- określenie definicji bezpieczeństwa i identyfikację zagrożeń,

- analizę uregulowań formalno-prawnych systemu zarządzania kryzysowego oraz ochrony infrastruktury krytycznej,
- identyfikację elementów infrastruktury krytycznej,
- zaprojektowanie procesu ochrony infrastruktury krytycznej,
- opracowanie modelu identyfikacyjnego i decyzyjnego systemu zarządzanie bezpieczeństwem infrastruktury krytycznej,
- opracowanie modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej.

Problematyka ochrony infrastruktury krytycznej w wymiarze międzynarodowym jest stosunkowa młoda, wobec czego ramy czasowe prowadzonych badań zostały ograniczone w wymiarze globalnym do końca XX w. i pierwszego dziesięciolecia XXI w., natomiast w odniesieniu do Polski od wprowadzenia w życie *Ustawy o zarządzaniu kryzysowym z 26 kwietnia 2007 roku* do chwili obecnej.

Wstępna analiza podjętej problematyki badawczej wykazała, że *zbudowanie modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej* wymaga uwzględnienia w procesie badawczym pojęcia i teorii bezpieczeństwa, umiejscowienia ochrony infrastruktury krytycznej w systemie zarządzania kryzysowego, analizy procesu ochrony infrastruktury krytycznej, wykorzystania metod modelowania matematycznego oraz opracowania modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej.

Definiując problem badawczy, jako trudność lub przeszkodę, którą należy pokonać, aby osiągnąć zamierzony cel badawczy, przyjęto, że **głównym problemem badawczym** prowadzonych badań będzie znalezienie odpowiedzi na następujące pytanie: *jak powinien być zbudowany oraz w jaki sposób powinien funkcjonować system zarządzania bezpieczeństwem infrastruktury krytycznej, aby proces ochrony infrastruktury krytycznej spełniał przyjęte standardy bezpieczeństwa?*

Podjęty problem badawczy dotyczy więc analizy potrzeb w zakresie bezpieczeństwa infrastruktury krytycznej i możliwości ich zaspokojenia przez dostępny potencjał organizacyjno-funkcjonalny i wykonawczy. Najważniejszym elementem tego problemu jest opracowanie modelowej koncepcji systemu zarządzania bezpieczeństwem infrastruktury krytycznej, bazującej na obowiązujących uregulowaniach formalno-prawnych i w oparciu o istniejące jednostki organizacyjne.

Rozwiązanie tak sformułowanego problemu badawczego wymagało znalezienia odpowiedzi na szereg dodatkowych pytań, które identyfikują poszczególne **problemy szczegółowe**, warunkujące osiągnięcie głównego celu pracy. Należą do nich:

- *Jak jest definiowane bezpieczeństwo we współczesnym świecie?*
- *Jaką rolę pełni zarządzanie kryzysowe w systemie bezpieczeństwa narodowego?*
- *Jakie jest miejsce ochrony infrastruktury krytycznej w systemie zarządzania kryzysowego?*
- *Jaka jest struktura organizacyjno-funkcjonalna systemu infrastruktury krytycznej?*
- *Jak można usprawnić i zwiększyć efektywność systemu zarządzania bezpieczeństwem infrastruktury krytycznej?*
- *Jak należy oceniać ochronę infrastruktury krytycznej?*

Analiza materiałów źródłowych, uczestnictwo w konferencjach krajowych i międzynarodowych, sympozja, rozmowy z ekspertami zarządzania kryzysowego, odbycie stażu zawodowego w Wydziale Bezpieczeństwa i Zarządzania Kryzysowego Pomorskiego Urzędu Wojewódzkiego oraz nabyte doświadczenie pozwoliły przyjąć autorowi następująca hipotezę badawczą podejmującą rozwiązanie celu poznawczego: *system zarządzania bezpieczeństwem infrastruktury krytycznej powinien odznaczać się wysoką efektywnością i skutecznością przedsięwzięć podejmowanych w celu zapewnienia funkcjonalności, ciągłości działania i integralności infrastruktury krytycznej, zapobiegania zagrożeniom, ryzykom lub słabym punktom, ograniczenia i neutralizacji ich skutków, szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.*

Zweryfikowanie tak postawionej hipotezy badawczej wymagało z kolei skonstruowania pomocniczych hipotez roboczych, które pozwoliły na dowodzenie prawdziwości lub fałszu hipotezy głównej. Sformułowane powyżej szczegółowe problemy badawcze prowadzą do zbudowania następujących szczegółowych hipotez roboczych:

- *fundamentem funkcjonowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej są obowiązujące uregulowania formalno-prawne wydawane przez organa władzy administracyjnej na szczeblach centralnych, regionalnych i lokalnych,*

- *budowa efektywnego i skutecznego systemu zarządzania bezpieczeństwem infrastruktury krytycznej wymaga stworzenia modelu identyfikacyjnego i decyzyjnego tego systemu,*
- *opracowanie metodyki oceny bezpieczeństwa infrastruktury krytycznej pozwoli ocenić funkcjonowanie systemu zarządzania bezpieczeństwem infrastruktury krytycznej.*

Podjęta w dysertacji problematyka ochrony infrastruktury krytycznej w ostatnich kilku latach jest żywo dyskutowana przez rodzimych specjalistów zarządzania kryzysowego. Szczególnie intensywne rozmowy prowadzone były w aspekcie bezpieczeństwa obiektów użyteczności publicznej podczas mistrzostw UEFA EURO 2012™. Infrastruktura krytyczna staje się coraz częściej tematem konferencji krajowych i międzynarodowych, natomiast brakuje jednolitego opracowania zawierającego kompleksową analizę systemu ochrony infrastruktury krytycznej. W fazie opracowywania znajduje się Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) nadzorowany przez Dyrektora Rządowego Centrum Bezpieczeństwa (RCB).

Problemy bezpieczeństwa i ochrony infrastruktury krytycznej poruszane są w licznych artykułach i wystąpieniach prezentowanych na konferencjach naukowych. Należy tutaj wskazać monografię *Zasadnicze problemy zarządzania kryzysowego w organizacjach zhierarchizowanych*[9] zawierającą rozważania dotyczące ochrony infrastruktury krytycznej w Polsce w kontekście zadań organizacji zhierarchizowanych oraz monografię *Ochrona infrastruktury krytycznej*[10], w której można znaleźć szereg opracowań z zakresu infrastruktury krytycznej i problemów bezpieczeństwa narodowego, koncepcji i unormowań prawnych ochrony infrastruktury krytycznej, zagrożeń elementów kluczowych infrastruktury krytycznej, doświadczeń i dobrych praktyk oraz wybrane przykłady przedsięwzięć podejmowanych na rzecz ochrony infrastruktury krytycznej i edukacji w zakresie ochrony infrastruktury krytycznej.

Ważnym źródłem informacji z zakresu zarządzania kryzysowego, uwzględniającym problematykę modelowania matematycznego prakseologicznych systemów działania jest monografia *Inżynieria*

[9] J. Stawnicka, B. Wiśniewski, R. Socha, *Zasadnicze problemy zarządzania kryzysowego w organizacjach zhierarchizowanych*, KWP, Katowice 2011.
[10] A. Tyburska, *Ochrona infrastruktury krytycznej*, WSPol, Szczytno 2010.

zarządzania kryzysowego. Podejście systemowe[11] oraz monografia *System reagowania kryzysowego* [12] przybliżająca problematykę zarządzania kryzysowego ze szczególnym podkreśleniem reagowania na sytuacje kryzysowe.

Osiągnięcie zamierzonych celów poznawczych oraz rozwiązanie postawionego problemu badawczego na drodze weryfikacji hipotez roboczych wymagało odwołania się do naukowych metod i narzędzi badawczych.

Interdyscyplinarny charakter podjętego problemu badawczego wymusił zastosowanie w procesie badawczych metod teoretycznych oraz empirycznych. Ich wykorzystanie uzależnione było od typu rozwiązywanego problemu. Rozwiązanie podjętego problemu badawczego oraz weryfikacja postawionej hipotezy roboczej wymagała wykorzystania następujących metod badawczych: analizy, syntezy, uogólnień, wnioskowania i symulacji komputerowej.

Etapem wyjściowym były badania teoretyczne, które uporządkowały wiedzę i kompetencje oraz stworzyły podstawy do przeprowadzenia badań empirycznych.

W wyniku przeprowadzenia analizy i krytyki ogólnie dostępnej literatury polskiej i obcojęzycznej stwierdzono, że problematyka budowy modelu kompleksowego systemu zarządzania bezpieczeństwem infrastruktury krytycznej nie doczekała się jednolitego opracowania. Metoda ta została również wykorzystana do zebrania informacji z zakresu funkcjonowania systemu zarządzania kryzysowego, systemu infrastruktury krytycznej oraz ochrony infrastruktury krytycznej.

Analiza instytucjonalno-prawna posłużyła do analizy uregulowań formalno-prawnych funkcjonowania systemu zarządzania kryzysowego oraz przepisów dotyczących ochrony infrastruktury krytycznej. Wyniki analizy pozwoliły określić ograniczenia prawne wpływające na możliwości funkcjonalne systemu ochrony infrastruktury krytycznej.

Analiza historyczna została wykorzystana do określenia genezy zarządzania kryzysowego oraz ochrony infrastruktury krytycznej w Polsce i na świecie. Dostarczyła informacji o ewolucji postrzegania pojęcia bezpieczeństwa oraz podejścia do organizacji procesu ochrony infrastruktury krytycznej.

---

[11] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, BEL Studio, Warszawa 2007.
[12] J. Gryz, W. Kitler, *System reagowania kryzysowego*, Adam Marszałek, Toruń 2007.

Wykorzystanie syntezy umożliwiło łączenie w całość wyodrębnionych i zebranych wcześniej elementów, dzięki czemu możliwe było dokonanie uogólnień oraz budowanie modelu matematycznego systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

Szczególnie przydatną podczas konstruowania modelu identyfikacyjnego i decyzyjnego systemu zarządzania bezpieczeństwem infrastruktury krytycznej oraz modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej była metoda porównawcza. Dzięki niej można było zastosować rozwiązania zastosowane w modelach systemów prakseologicznego działania.

Zastosowanie metody uogólnień umożliwiło przejście od pojedynczych twierdzeń i obserwacji dotyczących podstawowych elementów infrastruktury krytycznej do twierdzeń o wyższym poziomie ogólności i złożoności odnoszących się do całych systemów.

Prawidłowe przeprowadzenie procesu badawczego wymagało zastosowania wnioskowania, jako podstawowej metody badawczej. Jej wykorzystanie pozwoliło wypracować nowe twierdzenia, bazujące na dorobku naukowym z zakresy zarządzania kryzysowego i ochrony infrastruktury krytycznej.

W badaniach została wykorzystana również symulacja komputerowa do projektowania procesów ochrony infrastruktury krytycznej. Procesy zostały zbudowane i zweryfikowane z wykorzystaniem narzędzia informatycznego *Bizagi Process Modeler* służącego do modelowania procesów biznesowych w terminologii *Business Process Modeling Notation* (BPMN).

W trakcie procesu badawczego wykorzystano dedukcję do opracowania modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej oraz modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej. Indukcja posłużyła natomiast do opracowania uogólnionych sformułowań, wprowadzaniu nowych pojęć i twierdzeń.

Metoda wywiadu skategoryzowanego była wykorzystywana podczas weryfikacji rozwiązań teoretycznych w praktyce. Wywiady te było przeprowadzane w trakcie rozmów z ekspertami i praktykami zarządzania kryzysowego oraz infrastruktury krytycznej, które autor prowadził podczas ćwiczeń, szkoleń oraz stażu zawodowego w Wydziale

Bezpieczeństwa i Zarządzania Kryzysowego Pomorskiego Urzędu Wojewódzkiego.

Rozwiązanie zdefiniowanego w niniejszej dysertacji głównego problemu badawczego oraz problemów szczegółowych zostało zrealizowane w pewnym chronologicznym ciągu badawczym obejmującym trzy zasadnicze etapy: etap badań wstępnych (rozpoznanie problemu), etap badań zasadniczych (badania właściwe), etap badań końcowych (sprawozdanie z badań).

Etap wstępny, inicjujący program badań polegał na planowaniu, organizowaniu i stymulowaniu procesu badawczego, zgodnie z przyjętą koncepcją metodologiczną rozprawy. Na tym etapie m.in. doprecyzowano cele badawcze, ostatecznie sformułowano problemy badawcze, przeprowadzono kwerendę i analizę krytyczną źródeł piśmiennictwa, sformułowano tezy i hipotezy robocze rozprawy, wybrano adekwatne do potrzeb metody i narzędzia badawcze.

Na etapie badań właściwych w pierwszej kolejności został przedstawiony szczegółowy program badań oraz czasowy harmonogram ich realizacji. Procedury te uruchomiły szczegółowe czynności badawcze obejmujące specyfikację i przygotowanie zmiennych niezależnych, wypracowanie funkcji transformacji zmiennych niezależnych do postaci zmiennej zależnej, weryfikacji zaproponowanej funkcji transformacji i ocenę zgodności jej formuły z wartością oczekiwaną, przygotowanie wartości zmiennych niezależnych, przeprowadzenie badań na obiektach modelowych.

Etap badań końcowych polegał na analizie uzyskanych wyników badań i porównaniu ich z przyjętymi na wstępie hipotezami badawczymi. W efekcie uzyskane wyniki badawcze zostały zebrane, poklasyfikowane i posłużyły do licznych uogólnień i wyciągnięcia szeregu wniosków natury teoretycznej i praktycznej.

Ostatecznym wynikiem procesu badawczego, zaliczanym do etapu badań końcowych, jest niniejsze sprawozdanie z badań, które zostało zredagowane w formie rozprawy naukowej składającej się ze wstępu, pięciu rozdziałów, zakończenia, bibliografii, wykazu rysunków, oraz załączników.

W **rozdziale pierwszym** przeprowadzono analizę teorii bezpieczeństwa zwracając szczególną uwagę na różnorodność definicji, ewolucję postrzegania i pojmowania bezpieczeństwa. Przedstawiono klasyfikację bezpieczeństwa oraz omówiono podstawowe zagrożenia.

Ważnym wnioskiem płynącym z przeprowadzonej analizy jest stwierdzenie, że bezpieczeństwo jest traktowane jednocześnie, jako wartość, potrzeba, cel, prawo, a także, jako pożądany stan i dynamiczny proces. Stanowi ono bardzo ważną wartość w sensie egzystencjalnym, moralnym, społecznym, a także osobistym. Bezpieczeństwo jest naturalną normą, którą cywilizowane społeczeństwa powinny gwarantować całej swojej społeczności razem i wszystkim jej członkom z osobna. Od zawsze konieczność zachowania bezpieczeństwa odgrywała ogromną rolę w kształtowaniu polityki, rozwoju działalności gospodarczej czy stymulowaniu postępu naukowo-technicznego.

Najczęściej pojęcie bezpieczeństwa odnoszone jest do pewnego stanu braku zagrożeń, do normy, którą cywilizowane społeczeństwa gwarantują całej swojej społeczności razem i wszystkim jego członkom osobno, do stanu kontroli nad tym, co zagraża szczególnie cenionym wartościom, w tym również elementom infrastruktury krytycznej.

W **rozdziale drugim** przedstawione zostało miejsce procesu ochrony infrastruktury krytycznej w systemie zarządzania kryzysowego. Rozważania rozpoczęto od przestawienia istoty, celów i zadań zarządzania kryzysowego. Wynika z nich, że przez szereg lat problematyka zarządzania kryzysowego budziła wiele kontrowersji i zastrzeżeń. W wielu kryzysowych sytuacjach brakowało niezbędnych uregulowań formalno-prawnych oraz rozwiązań organizacyjno-funkcjonalnych. Uporządkowanie systemu nastąpiło dopiero po wprowadzeniu w życie *Ustawy o zarządzaniu kryzysowym z 26 kwietnia 2007 roku*. Nowym zadaniem realizowanym przez system zarządzania kryzysowego jest ochrona infrastruktury krytycznej obejmująca wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. Przeprowadzona analiza pozwoliła przygotować niezbędne zasoby informacyjne do zaprojektowania procesu zarządzania bezpieczeństwem infrastruktury krytycznej, zbudowania matematycznego modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej oraz opracowania modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej.

Rozdział trzeci zawiera projekt procesu ochrony infrastruktury krytycznej zbudowany z wykorzystaniem graficznej notacji procesów biznesowych BPMN. Opracowane rozwiązania zostały zweryfikowane przy pomocy analitycznego oprogramowania *Bizagi Process Modeler*. Wykorzystując wyniki przeprowadzonej analizy oraz badań w rozdziale drugim stworzono modelowy przebieg procesu ochrony infrastruktury krytycznej analogiczny do procesu zarządzania kryzysowego. W skład procesu ochrony infrastruktury krytycznej zostały zaliczone podprocesy zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej, przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną, reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej i odtwarzanie infrastruktury krytycznej. Takie podejście odpowiada stosowanemu cyklowi zarządzania kryzysowego w postaci zapobieganie-przygotowanie-reagowanie-odbudowa.

W **rozdziale czwartym** przedstawiono model matematyczny systemu zarządzania bezpieczeństwem infrastruktury krytycznej złożony z modelu identyfikacyjnego oraz decyzyjnego. Proces modelowania został zdekomponowany na dwa etapy konceptualne dotyczące odpowiednio budowy modelu indentyfikacyjnego i na jego bazie modelu decyzyjny. Przedstawiono również ogólne podejście do formalnego modelowania prakseologicznego systemu działania, jakim jest system zarządzania bezpieczeństwem infrastruktury krytycznej państwa.

Na początku zdefiniowano zadania i strukturę modelu identyfikacyjnego, który zgodnie z ogólną teorią systemów został opisany przy pomocy uporządkowanej trójki obejmującej: cel działania i podstawowe funkcje, składowe elementy struktury organizacyjnej oraz topologiczne relacje i różnorodne powiązania między tymi elementami. Wyodrębnione elementy systemu zarządzania bezpieczeństwem infrastruktury krytycznej zostały przedstawione w jednolitej konwencji za pomocą aparatu analizy i topologii matematycznej.

Budując model decyzyjny starano się ustalić zbiór ograniczeń oraz funkcję kryterium, determinującą proces zarządzania bezpieczeństwem infrastruktury krytycznej. Modelowanie decyzyjne ujmuje system zarządzania bezpieczeństwem infrastruktury krytycznej w dynamice działań, jako ciąg kolejno podejmowanych decyzji,

sterujących procesem zarządzania bezpieczeństwem infrastruktury krytycznej.

Rozdział piąty zawiera model konceptualny systemu oceny bezpieczeństwa infrastruktury krytycznej zbudowany w oparciu o taksonomiczną formułę potencjałową wykorzystaną do oceny poziomu przygotowania zasobów infrastruktury krytycznej do sytuacji kryzysowych. Formuła ta z powodzeniem była stosowana do oceny potencjału złożonych systemów broni, potencjału morskiego państwa oraz poziomu zagrożeń w aglomeracjach miejskich. Model systemu oceny bezpieczeństwa infrastruktury krytycznej został oparty na wynikach badań uzyskanych w poprzednich rozdziałach i posłużył do budowy systemu informatycznego, będącego narzędziem analitycznym z zakresu ochrony infrastruktury krytycznej.

Rozprawę kończy **zakończenie**, w którym zostały przedstawione zasadnicze wnioski uzyskane w trakcie przeprowadzonego procesu badawczego oraz odniesiono się do weryfikacji podjętego w rozprawie głównego problemu badawczego, problemów szczegółowych, hipotezy badawczej oraz hipotez roboczych.

Pomyślna realizacja całego procesu badawczego nie byłaby możliwa bez merytorycznego wsparcia ze strony pracowników Wydziału Dowodzenia i Operacji Morskich, służących życzliwą pomocą, radą a także krytycznym słowem. Sprawną realizację koncepcji metodologicznej rozprawy zawdzięczam przede wszystkim doświadczonej kadrze profesorskiej Wydziału Dowodzenia i Operacji Morskich, w tym szczególnie Panu prof. dr. hab. inż. Krzysztofowi Ficoniowi. Wielkiego wsparcia i pomocy udzielił mi także Pan kmdr dr hab. Tomasz Szubrycht - Dziekan Wydziału Dowodzenia i Operacji Morskich. Przy rozwiązywaniu większości problemów merytorycznych służyli mi pomocą pracownicy Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Pomorskiego Urzędu Wojewódzkiego w Gdańsku, a szczególnie Pan Dyrektor dr Ryszard Sulęta. Cytowane prace naukowe i źródła piśmiennictwa stanowiły dla mnie bezcenne źródło wiedzy. Bardzo przydatne okazały się również moje kontakty służbowe z instytucjami i organami odpowiedzialnymi za bezpieczeństwo i zarządzanie kryzysowe na różnych szczeblach władzy i administracji publicznej.

ROZDZIAŁ 1
POJĘCIE I ELEMENTY TEORII BEZPIECZEŃSTWA

Prowadząc rozważania nad pojęciem i istotą „bezpieczeństwa" nasuwa się proste i jednoznaczne pytanie o to, czym jest bezpieczeństwo? Wydawać by się mogło, że odpowiedź nie powinna być trudna jednak analiza materiałów źródłowych wykazała, iż pojęcie bezpieczeństwa jest kategorią uniwersalną i trudno definiowalną, funkcjonującą wyłącznie w teorii oraz w mowie potocznej[13]. Istnieją poglądy, iż pojęcie to jest subiektywne i elastyczne, że może znaczyć wszystko, cokolwiek ma na myśli jego użytkownik. W opracowaniach z dziedziny nauk społecznych mówi się, że bezpieczeństwo należy do „pojęć spornych ze swej istoty", których znaczenia nie da się do końca zdefiniować[14]. Twierdzenie to jest z pewnością prawdziwe przy założeniu, że dla każdego, bezpieczeństwo oznacza coś innego.

1.1. WYBRANE DEFINICJE BEZPIECZEŃSTWA

Termin bezpieczeństwo pochodzi od łacińskiego słowa *sine cura = securitas* (bez pieczy). W potocznym rozumieniu bezpieczeństwo jest ujmowane negatywnie, jako brak zagrożeń, zaś w definicjach słownikowych zazwyczaj występuje ujęcie pozytywne utożsamiające bezpieczeństwo z pewnością, jako stanem przeciwstawnym zagrożeniom[15].

Zamieszczona w *Leksykonie bezpieczeństwa morskiego* definicja „bezpieczeństwa" mówi o tym, że jest to stan psychiczny pozwalający na

[13] K. Ficoń, *Bezpieczeństwo …*, *dz. cyt.*
[14] P. D. Wiliams, Studia bezpieczeństwa, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012, s. 1.
[15] R. Zięba, *Teoria ogólna bezpieczeństwa państwa w stosunkach międzynarodowych*, [w:] *Stosunki międzynarodowe w XXI wieku. Księga jubileuszowa z okazji 30-lecia Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego*, WN Scholar, Warszawa 2006, s. 935–953.

wzbudzenie przekonania o braku ryzyka straty czegoś lub możliwości wystąpienia negatywnych zdarzeń[16].

W tym samym źródle mówi się również, że „bezpieczeństwo" to wolność od lęku i niepewności. Wolność od zagrożeń i możliwość zaspokojenia podstawowych potrzeb człowieka, za które uznaje się istnienie, przetrwanie, tożsamość, niezależność, spokój, posiadanie czy pewność rozwoju.

Zwraca się uwagę, że „bezpieczeństwo" jest jednocześnie stanem i procesem. Rozumiane jako stan oznacza brak występowania zagrożeń, poczucie bezpieczeństwa, wolność od zagrożeń, strachu lub ataku. Jako proces cechuje się zmiennością w czasie i przestrzeni. Jest ono (lub jego postrzeganie) podatne na zmiany układu sił oraz stan wzajemnych relacji pomiędzy poszczególnymi podmiotami na scenie międzynarodowej. Ma więc charakter swego rodzaju naczyń połączonych. Wynika to między innymi z faktu, że poszerzenie sfery bezpieczeństwa państwa, sojuszu lub koalicji skutkuje (lub może skutkować) subiektywnie postrzeganym obniżeniem bezpieczeństwa innych podmiotów.

Nieco inna definicja została zamieszczona w *Operacyjno-taktycznym leksykonie morskim*. Zgodnie z nią „bezpieczeństwo" to stan osiągany wtedy, gdy określone informacje, materiały, personel, czynności i obiekty zostają zabezpieczone przed szpiegostwem, sabotażem, dywersją i terroryzmem, a także przed utratą lub nieautoryzowanym dostępem[17].

K. Ficoń w opracowaniu *Bezpieczeństwo jako systemowa kategoria ontologiczna* uważa, że „bezpieczeństwo" jako uniwersalna kategoria ontologiczna jest pojmowane jednocześnie jako: wartość, potrzeba, cel, prawo, a także jako pożądany stan i dynamiczny proces. Bezpieczeństwo jest wartością m.in. w sensie egzystencjalnym, moralnym, społecznym, a także osobistym. Jako wartość fundamentalna w hierarchii aksjologicznej zajmuje jedno z najwyższych miejsc. Nie jest to jednak wartość autoteliczna, lecz utylitarna i instrumentalna. Bezpieczeństwo cenimy przede wszystkim dlatego, że zapewnia i gwarantuje nam uzyskanie innych równie cennych wartości lub stanowi środek do ich uzyskania, takich jak np. standardy życia

[16] T. Szubrycht (red.), *Leksykon …, dz. cyt.*, s. 17.
[17] H. Sołkiewicz (red.), *Operacyjno-taktyczny leksykon morski*, Tom 1, AMW, Gdynia 2012, s. 84.

i zdrowia, sukcesy zawodowe i satysfakcja osobista itp. Jest ono niezbywalną i niezamienialną wartością każdego prakseologicznego systemu działania i stanowi podstawę jego istnienia i trwania w przyszłości[18].

Traktując bezpieczeństwo, jako proces, którego celem działania jest zapewnienie poczucia braku zagrożeń danego podmiotu, można stwierdzić, iż bezpieczeństwo to ta dziedzina aktywności podmiotu, której treścią jest zapewnianie możliwości przetrwania (egzystencji) i swobody realizacji własnych interesów w niebezpiecznym środowisku, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), stawianie czoła wyzwaniom, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów[19]. Podmiotem bezpieczeństwa mogą być wszystkie jednostki mające własne interesy i wyrażające ambicje realizacji tych interesów. Mogą to być pojedyncze osoby, różne grupy społeczne, narody, społeczności międzynarodowe i wreszcie cała ludzkość. Stosownie do tego możemy wyodrębniać różne rodzaje bezpieczeństwa: indywidualne (personalne), grupowe (rodowe, plemienne), narodowe (państwowe) międzynarodowe (regionalne, globalne).

Według E. Nowaka „bezpieczeństwo" zaliczyć można do grupy najpowszechniejszych pojęć w życiu codziennym oraz organizacji i funkcjonowaniu państwa, społeczeństwa, również w nauce. Powszechność tego pojęcia pociąga za sobą jego wieloznaczność, w związku z czym współcześnie celem dokładnego określenia obszaru bezpieczeństwa stosowane są między innymi przymiotniki: publiczne, militarne, osobiste, energetyczne, ekonomiczne, narodowe, informacyjne[20].

Definicje słownikowe najczęściej określają „bezpieczeństwo jako stan niezagrożenia, spokoju, pewności"[21]. Pojęcie „bezpieczeństwo" w znaczeniu ogólnospołecznym obejmuje zabezpieczenie potrzeb, takich jak istnienie, przetrwanie, pewność, stabilność, niezależność, tożsamość,

[18] K. Ficoń, *Bezpieczeństwo …*, *dz. cyt.*
[19] S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Kwartalnik bezpieczeństwo Narodowe, Nr 18, BBN, Warszawa 2011, s. 20.
[20] E. Nowak, *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Akademia Obrony Narodowej, Warszawa 2007, s. 9.
[21] *Słownik języka polskiego,* t. 1, Wydawnictwo PWN, Warszawa 1978, s. 147.

ochrona poziomu i jakości życia. Bezpieczeństwo jest naczelną potrzebą człowieka oraz grup społecznych, a zarazem główną potrzebą państw oraz międzynarodowych systemów. Brak bezpieczeństwa prowadzi do niepokoju i poczucia zagrożenia.

Bez wątpienia bezpieczeństwo to naczelna potrzeba człowieka oraz grup społecznych, a także najistotniejszy ich cel. Jego zadaniem jest bowiem zaspokojenie naczelnych żywotnych potrzeb trwania, przewidywalności, stabilizacji, dobrobytu, rozwoju, a w konsekwencji szczęścia ludzkiego. Bezpieczeństwo to stan, a zarazem ciągły proces, systematyczne działanie celem jego tworzenia oraz utrzymywania. Jest to najwyższa wartość i potrzeba jednostek, grup społecznych, państw, wspólnot wielopaństwowych, jest to wytwór wszystkich podmiotów bezpieczeństwa, które muszą być gotowe i zdolne do tego[22].

Z perspektywy jednostki na budowanie poczucia własnego bezpieczeństwa mają wpływ głównie procesy poznawcze, emocjonalne, drążeniowe uświadamiające człowiekowi jego uczestnictwo w sytuacjach oraz czynnościach, wskazujące na jego powinności związane z bezpieczeństwem, kreujące nastawienia, motywy oraz potrzeby, a także wpływające na jego zachowania. Z kolei z szerszej perspektywy, a więc narodowej, społecznej, środowiskowej, globalnej, „bezpieczeństwo" to działania gromadzące wiedzę o nim w środowisku lokalnym, narodowym, ponadnarodowym. Wypracowują one wzory i metody typów zachowań, które mają chronić i ratować ludzi, substancję materialną oraz środowisko, a także kodyfikują te wzory i zobowiązują do ich przestrzegania[23].

J. Świniarski definiuje „bezpieczeństwo" jako stan, który zapewnia człowiekowi warunki samorealizacji. Stan, w którym jednostki, grupy społeczne, organizacja państwa nie odczuwają zagrożenia swego istnienia, a także podstawowych swych interesów. Bezpieczeństwo to stan, w którym istnieją formalne, instytucjonalne i praktyczne gwarancje ochrony tego, co stanowi istotę pełnej samorealizacji[24].

„Bezpieczeństwo" wiąże się z poczuciem stabilności i trwałości określonego stanu rzeczy, odczuciem braku zagrożenia wewnętrznego

[22] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Wydawnictwo ISP PAN, Warszawa 1996, s. 8.
[23] J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego. Część 1. Zarządzanie kryzysowe w administracji publicznej*, Krakowska Szkoła Wyższa, Kraków 2009, s. 10-11.
[24] J. Świniarski, *Filozoficzne podstawy edukacji dla bezpieczeństwa*, MON, Warszawa 1999, s. 13.

i zewnętrznego, a nadto także z doznawaniem pewności i spokoju w codziennym bytowaniu, ufności i zaufaniu do przyszłości[25].

Pojęcie bezpieczeństwa dysponuje rozmaitymi wymiarami, tak w sferze ogólnej, publicznej, jak indywidualnej, czyli osobistej, chociaż zawsze odnoszącymi się do stanu zagrożenia i niepewności. W znaczeniu powszednim „bezpieczeństwo to stan braku zagrożenia, stan pewności, spokoju, zabezpieczenia" [26]. W sferze psychicznej, jak i realnej bezpieczeństwo jest zaaprobowane, jako stan pozytywny i pożądany, który zasługuje na realizację i ochronę.

Leksykalna definicja ujmuje „bezpieczeństwo", jako stan niezagrożenia, spokoju, pewności, uwzględniając fakt, że bezpieczeństwo nie jest jednorodzajowym stanem rzeczy życia jednostkowego i zbiorowego człowieka. Nie jest również absolutnie uściślonym celem lub zadaniem jednostek lub całych wspólnot ludzkich. Zarazem jest zjawiskiem bardzo rozmaitym, który obejmuje różne sfery: społeczną, polityczną, militarną, ekonomiczną, kulturową, prawną, ekologiczną oraz egzystencjalną[27].

„Bezpieczeństwo jest rozumiane, jako pewność, którą powinien mieć każdy członek społeczeństwa, mając uczucie, że pod ochroną prawa może dysponować swoją osobą i posiadanymi dobrami"[28].

W Słowniku terminów z zakresu bezpieczeństwa narodowego przedstawiono wiele pojęć związanych z bezpieczeństwem i obronnością. Wśród nich odnaleźć można definicję mówiącą, że „bezpieczeństwo państwa, to taki rzeczywisty stan stabilności wewnętrznej i suwerenności państwa, który odzwierciedla brak lub występowanie jakichkolwiek zagrożeń w sensie zaspokojenia podstawowych potrzeb egzystencjalnych i behawioralnych społeczeństwa oraz traktowania państwa, jako suwerennego podmiotu w stosunkach międzynarodowych"[29].

---

[25] J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] P. Tyrała (red.), *Zarządzanie bezpieczeństwem*, Kraków 2000, s. 46.

[26] D. Dudek, *Bezpieczeństwo Rzeczypospolitej jako wartość konstytucyjna*, [w]: L. Antonowicz, T. Guz, M. R. Pałubska (red.), *Bezpieczeństwo Polski. Historia i współczesność*, KUL, Lublin 2010, s. 167.

[27] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Adam Marszałek, Toruń 2005, s. 14.

[28] R. Rosa, *Filozofia bezpieczeństwa*, Bellona, Warszawa 1995, s. 126.

[29] J. Pawłowski, *Słownik terminów z zakresu bezpieczeństwa narodowego,* Warszawa 2002, s. 10.

Nauki społeczne definiują „bezpieczeństwo", jako zaspokajanie potrzeb typu: „posiadanie, przetrwanie, całość, tożsamość (identyczność), niezależność, spokój, posiadanie i pewność rozwoju"[30]. „Bezpieczeństwo" będąc naczelną potrzebą człowieka i różnych grup społecznych, jest jednocześnie podstawową potrzebą państw i systemów międzynarodowych. Jego brak wywołuje niepokój oraz poczucie zagrożenia[31].

Według J. Stańczyka „bezpieczeństwo" jest wartością, którą można rozmaicie rozumieć i w różnym stopniu określić jej rolę we współczesnym świecie. Jest ona nieodłączną częścią zbioru wartości cenionych zarówno przez indywidualnego człowieka, jak i naród oraz szeroko rozumianą społeczność międzynarodową[32]. J. Kukułka definiuje „bezpieczeństwo", jako przetrwanie państwa zachowującego integralność terytorialną oraz niezależność polityczną[33].

Nie ulega wątpliwości, że pojęcie „bezpieczeństwa" prze cały czas się zmienia, a jego ewoluowanie zależy od konkretnych warunków panujących w wybranym państwie cz też regionie. Interesy bezpieczeństwa powszechnego w wymiarze globalnym nie zawsze pokrywają się z poczuciem bezpieczeństwa wybranego kraju.

1.2. EWOLUCJA POJĘCIA

Zmiany uwarunkowań geopolitycznych na świecie spowodowały, że definiowanie pojęcia „bezpieczeństwo" ulega zmianom. Przestało już ono dotyczyć tylko kwestii związanych z naruszeniem integralności terytorialnej państwa, ale zaczęto również brać pod uwagę szeroki zakres problemów począwszy od stabilności ekonomicznej a skończywszy na degradacji środowiska naturalnego człowieka.

W obliczu współczesnych konfliktów, pojmowanie definicji „bezpieczeństwa" nadal ewoluuje. Kiedyś pojęcie to odnosiło się głównie do obrony terytorium przed zewnętrznym atakiem, natomiast dzisiaj

[30] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje-struktury-funkcjonowanie*, Scholar, Warszawa 1999, s. 27.
[31] R. Zięba, *Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych*, Sprawy międzynarodowe, 1989, s. 50.
[32] J. Stańczyk, *Współczesne …, dz.* cyt., s. 9.
[33] J. Kukułka, *Bezpieczeństwo a współpraca europejska: współzależności i sprzeczności interesów. Sprawy międzynarodowe,* Warszawa 1982, nr 7, s. 34.

przekształciło się w konieczność zapewnienia ochrony osób i społeczności także przed przemocą wewnętrzną[34].

Wyraźnie widać, że postrzeganie pojęcia pokoju i bezpieczeństwa ulega poszerzeniu. Pokój oznacza dużo więcej niż brak wojny, natomiast bezpieczeństwo przestaje być rozumiane przez ludzi tylko w kategoriach czysto wojskowych. Wymaga się, aby bezpieczeństwo zapewniało warunki do rozwoju gospodarczego, sprawiedliwości społecznej, ochrony środowiska, demokratyzacji, rozbrojenia, a także poszanowania praw człowieka i państwa.

Bezpieczeństwo, w jego najszerszym znaczeniu, obejmuje znacznie więcej niż brak konfliktów. Obejmuje ono poszanowanie praw człowieka, dobre zarządzanie, dostęp do edukacji i opieki zdrowotnej oraz zapewnienie każdej osobie możliwości do rozwoju osobowości. Każdy krok w tym kierunku powinien zmierzać do zmniejszenia ubóstwa, osiągnięcia wzrostu gospodarczego i zapobiegania konfliktom.

Zniesienie biedy, uwolnienie od zagrożeń i zapewnienie przyszłym pokoleniom zdrowego środowiska naturalnego są najważniejszymi elementami w procesie budowy bezpieczeństwa międzynarodowego.

Utrzymanie oraz utrwalanie bezpieczeństwa wymaga:

- zapewnienia wszystkim obywatelom warunków do życia w pokoju w granicach własnego państwa (oznacza to konieczność zapobiegania konfliktom i rozwiązywania spornych sytuacji z wykorzystaniem środków pokojowych i bez użycia przemocy, a w wypadku zajścia konfliktu doprowadzenie do jak najszybszego pojednania),
- zapewnienie warunków do korzystania bez dyskryminacji ze wszystkich praw i obowiązków w danym państwie (praw człowieka, praw politycznych, praw społecznych, praw gospodarczych),
- zapewnienie równego dostępu do prowadzenia działalności społecznej, politycznej i ekonomicznej,
- zapewnienie rządów prawa oraz niezależności sądownictwa.

Problematykę bezpieczeństwa w ujęciu międzynarodowym należy rozpatrywać w dwóch aspektach. Pierwszy z nich dotyczy

[34] United Nations Secretary-General Kofi Annan, *Millenium Report*, Chapter 3, s. 43-44, (*www.un.org/millennium/sg/report*).

ochrony społeczeństw przed typowymi zagrożeniami takimi jak głód, choroby oraz represje. Natomiast drugi aspekt związany jest z ochroną przed nagłymi i nieuchronnymi zagrożeniami niosącymi dotkliwe skutki dla gospodarstw domowych, gospodarki oraz społeczeństwa. Wśród tych zagrożeń znajduję się również zagrożenie identyfikowane w procesie zarządzania kryzysowego oraz odnoszące się do infrastruktury krytycznej.

Na przełomie lat 40. i 50. uważano, że idea bezpieczeństwa międzynarodowego wyraża właściwe każdemu narodowi i każdemu państwu pragnienie zabezpieczenia przed agresją militarną i opiera się na posiadanej przez państwo pewności, że nie zostanie zaatakowane lub, że w przypadku ataku otrzyma natychmiastową i skuteczną pomoc ze strony innych państwa. W tym rozumieniu głównym środkiem zapewnienia bezpieczeństwa była siła wojskowa. Stopień tak rozumianego bezpieczeństwa zależał od wielkości możliwych zagrożeń i zakresu gwarancji otrzymanej przez dane państwo. Bezpieczeństwo było wówczas pojmowane, jako zewnętrzne, a więc międzynarodowe zapewnienie państwu wolności od zagrożeń, strachu i ataku. Natomiast jego prawno-międzynarodowym odzwierciedleniem był stopień zorganizowania się społeczności międzynarodowej. Ten ostatni aspekt zachowuje swą aktualność, jako jeden z istotnych czynników bezpieczeństwa zarówno w wymiarze międzynarodowym, jak i wewnętrznym[35].

Przełomowym momentem w postrzeganiu bezpieczeństwa był z pewnością rozpad dwubiegunowego świata. Od tego momentu główne źródło zagrożeń bezpieczeństwa, czyli konflikt pomiędzy supermocarstwami straciło na ważności. Bezpieczeństwo państwa zaczęto traktować holistycznie ze względu na internacjonalizację zagrożeń. Takim poglądom sprzyjało dynamiczne rozprzestrzenianie się zagrożeń związanych z handlem bronią i narkotykami, przestępczość zorganizowana, korupcja, nielegalna imigracja oraz terroryzm. Zagrożenia te stały się globalne i wspólne dla wielu państw. Na płaszczyźnie międzynarodowej podejmowane są działania, które umacniając bezpieczeństwo jednego państwa, służą również bezpieczeństwu innych. Bezsprzecznie istotnym wydarzeniem, które

[35] M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wyd. AP, Siedlce 2009, s. 27-28.

wpłynęło na takie pojmowanie bezpieczeństwa był atak na World Trade Center (11 września 2001), zamachy w Madrycie (11 marca 2004) oraz zamachy w Londynie (7 lipca 2005).

1.3. BEZPIECZEŃSTWO JAKO PROCES I JAKO STAN

Przeprowadzona analiza definicji pojęcia „bezpieczeństwo" pokazała dualny jego charakter. Bezpieczeństwo może być rozpatrywane jako stan spokoju, pewności, wolności od zagrożeń, strachu lub ataku oraz jako losowy proces, w którym stan bezpieczeństwa i jego organizacja podlegają permanentnym, dynamicznym zmianom stosownie do zewnętrznych oddziaływań i uwarunkowań. Bezpieczeństwo jako proces oznacza ciąg działań wykonywanych przez jednostki, społeczności lokalne, państwa, organizacje międzynarodowe w celu tworzeniu pożądanego stanu bezpieczeństwa.

Biorąc pod uwagę fakt, że bezpieczeństwo jest funkcją zagrożeń, a spektrum potencjalnych zagrożeń jest praktycznie nieskończone, bardziej adekwatna definicja bezpieczeństwa powinna orzekać, że bezpieczeństwo jest stanem, w którym poziom realnych zagrożeń jest akceptowalny i znajduje się pod kontrolą. W tym sensie można mówić o procesie zarządzania bezpieczeństwem, jako działalności polegającej na osiąganiu pożądanych stanów według określonych zasad i kryteriów sterowania[36].

Określony stan względnego bezpieczeństwa jest chwilowym, zmiennym stanem osiąganym na wyjściu procesu. Oddziaływanie i presja czynników zewnętrznych powoduje, że stan ten nie może być utrzymywany przez długi czas. Wytrącenie systemu z pożądanego stanu bezpieczeństwa może być powodowane nie tylko przez czynniki przypadkowe i niezamierzone, ale również przez celowe działanie oraz osiąganie pewnych kompromisów pomiędzy innymi systemami.

Prowadząc rozważania nad bezpieczeństwem w systemowych kategoriach prakseologicznych dochodzi się do wniosku, że pożądany stan bezpieczeństwa to stan, który gwarantuje realizację głównego celu działania danego systemu. Stan ten zapewnia warunki do realizacji przyjętych planów i założonej strategii rozwojowej systemu. Utrzymanie

[36] K. Ficoń, *Bezpieczeństwo…*, *dz. cyt.*

tego stanu jak najdłużej wymaga akceptacji zidentyfikowanych i realnych zagrożeń systemowych oraz ciągłego ich monitorowania i przeciwdziałania. Osiągnięty w ten sposób stan bezpieczeństwa daje gwarancje niezmienności w danej chwili oraz swobodnego i planowanego rozwoju w realnie zakreślonej przyszłości.

Zapewnienie przetrwania i gwarancje rozwoju systemu są niezbędne do racjonalnej strategii kształtowania bezpieczeństwa, której podstawą wyjściową jest akceptowany poziom i poczucie bezpieczeństwa. Docelowa wizja rozwoju zgodnie z własnymi planami reprezentuje składową dynamiczną zmienną w czasie, natomiast aktualny stan to składowa statyczna procesu bezpieczeństwa, akceptowana wartość.

S. Koziej twierdzi, iż rozpatrując bezpieczeństwo jako proces, którego celem działania jest zapewnienie poczucia braku zagrożeń danego podmiotu, można stwierdzić, iż jest to ciąg działań realizowanych przez podmiot, których celem jest zapewnianie możliwości przetrwania i swobody realizacji własnych interesów przez system w dynamicznie zmieniającym się otoczeniu, w szczególności poprzez wykorzystywanie szans, stawianie czoła wyzwaniom, redukowanie ryzyka oraz przeciwdziałanie zagrożeniom dla podmiotu[37]. Przyjmuje się, że podmiotem bezpieczeństwa mogą być wszystkie jednostki mające własne interesy i wyrażające ambicje realizacji tych interesów. Zalicza się do nich pojedyncze osoby, różne grupy społeczne, narody, społeczności międzynarodowe i całą ludzkość.

Losowość i niepewność procesu bezpieczeństwa jest wskazywana przez K. Ficonia[38]. Na poziom bezpieczeństwa oddziałuje zbyt dużo czynników, zmiennych i zakłóceń, aby można było w porę wszystkie eliminować i skutecznie redukować ich negatywne skutki i konsekwencje. Uważa on również, że spektrum rozmaitych zmiennych, zagrożeń i zakłóceń jest praktycznie nieskończone, a jego źródłem jest przede wszystkim dalsze i bliższe otocznie zewnętrzne i w mniejszym stopniu otoczenie wewnętrzne badanego systemu czy podmiotu. Dlatego niepewność i losowość są permanentnymi cechami każdej rzeczywistości, każdego bytu czy też każdego wielkiego systemu.

---

[37] S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Kwartalnik bezpieczeństwo Narodowe, Nr 18, BBN, Warszawa 2011, s. 20.

[38] K. Ficoń, *Wykorzystanie funkcji potęgowo-wykładniczej w procesie zarządzania bezpieczeństwem*, ZN AMW, Nr 1, AMW, Gdynia 2009, s. 34.

W swoim opracowaniu K. Ficoń posłużył się pojęciem zdarzenie w celu uściślenia pojęcia bezpieczeństwa jako procesu. Zbiór zdarzeń został podzielony rozłącznie na zdarzenia korzystne (pozytywne), zdarzenia niekorzystne (negatywne) oraz zdarzenia obojętne (neutralne), które nie wpływają na poziom bezpieczeństwa. Zdarzenia korzystne zwiększają poziom bezpieczeństwa, a niekorzystne obniżają ten poziom, aż do pewnego krytycznego stanu, zwanego kryzysem, który w zależności od rozpatrywanej dziedziny może przekształcić się przykładowo w awarię, rozruchy, klęskę, katastrofę, kataklizm czy wojnę. Wykorzystując pojęcie zdarzenia, została zaproponowana definicja bezpieczeństwa mówiąca o tym, że bezpieczeństwo jako proces losowy jest sumą (superpozycją, funkcją) pewnych zdarzeń losowych, zarówno korzystnych, jak i niekorzystnych, co symbolicznie przedstawia następujące wyrażenie (1.1):

$$B = f(Z_K, Z_N, Z_U, V) \tag{1.1}$$

gdzie:

B – kategoria (stan) bezpieczeństwa,
Z_K – zbiór zdarzeń korzystnych, zwiększających stan bezpieczeństwa,
Z_N – zbiór zdarzeń niekorzystnych, zmniejszających stan bezpieczeństwa,
Z_U – zbiór zdarzeń neutralnych bez wpływu na stan bezpieczeństwa,
V – akceptowany (dopuszczalny) poziom zdarzeń niekorzystnych, które nie zmieniają stanu bezpieczeństwa w stan niebezpieczeństwa.

1.4. TYPOLOGIA BEZPIECZEŃSTWA

Ewolucja pojęcia „bezpieczeństwa", zmiana interpretacji oraz jego dualny charakter spowodowały, że odnosi się ono do wielu dziedzin naszego życia np. społecznego, gospodarczego, politycznego. Bezpieczeństwo jest także przedmiotem badań naukowych i projektów wdrożeniowych w takich dyscyplinach naukowych jak: nauki o bezpieczeństwie, nauki o obronności, filozofia, politologia, stosunki międzynarodowe, ekonomia, ekologia, socjologia, psychologia, prawo.

Rys. 1.1. Ogólna klasyfikacja bezpieczeństwa

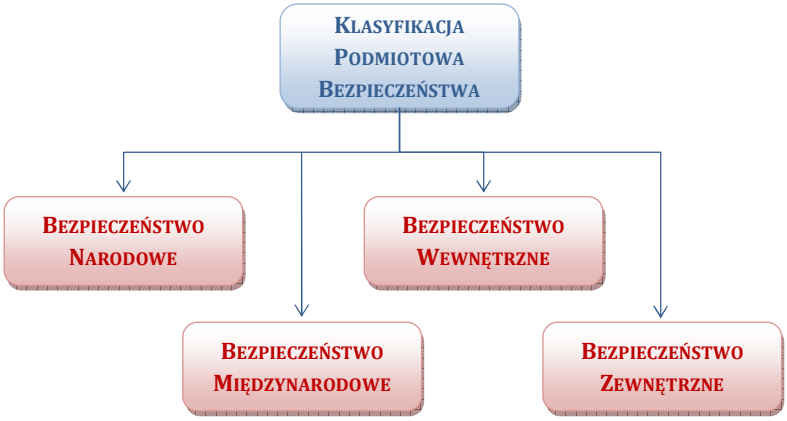
Powszechność bezpieczeństwa, zarówno w wymiarze praktycznym jak i teoretycznym powoduje, że mamy do czynienia z wieloma klasyfikacjami stosowanymi wg różnych kryteriów. Najczęściej można spotkać się z podziałem ze względu na aspekt bezpieczeństwa (Rys. 1.1)[39]:

- podmiotowy (bezpieczeństwo narodowe i bezpieczeństwo międzynarodowe),
- przedmiotowy (bezpieczeństwo polityczne, wojskowe, gospodarcze, społeczne, kulturowe, ideologiczne, ekologiczne, informacyjne itd.),
- przestrzenny (bezpieczeństwo personalne (dotyczące indywidualnych ludzi - osób), lokalne (państwowo-narodowe), subregionalne, regionalne (koalicyjne), ponadregionalne i globalne (uniwersalne)).

W klasyfikacji podmiotowej brane są pod uwagę zależności bezpieczeństwa od podmiotu, którego żywotne interesy są chronione przed zagrożeniami wewnętrznymi i zewnętrznymi (Rys. 1.2). Prowadzi to do podziału na bezpieczeństwo narodowe (państwowe) i międzynarodowe, które może być kształtowane w dwóch obszarach:

- wewnętrznym (bezpieczeństwo wewnętrzne) – dotyczy zapewniania stabilności wewnętrznej podmiotu bezpieczeństwa,
- zewnętrznym (bezpieczeństwo zewnętrzne) – dotyczy przeciwdziałania zagrożeniom zewnętrznym.

[39] K. Malak, *Typologia bezpieczeństwa. Nowe wyzwania*, stosunki-miedzynarodowe.pl/bezpieczenstwo/954-typologia-bezpieczenstwa-nowe-wyzwania, [10.2012].



Rys. 1.2. Klasyfikacja podmiotowa bezpieczeństwa

Podstawę podziału podmiotowego stanowią granice terytorialne – państwowe, kontynentalne, sojusznicze, środowiskowe i granice innych podmiotów bezpieczeństwa. W warunkach globalizacji i internacjonalizacji większości sfer życia społecznego, granica między bezpieczeństwem wewnętrznym i zewnętrznym jest rozmyta, a wiele zagrożeń, takich jak, np. terroryzm międzynarodowy, narkotyki, katastrofy naturalne i ekologiczne, zagrożenia infrastruktury krytycznej, zagrożenia z cyberprzestrzeni niekiedy trudno dowiązać do wyraźnie określonego źródła.

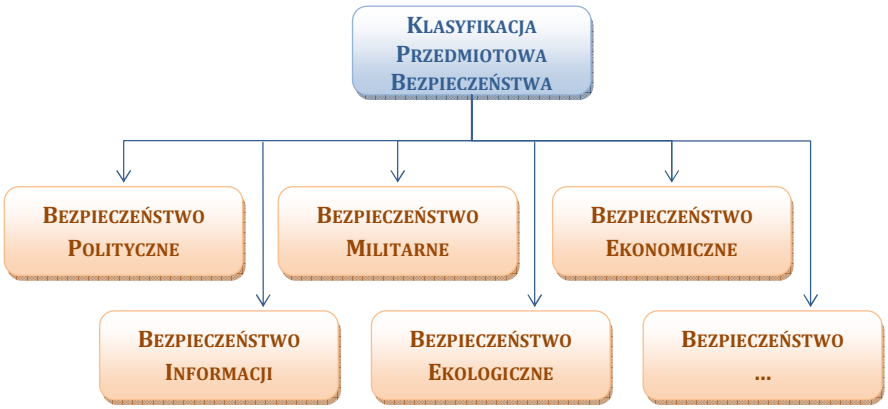
Bezpieczeństwo narodowe[40] w znaczeniu funkcjonalnym jest naczelną misją narodową całego społeczeństwa i jego organizacji państwowej, polegającą na stałej realizacji dwóch współzależnych funkcji, pierwszej podstawowej: ochrony i obrony wartości i interesów narodowych przed istniejącymi lub potencjalnymi zagrożeniami zapewniającej warunki konieczne do realizacji drugiej funkcji: tworzenia wewnętrznych i zewnętrznych warunków dla swobodnego rozwoju i sprostania wyzwaniom, jakie niesie dla narodu zmienność, nieprzewidywalność i postęp cywilizacyjny. W znaczeniu strukturalnym (systemowym) – bezpieczeństwo narodowe to całokształt przygotowania i organizacji państwa dla ciągłego tworzenia bezpieczeństwa narodowego, obejmujący następujące podstawowe elementy:

– prawne podstawy bezpieczeństwa,

[40] T. Szubrycht (red.), *Leksykon …*, *dz. cyt.*, s. 21.

- politykę i strategie bezpieczeństwa narodowego,
- cywilną i wojskową organizację ochrony i obrony narodowej,
- infrastrukturę bezpieczeństwa,
- edukację dla bezpieczeństwa,
- sojusze i współpracę międzynarodową w zakresie bezpieczeństwa.

Bezpieczeństwo międzynarodowe w zakresie przedmiotowym obejmuje zespół uwarunkowań, w których państwa nie czują się zagrożone atakiem militarnym oraz presją polityczną lub gospodarczą, mając możliwości swobodnej realizacji własnego rozwoju i postępu[41].



Rys. 1.3. Klasyfikacja przedmiotowa bezpieczeństwa

Klasyfikacja przedmiotowa oparta jest na żywotnych interesach obiektów bezpieczeństwa, które mogą znajdować się pod wpływ różnych zagrożeń. Według tej zasady klasyfikujemy żywotne interesy, zagrożenia i kierunki zapewniania bezpieczeństwa. Przez bezpieczeństwo rozpatrywane przedmiotowo rozumie się ochronę żywotnych interesów jednostki, społeczeństwa i państwa oraz innych podmiotów bezpieczeństwa celem zapewnienia możliwości skutecznego działania we wskazanej sferze działalności ludzkiej, przed zagrożeniami wewnętrznymi i zewnętrznymi[42]. Do najczęściej spotkanych typów bezpieczeństwa przedmiotowego należą (Rys. 1.3):

- bezpieczeństwo polityczne,
- bezpieczeństwo informacji,

[41] *Tamże*, s. 19.
[42] K. Ficoń, *Bezpieczeństwo..., dz. cyt.*, s. 11.

- bezpieczeństwo militarne,
- bezpieczeństwo ekologiczne,
- bezpieczeństwo ekonomiczne.

Bezpieczeństwo polityczne traktowane, jako proces obejmuje szereg działań podejmowanych w celu zapewnienia trwałości i rozwoju systemu politycznego wybranego państwa bądź grupy państw, stabilności społecznej oraz ustrojowej i wewnętrznej państw oraz organizacji państw. Utrzymanie suwerenności wewnętrznej, związanej z rzeczywistą kontrolą określonego terytorium przez legalne władze podmiotu polityki. Bezpieczeństwo polityczne dotyczy przede wszystkim poziomu państwa, ale także poziomu systemu międzynarodowego oraz jednostki (prawa człowieka).

Bezpieczeństwo informacji obejmuje ochronę informacji przed nieupoważnionym rozpowszechnianiem, przekazywaniem, wprowadzaniem zmian lub zniszczeniem zarówno przypadkowym, jak i zamierzonym. Zapewnienie bezpieczeństwa informacji nie ogranicza się jedynie do systemów komputerowych ani informacji znajdujących się w urządzeniach elektronicznych. Odnosi się do wszystkich rodzajów zabezpieczeń lub ochrony informacji przed nieautoryzowanym dostępem do nich. Zapewnienie bezpieczeństwa informacji jest różne ze względu na stopień jej ważności[43].

Bezpieczeństwo militarne to stan uzyskany w rezultacie utrzymywania odpowiednio zorganizowanych i wyposażonych sił zbrojnych oraz zawarcia sojuszów wojskowych, a także posiadania koncepcji strategicznej wykorzystania będących w dyspozycji sił, stosowanie do zaistniałej sytuacji[44].

Bezpieczeństwo ekologiczne określa stan biosfery, w którym wzajemne relacje pomiędzy działalnością populacji ludzkiej a środowiskiem naturalnym nie prowadzą do powstania zagrożeń dla zdrowej egzystencji człowieka, jako jednostki i populacji, jako całości. […] Pojęcie bezpieczeństwa ekologicznego może posiadać wymiar:

- globalny, czyli obejmujący problemy mające znaczenie dla całej ludzkości, jak np. emisja gazów cieplarnianych albo rabunkowa eksploatacja lasów tropikalnych,

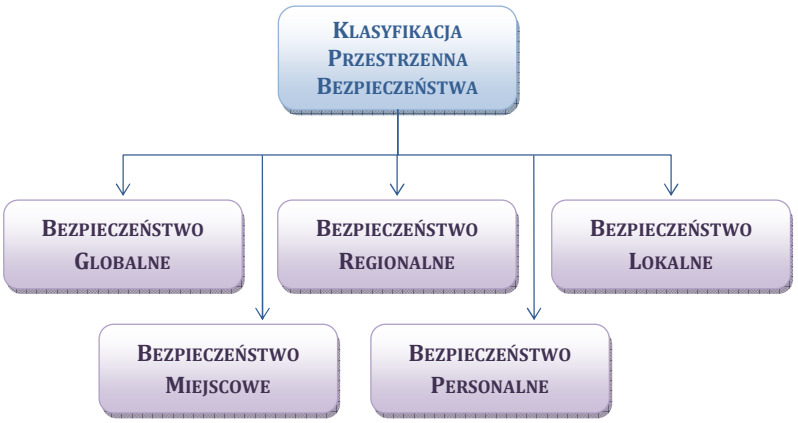
[43] H. Sołkiewicz (red.), *Operacyjno-taktyczny …*, *dz. cyt.*, s. 84.
[44] T. Szubrycht (red.), *Leksykon …*, *dz. cyt.*, s. 24.

- regionalny, czyli obejmujący kwestia mające znaczenie w mniejszym obszarze geograficznym, jak np. w basenie Morza Bałtyckiego,
- lokalny, a więc obejmujący zagadnienia o znaczeniu dla poszczególnych społeczności lokalnych, jak np. bezpieczeństwo ekologiczne Zatoki Gdańskiej, czy jeszcze o mniejszym wymiarze geograficznym, jak np. bezpieczeństwo ekologiczne rejonu samej Zatoki Puckiej.

Bezpieczeństwo ekonomiczne państwa to taki stan rozwoju krajowego systemu gospodarczego, który zapewnia wysoką sprawność jego funkcjonowania - poprzez należyte wykorzystanie wewnętrznych czynników rozwoju – oraz zdolność do skutecznego przeciwstawienia się zewnętrznym naciskom, mogącym doprowadzić do zaburzeń rozwojowych[45].

Kryterium przestrzenne dzieli bezpieczeństwo na (Rys. 1.4):

- globalne (uniwersalne),
- regionalne,
- lokalne,
- miejscowe,
- personalne (dotyczące indywidualnych osób).



Rys. 1.4. Klasyfikacja przestrzenna bezpieczeństwa

[45] Z. Stachowiak, *Bezpieczeństwo ekonomiczne*, [w:] W. Stankiewicz, (red.), *Ekonomika obrony,* AON, Warszawa 1994, s. 189.

Bezpieczeństwo globalne wyraża zdolność zapewnienia stabilnego rozwoju cywilizacji światowej, przeciwdziałania i zapobiegania katastrofom naturalnym w wymiarze globalnym oraz ochronę systemu wzajemnych relacji społeczności światowej przed destabilizacją, kryzysami, konfliktami zbrojnymi i wojnami. Uogólniając można przyjąć, że bezpieczeństwo globalne polega na zapobieganiu, przeciwdziałaniu, zwalczaniu i likwidacji zagrożeń dla żywotnych interesów całego świata traktowanego, jako jedność i całość.

Bezpieczeństwo regionalne dotyczy ochrony systemu stosunków wzajemnych państw regionu przed zagrożeniami destabilizacji sytuacji, kryzysami, konfliktami zbrojnymi i wojnami o charakterze regionalnym. Podstawą budowania bezpieczeństwa regionalnego jest układ działający w obrębie wybranego regionu świata (Europa, Azja, Ameryka Łacińska, Azja Południowo-Wschodnia).

Bezpieczeństwo lokalne uwzględnia lokalną specyfikę zagrożeń oraz metod i środków przeciwdziałania, szczególnie w zakresie zagrożeń ekologicznych i katastrof naturalnych. Coraz większe znaczenie ma kształtowanie lokalnego kompleksu bezpieczeństwa obejmującego część państwa i społecznej wspólnoty, na danym terytorium. Bezpieczeństwo lokalne polega na ochronie żywotnych oraz ważnych interesów lokalnej wspólnoty społecznej i lokalnych instytucji bezpieczeństwa przed zagrożeniami wewnętrznymi i zewnętrznymi, a także zapewnienie warunków dla realizacji tych interesów.

Bezpieczeństwo miejscowe obejmuje problemy bezpieczeństwa wielkich miast, dzielnic, powiatów i gmin, tzn. jednostek administracyjnych mających status samorządowy. Jednostkom administracyjnym zagrażają charakterystyczne, w dużej części tylko dla nich, zagrożenia dla żywotnych interesów jednostki i wspólnoty społecznej, takie jak, np.: bezrobocie, brak niezbędnej infrastruktury społecznej i bytowej, ograniczona dostępność opieki lekarskiej i innych usług, niski poziom komunikacji, oddalenie od duchowych źródeł kultury itd.

Ostatnim typem bezpieczeństwa wyróżnianym ze względu na kryterium przestrzenne jest bezpieczeństwo personalne, dotyczące bezpośrednio lub pośrednio każdego mieszkańca, każdej osoby. Istotą tego rodzaju bezpieczeństwa jest ochrona i zapewnienie żywotnych i ważnych interesów życiowych i społecznych jednostki przed zagrożeniami wewnętrznymi i zewnętrznymi.

1.5. ZAGROŻENIA BEZPIECZEŃSTWA

Najbardziej podstawowa definicja bezpieczeństwa mówi, że jest to stan pewności, spokoju i braku zagrożenia. Na podstawie tej definicji możemy wyciągnąć wniosek, że z pojęciem „bezpieczeństwo" ściśle związane jest pojęcie „zagrożenie".

Zagrożenie to z jednej strony pewien stan psychiczny lub świadomościowy wywołany postrzeganiem zjawisk, które subiektywnie ocenia się, jako niekorzystne lub niebezpieczne, a z drugiej jako czynnik obiektywny powodujący stany niepewności i obaw[46]. Zagrożenie to również sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia.

Przyjmując za podstawę dziedziny, w których może wystąpić zagrożenie, wyróżnia się zagrożenia militarne i niemilitarne. Wśród zagrożeń niemilitarnych można z kolei wyróżnić zagrożenia polityczne, zagrożenia gospodarcze, zagrożenia psychospołeczne, zagrożenia ekologiczne, zagrożenia wewnętrzne i inne.

W prowadzonym procesie badawczym istotną definicją będzie również definicja zagrożenia bezpieczeństwa państwa w myśl, której jest to splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju wewnętrznego bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej, itp.[47]

Podmiotowy charakter bezpieczeństwa powoduje, że jest ono naczelną potrzebą człowieka, grup społecznych oraz państwa. Każdy podmiot stara się więc oddziaływać na swoje otoczenie zewnętrzne i sferę wewnętrzną tak, aby usuwać, łagodzić lub oddalać wszelkie zagrożenia.

Rozwój cywilizacyjny, zmiany geopolityczne na świecie oraz degradacja środowiska naturalnego człowieka powodują, że zbiór zagrożeń jest praktycznie nieograniczony. Dużo problemów stwarza ich

[46] T. Szubrycht (red.), *Leksykon …*, *dz. cyt.*, s. 187.
[47] Tamże, s. 187.

poprawna klasyfikacja. Do najczęściej używanych kryteriów klasyfikacji zagrożeń należą[48]:

- źródła oraz przyczyny powstania zagrożeń,
- podział rodzajowy zagrożeń i skala negatywnych następstw,
- prognozowany czas usuwania skutków i następstw zagrożeń,
- prognozowany obszar lub dziedzina oddziaływania zagrożeń,
- prognozowany zakres i skala następstw zagrożeń kryzysowych,
- determinizm i dynamika przyczyn wywołujących zagrożenia,
- prognozowany zasięg przestrzenny oddziaływania zagrożeń,
- potencjalne możliwości antycypacji i zwalczania skutków zagrożeń.

Przyjmując za kryterium klasyfikacji zagrożeń źródło ich generowania, otrzymujemy następujący podział:

- zagrożenia naturalne (Rys. 1.5),
- zagrożenia techniczne (Rys. 1.6),
- zagrożenia społeczne (Rys. 1.7).

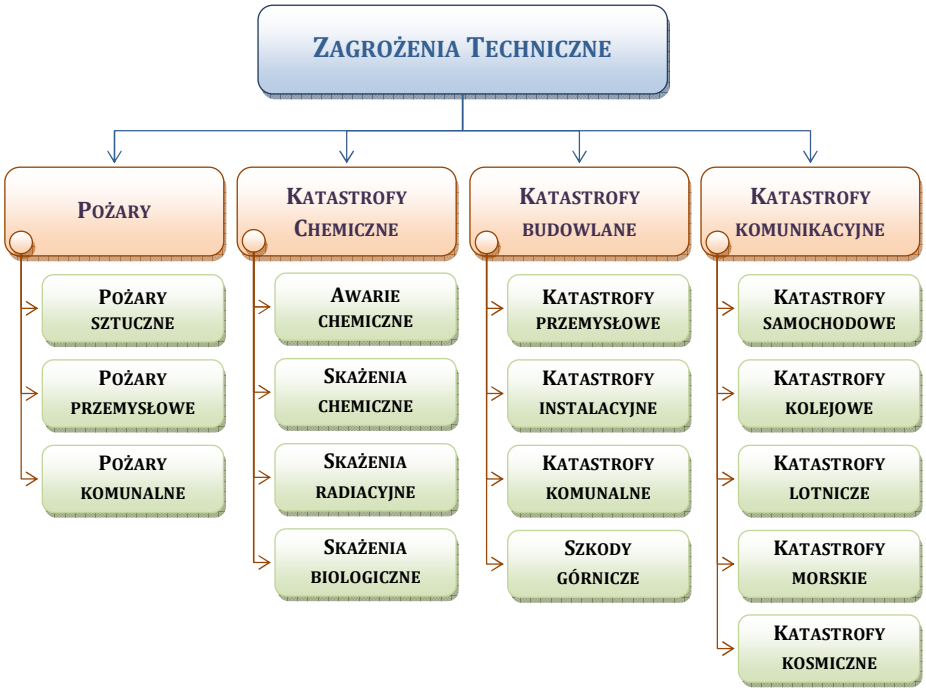
Wynikiem zagrożeń naturalnych są katastrofy naturalne powstające w wyniku obecności żywiołu (np. lawa wulkaniczna, wstrząs sejsmiczny, nadmiar wody – słodkiej lub słonej, lawina śnieżna lub błotna, upał, mróz, silny wiatr, ogień, uderzenie pioruna czy susza) na obszarze o istotnym potencjale strat – ludzkich lub ekonomicznych. Wystąpienie erupcji wulkanu czy trzęsienia ziemi na obszarach niezamieszkałych, na których człowiek nie inwestował (np. w linie kolejowe, szosy czy kopalnie) nie prowadzi do katastrofy naturalnej. Jednak w sytuacji, gdy ekstremum geofizyczne (np.: bardzo silny wiatr, bardzo wysoka lub bardzo niska temperatura, niszczący nadmiar albo długotrwały brak wody) wystąpi na gęsto zaludnionym obszarze o znacznej podatności na zagrożenia, straty są nieuniknione[49].

[48] K. Ficoń, *Inżynieria …*, *dz. cyt.*, s. 76.
[49] Z. W. Kundzewicz, P. Matczak, *Zagrożenia naturalnymi zdarzeniami ekstremalnymi*, Nauka Nr 4, Warszawa 2010, s. 77.

Rys. 1.5. Klasyfikacja zagrożeń naturalnych

Zagrożenia techniczne związane są przede wszystkim z działalnością gospodarczą człowieka, a ściśle z postępem naukowo-technicznym i stopniem zaawansowania cywilizacyjnego społeczeństwa. Są one konsekwencją wysokiego stopnia opanowania przez człowieka praw przyrody i rozwiniętej cywilizacji technicznej. Gwałtowna ingerencja człowieka w naturalne środowisko przyrodnicze powoduje, że następuje zachwianie naturalnych zasad i praw ewolucji i rozwoju, co początkowo uaktywnia mechanizmy obronne środowiska przyrodniczego, lecz w skrajnych przypadkach następuje eliminacja wszelkich mechanizmów obronnych i samozachowawczych „skutecznie" porażonej przyrody. W efekcie prowadzi to do załamania się linii

ewolucyjnych całych gatunków przyrodniczych włącznie z krajobrazami i bezpieczeństwem naturalnej egzystencji człowieka[50].

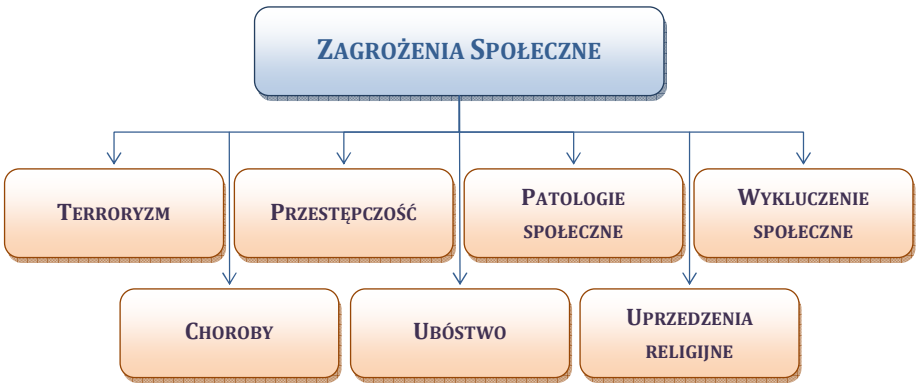


Rys. 1.6. Klasyfikacja zagrożeń technicznych

Zagrożenia społeczne należą do tej kategorii zagrożeń, których źródłem i sprawcą, a najczęściej także ofiarą jest człowiek i społeczeństwo znajdujące się w określonym stadium niezadowolenia społecznego, socjalnego, ekonomicznego, politycznego czy kulturalno-obyczajowego lub religijnego. W społeczeństwach demokratycznych powszechną formą okazywania wszelkiego niezadowolenia (rzadziej akceptacji) są masowe zgromadzenia ludności, manifestacje uliczne i różnego rodzaju przejawy niepokojów społecznych czy politycznych. Niepokoje społeczne mogą polegać na organizowaniu masowych zgromadzeń i różnych form strajków, demonstracji i rozruchów ulicznych oraz mniej lub bardziej zorganizowanych masowych akcji okazywania niezadowolenia społecznego i artykułowania określonych żądań, głównie pod adresem władzy i jej klasy politycznej. Nową i bardzo groźną kategorią zagrożeń stały się w ostatnich czasach zagrożenia

[50] K. Ficoń, *Inżynieria ..., dz. cyt.*, s. 90.

społeczne, których najbardziej spektakularnym rodzajem jest terroryzm międzynarodowy, funkcjonujący w wielu różnych odmianach i obliczach[51].



Rys. 1.7. Klasyfikacja zagrożeń społecznych

Poprawna identyfikacja i analiza zagrożeń jest kluczowym działaniem w procesie zarządzania bezpieczeństwem infrastruktury krytycznej państwa. Opracowywane plany ochrony infrastruktury krytycznej zawierają charakterystykę zagrożeń dla infrastruktury krytycznej oraz ocenę ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń. Działania te realizowane są w fazie zapobiegania oraz przygotowania do zdarzeń kryzysowych w odniesieniu do obiektów, systemów, usług oraz urządzeń infrastruktury krytycznej.

Ostatnie wydarzenia pokazują, że elementy infrastruktury krytycznej mogą być zniszczone lub uszkodzone, co prowadzi do zakłócenia ich funkcjonowania na poziomie właściciela, regionalnym czy też państwowym. Takie sytuacje mogą nieść ze sobą dalekosiężne skutki społeczne i gospodarcze.

Identyfikując zagrożenia infrastruktury krytycznej należy przede wszystkim wziąć pod uwagę zjawiska naturalne, awarie techniczne, błędy ludzkie oraz zamierzone działania człowieka.

Właściciele infrastruktury krytycznej muszą być świadomi tych zagrożeń i powinni prowadzić wszelkie możliwe działania mające na

[51] *Tamże*, s. 97.

celu przygotowanie się do reagowania w sytuacjach kryzysowych, poprzez ocenę ryzyka i redukowanie go tak dalece jak to możliwe.

W dobie rozwoju społeczeństwa informacyjnego do rangi najpoważniejszego zagrożenia infrastruktury krytycznej urastają zagrożenia z cyberprzestrzeni. Bardzo często zwykli ludzie, właściciele firm, korporacji, decydenci nie zdają sobie sprawy z tego, jak łatwo uzyskać dostęp do danych w postaci cyfrowej. Nawet jeśli szkody, wywołane ingerencją osób niepowołanych, zostaną naprawiane szybko a zasoby sieciowe zabezpieczone, nie daje to gwarancji całkowitego bezpieczeństwa. Sytuacja w każdej chwili może się powtórzyć, gdyż najbardziej wyszukane sposoby zabezpieczeń wraz z upływem czasu stają się przestarzałe. Pozornie zabezpieczony system może zostać zaatakowany przez włamywaczy, którzy zwykle nie muszą w tym celu używać wyrafinowanych narzędzi[52].

Do najczęściej wymienianych zagrożeń krytycznej infrastruktury teleinformatycznej należą:

- uszkodzenia i nieuprawnione modyfikacje łączy telekomunikacyjnych,
- niewłaściwa ochrona sesji zarządzania i konfiguracji elementów aktywnych sieci,
- brak świadomości i wiedzy w zakresie bezpieczeństwa teleinformatycznego wśród personelu, a przede wszystkim kadry zarządzającej,
- błędy i luki w oprogramowaniu,
- świadome wprowadzanie szkodliwego oprogramowania do systemów teleinformatycznych, nieuprawnione modyfikacje lub celowe uszkodzenia systemów operacyjnych lub oprogramowania aplikacyjnego (szczególnie systemów baz danych),
- nieuprawnione działania użytkowników lub administratorów, krótki czas „życia" technologii teleinformatycznych.

Znaczenie teleinformatycznej infrastruktury krytycznej we współczesnym świecie jest tak wielkie, że stała się ona bardzo wrażliwym elementem funkcjonalnym całego państwa. Szybkie tempo

[52] G. Krasnodębski, *Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego,* [w:] *Problemy zapewnienia bezpieczeństwa regionalnego*, Olsztyn 2008.

rozwoju technologii informacyjnych oraz produkcji oprogramowania spowodowało, że nie nadążano z rozwojem mechanizmów oraz procedur bezpieczeństwa. Obecnie jest to znaczący problem, który powoduje wielkie straty firm oraz instytucji państwowych. Kłopot również stanowi globalna sieć komputerowa, której tak intensywny rozwój trudny był do przewidzenia. Łączy ona ze sobą miliony komputerów stając się doskonałym środowiskiem do prowadzenia działalności przestępczej. Należy się również liczyć z tym, że w przyszłości nowoczesne armie będą coraz częściej wykorzystywać cyberprzestrzeń do prowadzenia działań mających na celu unieszkodliwienie infrastruktury krytycznej innych państw. Jedyną receptą na zmianę takiego stanu rzeczy jest konsekwentne i rygorystyczne prowadzenie polityki bezpieczeństwa teleinformatycznego w obszarze krajowym oraz międzynarodowym.

* * *

Badania prowadzone nad bezpieczeństwem pokazują, że jest ono pojmowane jednocześnie, jako wartość, potrzeba, cel, prawo, a także, jako pożądany stan i dynamiczny proces. Stanowi ono bardzo ważną wartość w sensie egzystencjalnym, moralnym, społecznym, a także osobistym.

Bezpieczeństwo rozpatrywane w kategoriach jakościowych może być postrzegane, jako zdeterminowany i pożądany stan mający wymiar, skalę trwałości, zasięg terytorialny, natomiast w kategoriach ilościowych, jako proces charakteryzujący się dużą zmiennością w czasie, polegający na ciągłym kształtowaniu i umacnianiu bezpieczeństwa.

Przeprowadzona analiza teorii bezpieczeństwa pozwoliła określić stan równowagi, do którego będzie dążył system zarządzania bezpieczeństwem infrastruktury krytycznej, aby zagwarantować określony standard ochrony kluczowych systemów państwa.

Badania pozwoliły zebrać niezbędne informacje do zrozumienia istoty i celu zarządzania kryzysowego, jako działalności prowadzonej dla zapewnienia stanu bezpieczeństwa w obliczu zagrożeń militarnych i niemilitarnych.

ROZDZIAŁ 2
INFRASTRUKTURA KRYTYCZNA W ZARZĄDZANIU KRYZYSOWYM

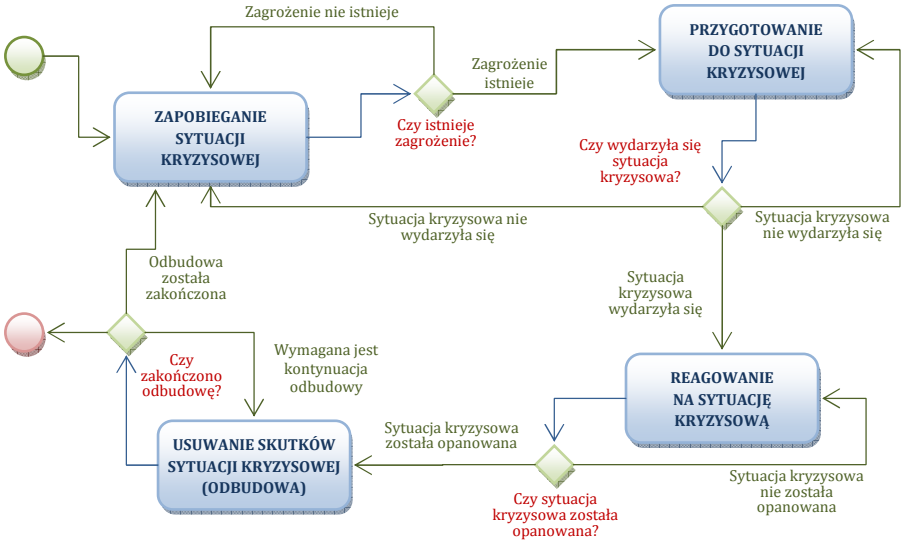
Definiowanie procesu zarządzania kryzysowego przez wiele lat budziło wiele kontrowersji oraz zastrzeżeń. Działalność ta była określana jako[53]: *zarządzanie w kryzysie, zarządzanie sytuacją kryzysową, zarządzanie w sytuacjach kryzysowych czy też sterowanie kryzysem*. Ujednolicenie poglądów w tej materii przyniosła *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[54], która wprowadziła jednolity zakres pojęciowy, zdefiniowała strukturę hierarchicznego systemu zarządzania kryzysowego oraz, co jest istotne z punktu wiedzenia prowadzonych badań, wprowadziła obowiązek ochrony infrastruktury krytycznej.

2.1. ISTOTA, CELE I ZADANIA ZARZĄDZANIA KRYZYSOWEGO

Zarządzanie kryzysowe *(crisis management)* to pojęcie, którego definicja została sformułowana w *Ustawie o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku*. Zgodnie z tą Ustawą *zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej*[55]. Przytoczona definicja uporządkowała i ujednoliciła w dużej mierze poglądy teoretyczne oraz podejście praktyczne do rozważanego problemu. Stworzona została podstawa do budowy hierarchicznego systemu

[53] J. Gryz, W. Kitler, *System…*, *dz. cyt.*, s. 27.
[54] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz. U. z 2007 r. Nr 89, poz. 590.
[55] *Tamże*.

zarządzania kryzysowego [56] realizującego ściśle określony proces (Rys. 2.1).



Rys. 2.1. Proces zarządzania kryzysowego

Wcześniejsze opracowania w różny sposób definiowały ten typ zarządzania i jak pisze W. Kitler, w swoich rozważaniach nad istotą zarządzania kryzysowego[57], można było napotkać w drodze badań tego problemu różne określenia odnoszące się do procesu zarządzania w fazie rodzenia się kryzysu, rozwoju kryzysu, przesilenia i powrotu do stabilności po kryzysie. Najczęściej spotykanymi były pojęcia: *zarządzanie w kryzysie, zarządzanie sytuacją kryzysową, zarządzanie w sytuacjach kryzysowych oraz sterowanie kryzysem.*

Przytoczone określenia oraz treść ich definicji wynikała z różnych sposobów podejścia do problemu. Poniżej zaprezentowano wybrane z literatury przedmiotu przykładowe definicje w chronologicznej kolejności ich publikacji.

Pierwszą z nich jest definicja zaproponowana przez R. Wróblewskiego mówiąca, że *zarządzanie sytuacją kryzysową* jest

[56] W *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* została również umieszczona definicja **sytuacji kryzysowej**, czyli sytuacji wpływającej negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującej znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.
[57] J. Gryz, W. Kitler, *System…*, *dz. cyt.*, s. 27.

procesem kierowania w państwie, mającym na celu zapobieganie sytuacjom kryzysowym, a w wypadku ich zaistnienia – zawrócenie kierunku rozwoju nagłych i niebezpiecznych wydarzeń, zagrażających żywotnym interesom społeczeństwa, a w szczególności mogącym doprowadzić do wojny[58].

Kolejną jest definicja przedstawiona w 1998 roku przez Komendę Główną Policji. Według niej *zarządzanie kryzysowe* to jeden z elementów kompleksu przedsięwzięć (planistycznych, organizacyjnych i logistycznych) mających na celu przygotowanie społeczeństwa i struktur państwa do skutecznego działania w warunkach nadzwyczajnych spowodowanych[59]:

- katastrofami naturalnymi lub awariami technicznymi, których skutki zagrażają życiu lub zdrowiu znacznej liczby ludzi (zagrożenia naturalne i technologiczne),
- zagrożeniami konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego (zagrożenia wewnętrznego bezpieczeństwa państwa),
- zewnętrznymi zagrożeniami bezpieczeństwa państwa (zagrożenia wojenne).

W opracowaniu D. Ladak i T. Pilcha z 1999 roku można znaleźć definicję mówiącą o tym, że *zarządzanie kryzysowe* to zespół przedsięwzięć organizacyjnych, logistycznych i finansowych, których celem jest zapobieganie powstawaniu sytuacji kryzysowych, zapewnienie sprawności struktur decyzyjnych na wszystkich szczeblach zarządzania, utrzymanie ciągłej gotowości sił i środków do podjęcia działań, sprawne reagowanie oraz likwidacje skutków zaistniałej sytuacji[60].

Nieco inną definicję przedstawił J. Konieczny w 2001 roku. Mówi ona, że *zarządzanie w sytuacji kryzysowej* to systematyczne i metodyczne przedsięwzięcia zmierzające do zapobieżenia lub zredukowania wpływu

[58] R. Wróblewski, *Zarys teorii kryzysu, zagadnienia prewencji i zarządzania kryzysowego*, Wydawnictwo AON, Warszawa 1996, s. 39.
[59] *Koncepcja systemu zarządzania kryzysowego*, Komenda Główna Policji, Warszawa 1998.
[60] D. Ladak, T. Pilch (red.), *Elementarne pojęcia pedagogiki społecznej i pracy socjalnej*, Wydawnictwo ŻAK, Warszawa 1999, s. 72.

kryzysu na zasoby i wartości społeczne za pomocą środków kierowania i kontroli oraz koordynacji[61].

Kolejna definicja określa *zarządzanie kryzysowe*, jako proces decyzyjny zmierzający do wyboru racjonalnej strategii przeciwdziałania realnym i/lub potencjalnym sytuacjom kryzysowym, sposób zarządzania specyficznymi zasobami systemu zapewniający powrót do stanu normalnego ze stanu kryzysu lub utrzymania tego stanu mimo wystąpienia symptomów sytuacji kryzysowej[62].

Następna definicja mówi, że *zarządzanie w sytuacjach kryzysowych (kryzysowe)* to reagowanie na nadciągający lub trwające kryzys i usuwanie jego skutków w cyklu zdarzeń i czynności, od przewidywania i planowania antykryzysowego wraz z reagowaniem na codzienne zdarzenia, aż po zakończenie odbudowy ze zniszczeń (przygotowanie, reagowanie, odbudowa)[63].

Projekt ustawy o bezpieczeństwie obywatelskim z 28 kwietnia i 27 maja 2003 r. definiował *zarządzanie kryzysowe* jako uporządkowaną działalność polegającą na zapobieganiu sytuacjom kryzysowym lub przejmowaniu nad nimi kontroli i kształtowania ich przebiegu w drodze zaplanowanych działań oraz na odtworzeniu zasobów lub przywróceniu im ich pierwotnego charakteru[64].

Rządowy projekt ustawy o zarządzaniu kryzysowym z 2005 r. zawierał definicję wg, której *zarządzanie kryzysowe* to działalność organów administracji rządowej i samorządu terytorialnego polegająca na:

- zapobieganiu stanom narastającej destabilizacji, niepewności lub napięcia społecznego, stwarzającym powszechne zagrożenie dla życia, zdrowia lub mienia,
- przejmowaniu kontroli nad powyższymi stanami, w drodze zaplanowanych działań,
- odtwarzaniu infrastruktury lub przywróceniu jej pierwotnego charakteru.

[61] J. Konieczny, *Zarządzanie w sytuacjach kryzysowych*, wypadkach i katastrofach, Wydawnictwo Garmond, Poznań-Warszawa, 2001.
[62] P. Sienkiewicz, P. Górny, *Analiza systemowa sytuacji kryzysowych*, Wydawnictwo AON, Warszawa 2001, s. 32.
[63] J. Pawłowski, *Słownik …*, *dz. cyt.*, s. 166.
[64] J. Gryz, W. Kitler, *System …*, *dz. cyt.*, s. 31.

W projekcie była mowa o tym, że *zarządzanie kryzysowe* polega również na zapobieganiu i zwalczaniu stanów wywołanych czynem popełnionym w celu spowodowania masowej paniki lub zmuszenia organu władzy lub administracji publicznej RP lub innego państwa lub organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności albo w celu wywołania poważnych zakłóceń w funkcjonowaniu RP lub innego państwa albo organizacji międzynarodowej, a także groźbą popełnienia takiego czynu[65].

Ostatnia przytoczona definicja *zarządzania kryzysowego* mówi, że jest to zarządzanie organizacją (systemem) pod presją, realizowane na rzecz rozwiązywania napiętych sytuacji, którego zadaniem jest przygotowanie się i działanie mające na celu zapobieganie, przeciwdziałanie i reagowanie w razie wystąpienia zakłóceń stabilności organizacji (systemu) oraz przywrócenie normalnego stanu jego funkcjonowania[66].

Z powyższych definicji wynika, iż celem zarządzania kryzysowego jest przede wszystkim minimalizacja potencjalnych zagrożeń, ograniczanie prawdopodobieństwa ich wystąpienia, sprawne i skuteczne reagowanie na zidentyfikowane zagrożenia, szybkie przywracanie funkcjonowania procesów społecznych i gospodarczych do stanu sprzed zdarzenia kryzysowego oraz maksymalizacja poziomu bezpieczeństwa.

W zarządzaniu kryzysowym kładzie się duży nacisk na przygotowanie na wypadek wystąpienia potencjalnych zagrożeń, planowanie działań, podział odpowiedzialności i kompetencji, technologie, zagospodarowanie przestrzenne i systemy zabezpieczeń. Zarządzanie kryzysowe opiera się na takich zasadach, jak[67]:

- Zasada prymatu jednoosobowego kierownictwa, która polega na powierzeniu kompetencji decyzyjnych jednoosobowym organom, które sprawują władzę ogólną w danym zakresie kompetencji. Organami takimi są: wójt (burmistrz), starosta (prezydent miasta), wojewoda i premier.
- Zasada odpowiedzialności organów władzy publicznej, będąca regułą określającą odpowiedzialność za zarządzanie w sytuacjach

[65] *Tamże*, s. 31.
[66] *Tamże*, s. 33.
[67] K. Sienkiewicz-Małyjurek, F. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej*, Wydawnictwo Difin, Warszawa 2010, s. 15.

kryzysowych przez funkcjonujące w państwie organy administracji rządowej i samorządowej. Wiąże się ona ze stałą, historycznie uwarunkowaną, podstawową rolą administracji, która sprowadza się do usuwania zagrożeń i zapewnienie bezpieczeństwa w powierzonym jej zakresie władzy administracyjnej.

- Zasada prymatu układu terytorialnego, która określa, że podstawę działania organów władzy stanowi podział terytorialny państwa.
- Zasada powszechności, która zobowiązuje wszystkie podmioty prawa państwowego do uczestnictwa w działaniach antykryzysowych, każdy stosownie do jego statusu prawnego i organizacyjnego.
- Zasada funkcjonalnego podejścia, polegająca na określeniu względnie stałych, zwykle powtarzalnych, typowych i sformalizowanych proceduralnie działań, wyodrębnionych ze względu na ich rodzaj i charakter, ukierunkowanych na realizację celów bezpieczeństwa narodowego.
- Zasada zespolenia, w myśl której organom administracji ogólnej (wójt, starosta i wojewoda) nadaje się władztwo – według zasad określonych ustawami - nad wszelkimi pozostałymi formami administracji zarówno zespolonej, jak i niezespolonej.
- Zasada ciągłości funkcjonowania państwa, która określa, że bez względu na stan i okoliczności funkcjonowania państwa niezmienne pozostają formy organizacyjne władzy państwowej, a poszczególne organy realizują swoje funkcje zarówno w czasie pokoju, kryzysu, jak i wojny.

Proces zarządzania kryzysowego, zgodnie z przytoczoną na początku podrozdziału definicją z Ustawy[68], realizowany jest w pewnym zamkniętym czteroetapowym cyklu kierowania, w którym poszczególne etapy wzajemnie się warunkują i przenikają. Pierwszym etapem jest faza zapobiegania realizowana w trybie ciągłym jako proces monitorowania i analizowania zagrożeń, ich identyfikacji i prognozowania pod kątem możliwości wystąpienia sytuacji kryzysowej. Wyniki przeprowadzonej analizy w fazie zapobiegania stanowią podstawę działań w drugiej fazie -

[68] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz. U. z 2007 r. Nr 89, poz. 590.

przygotowaniu, w której są oceniane zidentyfikowane zagrożenia i ich negatywne następstwa pod względem jakościowo-ilościowym i wykonywane odpowiednie zadania z zakresu planowania. Trzecia faza zarządzania kryzysowego, czyli reagowanie jest realizowane w sytuacji, kiedy zdarzenie kryzysowe zaistnieje i istnieje pilna potrzeba opanowania go i ograniczenia negatywnych skutków. Ostatnim etapem jest odbudowa i odtwarzania zniszczonej infrastruktury, który formalnie zamyka cykl zarządzania kryzysowego[69].

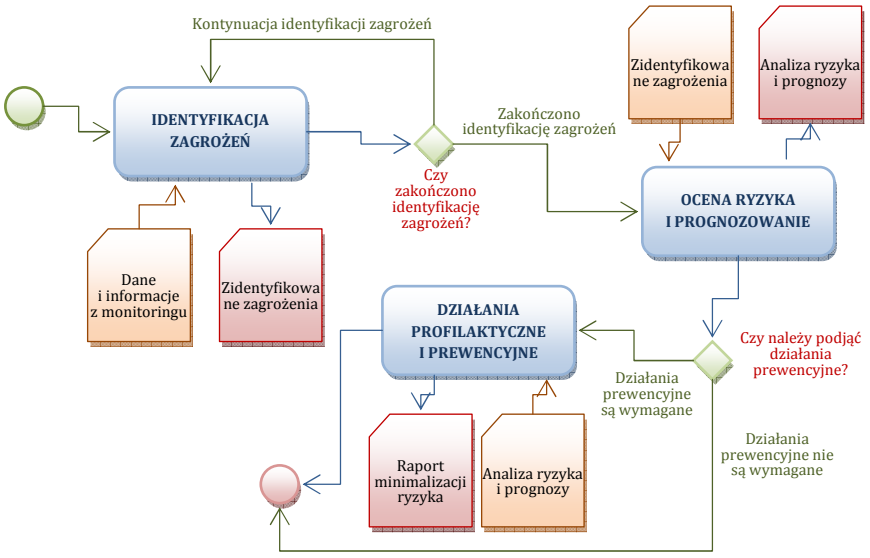
Rys. 2.2. Zadania w procesie zarządzania kryzysowego

Zadania realizowane w zarządzaniu kryzysowym można podzielić na cztery grupy (Rys. 2.2):

- zadanie realizowane w fazie zapobiegania sytuacjom kryzysowym,
- zadania realizowane w fazie przygotowania do przejmowania kontroli nad sytuacjami kryzysowymi,
- zadania realizowane podczas reagowania w przypadku wystąpienia sytuacji kryzysowych,

[69] K. Ficoń, *Logistyka kryzysowa. Procedury, potrzeby, potencjał*, BEL Studio, Warszawa 2011, s. 116.

– zadania realizowane podczas odbudowy (usuwania skutków sytuacji kryzysowych oraz odtwarzania zasobów i infrastruktury krytycznej).



Rys. 2.3. Działania fazy zapobiegania

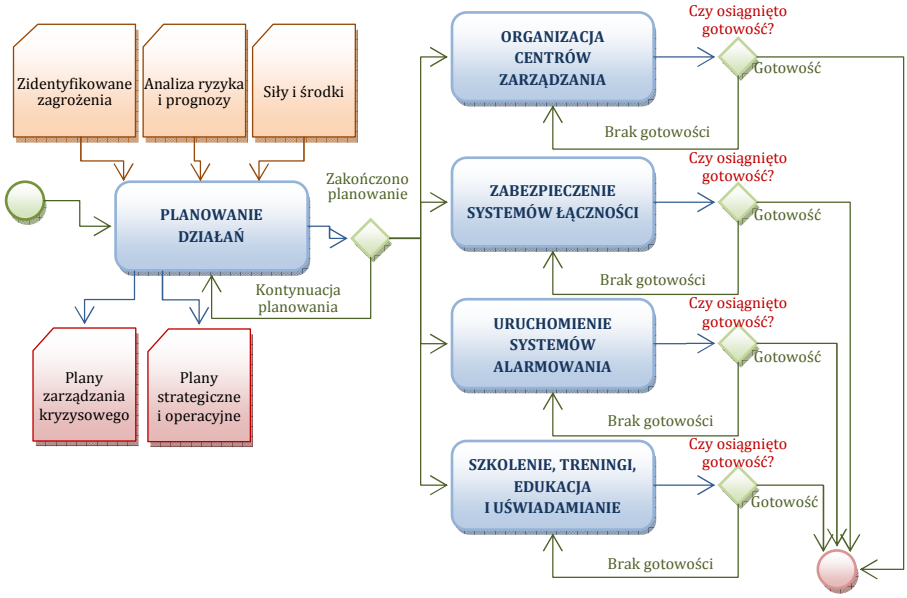
W fazie zapobiegania podejmowane są działania, których celem jest identyfikacja zagrożeń oraz redukcja prawdopodobieństwa ich wystąpienia (Rys. 2.3). Skuteczne zapobieganie powinno doprowadzić do zatrzymania zaobserwowanych symptomów sytuacji kryzysowej i racjonalnego powrotu do stanu pełnego bezpieczeństwa. Działania te są uzależnione od typu identyfikowanych zagrożeń. W dużym stopniu uogólnienia należą do nich takie działania, jak[70]:

– monitorowanie przestrzeni potencjalnych zagrożeń,
– identyfikacja symptomów i rodzajów zagrożeń,
– ocena podatności środowiska na skutki zagrożeń,
– analiza możliwości obronnych przed zagrożeniami,
– opracowanie odpowiednich aktów i uregulowań prawnych,
– przygotowanie niezbędnych środków finansowych,
– podjęcie skutecznych działań zapobiegawczych,
– prognozowanie strat i ofiar wśród ludności,

[70] K. Ficoń, *Logistyka …*, *dz. cyt.*, s. 117.

– prognozowanie ewentualnych strat i zniszczeń,
– uruchomienie mechanizmów i procedur zaradczych,
– monitorowanie tendencji rozwojowych sytuacji kryzysowej.
poszukiwanie dodatkowego wsparcia i sojuszników.

Zadania realizowane podczas fazy zapobiegania mają charakter ciągły i prowadzone są przez powołane do tego celu instytucje publiczne. Należy podkreślić, że jest to najbardziej efektywny etap zarządzania kryzysowego, ponieważ przy niewielkich nakładach można odnieść znaczne korzyści. Prowadzone w tej fazie czynności profilaktyczno-prewencyjnych mogą przyczynić się do skutecznego ograniczenia skutków sytuacji kryzysowych.



Rys. 2.4. Działania fazy przygotowania

Przygotowanie do przejmowania kontroli nad sytuacjami kryzysowymi w drodze zaplanowanych działań w głównej mierze polega na przygotowywaniu planów oraz zabezpieczeń dla całego systemu. Najważniejszym celem tej fazy jest zwiększenie możliwości społeczeństwa do podjęcia działań antykryzysowych (Rys. 2.4). Może się ono odbywać się poprzez odpowiednie przygotowanie zasobów ludzkich, materiałowych i finansowych, zapewnienie przepływu strumieni informacyjnych w systemach bezpieczeństwa oraz

podniesienie sprawności działań operacyjnych. Optymalne wykorzystanie zgromadzonych sił i środków uzależnione jest od umiejętności organów władzy administracyjnej. Etap przygotowania obejmuje szereg bardzo ważnych zadań i przedsięwzięć, do których należy zaliczyć m.in.[71]:

- uaktualnienie planu zarządzania kryzysowego,
- reaktywację centrum zarządzania kryzysowego,
- usprawnienie systemu łączności kryzysowej,
- podwyższenie gotowości dla służb i ekip ratowniczych,
- przygotowanie dodatkowych środków transportu,
- sprawdzenie systemów alarmowania ludności,
- przeprowadzenie treningu dla etatowej obsady centrum,
- gromadzenie i aktualizacja danych o sytuacji kryzysowej,
- uzupełnienie zapasów i rezerw materiałowych,
- przeprowadzenie konserwacji i napraw sprzętu technicznego,
- sprawdzenie szlaków i sieci komunikacyjnej,
- wzmocnienie kadrowe i sprzętowe służb komunalnych,
- ustalenie procedur zabiegania o pomoc i wsparcie,
- przygotowanie najbardziej typowych scenariuszy działań,
- utrzymywanie łączności ze służbami porządkowymi,
- przedstawienie katalogu potrzeb dla służb publicznych,
- tworzenie doraźnych składów materiałowych,
- sprawdzenie kontaktów i gotowości wszystkich kontrahentów,
- stymulowanie ludności do gromadzenia dodatkowych zapasów,
- aktywizację ludności do działań społecznych i samopomocy.

Zadania realizowane w fazie przygotowania do sytuacji kryzysowych nigdy nie dadzą gwarancji na zażegnanie kryzysu w fazie początkowej. Wynika to z dynamiki zjawisk oraz zmienności czynników kształtujących sytuację kryzysową. Wynikiem końcowym etapu przygotowania powinno być osiągnięcie gotowości do skutecznych działań operacyjnych w razie przekształcenia się sytuacji kryzysowej w stan kryzysu. W żadnym wypadku poniesione koszty w fazie przygotowania nie powinny być traktowane, jako straty w wypadku gdy do kryzysu nie dojdzie, gdyż zwalczanie zagrożeń i sytuacji kryzysowych

[71] K. Ficoń, *Logistyka …*, *dz. cyt.*, s. 119.

jest często zasługą przygotowań, które w różnym stopniu osłabiają potencjał zagrożeń i nie dopuszczają do ich eskalacji do postaci kryzysu.

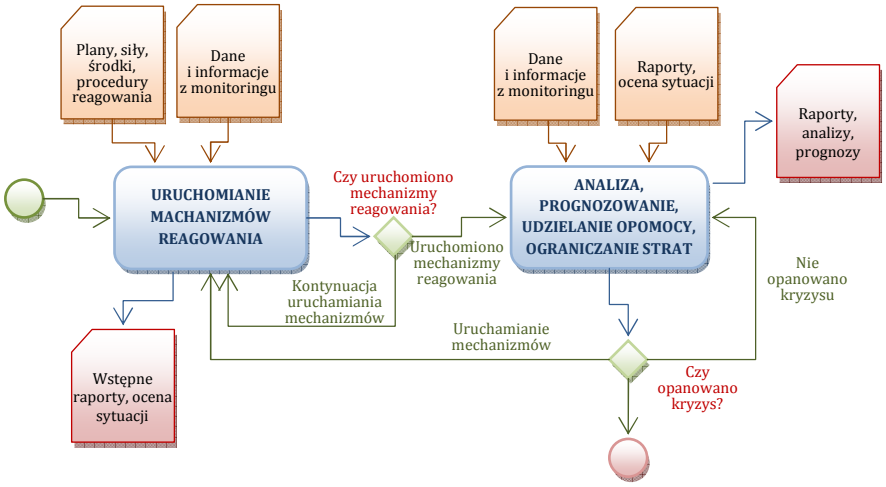
Do trzeciej grupy należą zadania wykonywane w ramach reagowania kryzysowego. Faza ta następuje w sytuacji zajścia zdarzenia kryzysowego i trwa tak długo, dopóki nie uda się skutecznie zażegnać kryzysu. Podstawowymi zadaniami, które są wykonywane podczas walki z kryzysem są działania ratownicze i ewakuacyjne podejmowane w pierwszej kolejności przez ekipy ratownictwa medycznego, a w dalszej kolejności przez inne służby ratownictwa specjalistycznego, stosownie do zaistniałej sytuacji kryzysowej.

Sprawne prowadzenie reagowania kryzysowego wymaga posiadania efektywnego systemu działania, w którym można wyróżnić organa kierownicze z niezbędnymi kompetencjami i jednostki wykonawcze wyposażone w odpowiedni potencjał osobowy, informacyjny, materiałowy i techniczny.

Zadania realizowane w fazie reagowania kryzysowego to[72]:

- ukompletowanie składu centrum zarządzania kryzysowego,
- rozwinięcie polowej infrastruktury krytycznej w miejscu zdarzenia,
- utrzymanie nieprzerwanej łączności na wielu kanałach,
- zagwarantowanie serwisu informacyjnego dla ludności,
- uruchomienie systemów ostrzegania i alarmowania,
- uruchomienie procedur i ekip ratowniczych,
- udzielanie pierwszej pomocy medycznej wszystkim potrzebującym,
- uruchomienie procesu ewakuacji medycznej rannych i chorych,
- neutralizowanie ognisk rozmaitych zagrożeń wtórnych,
- uruchomienie punktów i serwisów pomocy społecznej,
- uruchomienie punktów zbiorowego żywienia,
- dostawy podstawowych asortymentów gospodarczo-bytowych,
- organizowanie doraźnej samopomocy,
- włączenie organizacji społecznych i humanitarnych,
- budowa miejsc tymczasowego schronienia dla ludności,
- monitorowanie efektywności reagowania kryzysowego.

[72] K. Ficoń, *Logistyka …*, *dz. cyt.*, s. 123.



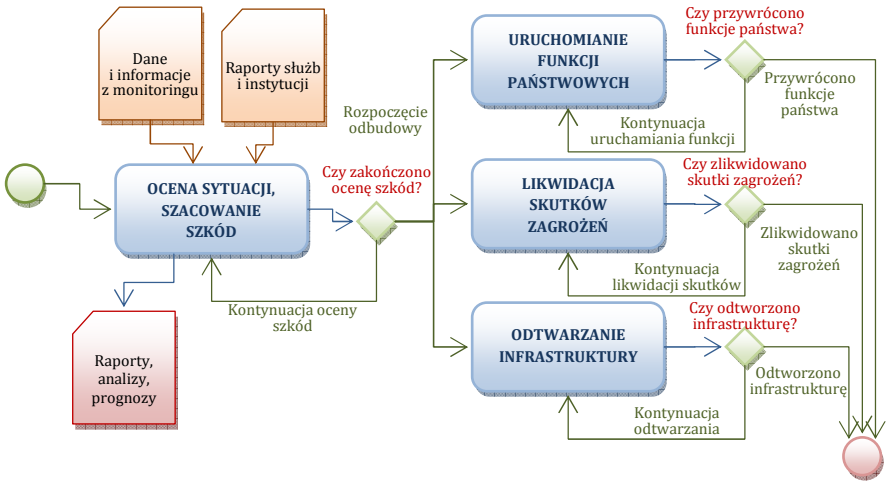
Rys. 2.5. Działania fazy reagowania

Działanie wykonywane w reagowaniu kryzysowym powinny być przede wszystkim uporządkowane i realizowane w następującym cyklu wykonawczym (Rys. 2.5):

- analiza zadania i ocena sytuacji,
- ocena potrzeb sytuacyjnych,
- prognozowanie rozwoju zdarzeń,
- przygotowanie niezbędnego potencjału,
- ustalenie terminu i miejsca akcji,
- przygotowanie własnego planu działania,
- zorganizowanie pomocy i współdziałania,
- podjęcie dobrze zorganizowanej akcji,
- utrzymanie łączności z centrum koordynacji[73].

Skuteczność reagowania kryzysowego jest uzależniona od sumiennego wykonywania działań w fazie zapobiegania i przygotowania do sytuacji kryzysowych. Pełna identyfikacja zagrożeń, analizy ryzyka ich wystąpienia, przygotowanie systemu reagowania kryzysowego do działania mają istotny wpływ na czas opanowania kryzysu i niezwłoczne rozpoczęcie ostatniej fazy zarządzania kryzysowego, w której następuje usuwanie skutków kryzysu oraz odbudowa.

[73] K. Ficoń, *Logistyka …*, *dz. cyt.*, s. 124.



Rys. 2.6. Działania fazy odbudowy

Podczas odbudowy realizowane są zadania mające na celu przywrócenie przebiegu procesów społecznych i gospodarczych do stanu sprzed wystąpienia sytuacji kryzysowej (Rys. 2.6). Wymaga to podjęcia następujących działań:

- świadczenia opieki medycznej i lekarskiej,
- utrzymania ekip ratowniczych w odpowiedniej gotowości,
- prowadzenia zabiegów i szczepień profilaktycznych,
- utrzymania przejezdności szlaków komunikacyjnych,
- utrzymania ciągłości funkcjonowania administracji publicznej,
- szacowania szkód materialnych i wielkości strat,
- oceny skali zniszczeń infrastrukturalnych,
- zapewnienia doraźnej pomocy socjalnej dla ludności,
- budowy miejsc tymczasowego zakwaterowania,
- informowania o prawach i obowiązkach ludności poszkodowanej,
- odtwarzania niezbędnych zapasów i rezerw materiałowych,
- odtwarzania gotowości służb logistycznych,
- pozyskiwania nowych inwestorów i wykonawców,
- podejmowania inicjatyw legislacyjnych i stanowienie prawa,
- ochrony wszystkich obiektów i urządzeń w strefie katastrofy,
- prowadzenia prac ewidencyjno-dokumentacyjnych,
- przygotowania nowych projektów inwestycyjnych,

– pozyskiwania nowych środków finansowych.

Omówione powyżej zadania należące do czterech faz zarządzania kryzysowego obrazują złożoność tego procesu. Ich wyniki w formie analiz powinny być przekazywane z jednej fazy do drugiej i stanowić podstawę do kolejnych przedsięwzięć. Fazy zarządzania kryzysowego powinny się wzajemnie przenikać i elastycznie inicjować procedury formalno-prawne lub nakazane działania operacyjne.

2.2. UREGULOWANIA FORMALNO-PRAWNE ZARZĄDZANIA KRYZYSOWEGO

Uregulowania formalno-prawne z zakresu zarządzania kryzysowego były tworzone pod wpływem transformacji ustrojowych w Polsce w latach 60., 80., i 90. XX wieku. Duży wpływ na ich kształt mają także obecne zmiany oraz rosnąca liczba zagrożeń.

Prześledzenie najważniejszych aspektów bezpieczeństwa dla naszego kraju na przestrzeni wymienionych lat pozwala zauważyć, że były one związane z rolą i usytuowaniem Polski w Radzie Wzajemnej Pomocy Gospodarczej (RWPG) i strukturach Układu Warszawskiego (UW). Szczególnie jest to widoczne w kontekście zmian jakie następowały w ustawie o powszechnym obowiązku obrony RP[74] do 1999 roku, tj. wstąpienia Polski do Paktu Północnoatlantyckiego (NATO). Niewątpliwie bardzo ważnym dla Polski okresem transformacji bezpieczeństwa była akcesja do Unii Europejskiej w 2004 roku[75].

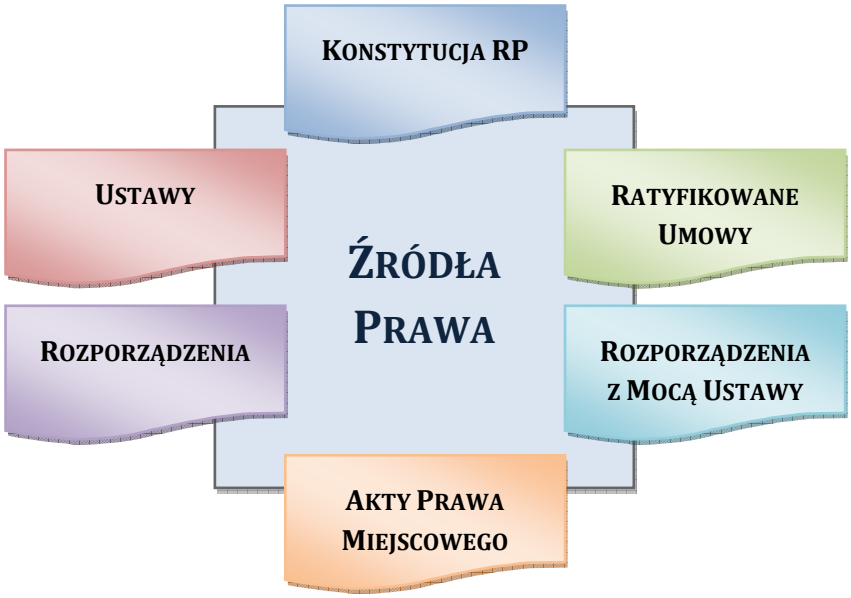
Aktami normatywnymi, które stanowią podstawę krajowego systemu zarządzania kryzysowego są źródła prawa powszechnie obowiązującego. Do tych źródeł należą: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia, rozporządzenia z mocą ustawy oraz akty prawa miejscowego[76] (Rys. 2.7).

[74] *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*, Dz. U. z 2004 r. Nr 241, poz. 2416.

[75] W. R. Sulęta, *System zarządzania kryzysowego województwa pomorskiego*, AMW, Gdynia 2010, s. 19.

[76] Artykuł 87 Konstytucji RP mówi, że źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia oraz akty prawa miejscowego na obszarze działania organów, które je ustanowiły. Dodatkowo w artykule 234 Konstytucji RP jest powiedziane, że jeżeli w czasie stanu wojennego Sejm nie może zebrać się na posiedzenie, Prezydent Rzeczypospolitej na wniosek Rady Ministrów wydaje

Analizując poszczególne akty prawne w zakresie organizacji zarządzania kryzysowego należy stwierdzić, że są one coraz bardziej doskonalsze, dając tym samym dobre podstawy do budowy efektywnego systemu bezpieczeństwa publicznego. Najlepszym tego przykładem jest Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[77].



Rys. 2.7. Źródła prawa regulujące funkcjonowanie krajowego systemu zarządzania kryzysowego

Należy podkreślić, aby prawo w tej materii było ponad partykularne, gdyż częste zmiany merytoryczne aktów prawnych, kadencyjnie co cztery lata powodują, iż pionowy system zależności organizacyjnej, tj. krajowy – regionalny - lokalny nie ma ze sobą powiązania organizacyjnego i prawnego.

Ideą powstania takiego systemu byłoby stworzenie silnego krajowego zarządzania kryzysowego w myśl zasady: *„silny lokalny przekłada się na silny regionalny, co powoduje powstanie bardzo mocnego i stabilnego systemu krajowego"*[78].

rozporządzenia z mocą ustawy w zakresie i w granicach określonych w art. 228 ust. 3-5. Rozporządzenia te podlegają zatwierdzeniu przez Sejm na najbliższym posiedzeniu.

[77] Dz. U. z 2007 r. Nr 89, poz. 590 ze zm.

[78] W. R. Sulęta, *System …*, *dz. cyt.*, s. 52.

Podstawy prawne zarządzania kryzysowego wymagają dalszego doskonalenia. Zakończeniem tego procesu będzie stworzenie doskonałego modelu funkcjonowania systemu opartego na jednym planie proceduralnym, uwzględniającym różne aspekty geopolityczne regionów. Plan ten będzie opracowany z wykorzystaniem wysoce zaawansowanych technologicznie narzędzi teleinformatycznych kompatybilnych dla całego kraju w myśl zasady: *„to co mówię to widzę oraz inni mnie widzą i słyszą"*[79]. Jest to system pionowy, który bardzo dobrze sprawdza się w standardach Unii Europejskiej i Stanów Zjednoczonych.

Omawiając problematykę uregulowań prawnych zarządzania kryzysowego należy przede wszystkim rozpocząć rozważania od **artykułu 228 Konstytucji RP**[80] z dnia 2 kwietnia 1997 roku. Przepis ten umożliwia wprowadzenie stanów nadzwyczajnych (stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej) w sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające. Zgodnie z tym przepisem stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, która określa między innymi zasady działania organów władzy publicznej, zakres w jakim mogą zostać ograniczone wolności i prawa człowieka i obywatela oraz może określić podstawy, zakres i tryb wyrównywania strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela.

Szczególnie przydatną ustawą, ułatwiającą zarządzanie w sytuacjach kryzysowych, była **ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej**[81] zwana dalej ustawą o stanie klęski żywiołowej. Brak takiej ustawy był mocno odczuwalny w okresie powodzi w 1997 r. na Dolnym Śląsku[82]. Ustawa ta określa tryb

[79] *Tamże*, s. 53,
[80] Dz. U. z 1997 r. Nr 78, poz. 483, ze zm.
[81] Dz. U. z 2002 r. Nr 62, poz. 558 ze zm.
[82] Brak ustawy o stanie klęski żywiołowej spowodował, że w lipcu i sierpniu 1997 roku przyjęto między innymi następujące ustawy: *o stosowaniu szczególnych rozwiązań w związku z likwidacją skutków powodzi (Dz. U. z 1997 r. Nr 80, poz. 491)*, *o szczególnych zasadach remontów i odbudowy obiektów budowlanych zniszczonych lub uszkodzonych wskutek powodzi (Dz. U. z 1997 r. Nr 80, poz. 492)*, *o szczególnych zasadach gospodarki gruntami i wywłaszczania nieruchomości na terenach objętych powodzią z lipca 1997 r. (Dz. U. z 1997 r. Nr 80 poz. 493)*, *o szczególnych zasadach postępowania administracyjnego i sądowego w związku z usuwaniem skutków powodzi z lipca 1997 r. (Dz. U. z 1997 r. Nr 80*

wprowadzenia i zniesienia stanu klęski żywiołowej, a także zasady działania organów władzy publicznej oraz zakres ograniczeń wolności i praw człowieka i obywatela w czasie stanu klęski żywiołowej. Zostały w niej zdefiniowane takie pojęcia, jak: klęska żywiołowa, katastrofa naturalna oraz awaria techniczna. Zgodnie z ustawą stan klęski żywiołowej może wprowadzić Rada Ministrów, w drodze rozporządzenia, z własnej inicjatywy lub na wniosek właściwego wojewody[83].

Regulacje dotyczące zapobiegania poważnym awariom przemysłowym zostały wprowadzone poprzez **ustawę z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska**[84] Ustawa ta zawiera instrumenty prawne służące do przeciwdziałania poważnym awariom przemysłowym oraz określa podstawowe obowiązki osób prowadzących zakłady stwarzające ryzyko wystąpienia poważnej awarii, jak również obowiązki organów właściwych w sprawach poważnych awarii. Dodatkowo ustawa ta umożliwia informowanie oraz udział społeczeństwa w sprawach dotyczących poważnych awarii. Przyjęcie niniejszej ustawy było wynikiem wprowadzenia w UE Dyrektywy SEVESO II[85], która była odpowiedzią na katastrofę we Włoszech w 1976 roku w miejscowości Seveso[86]. Zgodnie z tą Dyrektywą państwa członkowskie UE zostały zobowiązane do wprowadzenia odpowiednich przepisów do własnego prawodawstwa. Zakres unijnej dyrektywy

poz. 494), o stosowaniu szczególnych rozwiązań podatkowych w związku z likwidacją skutków powodzi, która miała miejsce w lipcu 1997 r. (Dz. U. z 1997 r. Nr 113 poz. 736).

[83] Dz. U. z 2002 r. Nr 62, poz. 558 ze zm.

[84] Tekst pierwotny Dz. U. z 2001 r. Nr 62, poz. 627, tekst jednolity Dz. U. z 2008 r. Nr 25 poz. 150.

[85] OJ L 10 z 1997, p. 13 ze zm. Dyrektywa Rady Unii Europejskiej 96/82/WE (SEVESO II) z 9 grudnia 1996 r. w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi. Dyrektywa SEVESO II została zmieniona poprzez Dyrektywę 2003/105/WE z 16 grudnia 2003 r. w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi. Konieczność zmian wynikała z zaistnienia między innymi takich zdarzeń, jak: rozlew cyjanku, który spowodował zanieczyszczenie Dunaju w następstwie awarii w Baia Mare w Rumunii w styczniu 2000 r., eksplozja składowiska sztucznych ogni w Enschede w Niderlandach w maju 2000 r., wybuch w fabryce nawozów sztucznych w Tuluzie we wrześniu 2001 r.

[86] Katastrofa w Seveso we Włoszech wydarzyła się 10 lipca 1976 r. W znajdujących się ok. 20 km od Mediolanu zakładach ICMESA, w których produkowano m.in. trichlorofenol, nastąpiła emisja około 2 ton toksycznych substancji chemicznych. Skażeniu uległo około 1500 ha gęsto zaludnionego obszaru, ewakuowano 730 osób, około 700 mieszkańców zostało poszkodowanych w wyniku zatrucia. Zginęło wiele zwierząt, wielkie areały zostały skażone i wyłączone na wiele lat z gospodarki rolnej. Straty materialne oszacowano na kwotę 72 mln ECU.

obejmował zarówno działalność przemysłu, jak i składowanie niebezpiecznych substancji chemicznych.

Dział V **Ochrona przed powodzią oraz suszą**[87] ustawy z dnia 27 kwietnia 2001 r. Prawo wodne, reguluje zasady organizowania ochrony ludzi i mienia przed powodzią i suszą. Nawiązuje ona do ustawy o stanie klęski żywiołowej. Zgodnie z nią zadania dotyczące ochrony przed powodzią oraz suszą zostały przekazane do organów administracji rządowej i samorządowej. Ustawa wprowadziła ograniczenia w sposobie użytkowania obszarów objętych wysokim ryzykiem wezbrań oraz przedstawiono w niej podział obszarów narażonych na niebezpieczeństwo powodzi na obszary potencjalnego zagrożenia powodzią oraz obszary bezpośredniego zagrożenia powodzią (tereny między wałem przeciwpowodziowym a linią brzegu, strefa wybrzeża morskiego oraz strefa przepływów wezbrań powodziowych).

Prawne usankcjonowanie wykorzystania oddziałów i pododdziałów wojskowych podczas reagowania kryzysowego nastąpiło po wejściu w życie **rozporządzenia Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad udziału pododdziałów i oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu**[88]. Rozporządzenie to zostało wydane na podstawie art. 18 ust. 3 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej. Na podstawie m.in. tego rozporządzenia zostało podpisane porozumienie o współdziałaniu w sytuacjach kryzysowych pomiędzy Pomorskim Urzędem Wojewódzkim a Marynarką Wojenną RP w 2004 r.[89].

Kluczową ustawą dotyczącą ratownictwa medycznego jest **ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym**[90]. Ustawa ta stała się podstawą stworzenia systemu Państwowego Ratownictwa Medycznego, którego głównym zadaniem jest zapewnienia pomocy każdej osobie znajdującej się w stanie nagłego zagrożenia zdrowotnego. Ustawa określa m.in. zasady organizacji, funkcjonowania i finansowania systemu oraz zasady zapewnienia edukacji w zakresie udzielania pierwszej pomocy. W ustawie zostały

[87] Tekst pierwotny Dz. U. z 2001 r. Nr 115, poz. 1229, tekst jednolity Dz. U. z 2005 r. Nr 239, poz. 2019 ze zm.
[88] Dz. U. z 2003 r. Nr 41, poz. 347.
[89] Porozumienie podpisał wojewoda pomorski Cezary Dąbrowski i dowódca Marynarki Wojennej RP admirał floty Roman Krzyżelewski 16 listopada 2004 r.
[90] Dz. U. z 2006 r. Nr 191, poz. 1410 ze zm.

zdefiniowane takie pojęcia, jak: dysponent jednostki, kwalifikowana pierwsza pomoc, lekarz systemu, medyczne czynności ratunkowe, miejsce zdarzenia, pielęgniarka systemu, pierwsza pomoc, stan nagłego zagrożenia zdrowotnego, szpitalny oddział ratunkowy, zespół ratownictwa medycznego.

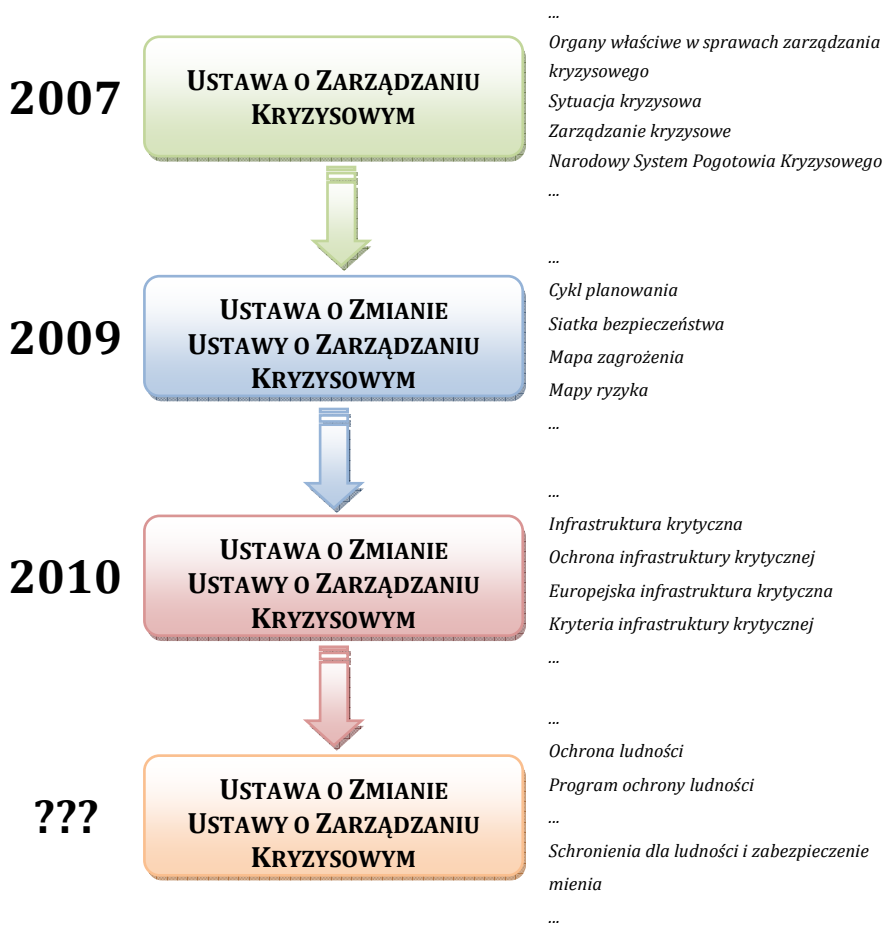
Na podstawie art. 6 ust. 2 pkt 5 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej[91] zostało wprowadzone **rozporządzenie Rady Ministrów z dnia 16 października 2006 r. w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach**[92]. Określiło ono organizację i warunki przygotowania oraz sposób funkcjonowania systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania o skażeniach na terytorium Rzeczypospolitej Polskiej oraz rolę organów administracji w tych sprawach, dla zapewnienia zewnętrznego bezpieczeństwa państwa i sprawowania ogólnego kierownictwa w dziedzinie obronności kraju. Rozporządzenie to definiowało również pojęcia: alarm, alarmowanie, analiza skażeń, monitoring skażeń, obserwacja, ostrzeganie, pomiar, powiadamianie, prognozowanie, rozpoznanie skażeń, skażenie, systemy wykrywania i alarmowania o skażeniach, wykrywanie skażeń oraz zakażenie.

Podstawowym aktem prawnym, który reguluje zadania wojewody na wypadek wystąpienia zdarzenia radiacyjnego o zasięgu wojewódzkim jest **rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych**[93]. Rozporządzenie to określa krajowy plan postępowania awaryjnego, w tym sposób współdziałania organów i służb biorących udział w likwidacji zdarzeń i usuwaniu ich skutków, wzór zakładowego oraz wojewódzkiego planu postępowania awaryjnego.

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym [94] była długo oczekiwanym aktem prawnym przez środowisko zajmujące się bezpieczeństwem wewnętrznym. Akt ten miał uporządkować funkcjonowanie systemu zarządzania kryzysowego tak, aby w razie zaistnienia sytuacji kryzysowej, państwo mogło nieść

[91] Dz. U. z 2004 r. Nr 241, poz. 2416, ze zm.
[92] Dz. U. z 2006 r. Nr 191, poz. 1415.
[93] Dz. U. z 2005 r. Nr 20, poz. 169.
[94] Dz. U. z 2007 r. Nr 89, poz. 590.

niezbędną pomoc potrzebującym. Wydawało się również, że po wprowadzeniu go w życie, skutecznie zostaną rozwiązane problemy dotyczące ochrony ludności w całym spektrum działania. Niezbędne było stworzenie jednego aktu prawnego ujmującego wszystkie zadania realizowane w obszarze ochrony ludności. W ocenie praktyków zarządzania kryzysowego, rozproszenie przepisów jest przyczyną braku czytelności i wielu niejasności w ustalaniu odpowiedzialności za realizowane zadania.



Rys. 2.8. Etapy nowelizacji Ustawy o zarządzaniu kryzysowym

Ustawa o zarządzaniu kryzysowym określiła organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania, a także sposoby finansowania zadań zarządzania

kryzysowego. Zdefiniowane zostało w niej m.in. pojęcie sytuacji kryzysowej, infrastruktury krytycznej oraz Narodowego Systemu Pogotowia Kryzysowego (NSPK). Wszystko to było niezwykle istotne, ale w samej ustawie zabrakowało niestety precyzyjnie określonych zadań z zakresu ochrony ludności, w tym również zadań dotyczących budowy, utrzymania i użytkowani budowli ochronnych. Należy podkreślić, że od samego początku brakowało aktów wykonawczych do tej ustawy, co powodowało wiele nieporozumień oraz sporów kompetencyjnych. Dodatkowo pojawiła się konieczność wniesienia poprawek.

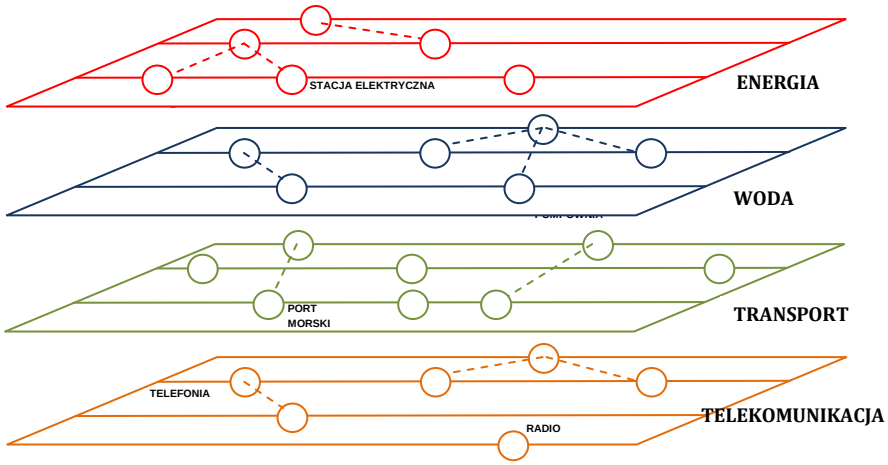
Pierwsza nowelizacja ustawy miała miejsce w lipcu 2009 roku[95] i dotyczyła m.in. doprecyzowania kryteriów wprowadzania nadzwyczajnych środków, w tym wojskowych w stosunku do obywateli, podczas sytuacji kryzysowych [96] (Rys. 2.8). Ustawa o zarządzaniu kryzysowym po nowelizacji upoważniła samorządy powiatowe i gminne do tworzenia centrów zarządzania kryzysowego dostosowanych do regionalnych potrzeb. Zgodnie z tymi zapisami centra nie musiały mieścić się w siedzibach urzędów, natomiast mogły zostać powiązane organizacyjnie z właściwymi służbami czy inspekcjami. Dodatkowo plany zarządzania kryzysowego miały podlegać regularnej aktualizacji, dokonywanej co dwa lata. Miał być również opracowany raport o zagrożeniach bezpieczeństwa narodowego, Krajowy Plan Zarządzania Kryzysowego oraz Narodowy Program Ochrony Infrastruktury Krytycznej. W znowelizowanych przepisach doprecyzowano pojęcie sytuacji kryzysowej, aby ułatwić wyodrębnienie i kwalifikację zdarzeń kryzysowych.

W ustawie zdefiniowano również pojęcia bezpośrednio związane z procesem zarządzania kryzysowego takie, jak: cykl planowania, siatkę bezpieczeństwa, mapy zagrożenia, mapy ryzyka, zdarzenia o charakterze terrorystycznym. Wprowadzono również do użytku termin

[95] Dz. U. z 2009 r. Nr 131, poz. 1076.

[96] Ustawa z dnia 26 kwietnia 2007 o zarządzaniu kryzysowym została zaskarżona przez posłów SLD do Trybunału Konstytucyjnego 9 listopada 2007 r. Grupa posłów SLD wniosła o stwierdzenie, że art. 3 pkt. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590 ze zm. dalej: ustawa) jest niezgodny z art. 2 i art. 31 ust. 3 Konstytucji, oraz że art. 3 pkt. 2 ustawy jest niezgodny z art. 2 i art. 22 w związku z art. 31 ust. 3 Konstytucji. Po rozpatrzeniu wniosku Trybunał Konstytucyjny wydał wyrok 21 kwietnia 2009 r. zgodnie, z którym Trybunał uznał definicję sytuacji kryzysowej (art. 3, pkt. 1 ustawy o zarządzaniu kryzysowym) za niezgodną z art. 2 Konstytucji RP oraz uznał za zgodną z Konstytucją RP definicję infrastruktury krytycznej (art. 3, pkt. 2. ustawy o zarządzaniu kryzysowym).

„infrastruktura krytyczna" - odnoszący się do obiektów i usług kluczowych dla bezpieczeństwa oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Pojęcie infrastruktury krytycznej oraz związane z nią regulacje oparte zostały na analogicznych przepisach stosowanych w innych państwach. Nowelizacja ustawy miała na celu przygotowanie organów władzy oraz odpowiednich służb do sytuacji kryzysowych tak, aby podejmowane działania pozwalały na szybkie i skuteczne ich rozwiązywanie.



Rys. 2.9. Przykład powiązań w infrastrukturze krytycznej państwa[97]

Kolejne zmiany w ustawie wprowadzono w październiku 2010 r.[98] Doprecyzowano pojęcie infrastruktury krytycznej (Rys. 2.9) oraz europejskiej infrastruktury krytycznej. W myśl tych przepisów *infrastruktura krytyczna państwa to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców*.

[97] D. D. Dudenhoeffer, M. R. Permann, M. Manic, *CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis*, 2006 (www.inl.gov/technicalpublications/Documents/3578215.pdf).

[98] Dz. U. z 2010 r. Nr 240 poz. 1600. *Ustawa o zmianie ustawy o zarządzaniu kryzysowym* dokonuje implementacji do prawa polskiego dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 2008.345.75).

Infrastruktura krytyczna obejmuje następujące systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Proces dostosowywania polskich przepisów w zakresie infrastruktury krytycznej do przepisów Unii Europejskiej wymusił konieczność zdefiniowania pojęcia europejskiej infrastruktury krytycznej, w myśl której są to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ, na co najmniej dwa państwa członkowskie.

Obecnie trwają prace nad kolejną nowelizacją[99], której głównym celem jest potrzeba uzupełnienia *Ustawy o zarządzaniu kryzysowym* o brakujące regulacje dotyczące ochrony ludności, wynikająca przede wszystkim z doświadczeń działania systemu mającego na celu zapewnienie bezpieczeństwa ludności. Doświadczenia z sytuacji kryzysowych pokazały, że należy wdrożyć systemowe rozwiązania mające na celu wykorzystanie istniejącego w państwie potencjału, zdolnego do podjęcia niezbędnych przedsięwzięć organizacyjnych w celu zapewnienia obywatelom bezpieczeństwa.

Niewątpliwie najważniejszą zmianą jakościową, która zostanie wprowadzona poprzez zmianę ustawy, będzie ciągłość odpowiedzialności za ochronę ludności w każdej sytuacji, nie zaś dopiero i tylko w momencie wystąpienia realnego zagrożenia.

[99] *Założenia projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym*, MSWiA, Warszawa 2011.

- Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa[100] (rozporządzenie aktualnie uchylone),
- Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania[101],
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego[102],
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej[103],
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej[104],
- Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa[105],
- Zarządzenie Nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego[106] (aktualnie uchylone),
- Zarządzenie Nr 78 Prezesa Rady Ministrów z dnia 11 października 2011 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego[107].

Proces wdrażania numeru alarmowego 112 w Polsce został rozpoczęty w 2000 roku. Pierwsze lata nie przyniosły jednak oczekiwanych wyników. Prace nabrały odpowiedniego tempa dopiero w 2007 roku po powołaniu Międzyresortowego Zespołu do spraw numeru alarmowego 112 oraz wdrażania systemu eCall. Wymiernym wynikiem prac tego Zespołu było opracowanie Rządowego programu „Koncepcja systemu 112" oraz **rozporządzenia z dnia 17 września**

[100] Dz. U. 2008 r. Nr 128 poz. 821.
[101] Dz. U. 2009 r. Nr 226 poz. 1810.
[102] Dz. U. 2010 r. Nr 83 poz. 540.
[103] Dz. U. 2010 r. Nr 83 poz. 541.
[104] Dz. U. 2010 r. Nr 83 poz. 542.
[105] Dz. U. 2011 r. Nr 86 poz. 471.
[106] M. P. 2008 r. Nr 61 poz. 538.
[107] M. P. 2011 r. Nr 93 poz. 955.

2007 r. Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowej organizacji centrów powiadamiania ratunkowego[108]. Podstawą tego rozporządzenia była ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym[109]. Rozporządzenie określało szczegółową organizację centrów powiadamiania ratunkowego, ich liczbę oraz sposób rozmieszczenia[110]. Zgodnie z nim przyjęto, że w każdym województwie powinno funkcjonować jedno centrum w ramach komórki organizacyjnej urzędu wojewódzkiego właściwej w sprawach zarządzania kryzysowego. Założono również, że centra powinny znajdować się w miastach będących siedzibami wojewodów, z wyjątkiem województwa mazowieckiego i województwa warmińsko-mazurskiego, w których centra miałyby być zlokalizowane, odpowiednio w Radomiu i Elblągu. Zgodnie z obecnie obowiązującą koncepcją, centra powiadamiania ratunkowego organizuje się na terenie obejmującym powiat liczący łącznie co najmniej 600 tys. mieszkańców. Dopuszcza się włączenie do terenu działania centrum powiadamiania ratunkowego, innych kolejno przyległych powiatów, jeśli wchodzą one w skład rejonów operacyjnych zespołów ratownictwa medycznego dysponentów właściwych dla miejsca lokalizacji centrum powiadamiania ratunkowego[111].

Aktem wykonawczym precyzującym zagadnienia zdefiniowane w **ustawie z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym**[112] jest **rozporządzenie Ministra Zdrowia z dnia 15**

[108] Dz. U. z 2007 r. Nr 178, poz. 1263.
[109] Dz. U. z 2006 r. Nr 191, poz. 1410 ze zm.
[110] Zgodnie z „Koncepcją systemu 112" oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowej organizacji centrów powiadamiania ratunkowego, zaplanowano stworzenie zintegrowanego, ogólnokrajowego systemu obsługi zgłoszeń alarmowych na numer „112", opartego o 16 wojewódzkich centrów obsługi zgłoszeń alarmowych (centrów powiadamiania ratunkowego). Podstawowym założeniem było zbudowanie jednolitego systemu wykorzystującego spójne oprzyrządowanie techniczne (m.in. wprowadzenie jednolitych standardów teleinformatycznych, wyposażenia centrów). Koncepcja uzyskała rekomendację Komitetu ds. Informatyzacji i Łączności Rady Ministrów oraz została przyjęta przez Komitet Stały Rady Ministrów. Centrum Powiadamiania Ratunkowego miało być punktem przyjmowania i przekierowywania zgłoszeń alarmowych kierowanych na numer alarmowy 112 do właściwej jednostki Policji, Państwowej Straży Pożarnej i pogotowia ratunkowego oraz miało współdziałać z innymi podmiotami ratowniczymi. Powstały w ten sposób system miał być zgodny z regulacjami Unii Europejskiej dotyczącymi usługi E-Call i E-112.
[111] Dz. U. z 2009 r. Nr 130, poz. 1073 ze zm.
[112] Dz. U. z 2006 r. Nr 191, poz. 1410 ze zm.

marca 2007 r. w sprawie szpitalnego oddziału ratunkowego[113]. Rozporządzenie to określa szczegółowe zadania szpitalnych oddziałów ratunkowych, szczegółowe wymagania dotyczące lokalizacji szpitalnych oddziałów ratunkowych w strukturze szpitala i warunków technicznych oraz minimalne wyposażenie, organizację i minimalne zasoby kadrowe szpitalnych oddziałów ratunkowych. Zgodnie z rozporządzeniem szpitalny oddział ratunkowy przeznaczony jest do udzielania świadczeń opieki zdrowotnej, polegających na wstępnej diagnostyce oraz podjęciu leczenia w zakresie niezbędnym dla stabilizacji funkcji życiowych osób, które znajdują się w stanie nagłego zagrożenia zdrowotnego. Oddział tego typu może posiadać w swojej strukturze zespoły ratownictwa medycznego.

Podstawowym dokumentem regulującym postępowanie organów zarządzania kryzysowego na poziomie wojewódzkim jest **Wojewódzki Plan Zarządzania Kryzysowego** (WPZK) opracowywany na podstawie art. 5 *Ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym* oraz w oparciu o wytyczne Ministra Spraw Wewnętrznych i Administracji z dnia 21 stycznia 2008 roku do wojewódzkich planów reagowania kryzysowego. Plan zapewnia także wypełnienie obowiązku, jaki nakłada na Wojewodę art. 15 pkt. 4 ustawy z dnia 5 czerwca 1998 r. o administracji rządowej w województwie[114].

Zasady organizacji krajowego systemu ratowniczo-gaśniczego zostały określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 grudnia 1999 roku[115]. System ten został zorganizowany na trzech poziomach: powiatowym, wojewódzkim i krajowym. Zgodnie z rozporządzeniem na poziomie powiatowym wykonuje się wszystkie podstawowe zadania systemu, związane z obszarem powiatu, natomiast poziomy wojewódzki i krajowy spełniają rolę wspomagającą i koordynacyjną w sytuacjach wymagających użycia sił i środków spoza obszaru danego powiatu lub województwa. Omawiane rozporządzenie oprócz przepisów regulujących organizację krajowego systemu ratowniczo-gaśniczego na obszarze powiatu, województwa i kraju zawierało również zadania dotyczące walki z pożarami i innymi klęskami żywiołowymi,

[113] Dz. U. z 2007 r. Nr 55, poz. 365.
[114] Dz. U. z 1998 r. Nr 91, poz. 577, tekst jednolity z dnia 2 sierpnia 2001 r. Dz. U. z 2001 r. Nr 80, poz. 872.
[115] Dz. U. z 1999 r. Nr 111, poz. 1311.

ratownictwa technicznego, chemicznego, ekologicznego i medycznego, organizacji stanowisk kierowania oraz dysponowanie sił i środków systemu do działań ratowniczych, kierowania działaniem ratowniczym, prowadzeniem dokumentacji zdarzeń oraz funkcjonowania krajowego systemu ratowniczo-gaśniczego oraz organizacji odwodów operacyjnych.

Kolejnym rozporządzeniem wynikającym z ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej[116] jest **rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2001 r. w sprawie szczegółowych zasad kierowania i współdziałania jednostek ochrony przeciwpożarowej biorących udział w działaniu ratowniczym**[117]. Definiuje ono przepływ informacji o pożarach, klęskach żywiołowych i innych miejscowych zagrożeniach oraz koordynację i organizację prowadzenia działań ratowniczych.

Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 r. reguluje szczegółowy zakres działania Szefa Obrony Cywilnej Kraju[118], szefów obrony cywilnej województw, powiatów i gmin oraz zasady i tryb kierowania, a także koordynowania przez nich przygotowań i realizacji przedsięwzięć obrony cywilnej[119].

Wprowadzanie ograniczeń wolności oraz praw człowieka i obywatela w czasie stanu nadzwyczajnego pociąga za sobą straty majątkowe. Problem rekompensat tych strat został rozwiązany po raz pierwszy w **ustawie z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela**[120]. Ustawa ta określa podstawy, zakres i tryb wyrównywania strat majątkowych, powstałych w następstwie ograniczenia wolności i praw człowieka i obywatela w czasie stanu nadzwyczajnego (stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej). Zgodnie z ustawą roszczenie

---

116 Dz. U. 1991 r. Nr 81, poz. 351, ze zm.
117 Dz. U. z 2001 r. Nr 82, poz. 895.
118 Obecny kształt Obrony Cywilnej w Polsce, oprócz Protokołu Dodatkowego I do Konwencji Genewskich z 12 sierpnia 1949 r., dotyczącego ochrony ofiar międzynarodowych konfliktów zbrojnych, sporządzonego w Genewie dnia 8 czerwca 1977 r. (Dz. U. z 1992 r. Nr 41, poz. 175), który Rzeczpospolita Polska przyjęła 19 września 1991 r., normuje ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (tekst jednolity, Dz. U. z 2004 r. Nr 241, poz. 2416 ze zm.) oraz akty wykonawcze do niej.
119 Dz. U. z 2002 r. Nr 96, poz. 850.
120 Dz. U. z 2002 r. Nr 233, poz. 1955.

o odszkodowanie przysługuje każdemu, kto poniósł stratę majątkową w następstwie ograniczenia wolności i praw człowieka i obywatela w czasie stanu nadzwyczajnego. Odszkodowanie to, obejmuje wyrównanie straty majątkowej przez Skarb Państwa, bez korzyści, które poszkodowany mógłby osiągnąć, gdyby strata nie powstała.

Wzięcie pod uwagę potrzeb obronności państwa w zagospodarowaniu przestrzennym wynika z rozporządzenia **Ministra Infrastruktury z dnia 7 maja 2004 r. w sprawie sposobu uwzględniania w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa** [121] . Wprowadzenie tego rozporządzenia miało m.in. na celu zapewnienie warunków do obrony terytorium Rzeczypospolitej Polskiej, przez:

- utrzymanie potencjału obronnego państwa,
- zapewnianie warunków do funkcjonowania sił zbrojnych w okresie pokoju oraz do działania w razie agresji militarnej,
- zapewnienie warunków do przyjęcia, rozmieszczenia, zaopatrywania i funkcjonowania sojuszniczych sił zbrojnych na terytorium Rzeczypospolitej Polskiej,
- zapewnianie funkcjonowania gospodarki państwa w razie agresji militarnej, w tym ewakuacji ludności i elementów materialnych gospodarki,
- tworzenie warunków umożliwiających lokalizację, realizację i adaptację obiektów i urządzeń niezbędnych na potrzeby obronne.

Zgodnie z rozporządzeniem potrzeby obronności i bezpieczeństwa państwa w planie zagospodarowania przestrzennego województwa uwzględnia się, określając: powiązania komunikacyjne oraz infrastrukturalne sieci osadniczej województwa, w tym kierunki powiązań trans granicznych, obszary problemowe wraz z zasadami ich zagospodarowania oraz obszary metropolitalne, obszary wsparcia, obszary narażone na niebezpieczeństwo powodzi, granice terenów zamkniętych i ich stref ochronnych, obszary występowania udokumentowanych złóż kopalin, obszary, na których będą rozmieszczone inwestycje celu publicznego o znaczeniu ponadlokalnym.

Ochrona dóbr narodowych jakimi są zabytki została sprecyzowana w **rozporządzeniu Ministra Kultury z dnia 25 sierpnia**

[121] Dz. U. z 2004 r. Nr 125, poz. 1309.

2004 r. w sprawie organizacji i sposobu ochrony zabytków na wypadek konfliktu zbrojnego i sytuacji kryzysowych[122]. Polega ona na planowaniu, przygotowaniu i realizacji przedsięwzięć zapobiegawczych, dokumentacyjnych, zabezpieczających, ratowniczych i konserwatorskich, mających na celu uratowanie zabytków przed zniszczeniem, uszkodzeniem lub zaginięciem. Organizację i sposób ochrony zabytków, na wypadek konfliktu zbrojnego i sytuacji kryzysowych, planuje się w jednostkach organizacyjnych posiadających zabytki oraz na poszczególnych stopniach administracji, ujmując stan zasobu podlegającego ochronie, zagrożenia, zamiar działania, sposób realizacji, niezbędne siły i środki oraz czas i koszty wykonania w sporządzanych w tym celu następujących dokumentach (planie ochrony zabytków jednostki organizacyjnej, gminnym planie ochrony zabytków, powiatowym planie ochrony zabytków, wojewódzkim planie ochrony zabytków, krajowym planie ochrony zabytków).

Konsekwencją wprowadzenia w życie ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym[123] było opracowanie **rozporządzenia Ministra Zdrowia z dnia 16 kwietnia 2007 r. w sprawie doskonalenia zawodowego dyspozytorów medycznych**[124]. Rozporządzenie to stworzyło podstawy do budowy systemu doskonalenia dyspozytorów medycznych. W rozporządzeniu zdefiniowano szczegółowy zakres kształcenia dyspozytorów obejmujący takie zagadnienia, jak:

- system ratownictwa medycznego na terytorium Rzeczypospolitej Polskiej i w innych krajach,
- jednostki współpracujące z systemem,
- organizacja systemu powiadamiania,
- zasady i procedury przyjmowania wezwań oraz dysponowania zespołami ratownictwa medycznego,
- wybrane zagadnienia z medycyny ratunkowej niezbędne do realizacji zadań dyspozytora medycznego,
- podstawy prawne i zasady współdziałania z jednostkami współpracującymi z systemem oraz innymi jednostkami realizującymi zadania z zakresu ratownictwa, a także służbami

[122] Dz. U. z 2004 r. Nr 212, poz. 2153.
[123] Dz. U. z 2006 r. Nr 191, poz. 1410 ze zm.
[124] Dz. U. z 2007 r. Nr 77, poz. 525.

porządku publicznego, w tym zadania i zasady działania Krajowego Systemu Ratowniczo-Gaśniczego,
- zasady zbierania wywiadu medycznego,
- podstawy i algorytmy zbierania wywiadu medycznego przez dyspozytorów medycznych,
- system kodowania i kwalifikacji wezwań,
- podstawy odpowiedzialności karnej i cywilnej dyspozytora medycznego,
- zasady komunikacji i postępowania dyspozytora medycznego z osobami z zaburzeniami psychosomatycznymi,
- zasady komunikacji i postępowania dyspozytora medycznego z dziećmi,
- zasady komunikacji i postępowania dyspozytora medycznego z osobami o utrudnionym kontakcie,
- zasady udzielania pierwszej pomocy oraz zasady przekazywania niezbędnych informacji osobom udzielającym pierwszej pomocy,
- zasady współpracy z lotniczymi zespołami ratownictwa medycznego, wskazania do ich użycia i sposób dysponowania,
- zasady korzystania ze środków łączności dla potrzeb systemu Państwowe Ratownictwo Medyczne,
- zasady korzystania ze sprzętu do nawigacji satelitarnej dla potrzeb systemu Państwowe Ratownictwo Medyczne,
- zasady czytania i analiza map w pozycjonowaniu zdarzeń,
- zasady postępowania w przypadku wystąpienia katastrof naturalnych lub awarii technicznych, zasady postępowania w przypadku zdarzeń masowych i katastrof,
- zasady koordynacji działań ratowniczych na poziomie województwa oraz w przypadku potrzeby użycia zespołów ratownictwa medycznego spoza obszaru województwa,
- zadania lekarza koordynatora ratownictwa medycznego i zasady współpracy.

Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa[125] jest dokumentem, na podstawie którego został ustalony pierwszy skład Rządowego Centrum Bezpieczeństwa (RCB). Zgodnie z tym rozporządzeniem do RCB wchodziły:

[125] Dz. U. z 2008 r. Nr 128, poz. 821.

- kierownictwo Centrum (dyrektor, zastępcy dyrektora),
- Biuro Monitorowania i Analizy Zagrożeń,
- Biuro Ochrony Infrastruktury Krytycznej i Planowania,
- Samodzielny Wydział Szkoleń i Ćwiczeń,
- Samodzielny Wydział do spraw Polityki Informacyjnej i Obsługi Rządowego Zespołu Zarządzania Kryzysowego,
- Samodzielny Wydział Administracyjno-Finansowy,
- Samodzielny Wydział Kontroli, Ochrony Informacji Niejawnych i Audytu.

Obecnie RCB składa się z[126]:

- Kierownictwa (dyrektor, zastępcy dyrektora),
- Zespołu doradców,
- Wydziału Operacyjny,
- Wydziału Polityki Informacyjnej,
- Wydziału Planowania,
- Wydziału Szkoleń i Ćwiczeń,
- Wydziału Analiz,
- Wydziału Ochrony Infrastruktury Krytycznej,
- Wydziału Ochrony Informacji Niejawnych,
- Wydziału Administracyjno – Finansowy.

RCB jest instytucją łączącą wszystkie działania z zakresu zarządzania kryzysowego na poziomie rządowym. Zapewnia w tym zakresie obsługę Rady Ministrów i Prezesa Rady Ministrów oraz Rządowego Zespołu Zarządzania Kryzysowego. Do głównych zadań RCB należy analizowanie zagrożeń oraz możliwości reagowania na nie, w oparciu o dane uzyskiwane ze wszystkich możliwych ośrodków funkcjonujących w ramach administracji publicznej, a także instytucji międzynarodowych[127].

Na podstawie art. 9 ust. 3 *Ustawy o zarządzaniu kryzysowym* zostało przygotowane zarządzenie nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego (RZZK)[128]. Zespół ten funkcjonuje przy Radzie Ministrów jako organ opiniodawczo-doradczy właściwy

[126] Na podstawie rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa, Dz. U. z 2011 r. Nr 86, poz. 471.
[127] rcb.gov.pl, 27.06.2011 r.
[128] M. P. z 2008 r., nr 61, poz. 538.

w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. W skład Zespołu wchodzą:

- Prezes Rady Ministrów - przewodniczący,
- Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych - zastępcy przewodniczącego,
- Minister Spraw Zagranicznych,
- Minister Koordynator Służb Specjalnych - jeżeli został powołany.

Do zadań Zespołu należy: przygotowywanie propozycji użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych, doradzanie w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych, opiniowanie sprawozdań końcowych z działań podejmowanych w związku z zarządzaniem kryzysowym, opiniowanie potrzeb w zakresie odtwarzania infrastruktury lub przywrócenia jej pierwotnego charakteru, opiniowanie i przedkładanie do zatwierdzenia Radzie Ministrów krajowego planu reagowania kryzysowego, opiniowanie i przedkładanie do zatwierdzenia Radzie Ministrów krajowego i wojewódzkich planów ochrony infrastruktury krytycznej, opiniowanie projektów zarządzeń Prezesa Rady Ministrów dotyczących wykazu przedsięwzięć NSPK, opiniowanie projektów decyzji Rady Ministrów dotyczących wprowadzania przedsięwzięć z wykazu przedsięwzięć NSPK, organizowanie współdziałania ze związkami ochotniczych straży pożarnych w sytuacjach kryzysowych.

Szczegółowy zakres danych objętych wojewódzkim planem działania systemu Państwowego Ratownictwa Medycznego, poziom szczegółowości danych objętych tym planem oraz kryteria kalkulacji kosztów działalności zespołów ratownictwa medycznego zostały określone w **rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie wojewódzkiego planu działania systemu Państwowe Ratownictwo Medyczne oraz kryteriów kalkulacji kosztów działalności zespołów ratownictwa medycznego**[129]. Zgodnie z rozporządzeniem plan zawiera:

- charakterystykę potencjalnych zagrożeń dla życia lub zdrowia ludzi, mogących wystąpić na obszarze województwa,
- informacje o jednostkach systemu Państwowe Ratownictwo Medyczne, centrach urazowych oraz o szpitalach posiadających

[129] Dz. U. z 2011 r. Nr 3, poz. 6.

jednostki organizacyjne wyspecjalizowane w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego,
- informacje o planowanych na kolejne lata, nowych, przenoszonych lub likwidowanych jednostkach systemu i centrach urazowych na obszarze województwa,
- opis struktury systemu powiadamiania o stanach nagłego zagrożenia zdrowotnego, informacje o lokalizacji wojewódzkich centrów powiadamiania ratunkowego i centrów powiadamiania ratunkowego, na obszarze województwa,
- sposób współpracy wojewody i dysponentów jednostek systemu z organami administracji publicznej i jednostkami systemu z innych województw,
- sposób współpracy jednostek systemu z jednostkami współpracującymi z systemem na obszarze województwa,
- kalkulację kosztów działalności zespołów ratownictwa medycznego na obszarze województwa, z wyłączeniem lotniczych zespołów ratownictwa medycznego.

Kolejnym aktem normatywnym wynikającym z ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym [130] jest **rozporządzenie Ministra Zdrowia z dnia 24 lutego 2009 r. w sprawie szczegółowego zakresu uprawnień i obowiązków lekarza koordynatora ratownictwa medycznego [131]**. Rozporządzenie to precyzuje uprawnienia lekarza koordynatora ratownictwa medycznego w zakresie uzyskiwanie informacji od dysponentów jednostek, zakładów opieki zdrowotnej i jednostek współpracujących z systemem oraz od dyspozytorów medycznych. Dodatkowo określone zostały w nim obowiązki lekarza koordynatora dotyczące:
- współpracy z dyspozytorami medycznymi, jednostkami systemu, jednostkami organizacyjnymi szpitali wyspecjalizowanymi w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego oraz jednostkami współpracującymi z systemem,
- współpracy z lekarzem koordynatorem ratownictwa medycznego z innego województwa w zakresie wykorzystania

[130] Dz. U. z 2006 r. Nr 191, poz. 1410 ze zm.
[131] Dz. U. z 2009 r. Nr 39, poz. 322.

w zdarzeniach jednostek systemu i jednostek współpracujących z systemem, sporządzania raportu z całodobowego dyżuru,
- sporządzania raportu z koordynowania działań podejmowanych w sytuacji wystąpienia katastrof naturalnych, klęsk żywiołowych i awarii technicznych, zdarzeń powodujących stan nagłego zagrożenia zdrowotnego znacznej liczby osób lub innych zdarzeń,
- bieżącego monitorowanie zdarzeń, których skutki mogą spowodować stan nagłego zagrożenia zdrowotnego znacznej liczby osób, wydawania polecenia dyspozytorowi medycznemu zadysponowania zespołem ratownictwa medycznego poza obszar działania dysponenta jednostki,
- udzielania dyspozytorom medycznym i kierującym akcją prowadzenia medycznych czynności ratunkowych niezbędnych informacji, zgodnie z aktualną wiedzą medyczną, w zakresie podejmowania medycznych czynności ratunkowych,
- współpracy z wyznaczoną przez ministra właściwego do spraw zdrowia, jednostką badawczo-rozwojową do wykonywania międzynarodowych przepisów zdrowotnych w zakresie pozyskiwania oraz wymiany informacji i analiz o zagrożeniach bezpieczeństwa zdrowotnego ludności.

Na podstawie art. 14e ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej[132] zostało wprowadzone **rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2009 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego i wojewódzkich centrów powiadamiania ratunkowego**[133]. Określa ono:
- szczegółową organizację, sposób funkcjonowania oraz realizacji zadań centrów powiadamiania ratunkowego i wojewódzkich centrów powiadamiania ratunkowego,
- ramowe procedury obsługi zgłoszeń przychodzących na numery alarmowe,
- kwalifikacje wymagane dla operatorów numerów alarmowych,
- sposób i organizację przeprowadzania szkolenia operatorów numerów alarmowych,

[132] Dz. U. 1991 r. Nr 81, poz. 351, ze zm.
[133] Dz. U. z 2009 r. Nr 130, poz. 1073 ze zm.

- zakres, formę, sposób tworzenia i przekazywania informacji niezbędnych do funkcjonowania systemu powiadamiania ratunkowego,
- kryteria do określenia liczby, lokalizacji i terenu działania centrum powiadamiania ratunkowego oraz liczby stanowisk dyspozytorów medycznych i stanowisk operatorów numerów alarmowych.

2.3. SYSTEM ZARZĄDZANIA KRYZYSOWEGO

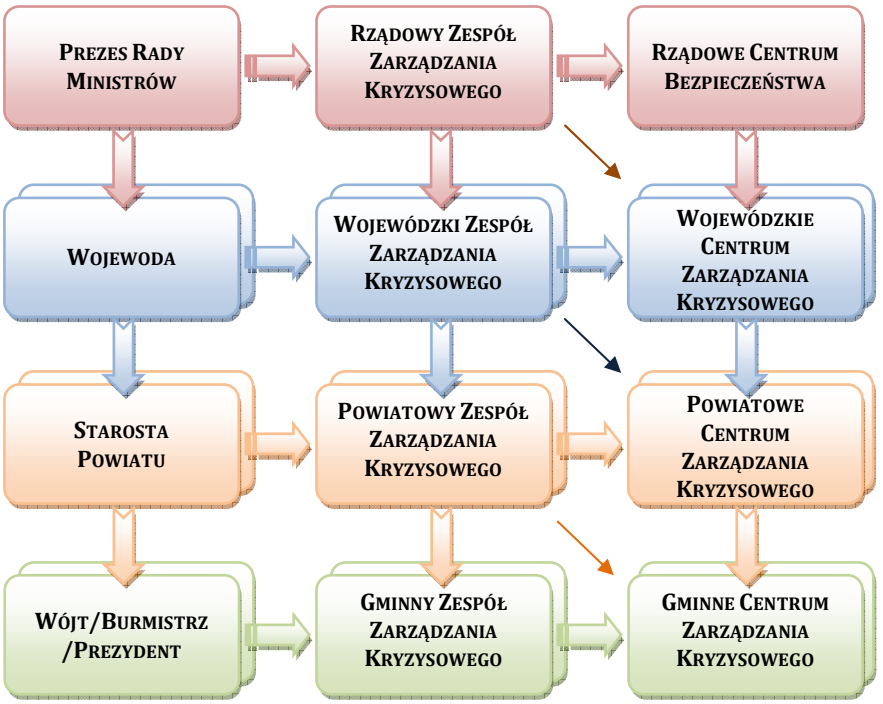
Definiując pojęcie systemu zarządzania kryzysowego należy je oprzeć o dwa pojęcia: *system* oraz *zarządzanie kryzysowe*. Zarządzanie kryzysowe zostało już omówione szczegółowo w podrozdziale 2.1., natomiast pojęcie *system* wymaga sprecyzowania. Najbardziej powszechne definicje pojęcia *system* mówią, że jest to:

- zbiór elementów i zachodzących między nimi relacji[134],
- byt przejawiający swe istnienie przez synergiczne współdziałanie swych elementów[135],
- uporządkowana para składająca się ze zbioru elementów (składników) i relacji łączących te elementy[136].

Szerokie rozważania na temat definiowania systemu zarządzania kryzysowego przedstawił W. Kitler[137]. Zaproponowana przez niego definicja mówi, że system zarządzania kryzysowego to skoordynowany wewnętrznie i tworzący pewną całość dynamicznie się rozwijający układ trzech zasadniczych podsystemów (podsystemu organów zarządzających – aparatu zarządzającego, podsystemu powiązań informacyjnych wewnątrz organizacji, podsystemu metod i działań, czyli reguł funkcjonowania organizacji) realizujących wspólnie jeden zasadniczy cel: obniżenie stopnia oddziaływania czynników sytuacji kryzysowej na funkcjonowanie organizacji, a w przypadku ich wystąpienia minimalizacji ich wpływu i skutków. System zarządzania kryzysowego stanowi integralną część systemu zarządzania organizacją

[134] M. Mazur, *Pojęcie systemu i rygory jego stosowania*. [w:] Materiały Szkoły Podstaw Inżynierii Systemów nr 2, Komitet Budowy Maszyn PAN, Orzysz1976.
[135] C. Cempel, *Teoria i inżynieria systemów*, Politechnika Poznańska, Poznań 2004.
[136] K. Ficoń, *Badania operacyjne stosowane. Modele i aplikacji*, BEL Studio, Warszawa 2006, s. 76.
[137] J. Gryz, W. Kitler, *System …*, *dz. cyt.*, ss. 34-41.

i służy przygotowaniu, a następnie zapewnieniu jej sprawnego funkcjonowania w czasie występowania sytuacji kryzysowych, w tym kryzysów.



Rys. 2.10. Struktura systemu zarządzania kryzysowego w Polsce[138]

Zdaniem autora pojęcie systemu zarządzania kryzysowego można zdefiniować, jako zbiór organów i instytucji administracji publicznej powiązanych ze sobą relacjami, których głównym celem funkcjonowania jest realizacja procesu zarządzania kryzysowego (Rys. 2.10).

W myśl Strategii Bezpieczeństwa Narodowego RP [139], zapewnienie odpowiedniego poziomu bezpieczeństwa wewnętrznego, akceptowanego przez naszych obywateli, wymaga między innymi wdrożenia efektywnego systemu zarządzania kryzysowego. Budowa takiego systemu wymaga współpracy administracji publicznej wszystkich szczebli oraz podmiotów spoza tego obszaru. Należy

[138] K. Ficoń, *Logistyka ..., dz. cyt.*, s. 62.
[139] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2007.

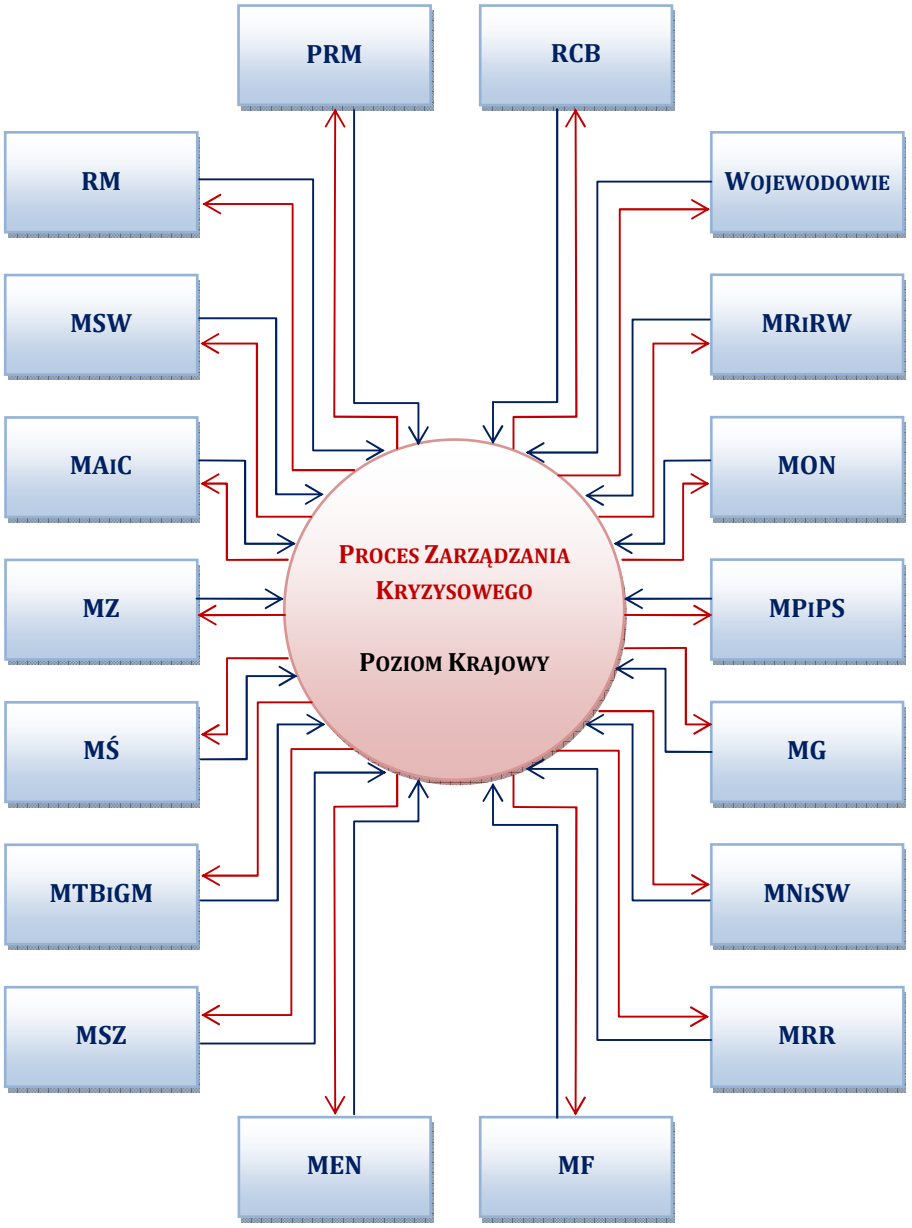
podkreślić, że uczyniono w tym zakresie już bardzo wiele. Stworzono podstawy formalno-prawne oraz zdefiniowano podstawowe pojęcia takie jak: sytuacja kryzysowa, zarządzanie kryzysowe czy też infrastruktura krytyczna. Ustawa o zarządzaniu kryzysowym[140] definiuje również hierarchiczną strukturę tego systemu oraz zakres zadań dla poszczególnych jego elementów.

Organy zarządzania kryzysowego wskazane na wszystkich poziomach administracji, mają określone zadania i obowiązki w sytuacji kryzysowej natomiast rzeczywiste działanie pokazało, że w stworzonym systemie brakuje jasnego wskazania odpowiedzialności za realizację wielu zadań. Problemem jest brak aktów wykonawczych do ustawy. W przeciągu pięciu lat od momentu wdrożenia *Ustawy o zarządzaniu kryzysowym* zostały opracowane do niej następujące akty wykonawcze:

- Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa (rozporządzenie aktualnie uchylone),
- Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania,
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego,
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej,
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej,
- Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa,
- Zarządzenie Nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego (aktualnie uchylone),

[140] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz. U. z 2007 r. Nr 89, poz. 590.

– Zarządzenie Nr 78 Prezesa Rady Ministrów z dnia 11 października 2011 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego.



Rys. 2.11. Struktura systemu zarządzania kryzysowego na szczeblu krajowym

Krajowy Plan Zarządzania Kryzysowego przewiduje, że proces zarządzania kryzysowego na poziomie krajowym będzie realizowany przez następujące elementy (Rys. 2.11):

PRM – Prezes Rady Ministrów,
RM – Rada Ministrów,
RCB – Rządowe Centrum Bezpieczeństwa,
– Wojewodowie,
MSW – Ministerstwo Spraw Wewnętrznych,
MAiC – Ministerstwo Administracji i Cyfryzacji,
MZ – Ministerstwo Zdrowia,
MŚ – Ministerstwo Środowiska,
MTBiGM – Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej,
MSZ – Ministerstwo Spraw Zagranicznych,
MEN – Ministerstwo Edukacji Narodowej,
MF – Ministerstwo Finansów,
MRiRW – Ministerstwo Rolnictwa i Rozwoju Wsi,
MON – Ministerstwo Obrony Narodowej,
MPiPS – Ministerstwo Pracy i Polityki Społecznej,
MG – Ministerstwo Gospodarki,
MNiSW – Ministerstwa Nauki i Szkolnictwa Wyższego,
MRR – Ministerstwo Rozwoju Regionalnego.

Proces zarządzania kryzysowego na terytorium Rzeczypospolitej Polskiej realizowany jest przez Radę Ministrów i stojącego na jej czele Premiera. W sytuacjach, kiedy wymagane jest podjęcie natychmiastowych działań funkcja ta może być realizowana przez ministra właściwego do spraw wewnętrznych, który zobowiązany jest do niezwłocznego zawiadomienia o swoich działaniach Prezesa Rady Ministrów.

Prezes Rady Ministrów, z zachowaniem przepisów o ochronie informacji niejawnych, określa, w drodze zarządzenia, wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego oraz organy odpowiedzialne za ich uruchamianie.

Organem opiniodawczo-doradczym właściwym w sprawach inicjowania i koordynowania działań podejmowanych w zakresie

zarządzania kryzysowego jest Rządowy Zespół Zarządzania Kryzysowego (RZZK)[141].

Rys. 2.12. Przepływ informacji na potrzeby zarządzania kryzysowego na obszarze Rzeczypospolitej Polskiej

Ważnym elementem systemu zarządzania kryzysowego jest Rządowe Centrum Bezpieczeństwa (Rys. 2.12). Realizuje ono zadania z zakresu:

[141] W zależności od potrzeb (zaistniałej sytuacji kryzysowej) w procesie zarządzania kryzysowego biorą udział: ministrowie kierujący działami administracji rządowej, Główny Geodeta Kraju, Główny Inspektor Ochrony Środowiska, Główny Inspektor Sanitarny, Główny Lekarz Weterynarii, Komendant Główny Państwowej Straży Pożarnej, Komendant Główny Policji, Komendant Główny Straży Granicznej, Prezes Krajowego Zarządu Gospodarki Wodnej, Prezes Państwowej Agencji Atomistyki, Prezes Urzędu Lotnictwa Cywilnego, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Obrony Cywilnej Kraju, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Wywiadu Wojskowego.

- planowania cywilnego i monitorowania potencjalnych zagrożeń,
- uzgadniania planów zarządzania kryzysowego sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych,
- uruchamiania procedur związanych z zarządzaniem kryzysowym,
- przygotowywania projektów opinii i stanowisk oraz obsługi techniczno-organizacyjna prac RZZK,
- koordynacji polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej,
- organizowania, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych,
- obiegu informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego,
- zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym,
- ochrony infrastruktury krytycznej oraz europejskiej infrastruktury krytycznej,
- informowania podmiotów o potencjalnych zagrożeniach oraz działaniach podjętych przez właściwe organy,
- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej.

W ramach krajowego systemu zarządzania kryzysowego zaczynają już funkcjonować centra zarządzania kryzysowego tworzone przez ministrów oraz centralne organy administracji rządowej, do których zakresu działania należą sprawy związane z zapewnieniem bezpieczeństwa narodowego, w tym ochrony ludności lub gospodarczych podstaw bezpieczeństwa państwa (Rys. 2.12). Docelowo centra zarządzania kryzysowego zostaną utworzone przez następujące organy[142]:

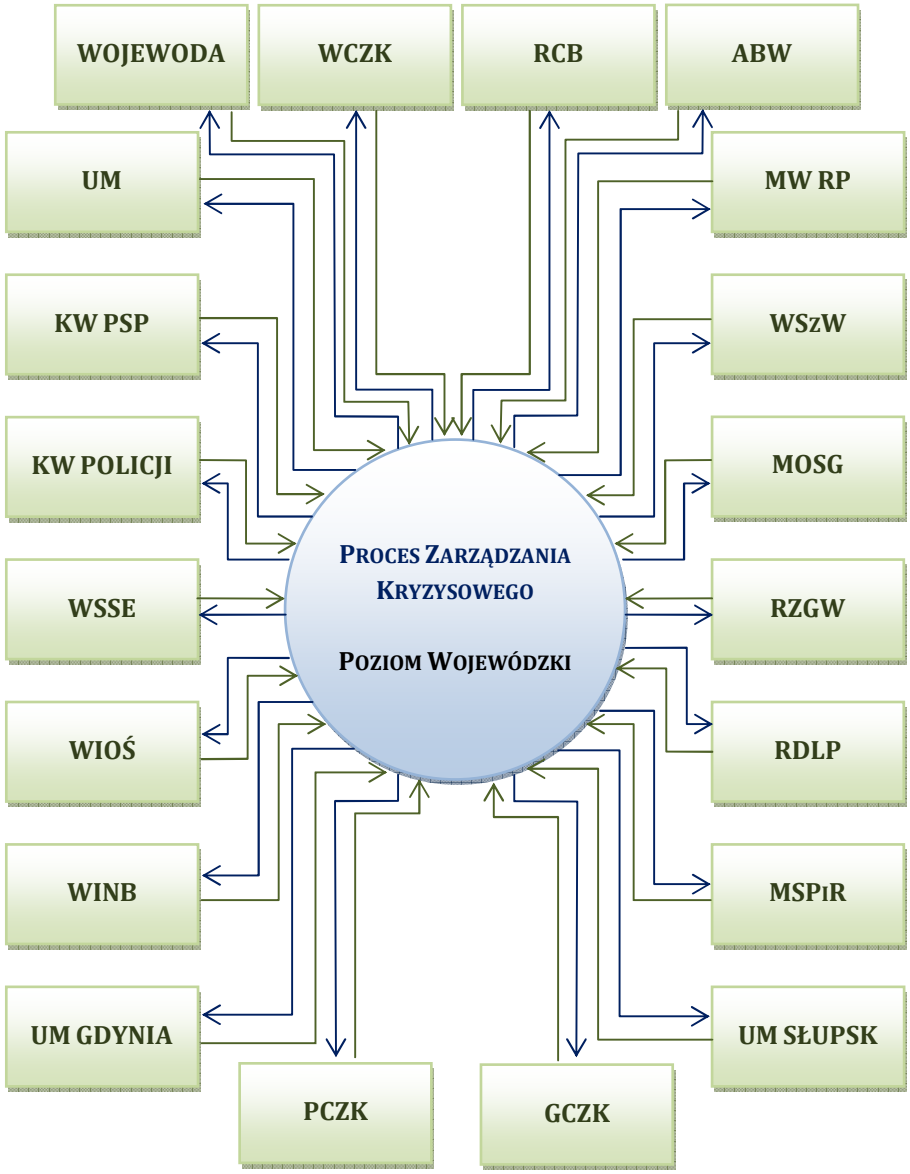
- Ministra Obrony Narodowej,
- Ministra Sprawiedliwości,
- ministra właściwego do spraw rolnictwa,

[142] *Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania*, Dz. U. 2009 nr 226 poz. 1810.

- ministra właściwego do spraw środowiska,
- ministra właściwego do spraw zagranicznych,
- ministra właściwego do spraw zdrowia,
- Komendanta Głównego Państwowej Straży Pożarnej,
- Komendanta Głównego Policji,
- Komendanta Głównego Straży Granicznej,
- Szefa Agencji Bezpieczeństwa Wewnętrznego,
- Szefa Agencji Wywiadu,
- Szefa Służby Kontrwywiadu Wojskowego,
- Szefa Służby Wywiadu Wojskowego.

Organem odpowiedzialnym za zarządzanie kryzysowe w województwie jest wojewoda (Rys. 2.13). Do zadań wojewody w sprawach zarządzania kryzysowego należy:

- kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa,
- realizacja zadań z zakresu planowania cywilnego, w tym:
- zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego,
- wnioskowanie o użycie pododdziałów lub oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań z zakresu zarządzania kryzysowego,
- wykonywanie przedsięwzięć wynikających z dokumentów planistycznych wykonywanych w ramach planowania operacyjnego realizowanego w województwie,
- zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym,
- współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym,
- organizacja wykonania zadań z zakresu ochrony infrastruktury krytycznej.



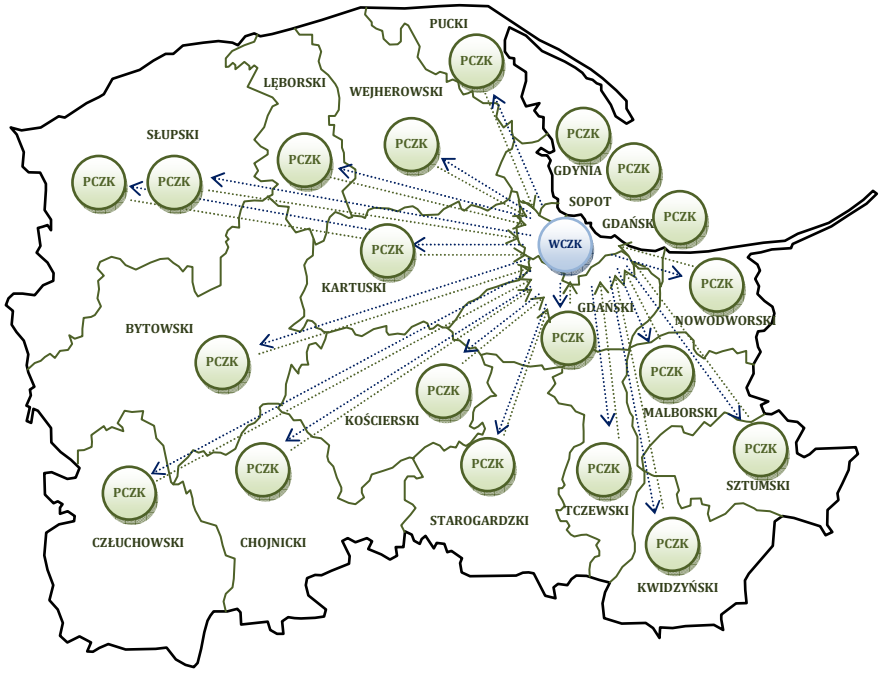
Rys. 2.13. Struktura systemu zarządzania kryzysowego na szczeblu województwa pomorskiego

W skład systemu zarządzania kryzysowego w województwie pomorskim wchodzą następujące elementy:

– Wojewoda,

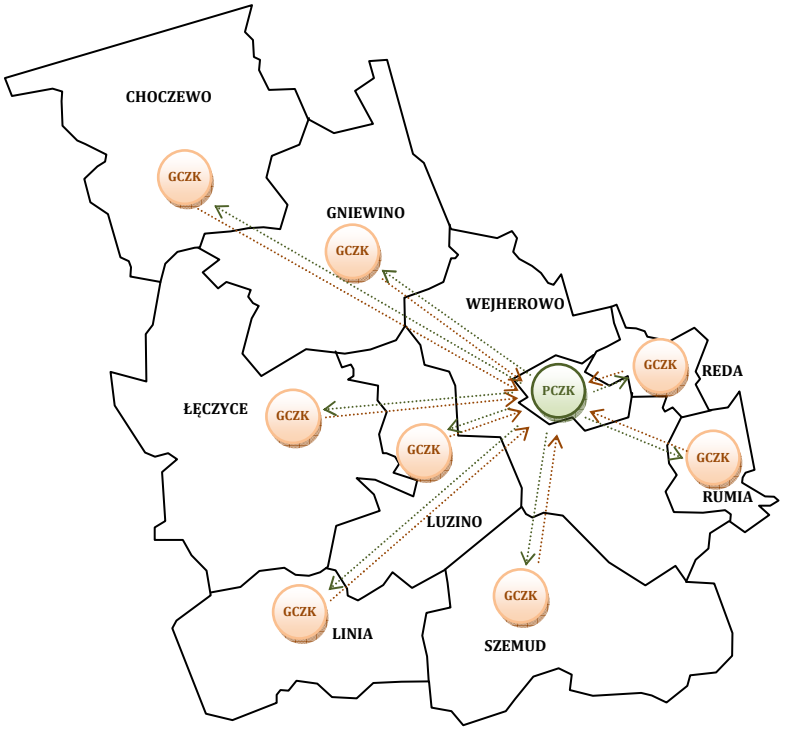
WCZK – Wojewódzkie Centrum Zarządzania Kryzysowego,

UM	–	Urząd Marszałkowski,
ABW	–	Agencja Bezpieczeństwa Wewnętrznego,
MW RP	–	Marynarka Wojenne RP,
KW PSP	–	Komenda Wojewódzka Państwowej Straży Pożarnej,
KW Policji	–	Komenda Wojewódzka Policji,
WSzW	–	Wojewódzki Sztab Wojskowy,
MOSG	–	Morski Oddział Straży Granicznej,
RZGW	–	Regionalny Zarząd Gospodarki Wodnej,
WIOŚ	–	Wojewódzki Inspektorat Ochrony Środowiska,
RDLP	–	Regionalna Dyrekcja Lasów Państwowych,
WINB	–	Wojewódzki Inspektorat Nadzoru Budowlanego,
MSPiR	–	Morska Służba Poszukiwania i Ratownictwa,
UM Gdynia	–	Urząd Morski w Gdyni,
UM Słupsk	–	Urząd Morski w Słupsku,
PCZK	–	Powiatowe Centra Zarządzania Kryzysowego,
GCZK	–	Gminne Centra Zarządzania Kryzysowego.



Rys. 2.14. Przepływ informacji na potrzeby zarządzania kryzysowego na obszarze województwa pomorskiego

W każdym województwie pracują centra zarządzania kryzysowego (WCZK) pełniące całodobowy dyżur w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego na obszarze Rzeczypospolitej Polskiej (Rys. 2.14).



Rys. 2.15. Przepływ informacji na potrzeby zarządzania kryzysowego na obszarze powiatu wejherowskiego

Wojewódzkie Centra Zarządzania Kryzysowego są zasilane informacyjnie przez centra zarządzania kryzysowego (PCZK) usytuowane w powiatach (Rys. 2.15). Poziom gminny systemu zarządzania kryzysowego pozostawia wiele do życzenia i wymaga jeszcze dużo pracy. Można się spotkać z opiniami, że jest to poziom „wirtualny".

2.4. INFRASTRUKTURA KRYTYCZNA

Poważne awarie techniczne, anomalie klimatyczne, wzrost zagrożenia atakami terrorystycznymi oraz wroga działalność w cyberprzestrzeni powodują, że bardzo istotnym zadaniem realizowanym przez system bezpieczeństwa narodowego, a w szczególności przez system zarządzania kryzysowego jest ochrona infrastruktury krytycznej.

Pojęcie infrastruktury krytycznej już na stałe zagościło w problematyce bezpieczeństwa i przez cały czas ewoluuje. Mimo, że ochrona najważniejszych obiektów czy instalacji prowadzona była już od dawna podczas trwania konfliktów zbrojnych to pod koniec XX i na początku XXI wieku cały ten proces nabrał szczególnego znaczenia. Okazało się bowiem, że podczas pokoju również należy chronić systemy sektora militarnego, społecznego oraz gospodarczego tak, aby nie dopuścić do przerwania ciągłości ich pracy. Przyczyniły się do tego poważne awarie sieci energetycznych w USA i Kanadzie[143], ataki terrorystyczne przeprowadzone na World Trade Center i Pentagon w USA[144], zamachy w Madrycie[145], zamachy w Londynie[146] oraz liczne klęski żywiołowe[147]. Ostatnie lata pokazują również, że dotkliwe koszty dla zaawansowanych technologicznie społeczeństw mogą przynieść ataki prowadzone w cyberprzestrzeni[148].

[143] 14 sierpnia 2003 roku miała miejsce awaria sieci energetycznej na obszarze stanu Michigan i Nowy Jork (USA) oraz prowincji Ontario (Kanada). Brak energii dotknął wówczas ponad 60 milionów ludzi.

[144] Zamach został przeprowadzony 11 września 2001 roku przez 19 zamachowców. W zamachu zginęło łącznie około 3 tys. osób (źródło: Final Report of the National Commission on Terrorist Attacks Upon the United States, www.c-span.org/pdf/911finalreportexecsum.pdf).

[145] 11 marca 2004 roku została przeprowadzona seria ataków na pociągi w Madrycie. Zginęło w nich 191 osób, a ponad 1800 zostało rannych (źródło: www.britannica.com/EBchecked/ topic/1279086/Madrid-train-bombings-of-2004).

[146] 7 lipca 2005 roku miały miejsce trzy eksplozje ładunków wybuchowych w londyńskim metrze oraz jedna w autobusie. W zamachach zginęło 52 osoby a ponad 700 zostało rannych. Sparaliżowano system komunikacji miejskiej w Londynie (źródło: www.britannica.com/EBchecked/ topic/1696348/London-bombings-of-2005).

[147] Podczas trzęsienia ziemi w Japonii (11 marca 2011 roku) zginęło około 15 tys. osób. W elektrowni atomowej Fukushima I doszło do serii wypadków jądrowych i skażenia środowiska.

[148] Koszty ponoszone przez USA w wyniku ataków w cyberprzestrzeni wynoszą około 9 mln $ rocznie, w Niemczech suma ta wynosi około 6 mln $, w Japonii około 5 mln $, www.networkworld.com/ news/ 2012/100812-ponemon-cyberattacks-263113.html.

Pierwsze inicjatywy w tym obszarze zostały podjęte w 1996 r. przez prezydenta Billa Clintona, który utworzył specjalną komisję do zbadania podatności infrastruktury krytycznej Stanów Zjednoczonych na zagrożenia. W skład komisji weszli przedstawiciele rządu, przedstawiciele organizacji pozarządowych oraz właściciele infrastruktury krytycznej z sektora prywatnego[149].

Komisja zaliczyła do infrastruktury krytycznej systemy telekomunikacyjne, systemy elektroenergetyczne, systemy zaopatrzenia w gaz, magazynowania i transportu ropy naftowej, bankowość i finanse, systemy transportowe, systemy zaopatrzenia w wodę oraz służby ratownicze. Zagrożenia zostały natomiast podzielone na dwie kategorie: zagrożenia fizyczne (uszkodzenia dóbr materialnych) i zagrożenia systemów teleinformatycznych (zagrożenia z cyberprzestrzeni). Pierwsze przedsięwzięcia z zakresu ochrony infrastruktury krytycznej obejmowały:

- przekazywanie wiedzy ekspertów dotyczącej wykrywania, zapobiegania, powstrzymywania lub ograniczania ataków na elementy infrastruktury krytycznej oraz przywracania elementów infrastruktury krytycznej do działania,
- wydawania ostrzeżeń o zagrożeniach,
- prowadzenie szkoleń dotyczących uodparniania elementów infrastruktury krytycznej na ataki oraz reagowania na zdarzenia,
- koordynację sił i służb podczas ataków i prowadzenia dochodzeń.

Obecnie proces ochrony infrastruktury krytycznej w USA obejmuje osiemnaście sektorów[150]. Należą do nich (Rys. 2.16):

- rolnictwo i żywność,
- przemysł obronny,
- energia,
- ochrona zdrowia,
- dziedzictwo narodowe,
- bankowość i finanse,
- woda,
- chemia,

[149] *Critical Infrastructure Threats and Terrorism*, DCSINT Handbook No. 1.02, 2006, s 1.
[150] *National Infrastructure Protection Plan 2009*, http://www.dhs.gov/national-infrastructure-protection-plan, s. 3.

- obiekty użyteczności publicznej,
- przemysł,
- gospodarka wodna,
- służby ratownicze,
- energetyka jądrowa,
- technologie informacyjne,
- łączność,
- poczta,
- transport,
- administracja rządowa.

Rys. 2.16. Sektory infrastruktury krytycznej w USA[151]

Departament spraw wewnętrznych USA został zobligowany ustawą w 2002 roku do opracowania narodowego planu ochrony infrastruktury krytycznej i kluczowych zasobów oraz koordynowania

[151] *http://www.dhs.gov/critical-infrastructure-sectors.*

działań pomiędzy partnerami odpowiedzialnymi za ochronę infrastruktury krytycznej.

Administracja rządowa Stanów Zjednoczonych jest świadoma tego, że ataki na infrastrukturę krytyczną mogą znacznie zakłócić funkcjonowanie rządu i gospodarki. Skutki ataków są zazwyczaj bardzo dotkliwe i wywołują efekt domina, wykraczając daleko poza fizyczne miejsce zdarzenia kryzysowego.

Bezpośrednie ataki terrorystyczne, zagrożenia naturalne, zdarzenia wywołane przez człowieka oraz zagrożenia w cyberprzestrzeni mogą powodować katastrofalne skutki w zakresie strat w ludziach, zniszczenia mienia i strat ekonomicznych, jak również utratę zaufania wśród społeczeństwa.

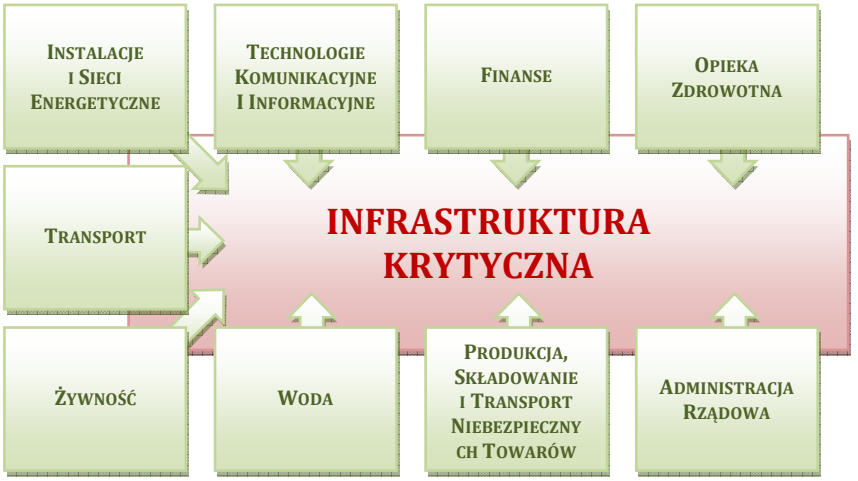
Opierając się na doświadczeniach Stanów Zjednoczonych również i inne państwa rozpoczęły projekty dotyczące ochrony infrastruktury krytycznej, w tym także Polska. Bardzo duży wpływ na kształtowanie się procesu ochrony infrastruktury krytycznej w Polsce mają akty normatywne NATO oraz Unii Europejskiej.

Prace nad stworzeniem mechanizmów ochrony infrastruktury krytycznej w Unii Europejskiej rozpoczęto po ataku terrorystycznym z 11 września 2001 roku na World Trade Center w USA, jednak ich faktyczna intensyfikacja miała miejsce dopiero w 2004 roku po atakach terrorystycznych w Madrycie, czyli w momencie kiedy zagrożenia bezpośrednio dotknęły „organizm" Unii Europejskiej. Rada Europejska w czerwcu 2004 r. zgłosiła postulat, aby opracować ogólną strategię zwiększenia ochrony infrastruktury krytycznej. W odpowiedzi na ten postulat już w październiku 2004 roku Komisja Wspólnot Europejskich wydała komunikat dotyczący ochrony infrastruktury krytycznej w walce z terroryzmem[152].

W wymienionym komunikacie zamieszczono jasne propozycje dotyczące sposobu usprawnienia europejskich systemów zapobiegania atakom terrorystycznym wymierzonym przeciwko infrastrukturze krytycznej, gotowości i reakcji na takie ataki. Przedstawiono definicję infrastruktury krytycznej, w myśl której są to *zakłady fizyczne i urządzenia technologii informacyjnych, sieci, usługi i aktywa, których*

[152] *Communication from the Commission to the Council and the European Parliament, Critical Infrastructure Protection in the fight against terrorism*, Brussels, 20.10.2004, COM(2004) 702 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF).

zakłócenie pracy lub zniszczenie miałoby poważny wpływ na zdrowie, bezpieczeństwo lub dobrobyt ekonomiczny obywateli lub na skuteczność funkcjonowania rządów w Państwach Członkowskich.



Rys. 2.17. Sektory infrastruktury krytycznej w UE (2004 rok)

Do infrastruktury krytycznej zaliczono następujące elementy (Rys. 2.17):

- instalacje i sieci energetyczne (np. produkcja energii elektrycznej, ropy naftowej i gazu, magazyny i rafinerie, system transmisji i dystrybucji),
- technologie komunikacyjne i informacyjne (np. telekomunikacja, radio i telewizja, oprogramowanie, sprzęt i sieci komputerowe, w tym Internet),
- finanse (np. bankowość, papiery wartościowe i inwestycje),
- opiekę zdrowotną (np. szpitale, zakłady opieki zdrowotnej i punkty krwiodawstwa, laboratoria i farmaceutyki, poszukiwania i ratownictwo, pogotowie ratunkowe),
- żywność (np. bezpieczeństwo, środki produkcji, dystrybucja hurtowa i przemysł spożywczy),
- wodę (np. tamy, zbiorniki, oczyszczalnie i sieci wodociągowe),
- transport (np. lotniska, porty, urządzenia intermodalne, sieci kolejowe i tranzytu masowego, systemy kontroli ruchu),

- produkcję, składowanie i transport niebezpiecznych towarów (np. materiały chemiczne, biologiczne, radiologiczne i nuklearne),
- administracja rządowa (np. usługi podstawowe, urządzenia, sieci informacyjne, aktywa i kluczowe krajowe lokalizacje i pomniki).

Zaproponowano również przygotowanie nowych instrumentów – Europejskiego Programu Ochrony Infrastruktury Krytycznej [153] (EPOIK) oraz Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej [154] (SOZIK). Sieć oprócz przesyłania informacji o prawdopodobnych zagrożeniach dla infrastruktury krytycznej, miała tworzyć możliwość wymiany informacji na temat najlepszych praktyk oraz środków zapewniających odpowiedni poziom bezpieczeństwa. Miała się ona stać płaszczyzną wymiany informacji pomiędzy ekspertami krajów członkowskich, przedstawicielami Komisji Wspólnot Europejskich oraz sektorem prywatnym.

Kolejnym ważnym dokumentem wydanym przez Komisję Wspólnot Europejskich była tzw. Zielona Księga przyjęta 17 listopada 2005 roku[155].

Głównym celem zielonej księgi było gromadzenie danych i informacji dotyczących możliwych opcji polityki EPOIK przy współudziale jak największej liczby zainteresowanych stron. Zwrócono uwagę, że efektywna ochrona infrastruktury krytycznej wymaga bezwzględnie skutecznej komunikacji, koordynacji i współpracy zarówno na poziomie krajowym jak i unijnym pomiędzy wszystkimi zainteresowanymi stronami:

- właścicielami i operatorami infrastruktury,
- organami regulacji,
- organizacjami zawodowymi i stowarzyszeniami branżowymi,
- władzami publicznymi na wszystkich poziomach,
- ogółem społeczeństwa.

Zielona księga zawierała również dokładniejsze informacje na temat utworzenia EPOIK i SOZIK oraz stanowiła drugą fazę procesu

[153] European Programme for Critical Infrastructure Protection (EPCIP).
[154] Critical Infrastructure Warning Information Network (CIWIN).
[155] *Green Paper on a European Programme for Critical Infrastructure Protection, Brussels*, 17.11.2005, COM(2005) 576 final (http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/ com2005_0576en01.pdf).

konsultacji dotyczącego ustanowienia Europejskiego Programu Ochrony Infrastruktury Krytycznej.

Założono, że celem EPOIK byłoby zapewnienie istnienia odpowiednich i jednakowych poziomów zabezpieczeń ochronnych w zakresie infrastruktury krytycznej, ograniczenie przypadków awarii do minimum oraz dostarczenie szybkich i sprawdzonych środków naprawczych w całej Unii.

Przyjęto, że poziom ochrony może być zróżnicowany dla poszczególnych elementów infrastruktury krytycznej i może być uzależniony od wagi skutków ewentualnej awarii. Podkreślono, że EPOIK powinien być ciągłym procesem, wymagającym systematycznego przeglądu w celu uwzględnienia nowych zagrożeń.

Bardzo istotnym elementem Zielonej Księgi było zaproponowanie podstawowych zasad funkcjonowania EPOIK. Należały do nich:

- **pomocniczość** (ochrona infrastruktury krytycznej leży przede wszystkim w kompetencji władz krajowych. Główna odpowiedzialność za ochronę infrastruktury krytycznej spoczywałaby na Państwach Członkowskich i właścicielach/ operatorach działających według wspólnych ram. Komisja z kolei skupiłaby się na aspektach związanych z ochroną infrastruktury krytycznej mającej charakter transgraniczny. Odpowiedzialność właścicieli i operatorów za podejmowanie własnych decyzji i opracowywanie planów ochrony swojego mienia nie powinna ulec zmianie),
- **komplementarność** (wspólne ramy EPOIK stanowiłyby uzupełnienie istniejących środków. Tam, gdzie już działają mechanizmy wspólnotowe, powinno się nadal z nich korzystać, gdyż pomagają one w ogólnej realizacji EPOIK),
- **poufność** (wymiana informacji dotyczących ochrony infrastruktury krytycznej odbywałaby się w atmosferze zaufania i poufności. Jest to konieczne, jeżeli weźmie się pod uwagę fakt, że szczególne informacje dotyczące infrastruktury krytycznej mogą zostać wykorzystane w celu spowodowania awarii lub wywołania niedopuszczalnych skutków w urządzeniach infrastruktury krytycznej. Informacje byłyby zastrzeżone na poziomie UE i Państw Członkowskich, a dostęp do nich przyznawano by jedynie w koniecznych przypadkach),

- **współpraca zainteresowanych stron** (wszystkie zainteresowane strony, w tym Państwa Członkowskie, Komisja, stowarzyszenia branżowe, organy normalizacyjne, właściciele, operatorzy i użytkownicy mają rolę do odegrania w ochronie IK. Wszystkie zainteresowane strony powinny współpracować i przyczyniać się do rozwoju i realizacji EPOIK zgodnie ze swoją szczególną rolą i odpowiedzialnością. Władze Państw Członkowskich przewodniczyłyby pracom nad spójnym krajowym podejściem do ochrony infrastruktury krytycznej i procesowi jego wdrażania oraz koordynowały te działania na obszarze swojej właściwości. Właściciele, operatorzy i użytkownicy aktywnie wspieraliby te działania na poziomie krajowym i UE. W dziedzinach, w których normy sektorowe nie istnieją lub nie ustanowiono jeszcze norm międzynarodowych, organizacje normalizacyjne mogłyby w stosownych przypadkach przyjąć wspólne normy),
- **proporcjonalność** (strategie i środki ochronne byłyby proporcjonalne do poziomu ryzyka, ponieważ nie wszystkie rodzaje infrastruktury mogą być chronione przed wszystkimi zagrożeniami. Dzięki zastosowaniu odpowiednich technik zarządzania ryzykiem szczególną uwagę poświęcono by obszarom największego ryzyka, przy uwzględnieniu zagrożenia, względnej krytyczności, stosunku kosztów do korzyści, poziomu zabezpieczeń ochronnych i skuteczności dostępnych strategii łagodzenia skutków).

Zaproponowane w Zielonej Księdze ramy EPOIK miały obejmować środki definiujące kompetencje i odpowiedzialność wszystkich zainteresowanych stron w dziedzinie ochrony infrastruktury krytycznej (OIK) oraz stanowić podstawę dla opracowania odrębnego podejścia dla każdego sektora. Wspólne ramy miały także uzupełnić istniejące środki sektorowe na poziomie wspólnotowym i w Państwach Członkowskich w celu zapewnienia najwyższego możliwego poziomu bezpieczeństwa infrastruktury krytycznej w Unii Europejskiej. Postanowiono również, że należy przyznać priorytet pracom nad osiągnięciem porozumienia w kwestii wspólnego wykazu definicji i sektorów IK (Tabela 2.1).

Rys. 2.18. Ramy ochrony infrastruktury krytycznej w UE (2005 rok)

Wspólne ramy obejmowały następujące elementy (Rys. 2.18):

- wspólne zasady OIK,
- wspólnie ustalone kody/normy,
- wspólne definicje, na podstawie których można ustalić definicje dla poszczególnych sektorów,
- wspólny wykaz sektorów IK,
- obszary priorytetowe OIK,
- opis zakresu odpowiedzialności zainteresowanych stron,
- ustalone wskaźniki,
- metodologię służąca porównaniu i przyznaniu priorytetowego znaczenia,
- infrastrukturę w różnych sektorach.

Tabela 2.1. Sektory infrastruktury krytycznej definiowane w Zielonej Księdze

Numer	Sektor	System, produkt lub usługa
I.	Energia	Produkcja ropy i gazu, rafinacja, przetwarzanie i przechowywanie, rurociągi
		Wytwarzanie energii elektrycznej
		Przesyłanie energii elektrycznej, gazu i ropy

Numer	Sektor	System, produkt lub usługa
		Dystrybucji energii elektrycznej, gazu i ropy naftowej
II.	Technologie informacyjno-komunikacyjne	Systemy informatyczne i ochrona sieci
		Systemy automatyzacji produkcji i kontroli
		Internet
		Telekomunikacja stacjonarna
		Telekomunikacja mobilna
		Telekomunikacja satelitarna
		Systemy transmisyjne
III.	Woda	Zaopatrzenia w wodę pitną
		Kontrola jakości wody
		Monitorowanie i kontrola ilości wody
IV.	Żywność	Systemy zaopatrzenia oraz zapewnienia ochrony i bezpieczeństwa żywności
V.	Zdrowie	Ochrona medyczna i szpitalna
		Lekarstwa, surowice, szczepionki i środki farmaceutyczne
		Laboratoria i czynniki biologiczne
VI.	Finanse	Usługi płatnicze/struktury płatnicze (prywatne)
		Rządowe operacje finansowe
VII.	Bezpieczeństwo publiczne	Utrzymanie porządku publicznego i porządku prawnego, ochrona i bezpieczeństwo
		Wymiar sprawiedliwości i więziennictwo
VIII.	Administracja publiczna	Funkcje rządowe

Numer	Sektor	System, produkt lub usługa
		Siły zbrojne
		Usługi administracji publicznej
		Służby ratunkowe
		Usługi pocztowe i kurierskie
IX.	Transport	Transport drogowy
		Transport kolejowy
		Transport powietrzny
		Transport wodny śródlądowy
		Transport oceaniczny i żeglugi bliskiego zasięgu
X.	Przemysł chemiczny i jądrowy	Produkcja i magazynowanie / przetwarzanie substancji chemicznych i jądrowych
		Rurociągi do transportu towarów niebezpiecznych (substancji chemicznych)
XI.	Badania przestrzeni kosmicznej	Przestrzeń kosmiczna
		Badania

Źródło: opracowanie na podstawie Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005, COM(2005) 576 final (http://eur-lex.europa.eu/LexUriServ/site/en/com/ 2005/ com2005_0576en01.pdf).

Niewątpliwie kluczowym dokumentem z zakresu ochrony infrastruktury krytycznej jest Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania Europejskiej Infrastruktury Krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[156].

Wymieniona Dyrektywa stanowiła pierwszy krok w podejściu do rozpoznania i wyznaczenia Europejskiej Infrastruktury Krytycznej (EIK) oraz do oceny potrzeb w zakresie poprawy jej ochrony. Dyrektywa jako

[156] *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Official Journal of the European Union, L 345/75, 23.12.2008.

taka koncentrowała się na dwóch sektorach infrastruktury krytycznej: energii i transporcie. Miała stanowić prototypowe rozwiązanie dla pozostałych elementów infrastruktury krytycznej.

Głównym celem Dyrektywy było stworzenie procedury rozpoznawania i wyznaczania EIK oraz opracowanie wspólnego podejścia do oceny potrzeb w zakresie poprawy jej ochrony. Ze względu na złożoność problemu sugerowano, iż najlepszym rozwiązaniem jest prowadzenie procesu ochrony infrastruktury krytycznej na poziomie Wspólnoty zgodnie z zasadą pomocniczości i proporcjonalności[157].

W Dyrektywie znalazły się definicje pojęć dających podstawę do prowadzenia dalszych badań i prac nad ochroną infrastruktury krytycznej. Należą do nich:

- „infrastruktura krytyczna" (składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji),
- „europejska infrastruktura krytyczna" (infrastruktura krytyczna zlokalizowana na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałoby istotny wpływ, na co najmniej dwa państwa członkowskie. To, czy wpływ jest istotny, ocenia się w odniesieniu do kryteriów przekrojowych. Obejmuje to skutki wynikające z międzysektorowych współzależności z innymi rodzajami infrastruktury),
- „analiza ryzyka" (uwzględnianie stosownych metod postępowania w przypadku zaistnienia zagrożeń, aby ocenić słabe punkty i potencjalne skutki zakłócenia lub zniszczenia infrastruktury krytycznej),
- „szczególnie chronione informacje dotyczące ochrony infrastruktury krytycznej" (fakty dotyczące infrastruktury krytycznej, które w przypadku ujawnienia mogłyby zostać wykorzystane do zaplanowania i przeprowadzenia działań

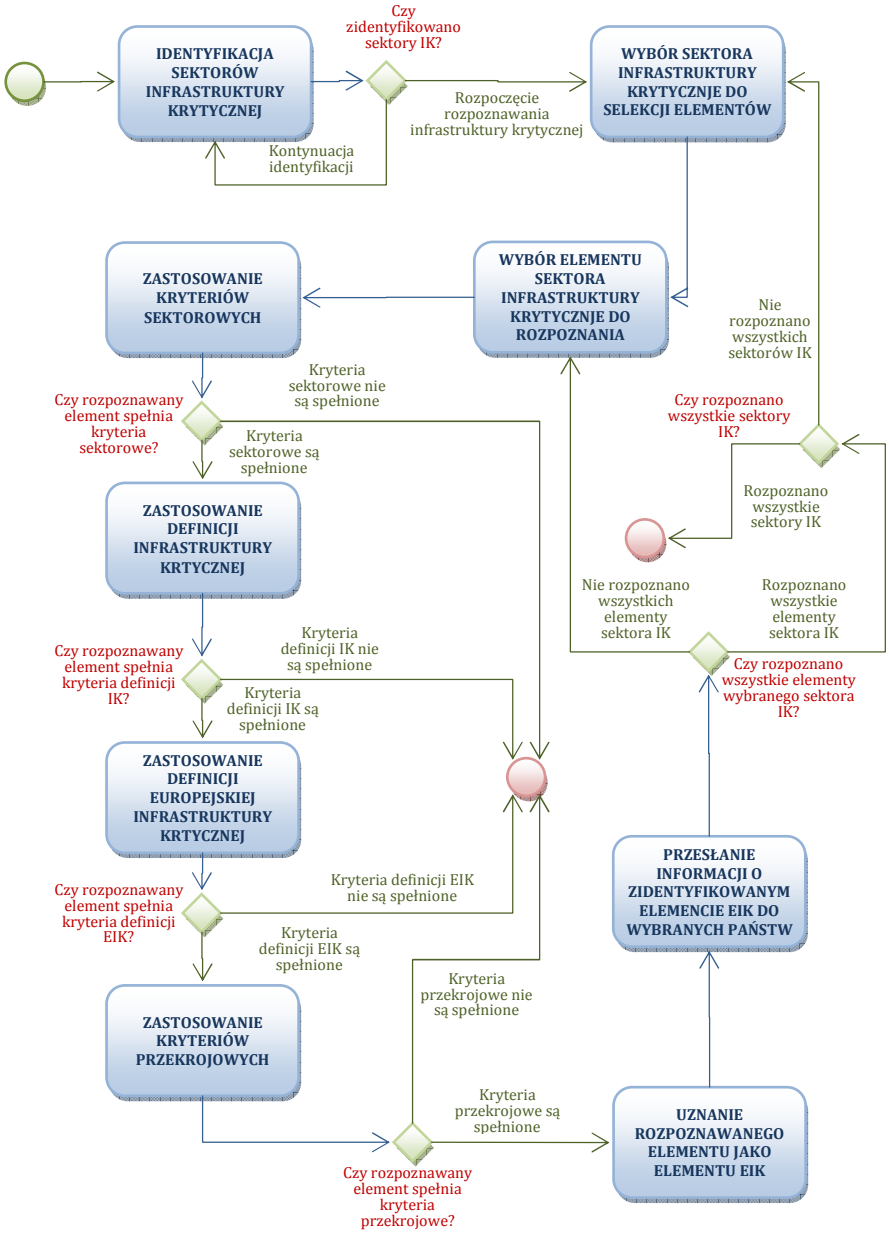
[157] Traktat o Unii Europejskiej, art. 5 mówi, że: *granice kompetencji Unii wyznacza zasada przyznania. Wykonywanie tych kompetencji podlega zasadom pomocniczości i proporcjonalności.*

zmierzających do spowodowania zakłócenia lub zniszczenia urządzeń infrastruktury krytycznej),
- „ochrona" (wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków),
- „właściciele/operatorzy europejskiej infrastruktury krytycznej" (podmioty odpowiedzialne za inwestycje lub bieżącą działalność danego składnika, systemu lub części infrastruktury krytycznej oraz za związane z nimi inwestycje).

Zdefiniowano również kryteria sektorowe oraz przekrojowe pozwalające zaliczyć do infrastruktury krytycznej poszczególne obiekty, systemy, urządzania oraz usługi. Kryteria sektorowe uwzględniają cechy charakterystyczne poszczególnych sektorów EIK, natomiast kryteria przekrojowe są następujące:
- kryterium ofiar w ludziach (oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych),
- kryterium skutków ekonomicznych (oceniane w odniesieniu do wielkości strat ekonomicznych lub pogorszenia towarów lub usług, w tym potencjalnych skutków ekologicznych),
- kryterium skutków społecznych (oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych i zakłócenia codziennego życia, w tym utraty podstawowych usług).

Progi kryteriów przekrojowych opierają się na rozmiarze strat wynikłych z zakłócenia lub zniszczenia danej infrastruktury. Dokładne progi mające zastosowanie do kryteriów przekrojowych określane są w poszczególnych przypadkach przez państwa członkowskie, których dotyczy dana infrastruktura krytyczna. Każde państwo członkowskie informuje co roku Komisję o liczbie infrastruktur w poszczególnych sektorach, w odniesieniu do których prowadzono dyskusje na temat progów kryteriów przekrojowych.

Komisja wraz z państwami członkowskimi opracowuje wytyczne w sprawie stosowania kryteriów przekrojowych i sektorowych oraz ustala przybliżone progi, które mają być stosowane do rozpoznawania EIK. Kryteria te są niejawne.



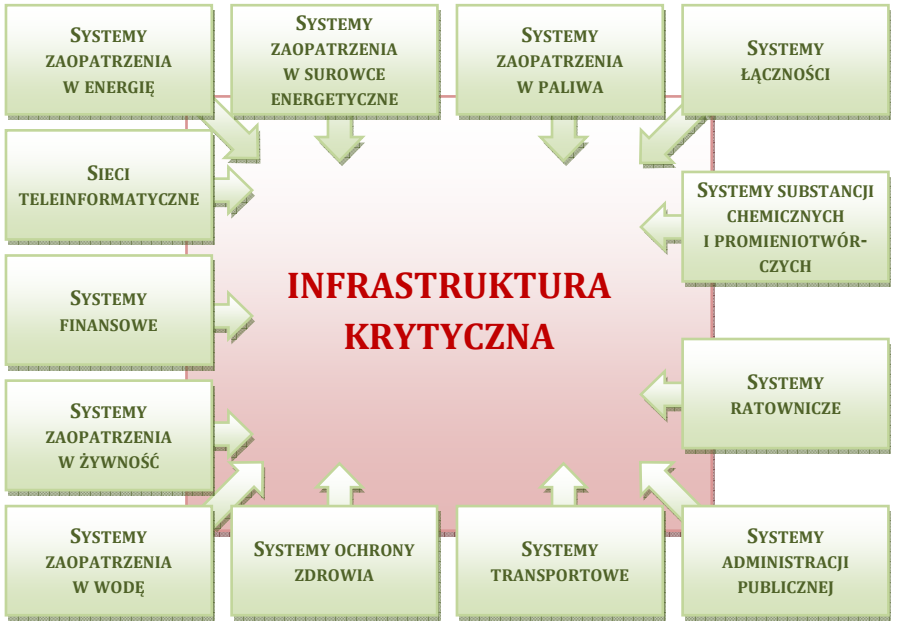
Rys. 2.19. Procedura rozpoznawania Europejskiej Infrastruktury Krytycznej

Zgodnie z Dyrektywą każde państwo członkowskie zobowiązane jest do rozpoznania infrastruktury krytycznej, która może być

wyznaczona jako EIK. Służy do tego celu procedura przedstawiona na Rys. 2.19.

Polska, jako członek Unii Europejskiej jest również zobligowana do stworzenia mechanizmów ochrony infrastruktury krytycznej oraz prowadzenia współpracy w tym zakresie na poziomie Wspólnoty. Zostały już przygotowane odpowiednie regulacje formalno-prawne dające podstawy do budowy systemu ochrony infrastruktury krytycznej. Znajdują się one w następujących dokumentach normatywnych:

- Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 roku,
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej[158],
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej[159],
- Rozporządzenie Prezesa Rady Ministrów z dnia 14 lipca 2010 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej[160].



Rys. 2.20. Sektory infrastruktury krytycznej w Polsce

[158] Dz. U. Nr 83, poz. 541.
[159] Dz. U. Nr 83, poz. 542.
[160] Dz. U. Nr 135, poz. 906.

Ustawa o zarządzaniu kryzysowym przede wszystkim definiuje podstawowe pojęcia takie, jak:

- infrastruktura krytyczna[161] (systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (Rys. 2.20)),
- europejska infrastruktura krytyczna (systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ, na co najmniej dwa państwa członkowskie),
- ochrona infrastruktury krytycznej (wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania

[161] W sensie etymologicznym termin „infrastruktura" wywodzi się od łacińskich wyrazów: infra (na dole, pod, poniżej) i struktura (budowa, sposób budowania). Według encyklopedii infrastruktura to podstawowe urządzenia i instytucje świadczące usługi niezbędne do należytego funkcjonowania produkcyjnych działów gospodarki. Z. Trejnis, *Infrastruktura krytyczna – koncepcje i zakres*, [w:] A. Tyburska (red.), *Ochrona infrastruktury krytycznej*, WSPol, Szczytno 2010, s. 67.

zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie).

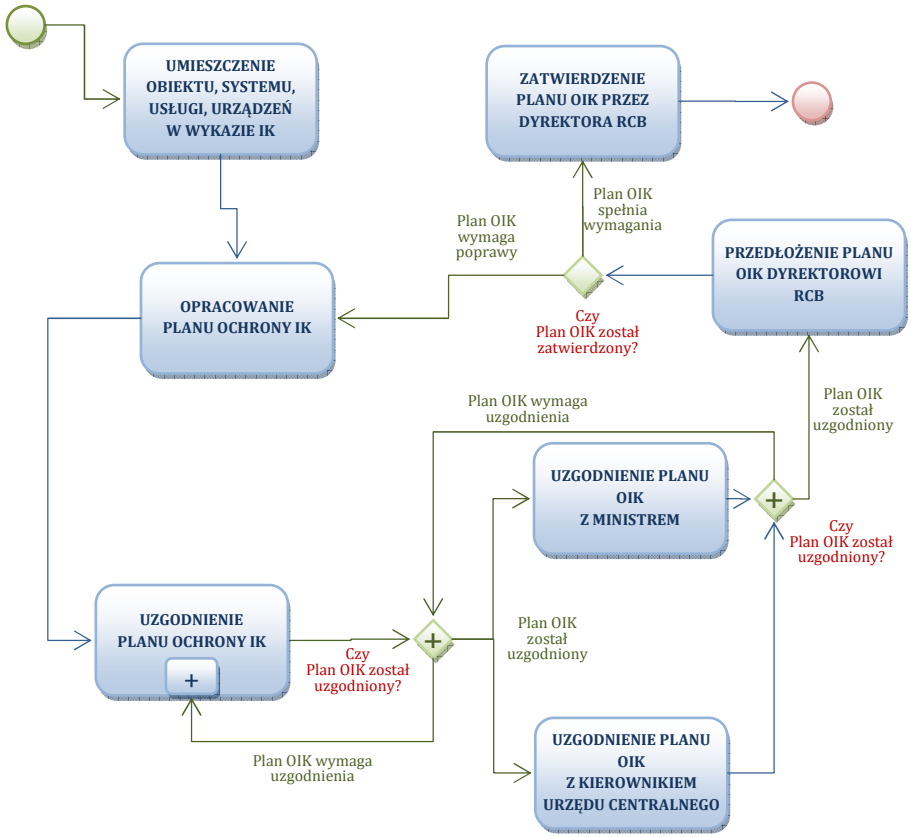
Ustawa mówi również o konieczności opracowania Narodowego Programu Ochrony Infrastruktury Krytycznej, którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, w szczególności w zakresie:

- zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej,
- przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,
- reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- odtwarzania infrastruktury krytycznej.

Narodowy Program Ochrony Infrastruktury Krytycznej ma określać:

- narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej,
- ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy infrastruktury krytycznej,
- szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej określa sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej opracowywanych przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej oraz warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej (Rys. 2.21).



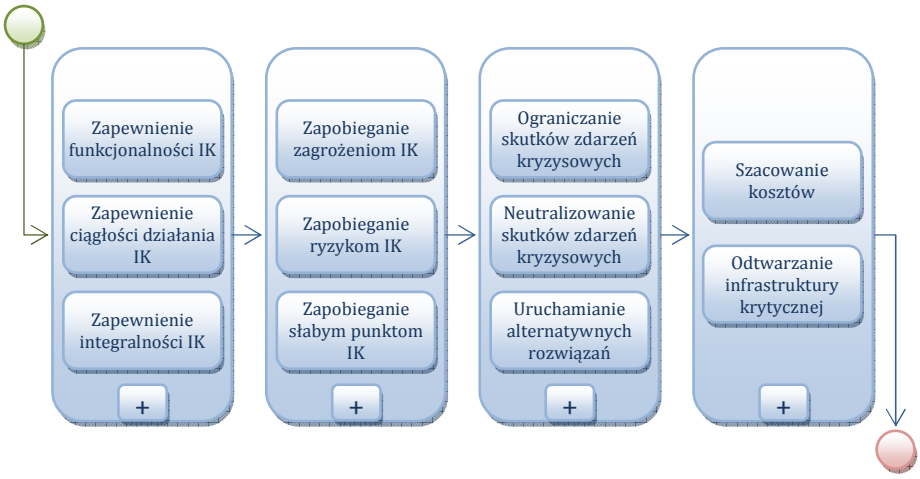
Rys. 2.21. Proces tworzenie planu ochrony infrastruktury krytycznej

* * *

Realizacja kolejnego etapu badań wymagała dokonania analizy regulacji formalno-prawnych oraz rozwiązań organizacyjno-funkcjonalnych systemu zarządzania kryzysowego w celu określenia miejsca systemu ochrony infrastruktury krytycznej w systemie zarządzania kryzysowego.

Poddana analizie została również ewolucja podejścia organów administracji publicznej do zagadnień związanych z ochroną kluczowych obiektów, instalacji, urządzeń oraz usług dla bezpieczeństwa oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców.

Wyniki przeprowadzonych badań wykorzystane zostały, jako materiał wejściowy do kolejnego etapu badań, którym jest konstruowanie procesu ochrony infrastruktury krytycznej.



Rys. 2.22. Podprocesy ochrony infrastruktury krytycznej

W procesie ochrony infrastruktury krytycznej zdefiniowano następujące działania:

- zapobieganie zakłóceniom funkcjonowania infrastruktury krytycznej,
- przygotowanie na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,
- reagowanie w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- odtwarzanie infrastruktury krytycznej.

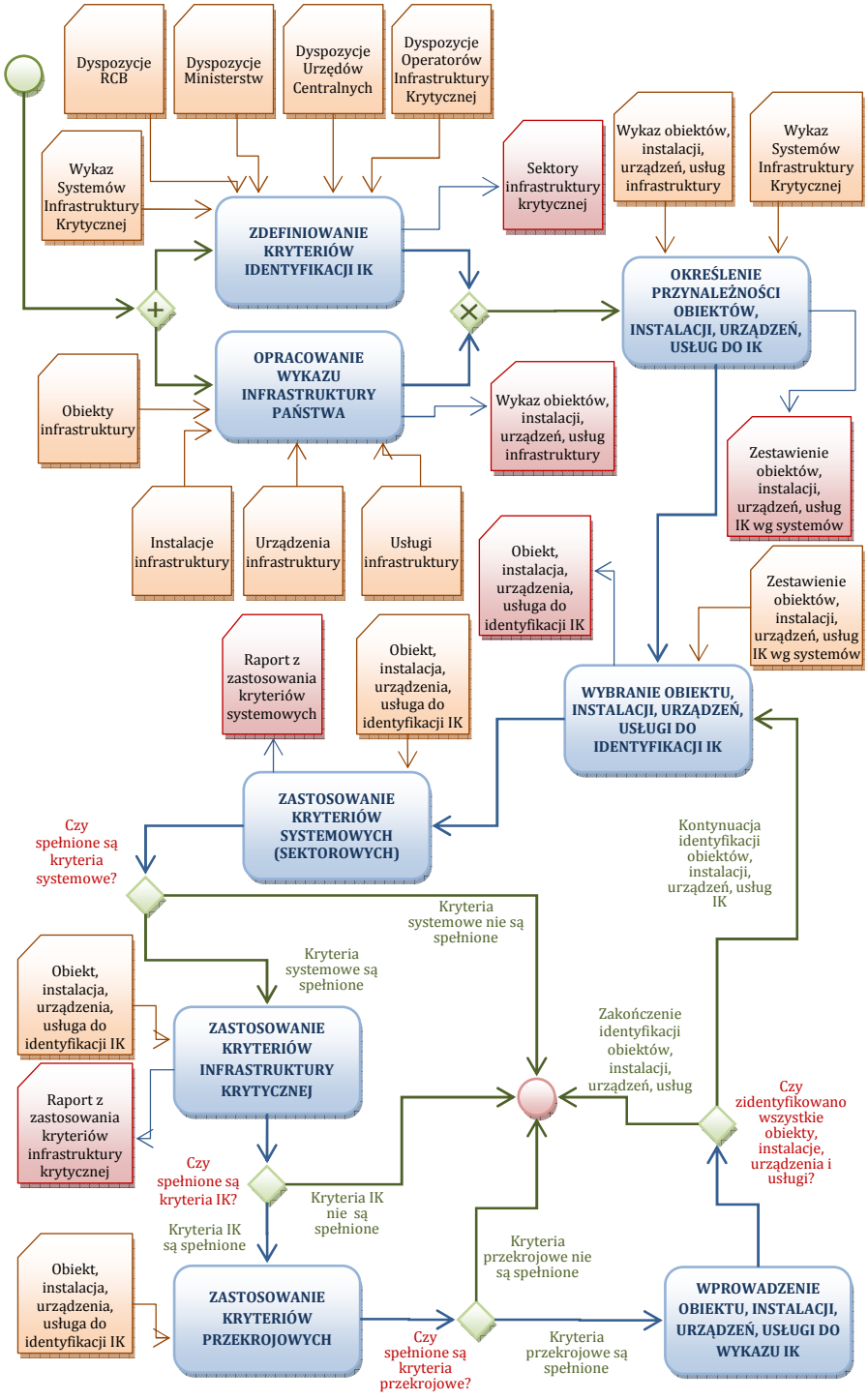
ROZDZIAŁ 3
PROCES ZARZĄDZANIA BEZPIECZEŃSTWEM INFRASTRUKTURY KRYTYCZNEJ

Proces zarządzania bezpieczeństwem infrastruktury krytycznej obejmuje wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom, ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

3.1. ZAPOBIEGANIE ZAKŁÓCENIOM PRACY INFRASTRUKTURY KRYTYCZNEJ

Zapobieganie zakłóceniom pracy infrastruktury krytycznej polega na opracowaniu regulacji formalno-prawnych, podejmowaniu działań, zmierzających do wskazania głównych celów ochrony infrastruktury krytycznej, identyfikacji infrastruktury krytycznej w ramach państwa oraz Unii Europejskiej, identyfikacji zagrożeń, oceny ryzyka, określenia sieci powiązań w ramach systemu infrastruktury krytycznej oraz identyfikacji relacji pomiędzy poszczególnymi systemami (Rys. 3.1).

Rys. 3.1. Podprocesy procesu zapobiegania zakłóceniom infrastruktury krytycznej



Rys. 3.2. Mapa procesu identyfikacji krajowej infrastruktury krytycznej

Proces identyfikacji krajowej infrastruktury krytycznej rozpoczyna się od wykonania dwóch działań, realizowanych w sposób niezależny od siebie: zdefiniowania kryteriów identyfikacji IK i opracowania wykazu infrastruktury państwa (Rys. 3.2).

Zdefiniowanie kryteriów identyfikacji IK realizowane jest przez dyrektora Rządowego Centrum Bezpieczeństwa na podstawie zapisów ustawowych oraz we współpracy z ministerstwami, urzędami centralnymi oraz operatorami infrastruktury krytycznej.

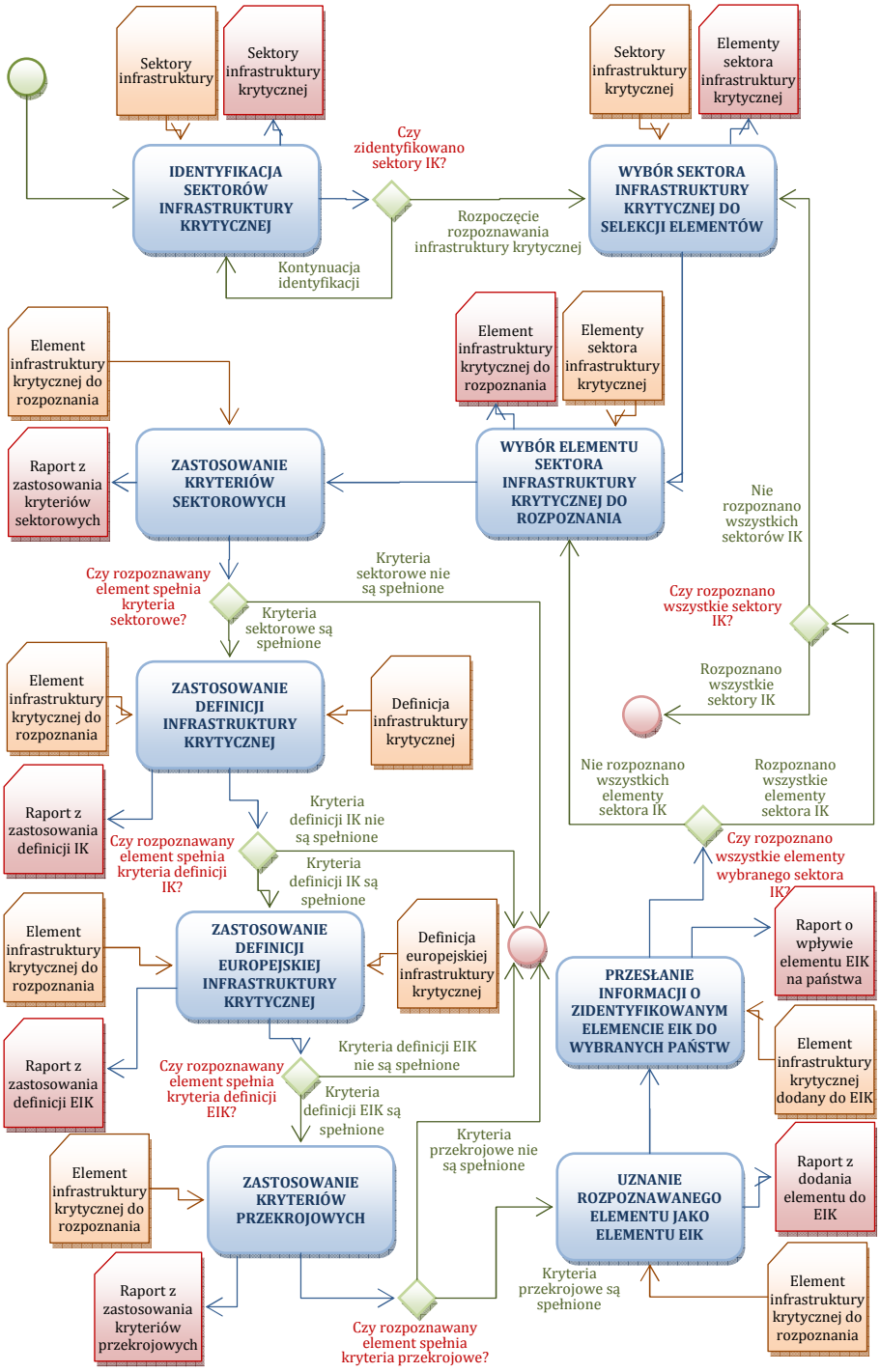
Opracowanie wykazu infrastruktury państwa jest niezbędne do zidentyfikowania wszystkich obiektów, instalacji, urządzeń oraz usług odpowiedzialnych za funkcjonowanie gospodarki oraz społeczeństwa.

Mając do dyspozycji kryteria wyłaniania infrastruktury krytycznej oraz wykaz infrastruktury krytycznej następuje przejście do kolejnego działania, którym jest określenie przynależności poszczególnych obiektów, instalacji, urządzeń oraz usług do systemów IK definiowanych przez *Ustawę o zarządzaniu kryzysowym*.

Opracowanie kompletnego wykazu obiektów, instalacji, urządzeń oraz usług wg przynależności do poszczególnych systemów stanowi podstawę do zastosowania kryteriów systemowych (sektorowych) w odniesieniu do każdego elementu z osobna. Na podstawie tego kryterium następuje przyporządkowanie obiektu, instalacji, urządzeń oraz usługi do konkretnego systemu infrastruktury krytycznej (zaopatrzenia w energię, zaopatrzenia w paliwa, zapatrzenia w żywność, zaopatrzenia w wodę, łączności, sieci teleinformatycznych, systemów finansowych, ochrony zdrowia, transportu, komunikacji, ratownictwa, ciągłości działania administracji publicznej, systemów substancji niebezpiecznych).

Kolejnym działaniem w procesie identyfikacji infrastruktury krytycznej jest zastosowanie kryteriów infrastruktury krytycznej sprawdzających, czy obiekty, instalacje, urządzenia oraz usługi są kluczowe dla bezpieczeństwa państwa i jego obywateli oraz czy służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Ostatnim etapem identyfikacja IK jest wskazanie potencjalnych skutków zniszczenia lub zakłócenia funkcjonowania weryfikowanych obiektów, instalacji, urządzeń oraz usług w odniesieniu do kryteriów przekrojowych.



Rys. 3.3. Mapa procesu identyfikacji Europejskiej Infrastruktury Krytycznej

Proces identyfikacji europejskiej infrastruktury krytycznej zaczyna się od zastosowania kryteriów sektorowych w celu dokonania pierwszej selekcji infrastruktury krytycznej w danym sektorze (Rys. 3.3).

Następnym działaniem jest zastosowanie do wyselekcjonowanych elementów infrastruktury, kryterium sprawdzającego czy składniki, systemy lub części infrastruktury zlokalizowane na terytorium państw członkowskich, mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz czy zakłócenie lub ich zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji. Istotność tego wpływu jest określana przy użyciu krajowych metod rozpoznawania infrastruktury krytycznej lub w odniesieniu do kryteriów przekrojowych, na odpowiednim szczeblu krajowym. W przypadku infrastruktury świadczącej niezbędne usługi bierze się pod uwagę to, czy dostępne są alternatywy, a także czas trwania zakłócenia/naprawy.

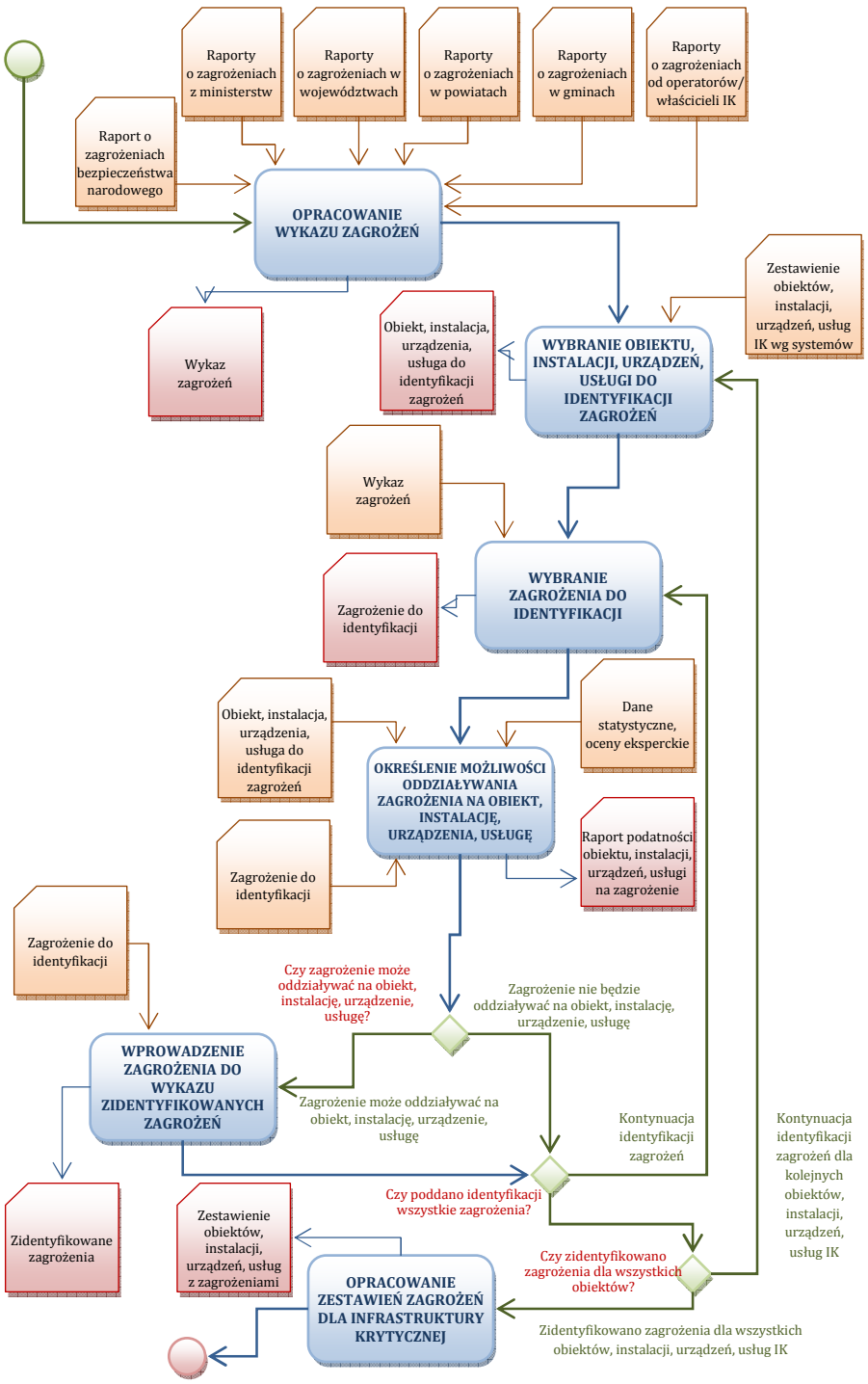
Kolejnym kryterium jest sprawdzenie czy rozpoznawany element spełnia definicję europejskiej infrastruktury krytycznej, tzn. czy zakłócenie lub zniszczenie tego elementu miałoby istotny wpływ, na co najmniej dwa państwa członkowskie. Istotność tego elementu ocenia się w odniesieniu do kryteriów przekrojowych oraz obejmuje skutki wynikające z międzysektorowych współzależności z innymi rodzajami infrastruktury.

Ostatnie działanie weryfikacyjne dotyczy zastosowania kryteriów przekrojowych, które uwzględniają: rozmiar strat oraz – w przypadku infrastruktury świadczącej niezbędne usługi – to, czy dostępne są alternatywy, a także czas trwania zakłócenia/naprawy.

Rozpoznawanie Europejskiej Infrastruktury Krytycznej obejmuje w pierwszym rzędzie sektor energii oraz transportu, a w dalszej kolejności sektor teleinformatyczny.

W sektorze energii zostały zidentyfikowane następujące podsektory: energia elektryczna, ropa naftowa, gaz.

W sektorze transportowym procesowi identyfikacji infrastruktury krytycznej podlega transport drogowy, transport kolejowy, transport lotniczy, transport wodny śródlądowy, żegluga oceaniczna, żegluga morska bliskiego zasięgu i porty.



Rys. 3.4. Mapa procesu identyfikacji zagrożeń

Identyfikacja zagrożeń jest kluczowym procesem w zarządzaniu bezpieczeństwem infrastruktury krytycznej państwa (Rys. 3.4). Wyniki tego procesu są wykorzystywane podczas opracowywania planów ochrony infrastruktury krytycznej zawierających szczegółową charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju niekorzystnych zdarzeń.

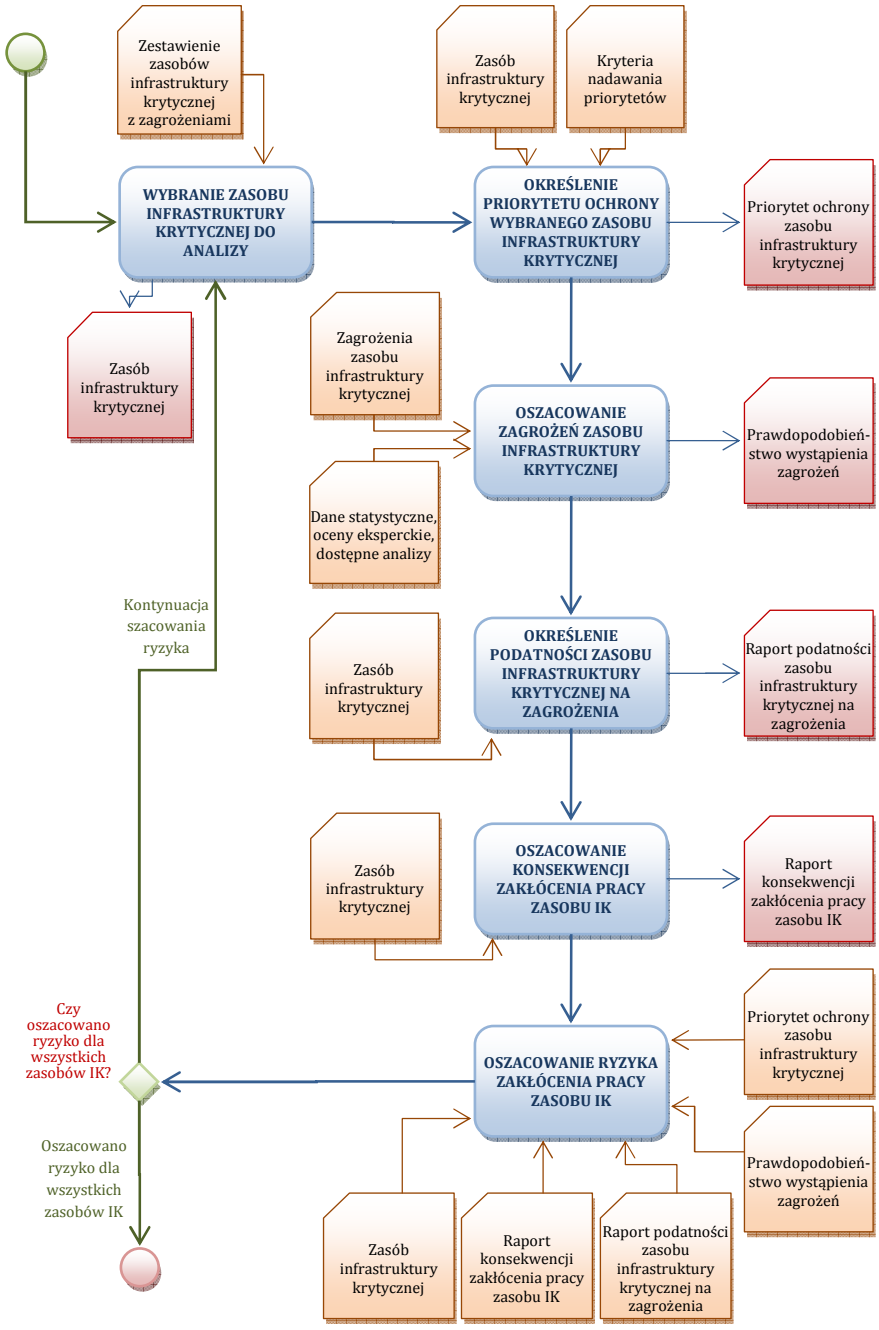
Identyfikując zagrożenia infrastruktury krytycznej należy przede wszystkim wziąć pod uwagę zjawiska naturalne, awarie techniczne, błędy ludzkie oraz zamierzone działania człowieka. Uzależnienie od nowoczesnych technologii przebiegu procesów gospodarczych, społecznych oraz funkcjonowania administracji publicznej spowodowało, że w społeczeństwach informacyjnych niebagatelne stały się również zagrożenia z cyberprzestrzeni. Okazuje się, że zagrożenia te mogą skutecznie zakłócić funkcjonowanie infrastruktury krytycznej znajdującej się nie tylko na terenie jednego państwa, ale również wielu państw połączonych ze sobą łączami telekomunikacyjnymi.

Właściciele infrastruktury krytycznej muszą być świadomi tych zagrożeń i powinni prowadzić wszelkie możliwe działania mające na celu przygotowanie się do reagowania w sytuacjach kryzysowych, poprzez ocenę ryzyka i redukowanie go tak dalece jak to możliwe.

Pierwszym działaniem podejmowanym w procesie identyfikacji zagrożeń jest opracowanie ogólnego wykazu zagrożeń na podstawie dostępnych raportów dotyczących zagrożeń bezpieczeństwa narodowego, zagrożeń zidentyfikowanych przez ministerstwa i urzędy centralne, zagrożeń zidentyfikowanych w poszczególnych województwach, powiatach i gminach oraz z raportów zagrożeń zidentyfikowanych przez operatorów infrastruktury krytycznej.

Mając do dyspozycji wykaz wszystkich zagrożeń dokonywana jest ocena możliwości ich oddziaływania na poszczególne obiekty, instalacje, urządzenia i usługi zakwalifikowane do infrastruktury krytycznej. Ocena ta może być prowadzona na podstawie dostępnych danych statystycznych z przeszłości, z wykorzystaniem wiedzy eksperckiej oraz oprzyrządowania prognostycznego i symulacji komputerowych.

Zidentyfikowane w ten sposób zagrożenia wprowadzane są do wykazu zagrożeń wybranego elementu infrastruktury krytycznej i poddawane w kolejnym procesie analizie ryzyka.



Rys. 3.5. Mapa procesu analizy ryzyka

Kolejnym podprocesem procesu zapobiegania zakłóceniom infrastruktury krytycznej jest analizy ryzyka stanowiąca podstawę do określenia standardów ochrony infrastruktury krytycznej i ustalenia priorytetów podejmowanych działań (Rys. 3.5).

Metodologia oceny ryzyka powinna być uniwersalna dla wszystkich zasobów infrastruktury krytycznej, jednoznaczna dla wszystkich instytucji ją przeprowadzających i generująca powtarzalne wyniki niezależnie od miejsca prowadzenia analiz.

Zaproponowane podejście do analizy ryzyka rozpoczyna się od przydzielenia priorytetów ochrony poszczególnym elementom zidentyfikowanej infrastruktury krytycznej. Działanie to ma istotne znaczenie przy określaniu znaczenia zasobów infrastruktury krytycznej w systemach, do których należą i decyduje o kolejności reagowania w niekorzystnych sytuacjach.

Drugim etapem analizy ryzyka jest oszacowanie prawdopodobieństwa wystąpienia zagrożeń w odniesieniu do wybranego zasobu infrastruktury krytycznej. Zagrożenia mogą potencjalnie oddziaływać w sposób niekorzystny na zasoby infrastruktury krytycznej, powodując straty. Straty te mogą występować w sposób ciągły lub też mogą być skutkiem pojedynczych incydentów.

Kolejnym działaniem podejmowanym w procesie analizy ryzyka jest określenie podatności wybranego zasobu infrastruktury krytycznej na zagrożenia, czyli sprawdzeniu czy obiekt, instalacja, urządzenia lub usługa posiada zabezpieczenia przed określonymi zagrożeniami. Podatnościami dla konkretnych zagrożeń w kontekście ryzyka mogą być słabe punkty, luki w systemie, niedostosowania organizacyjne, mankamenty techniczne, źle dobrane zasoby ludzkie, ułomne przepisy prawne.

Szacowanie zagrożeń jak również określanie podatności zasobów infrastruktury krytycznej należy prowadzić z wykorzystaniem informacji wewnętrznych systemów, jak również ze źródeł zewnętrznych, np. statystyk, opinii ekspertów, analiz wyspecjalizowanych instytucji.

Ostatnimi działaniami podejmowanymi w procesie analizy ryzyka są: oszacowanie konsekwencji zniszczenia lub zakłócenia pracy zasobu infrastruktury krytycznej oraz wyliczenie wartości nominalnej ryzyka.

3.2. PRZYGOTOWANIE INFRASTRUKTURY KRYTYCZNEJ NA SYTUACJE KRYZYSOWE

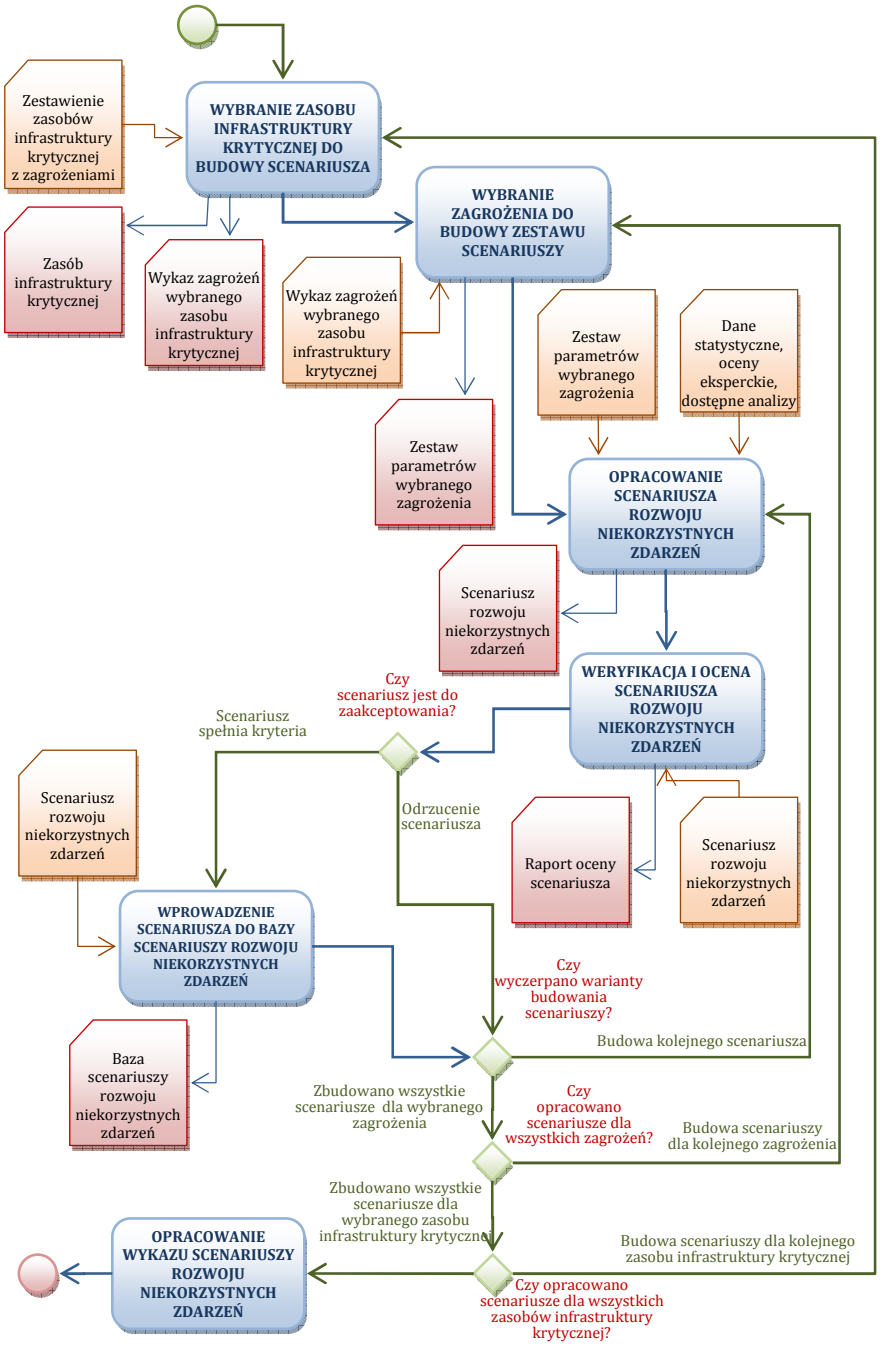
Przygotowanie infrastruktury krytycznej na sytuacje kryzysowe polega na wykonywaniu działań zmierzających do budowy mechanizmów służących zapewnieniu ciągłości działania najważniejszych dla społeczeństwa i gospodarki obiektów, instalacji, urządzeń i usług.

Głównym celem podejmowanych przedsięwzięć jest zwiększenie odporności infrastruktury krytycznej na zidentyfikowane zagrożenia. Przygotowanie to może odbywać się poprzez odpowiednie przydzielenie sił i środków oraz zapewnienie alternatywnych systemów zabezpieczających wszystkie potrzeby. Optymalne wykorzystanie zgromadzonych sił i środków będzie decydowało o skuteczności podejmowanych akcji podczas reagowania na sytuacje kryzysowe.

Rys. 3.6. Podprocesy procesu przygotowania infrastruktury krytycznej na sytuacje kryzysowe

W procesie przygotowania infrastruktury krytycznej na sytuacje kryzysowe główny ciężar został położony na opracowanie zbioru scenariuszy postępowania w razie zaistnienia sytuacji kryzysowych. Bardzo skomplikowanym elementem jest tworzenie planów ochrony infrastruktury krytycznej dla wszystkich obiektów, instalacji, urządzeń oraz usług zaklasyfikowanych do wykazu infrastruktury krytycznej (Rys. 3.6).

Wyzwaniem w skali państwa jest opracowanie Narodowego Planu Ochrony Infrastruktury Krytycznej stanowiącego swego rodzaju kompendium wiedzy o tym, jak należy chronić najważniejsze dla zasoby państwa.



Rys. 3.7. Mapa procesu tworzenia scenariuszy rozwoju niekorzystnych zdarzeń

Wykaz zagrożeń zidentyfikowanych w odniesieniu do poszczególnych zasobów infrastruktury krytycznej oraz analiza ryzyka stanowią podstawę budowy scenariuszy rozwoju niekorzystnych zdarzeń (Rys. 3.7). Scenariusze te pozwalają zrozumieć, jakie skutki mogą ze sobą nieść zagrożenia oraz są wykorzystywane w procesie podejmowania decyzji podczas reagowania na zdarzenia kryzysowe.

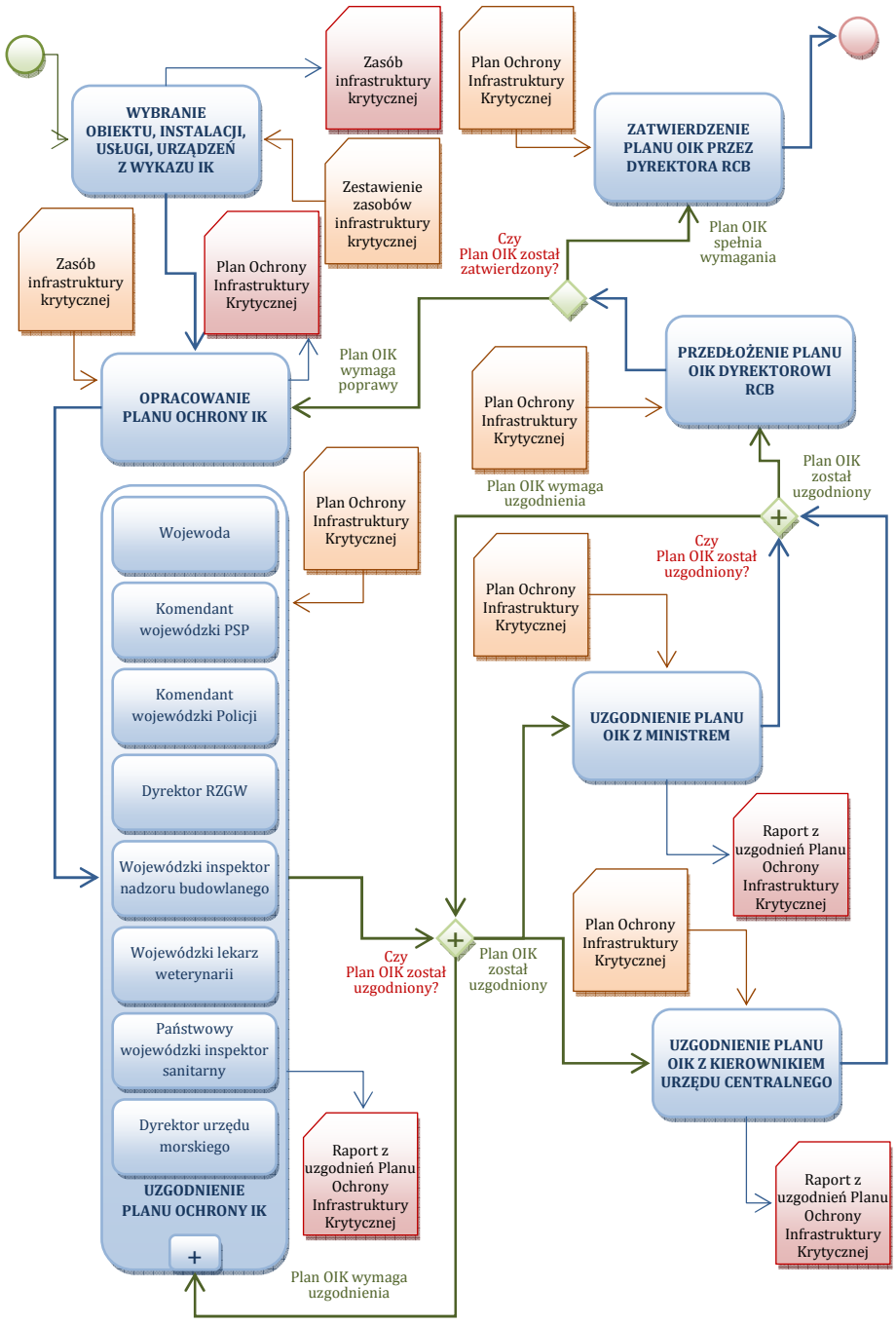
Budowa bazy scenariuszy dla wszystkich zidentyfikowanych zagrożeń niesie ze sobą wiele korzyści. Do najważniejszych z nich należą: obniżenie wskaźnika niepewności, pokazanie możliwości rozwoju zagrożeń, przeanalizowanie hipotetycznych konsekwencji zdarzeń kryzysowych, zidentyfikowanie słabych punktów zasobów infrastruktury krytycznej i ocenienie ich podatności na zagrożenia, przygotowanie zasobów infrastruktury krytycznej na zdarzenia kryzysowe.

Proces tworzenia scenariuszy rozwoju niekorzystnych zdarzeń powinien prowadzić do bardzo szczegółowego przeanalizowania wszystkich sytuacji problemowych związanych ze zniszczeniem bądź czasowym zakłóceniem funkcjonowania zasobów infrastruktury krytycznej dając w ten sposób możliwości wykrycia niedociągnięć oraz wskazania głównych zagrożeń.

Mając do dyspozycji maksymalnie duży zbiór scenariuszy, pokazujących, w jaki sposób mogą się rozwijać i jakie konsekwencje mogą ze sobą nieść zidentyfikowane zagrożenia w odniesieniu do konkretnych obiektów, instalacji, urządzeń i usług, należy przystąpić do ich weryfikacji. Akceptowane są tylko te, które faktycznie będą pokazywały słabości systemu i które zostaną wykorzystane w procesie usuwania słabych punktów w mechanizmach zabezpieczających.

Scenariusze rozwoju sytuacji niekorzystnych powinny charakteryzować się pewną elastycznością ze względu na brak możliwości dokładnego zaplanowania intensywności zagrożeń oraz precyzyjnego wskazania źródła zagrożenia, czy też metod ataku na zasoby infrastruktury krytycznej[162].

[162] Przykładowa metodyka tworzenia scenariuszy została opisana w opracowaniu - W. J. Tolone, S. Lee, W. Xiang, R. K. McNally, A. Schumpert, *Effective Scenario Composition for the Revelation of Blind Spots in Critical Infrastructure Protection Planning*, In Proceedings of the First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (ICCIP '07), Dartmouth College, Hanover, New Hampshire, USA, March 19-21, 2007.

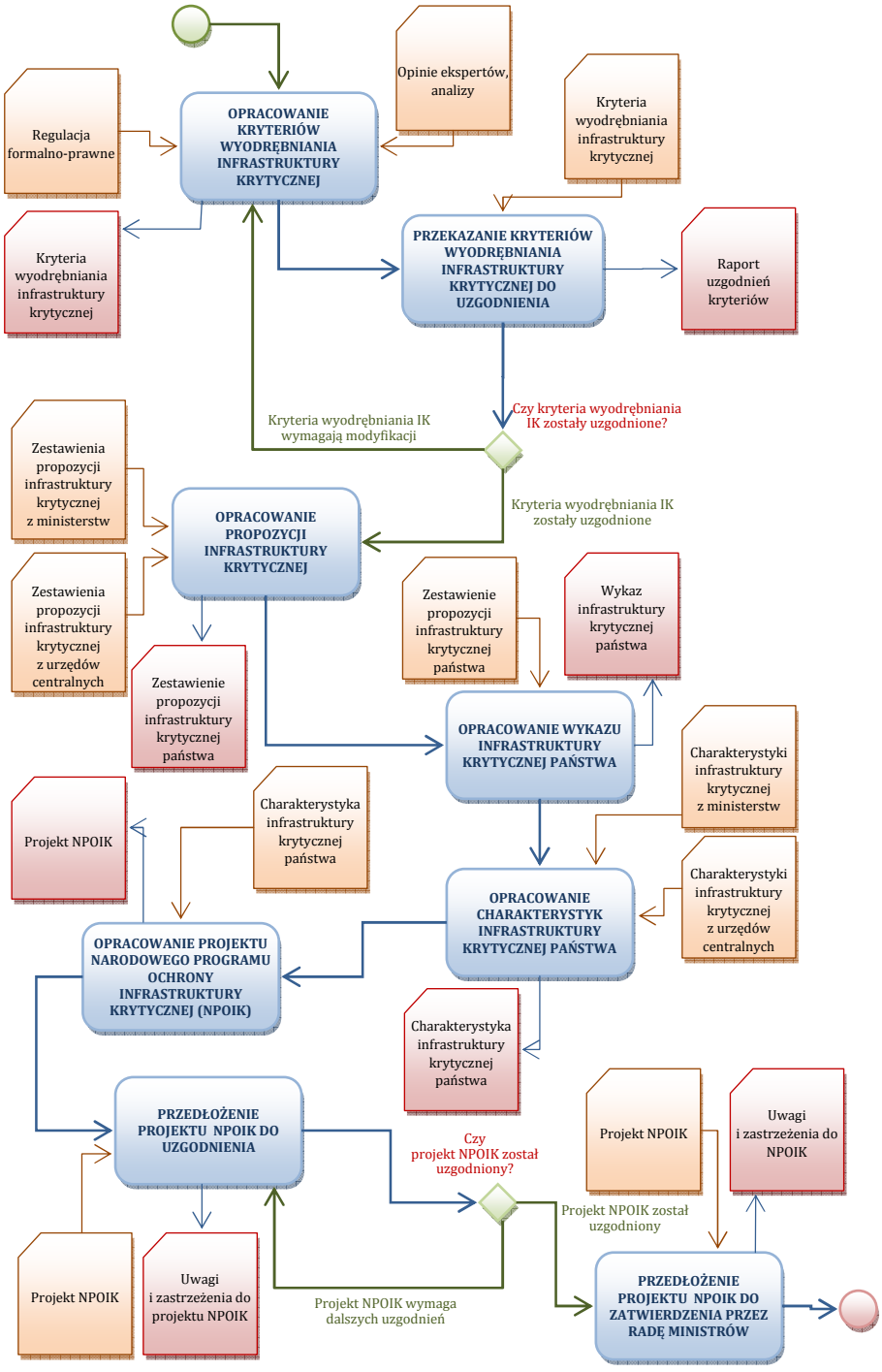


Rys. 3.8. Mapa procesu tworzenia Planu Ochrony Infrastruktury Krytycznej

Proces tworzenie planu ochrony infrastruktury krytycznej rozpoczyna się w momencie uznania obiektów, instalacji, urządzeń i usług za elementy infrastruktury krytycznej (Rys. 3.8).

Zgodnie z wytycznymi w skład planu ochrony infrastruktury krytycznej wchodzą dane ogólne (nazwa i lokalizacja infrastruktury krytycznej, adres i siedziba, numery REGON, NIP i KRS, dane służbowe osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej, imię i nazwisko osoby sporządzającej plan), dane infrastruktury krytycznej obejmujące (charakterystykę i podstawowe parametry techniczne, plan z naniesieniem lokalizacji obiektów, instalacji lub systemu, funkcjonalne połączenia z innymi obiektami, instalacjami, urządzeniami lub usługami), charakterystykę zagrożeń dla infrastruktury krytycznej oraz oceny ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń, zależności infrastruktury krytycznej od pozostałych systemów infrastruktury krytycznej oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach infrastruktury krytycznej, zasobów własnych możliwych do wykorzystania w celu ochrony infrastruktury krytycznej, zasobów właściwych terytorialnie organów, możliwych do wykorzystania w celu ochrony infrastruktury krytycznej, zasadnicze warianty działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej, zapewnienia ciągłości funkcjonowania infrastruktury krytycznej, odtwarzania infrastruktury krytycznej, zasady współpracy z właściwymi miejscowo centrami zarządzania kryzysowego i organami administracji publicznej.

Sporządzone plany ochrony infrastruktury krytycznej są uzgadniane z właściwymi terytorialnie wojewodą, komendantem wojewódzkim Państwowej Straży Pożarnej, komendantem wojewódzkim Policji, dyrektorem regionalnego zarządu gospodarki wodnej, wojewódzkim inspektorem nadzoru budowlanego, wojewódzkim lekarzem weterynarii, państwowym wojewódzkim inspektorem sanitarnym oraz dyrektorem urzędu morskiego. Następne uzgodnienia są dokonywane z ministrem lub kierownikiem urzędu centralnego we właściwości, którego znajduje się system, do którego została zaliczona dana infrastruktura krytyczna. Plan ochrony infrastruktury krytycznej zatwierdzany jest przez dyrektora RCB.



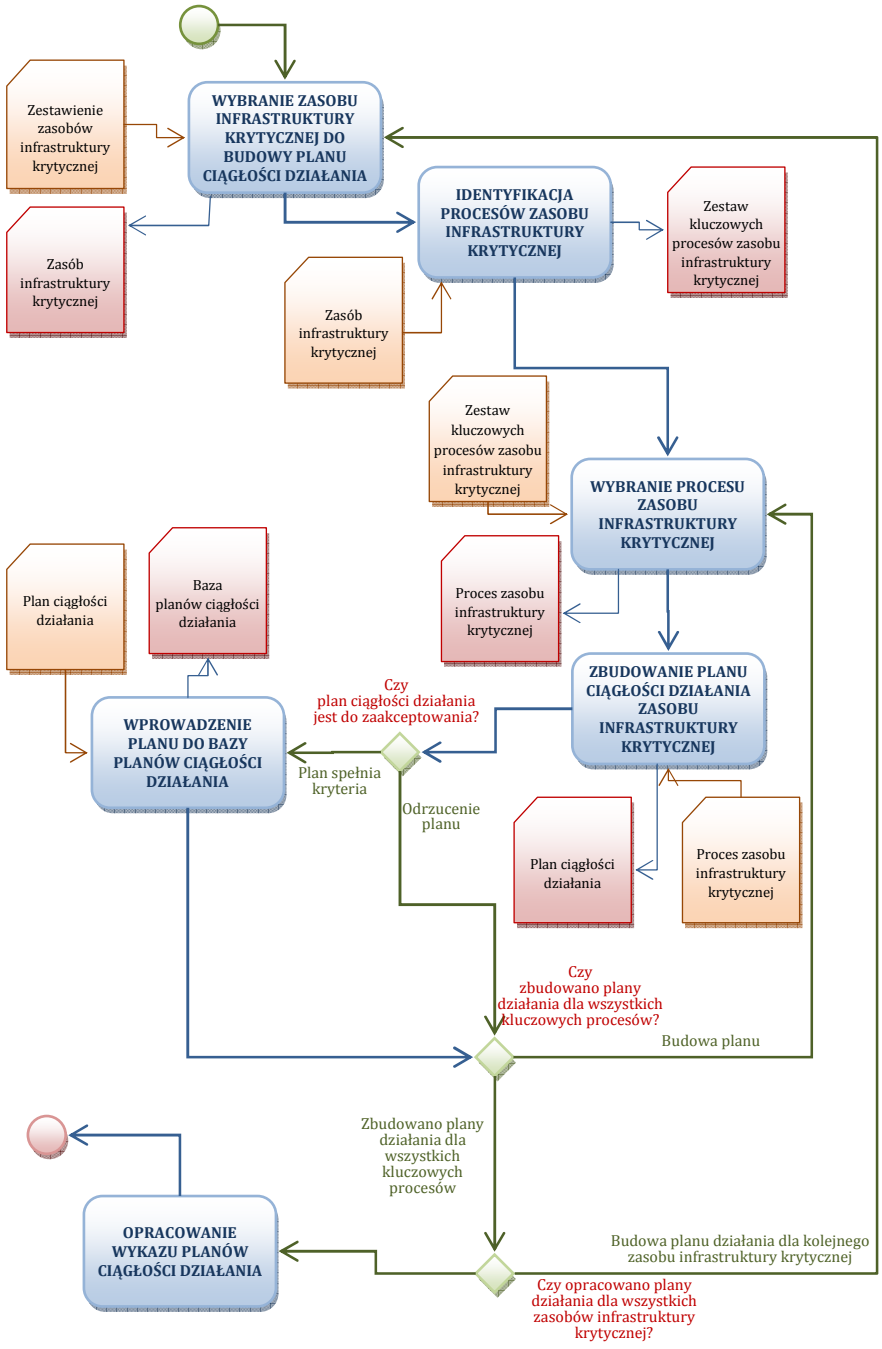
Rys. 3.9. Mapa procesu tworzenia Narodowego Programu Ochrony Infrastruktury Krytycznej

Proces budowy NPOIK rozpoczyna się od opracowania przez dyrektora RCB kryteriów pozwalających wyodrębnić infrastrukturę krytyczną i przekazuje je do uzgodnień ministrom i kierownikom urzędów centralnych (Rys. 3.9). Po uzgodnieniach i zatwierdzeniu tych kryteriów, ministrowie i kierownicy urzędów centralnych, każdy według swojej właściwości, przedkładają dyrektorowi Centrum propozycje infrastruktury krytycznej do zamieszczenia w wykazie obiektów, instalacji, urządzeń i usług kluczowych dla bezpieczeństwa państwa i jego obywateli oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Propozycje infrastruktury krytycznej są weryfikowane i na ich podstawie opracowywany jest wykaz infrastruktury krytycznej zawierający: nazwę i lokalizację infrastruktury krytycznej, podległość organizacyjną, w tym w stosunku do ministrów i kierowników urzędów centralnych, jeśli taka występuje, dane operatora infrastruktury krytycznej oraz dane zarządzającego w imieniu operatora infrastruktury krytycznej, jeśli taki występuje.

W kolejny działaniu opracowywana jest charakterystyka infrastruktury krytycznej państwa zawierająca: opis obszaru zadaniowego, obejmujący identyfikację zasobów, podsystemów, funkcji i zależności od innych systemów infrastruktury krytycznej, propozycje wymagań i standardów pozwalających zapewnić ciągłość funkcjonowania infrastruktury krytycznej, ogólną ocenę ryzyka dla funkcjonowania opisywanego obszaru zadaniowego, uwzględniającą zagrożenia, podatności na zagrożenie oraz konsekwencje zakłócenia funkcjonowania infrastruktury krytycznej, propozycje priorytetów w zakresie odtwarzania infrastruktury krytycznej, możliwe sposoby zapobiegania zakłóceniom funkcjonowania obszaru zadaniowego będącego skutkiem zakłócenia funkcjonowania infrastruktury krytycznej, propozycje programów badawczych i rozwojowych mogących przyczynić się do zwiększenia bezpieczeństwa infrastruktury krytycznej.

Ostatnim działaniem w procesie jest przygotowanie projektu NPOIK i uzgodnienie go z jego uczestnikami, którzy mogą wnieść poprawki i zastrzeżenia. Projekt NPOIK przedkładany jest do zatwierdzenia Radzie Ministrów.



Rys. 3.10. Mapa procesu tworzenia mechanizmów ciągłości działania infrastruktury krytycznej

Każdy obiekt, instalacja, urządzenia lub usługi zaliczone do wykazu infrastruktury krytycznej są potencjalnie zagrożone zniszczeniem lub zakłóceniem pracy, co pociąga za sobą bardzo często dotkliwe konsekwencje ekonomiczne i społeczne. Zagrożenia te mogą być spowodowane przez: klęski żywiołowe, wypadki, sabotaż, zakłócenia w dostawie energii elektrycznej, katastrofy komunikacyjne, zakłócenia w transporcie, problemy z usługami, wycieki materiałów niebezpiecznych, cyberataki i działalność hakerów.

Tworzenie i utrzymywanie mechanizmów ciągłości działania pozwala przygotować operatorom infrastruktury krytycznej zasoby oraz informacje niezbędne do utrzymania podstawowych procesów w nich realizowanych (Rys. 3.10).

Do najważniejszych działań podejmowanych w procesie przygotowania mechanizmów ciągłości działania należy:

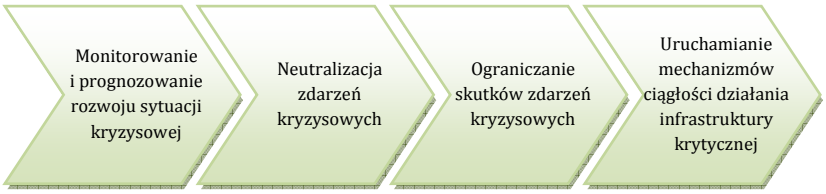
- identyfikacja krytycznych usług oraz produktów dostarczanych przez zasób infrastruktury krytycznej,
- nadanie priorytetów poszczególnym usługom i produktom w celu utworzenia rankingu wpływu na zakłócenie funkcjonowania zasobów infrastruktury krytycznej,
- określenie dopuszczalnego okresu niedostępności zasobów infrastruktury krytycznej oraz obszarów potencjalnych konsekwencji,
- identyfikacja powiązań między innymi zasobami infrastruktury krytycznej,
- analiza możliwości ograniczania ryzyka,
- analiza bieżących możliwości odtwarzania zasobów infrastruktury krytycznej,
- zapewnienie alternatywnych zasobów dla zapewnienia ciągłości dostarczania usług oraz produktów.

Utrzymanie mechanizmów ciągłości działania w gotowości wymaga prowadzenia systematycznych ćwiczeń oraz kontroli prowadzących do doskonalenia całego systemu. Identyfikacja nowych zagrożeń, zmiany organizacyjne zasobu infrastruktury krytycznej czy też wykazanie pewnych niedociągnięć podczas ćwiczeń powinno prowadzić do ponownej weryfikacji przygotowanych mechanizmów ciągłości działania.

3.3. REAGOWANIE NA SYTUACJE KRYZYSOWE

Reagowanie w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej to szereg działań podejmowanych przede wszystkim w celu zapewnienia ciągłości działania. Proces reagowania na sytuacje kryzysowe można podzielić na następujące podprocesy (Rys. 3.11):

- monitorowanie i prognozowanie rozwoju sytuacji kryzysowej,
- neutralizacja i ograniczanie zdarzeń kryzysowych,
- uruchamianie mechanizmów ciągłości działania zasobów infrastruktury krytycznej.

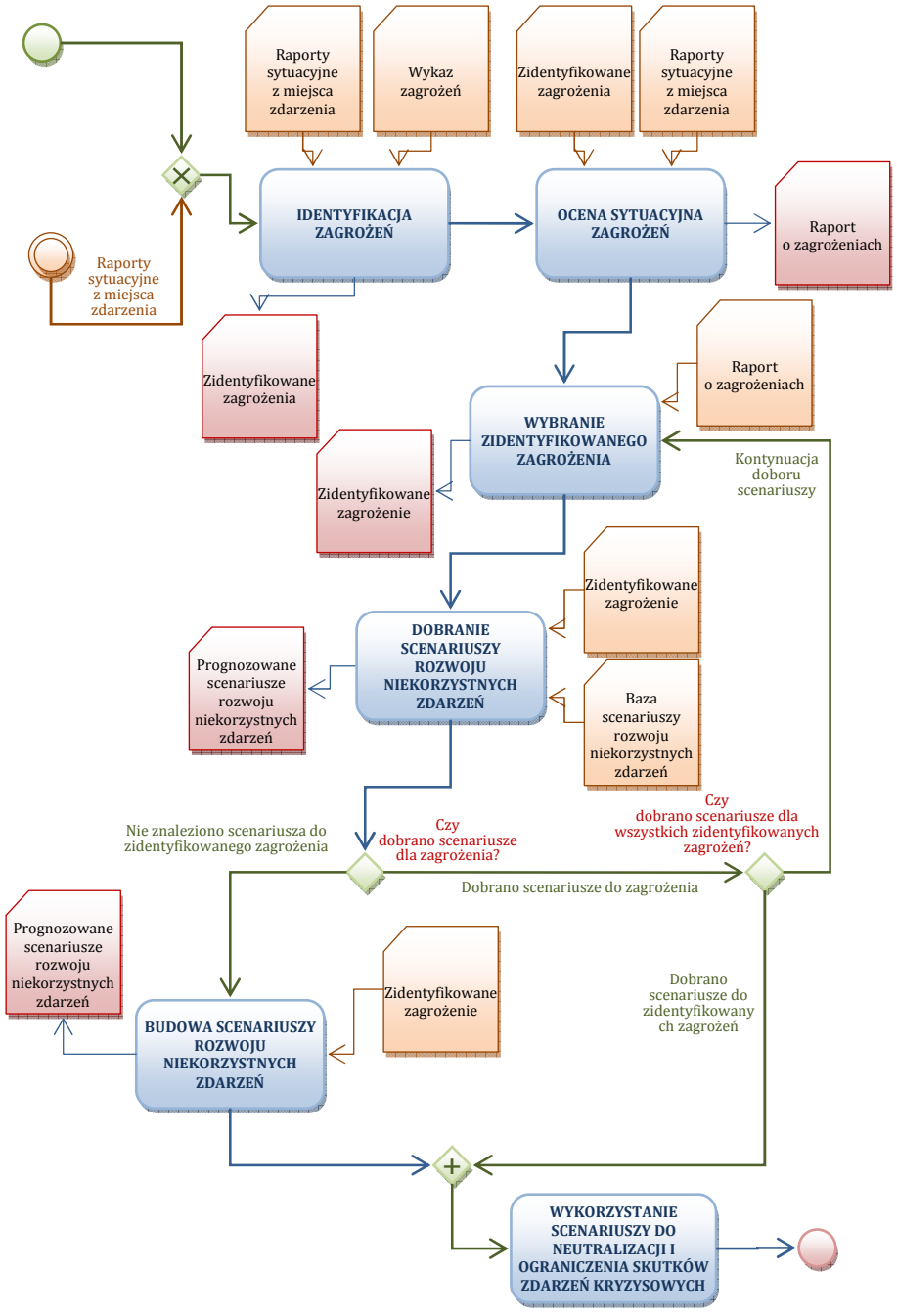


Rys. 3.11. Podprocesy procesu reagowania na sytuacje kryzysowe

Realizacja zadań podczas reagowania na sytuacje kryzysowe jest prowadzona zawsze w deficycie czasu oraz w warunkach stresogennych. Od samego początku prowadzenia działań należy uruchamiać proces monitorowania i prognozowania rozwoju sytuacji kryzysowej. Głównym zadaniem tego procesu jest dostarczenie jak największej ilości informacji niezbędnych do podejmowania racjonalnych decyzji przez osoby kierujące akcją reagowania.

Niezwłocznie należy przystąpić również do łagodzenia i neutralizacji sytuacji kryzysowej przy wykorzystaniu przeznaczonych do tego sił i środków oraz jak najszybszego przywracania ciągłości działania elementów infrastruktury krytycznej, których praca została zakłócona.

W dobie rozwoju nowoczesnych technologii proces reagowania na sytuacje kryzysowe powinien być wspierany przez rozwiązania sztucznej inteligencji, zastępujące człowieka w analizie ogromnych ilości danych i opracowywaniu optymalnych decyzji.



Rys. 3.12. Mapa procesu monitorowania i prognozowania rozwoju sytuacji kryzysowej

Zajście zdarzenia kryzysowego powoduje, że niezwłocznie uruchamiany jest proces monitoringu oraz prognozowania rozwoju sytuacji niekorzystnych, dający podstawy do podejmowania dalszych działań mających na celu neutralizację i ograniczanie skutków zdarzeń kryzysowych oraz zapewnienie ciągłości działania zasobów infrastruktury krytycznej (Rys. 3.12).

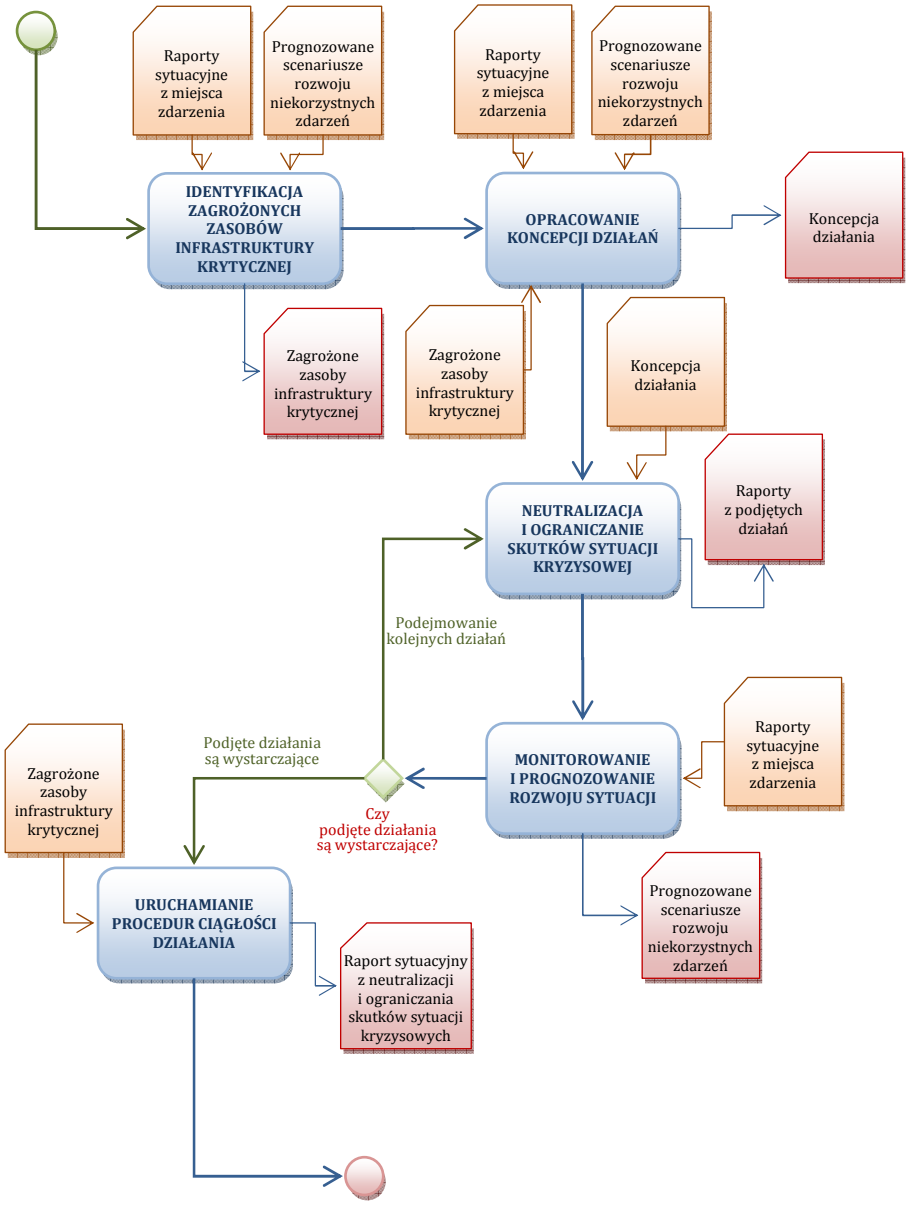
W pierwszej kolejności należy zidentyfikować rodzaj zagrożenia, jakie się zmaterializowało i ocenić jego intensywność. Skuteczność tego działania jest uzależniona od wiarygodności oraz kompletności danych zgromadzonych w postaci raportów sytuacyjnych. Dane z monitoringu powinny zawierać: typ zdarzenia, przyczynę zdarzenia, szczegółowy opis zasobu infrastruktury krytycznej, którego zdarzenie dotyczy, zakres szkód.

Zastosowanie nowoczesnych technologii w formie inteligentnych sensorów, szybkich łączy telekomunikacyjnych oraz rozwiązań sztucznej inteligencji pozwala w dużym stopniu zautomatyzować te czynności i wyeliminować niepotrzebne opóźnienia w dopływie i interpretacji danych źródłowych.

Kolejnym działaniem procesu jest znalezienie odpowiedniego scenariusza rozwoju niekorzystnych zdarzeń opracowanego podczas przygotowywania zasobów infrastruktury krytycznej na sytuacje kryzysowe lub opracowanie nowego scenariusz w przypadku, gdy infrastruktura krytyczna ma do czynienia z nową formą zagrożenia.

Wynikiem procesu jest: dokładna analiza sytuacji kryzysowej, identyfikacja zagrożenia oraz ocena jego intensywności, prognoza rozwoju sytuacji niekorzystnych w formie scenariuszy.

Pierwsze działania, realizowane zaraz po zajściu zdarzenia kryzysowego są prowadzone zwykle pod presją czasu, dlatego też szczególnie trudnym wyzwaniem jest identyfikacja zagrożeń, które formalnie nie zostały wyspecyfikowane w zbiorze zagrożeń lub scenariuszy, jako potencjalne niebezpieczeństwa zasobów infrastruktury krytycznej. Biorąc pod uwagę zmienność typów i źródeł zagrożeń oraz zróżnicowaną ich intensywność sytuacja tego typu może pojawiać się dość często i może prowadzić do trudności podczas podejmowania decyzji. W takich okolicznościach niezwykle przydatne wydają się być narzędzie programowe potrafiące w czasie rzeczywistym kreować nowe rozwiązania w zależności od napływających danych z monitoringu.



Rys. 3.13. Mapa procesu neutralizacji i ograniczania skutków sytuacji kryzysowej

Proces neutralizacji i ograniczania skutków sytuacji kryzysowej uruchamiany jest po zidentyfikowaniu i klasyfikacji zagrożeń oraz po znalezieniu scenariuszy rozwoju niekorzystnych zdarzeń (Rys. 3.13). Wymaga on ciągłego opracowywania planów działania, wdrażania ich oraz prowadzenia obserwacji zmian sytuacyjnych. Jeżeli podejmowane wysiłki przynoszą oczekiwane korzyści wówczas należy podtrzymywać zastosowane rozwiązania, aż do całkowitego zahamowania niekorzystnej sytuacji. W przeciwnym wypadku należy niezwłocznie weryfikować zastosowane podejście i uruchamiać alternatywne środki rozwiązywania problemów.

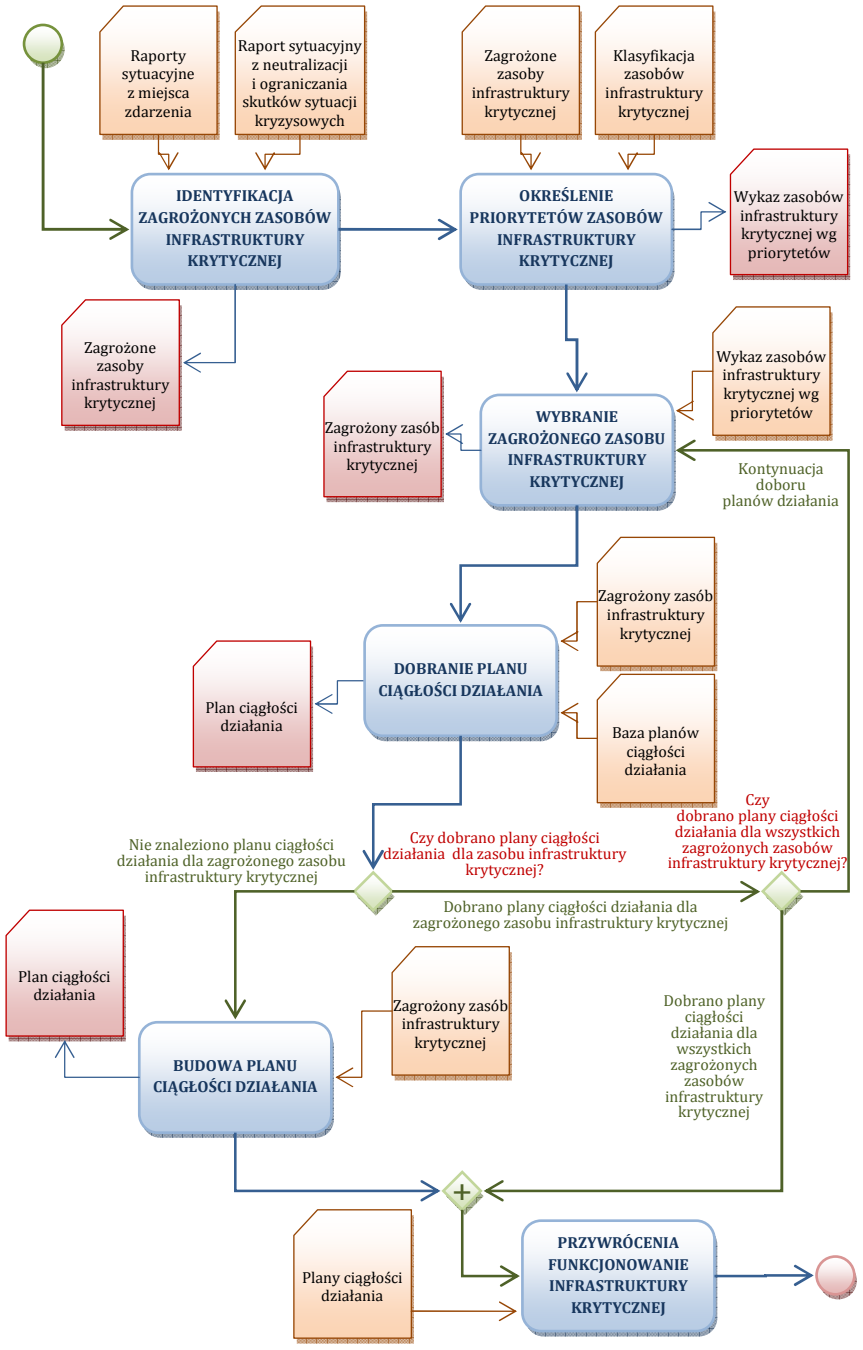
Skuteczność prowadzonych działań uzależniona jest w głównej mierze od posiadania dobrze przeszkolonego personelu, wydajnych kanałów informacyjnych zapewniających dopływ aktualnych i wiarygodnych danych, wsparcia materiałowego oraz przygotowanych mechanizmów współdziałania w razie konieczności z innymi uczestnikami procesu reagowania na sytuacje kryzysowe.

Podstawowymi zadaniami, które są wykonywane podczas neutralizacji i ograniczania skutków sytuacji kryzysowej są działania ratownicze i ewakuacyjne podejmowane w pierwszej kolejności przez ekipy ratownictwa medycznego, jeśli zostało narażone życie i zdrowie ludzkie, a w dalszej kolejności przez inne służby ratownictwa specjalistycznego, stosownie do zaistniałej sytuacji kryzysowej.

Ważnym działaniem procesu neutralizacji i ograniczania skutków sytuacji kryzysowej jest prowadzenie monitoringu oraz prognozowanie rozwoju sytuacji po zastosowaniu środków zaradczych.

Działanie to stanowi rodzaj informacyjnego sprzężenia zwrotnego w systemie zwalczania skutków i następstw zidentyfikowanych zagrożeń i dostarcza informacje diagnostyczne organom kierowniczym o skuteczności podejmowanych wysiłków antykryzysowych.

Skuteczne zahamowanie rozwoju niekorzystnych zdarzeń jest warunkiem przejścia do uruchamiania procedur zapewniających przywrócenie infrastruktury krytycznej do działania przynajmniej w minimalnym stopniu.



Rys. 3.14. Mapa procesu zapewnienia ciągłości działania infrastruktury krytycznej

Ciągłość działania zasobów infrastruktury krytycznej to stan nieprzerwanego funkcjonowania obiektu, instalacji, urządzeń oraz wykonywania usług, osiągnięty poprzez zastosowanie wszelkiego rodzaju środków zapobiegawczych o charakterze organizacyjnym, technicznym i personalnym (Rys. 3.14). Proces zapewnienia ciągłości działania powinien utrzymywać wszystkie kluczowe funkcje infrastruktury krytycznej po zajściu sytuacji kryzysowej oraz działalność operacyjną całego zasobu na wypadek utrzymujących się i poważnych zakłóceń powstałych w wyniku sytuacji kryzysowej.

Podejmując przedsięwzięcia zmierzające do utrzymania ciągłości działania zasobu infrastruktury krytycznej w sytuacji jej zniszczenie bądź zakłócenia pracy należy w pierwszej kolejności dokonać identyfikacji zagrożonych zasobów infrastruktury krytycznej oraz określić priorytety, wg których będą ograniczane zagrożenia oraz minimalizowane skutki niekorzystnych zdarzeń.

Kolejnym działaniem jest wskazanie odpowiedniego planu ciągłości działania, który został opracowany podczas realizacji zadań z zakresu przygotowania infrastruktury krytycznej do zdarzeń kryzysowych. Zmienność w czasie oraz identyfikowanie nowych zagrożeń może spowodować, że nie będzie przygotowanego gotowego planu działania, adekwatnego do zaistniałej sytuacji kryzysowej, wobec czego należy podjąć niezwłocznie kroki do przygotowania takiego planu i wykorzystanie go do przywrócenia funkcjonowania zasobów infrastruktury krytycznej.

W zależności od czasu trwania zakłócenia pracy zasobów infrastruktury krytycznej, ponoszone są znaczące straty. Szczególnie dotkliwe są zazwyczaj straty finansowe, w wielu sytuacjach dotkliwa jest utrata wizerunku. W ekstremalnych przypadkach zakłócenie ciągłości działania zasobu infrastruktury krytycznej może doprowadzić do jego destrukcji.

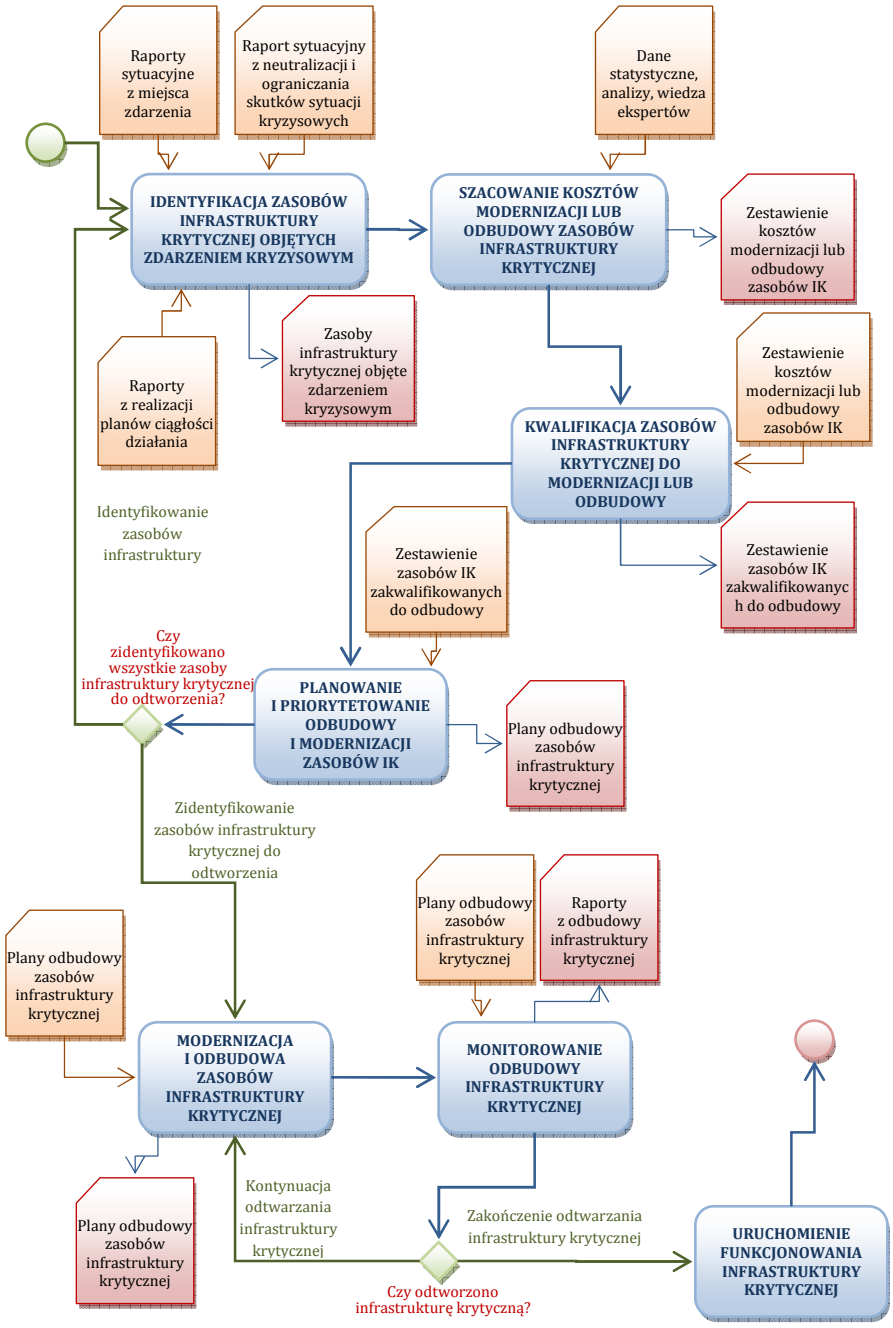
Rozpatrując cały system infrastruktury krytycznej, jako zbiór naczyń połączonych należy mieć na uwadze, że jeśli sytuacja kryzysowa dotknie jednego zasób infrastruktury krytycznej to w zależności od jego powiązań z innymi elementami, mamy do czynienie z tzw. „efektem domina", powodującym utratę ciągłości działania przez kolejne zasoby. Stąd też bardzo ważnym jest utrzymanie kluczowych zasobów w ciągłym działaniu tak, aby zatrzymanie ich funkcjonowania nastąpiło jak najpóźniej lub wcale.

3.4. ODBUDOWA INFRASTRUKTURY KRYTYCZNEJ

Odtwarzanie (odbudowa) infrastruktury krytycznej polega na przywróceniu jej możliwości funkcjonalnych do stanu sprzed zaistnienia sytuacji kryzysowej (Rys. 3.15). Głównymi działaniami, podejmowanymi niezwłocznie po zniszczeniu bądź zakłóceniu pracy infrastruktury krytycznej są przedsięwzięcia zapewniające jej ciągłość działania przynajmniej w minimalnym stopniu. Ma to miejsce jeszcze podczas reagowania na sytuacje kryzysowe. Natomiast po neutralizacji zagrożeń następuje szacowanie skutków zakłócenia pracy lub zniszczenia infrastruktury krytycznej, identyfikacja zasobów infrastruktury krytycznej do odbudowy, planowanie i priorytetowanie odbudowy infrastruktury krytycznej, modernizacja i odbudowa infrastruktury krytycznej.

Rys. 3.15. Podprocesy procesu odbudowy infrastruktury krytycznej

Przywracanie infrastruktury krytycznej do funkcjonowania po zajściu zdarzeń kryzysowych będzie obejmowało zazwyczaj długoterminową odbudowę, naprawę lub wymianę jej poszczególnych elementów. Kolejność wykonywanych prac będzie zależała od wpływu poszczególnych elementów na przebieg procesów społecznych i gospodarczych. W pierwszym rzędzie będą przywracane do użytku szlaki komunikacyjne (drogi, lotniska, porty morskie), środki łączności (telefon, Internet, radio), zaopatrzenie w energię elektryczną, zaopatrzenie w wodę pitną, usługi służby zdrowia, usługi finansowe, funkcjonowanie administracji publicznej, edukacja oraz zaopatrzenie w żywność.



Rys. 3.16. Mapa procesu odbudowy infrastruktury krytycznej

Odbudowa i przywracanie stanu pierwotnego infrastruktury krytycznej po opanowaniu sytuacji kryzysowej jest etapem zamykającym proces zarządzania ochroną infrastruktury krytycznej (Rys. 3.16). Wymaga on zaangażowania znacznych sił i środków materiałowych a także finansowych, co w odniesieniu do infrastruktury krytycznej należącej do operatorów prywatnych, jest kwestią bardzo trudną.

Działania odtwarzania infrastruktury krytycznej przebiegają w warunkach pewnej stabilizacji sytuacyjnej, gdy poziom zagrożeń i skala niebezpieczeństw zostały opanowane. Zadaniem tego etapu jest przywrócenie funkcjonalności zakłóconego obiektu, instalacji, urządzenia lub usługi i zapewnienie warunków do działania, czyli doprowadzenie do przynajmniej minimalnych standardów bezpieczeństwa.

Czas trwania etapu odbudowy infrastruktury krytycznej jest uzależniony przede wszystkim od poziomu destrukcji, wielkości strat i zniszczeń wywołanych określoną kategorią zagrożeń. Czynnikiem przyspieszającym wykonywanie działań tego procesu jest niewątpliwie nieuchronność kolejnych zdarzeń kryzysowych oraz znaczenie zniszczonych bądź uszkodzonych elementów infrastruktury krytycznej dla funkcjonowania gospodarki, społeczeństwa oraz administracji publicznej.

Pierwszym działaniem podejmowanym w procesie odtwarzania infrastruktury krytycznej jest identyfikacja zniszczeń i uszkodzeń. Na podstawie raportów sytuacyjnych z miejsca zdarzenie, wykonywane są operacje szacowania kosztów odbudowy lub modernizacji zniszczonych obiektów, instalacji, urządzeń i usług.

Mając przygotowane zestawienia kosztów, wykonywana jest kwalifikacja elementów do modernizacji i odbudowy. Podczas kwalifikacji dochodzi często to podejmowania decyzji o całkowitej odbudowie infrastruktury i wprowadzeniu nowoczesnych rozwiązań, co przyczynia się do podniesienia bezpieczeństwa systemów infrastruktury krytycznej.

Następnym działaniem jest planowanie i priorytetowanie kolejności przywracania infrastruktury do działania zgodnie z ważnością świadczonych przez nią usług[163]. Ostatnie działania to praktyczna

[163] International Recovery Platform Secretariat, *Guidance note on recovery: infrastructure*, Japan, www.recoveryplatform.org, 12.2012.

odbudowa i uruchamianie pełnej funkcjonalności infrastruktury krytycznej, która została zniszczona bądź uszkodzona podczas sytuacji kryzysowej.

* * *

Ochrona infrastruktury krytycznej jest procesem bardzo złożonym, obejmującym wiele obszarów zadaniowych oraz angażującym wiele podmiotów administracji rządowej, samorządowej oraz operatorów i właścicieli prywatnych.

W skład procesu ochrony infrastruktury krytycznej zostały zaliczone podprocesy zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej, przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną, reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej i odtwarzanie infrastruktury krytycznej.

Do szczegółowych zadań realizowanych na rzecz procesu zarządzania bezpieczeństwem infrastruktury krytycznej należą:

- opracowanie regulacji formalno-prawnych ochrony infrastruktury krytycznej,
- identyfikacja krajowej i Europejskiej Infrastruktury Krytycznej,
- identyfikacja zagrożeń,
- ocena ryzyka,
- opracowanie scenariuszy ochrony infrastruktury krytycznej,
- opracowanie planów ochrony infrastruktury krytycznej,
- opracowanie Narodowego Planu Ochrony Infrastruktury Krytycznej,
- przygotowanie mechanizmów ciągłości działania infrastruktury krytycznej,
- monitorowanie i prognozowanie rozwoju sytuacji kryzysowej,
- neutralizacja zdarzeń kryzysowych,
- ograniczanie skutków zdarzeń kryzysowych,
- uruchamianie mechanizmów ciągłości działania infrastruktury krytycznej,
- szacowanie skutków zakłócenia pracy lub zniszczenia infrastruktury krytycznej,
- identyfikacja zasobów infrastruktury krytycznej do odbudowy,

- planowanie i priorytetowanie odbudowy infrastruktury krytycznej,
- modernizacja i odbudowa infrastruktury krytycznej.

Przedstawione na rys. 3.1-3.16 mapy procesów[164] systemu ochrony infrastruktury krytycznej zostały skonstruowane na podstawie wyników analiz, przeprowadzonych we wcześniejszych etapach procesu badawczego. Niezbędna była identyfikacja zagrożeń bezpieczeństwa, identyfikacja elementów systemu zarządzania kryzysowego oraz analiza procesu zarządzania sytuacjami kryzysowymi. Bardzo przydatne okazały się również materiały źródłowe udostępnione przez Departament Bezpieczeństwa Wewnętrznego USA dotyczące sektorowych planów ochrony infrastruktury krytycznej[165]: *National Infrastructure Protection Plan, Banking and Finance Sector-Specific Plan, Chemical Sector-Specific Plan, Commercial Facilities Sector-Specific Plan, Communications Sector-Specific Plan, Critical Manufacturing Sector-Specific Plan, Dams Sector-Specific Plan, Defense Industrial Base Sector-Specific Plan, Education Facilities Sector-Specific Plan, Emergency Services Sector-Specific Plan, Energy Sector-Specific Plan, Food and Agriculture Sector-Specific Plan, Healthcare and Public Health Sector-Specific Plan, National Monuments and Icons Sector-Specific Plan, Nuclear Reactors, Materials, and Waste Sector-Specific Plan, Transportation Systems Sector-Specific Plan, Water Sector-Specific Plan.*

Projekt procesu ochrony infrastruktury krytycznej przedstawiono w postaci graficznych map z wykorzystaniem notacji procesów biznesowych BPMN. Mapy procesów zostały zweryfikowane przy pomocy analitycznego oprogramowania *Bizagi Process Modeler* i prezentują ciąg uporządkowanych działań podejmowanych na różnych etapach ochrony infrastruktury krytycznej.

[164] Przez proces należy rozumieć logiczny ciąg następujących po sobie działań lub równoległych czynności, których realizacja prowadzi do spełnienia oczekiwań. Mapa procesu to graficzna prezentacja przebiegu i sekwencji działań realizowanych w procesie (E. Skrzypek, M. Hofman, *Zarządzanie procesami w przedsiębiorstwie*, Oficyna a Wolters Kluwer business, Warszawa 2010, s. 12, s. 77),

[165] http://www.dhs.gov/critical-infrastructure-sectors.

ROZDZIAŁ 4
MATEMATYCZNY MODEL SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFRASTRUKTURY KRYTYCZNEJ

Kolejnym etapem przyjętej procedury badawczej jest budowa modelu matematycznego systemu zarządzania bezpieczeństwem infrastruktury krytycznej. Z przeprowadzonej analizy ogólnie dostępnych rozwiązań, opisywanych szeroko w literaturze międzynarodowej wynika, iż modelowanie odporności infrastruktury krytycznej na zniszczenie lub zakłócenia pracy jej zasobów nabrało w ostatnim dziesięcioleciu dużego tempa[166]. Wskazuje na to rosnąca liczba publikacji oraz prowadzonych prac badawczych szczególnie w krajach Unii Europejskiej[167], Stanach Zjednoczonych[168], Kanadzie[169] oraz Australii[170].

---

166 G. Satumtira, L. Dueñas-Osorio, *Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research* (http://link.springer.com/chapter/10.1007%2F978-3-642-11405-2_1#page-1).

167 Ch. Siaterlis, B. Genge, M. Hohenadel, M. Del Pra, *Enabling the Experimental Exploration of Operating Procedures on Critical Infrastructures* (http://www.thei3p.org/docs/events/ ifip2012presentation/ hohenadel.pdf), *Protecting Critical Infrastructures –Risk and Crisis Management, A guide for companies and government authorities*, Berlin 2008, www.bmi.bund.de, G. Giannopoulos, R. Filippini, M. Schimmer, *Risk assessment methodologies for Critical Infrastructure Protection,* Part I: A state of the art, European Commission Joint Research Centre Institute for the Protection and Security of the Citizen, Publications Office of the European Union, 2012 (http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf).

168 Sandia National Laboratories, *Optimal Recovery Sequencing for Critical Infrastructure Resilience Assessment*, New Mexico, USA 2010, (http://prod.sandia.gov/techlib/access-control.cgi/2010/106237.pdf, 12.2012), T. Brown, *Multiple Modeling Approaches and Insights for Critical Infrastructure Protection* (www.sandia.gov/nisac/ downloads288), K. Young-Suk, B.F. Spencer, Jr. Amr S. Elnashai, *Seismic Loss Assessment and Mitigation for Critical Urban Infrastructure Systems* (https://www.ideals.illinois.edu/bitstream/handle/2142/4603/NSEL.Report.007.pdf? sequence=4), New York State Comprehensive Emergency Management Plan, *Critical Infrastructure and Key Resources Functional Annex*, Prepared by the member agencies of the New York State Critical Infrastructure and Key Resources Branch, 01.2012, (http://www.dhses.ny.gov/planning/documents/cikr-branch-3.2012.pdf), The Heritage Foundation, *One Year Later: Lessons from Recovery after the Great Eastern Japan Earthquake*, special report, Washington 2012, (http://report.heritage.org/sr0108), *Critical Infrastructure Strategic Roadmap*,

Poniżej omówiono główne kierunki badań, prowadzonych w obszarze bezpieczeństwa infrastruktury krytycznej przez zagraniczne ośrodki i instytucje naukowe.

Pierwszym materiałem źródłowym omawiającym kompleksowe podejście do infrastruktury krytycznej jest opracowanie przedstawiające model zależności i powiązań między poszczególnymi systemami infrastruktury krytycznej pt. *Computational Support for Identifying Safety and Security Related Dependencies between National Critical Infrastructures*[171].

Kolejne źródło, pt. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* zawiera opis relacji pomiędzy systemami infrastruktury krytycznej, metody analizy oraz charakterystykę wiodących rozwiązań technologicznych do oceny bezpieczeństwa infrastruktury krytycznej[172].

Podobne podejście do bezpieczeństwa infrastruktury krytycznej zostało przedstawione w pracy pt. *Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS*[173]. Autorzy skupili się tutaj na modelowaniu danych i informacji o zależnościach między poszczególnymi systemami infrastruktury krytycznej.

Nielinearny charakter zachowań oraz zmienność funkcjonowania w czasie złożonych systemów infrastruktury krytycznej zostały poddane

Electricity Sub-Sector Coordinating Council, Princeton 2010, (http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V4_7_Oct2010_clean.pdf).

169 E. Bagheri, A. Ghorbani, *Towards an MDA-Oriented UML Profile for Critical Infrastructure Modeling* (www.ee.ryerson.ca/~bagheri/papers/pst2.pdf).

170 *Critical infrastructure resilience strategy*, Australia 2010, (www.tisn.gov.au, 12.2012), G. Pye, M. J. Warren, *Conceptual Modelling: Choosing a Critical Infrastructure Modelling Methodology*, Deakin University (http://ro.ecu.edu.au/isw/16/).

171 Ch. W. Johnson, R. Williams, *Computational Support for Identifying Safety and Security Related Dependencies between National Critical Infrastructures*, Department of Computing Science, University of Glasgow (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.139.4581).

172 P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory 2006 (http://www.inl.gov/technicalpublications/Documents/3489532.pdf).

173 R. Klein, E. Rome, C. Beyel, R. Linnemann, W. Reinhardt, *Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS* (http://www.irriis.org/Filebee4.pdf?lang=2&oiid=9206&pid=952).

analizie przez S. Bologna i T. Beera w pracy *An Integrated Approach to Survivability Analysis of Large Complex Critical Infrastructures*[174].

Autorzy artykułu *Risk Analysis and Crisis Scenario Evaluation in Critical Infrastructures Protection* podkreślają konieczność dysponowania nowoczesnymi narzędziami do oceny ryzyka oraz generowania scenariuszy rozwoju sytuacji kryzysowych w odniesieniu do bezpieczeństwa infrastruktury krytycznej[175].

Raport *Comparative Evaluation of Modeling and Simulation Techniques for Interdependent Critical Infrastructures, Scientific Report* zawiera opis oraz charakterystykę wybranych metod modelowania oraz symulacji wykorzystywanych do zarządzania bezpieczeństwem infrastruktury krytycznej[176].

Podejście do konkretnych sektorów infrastruktury krytycznej zostało przedstawione przez K. Niemeyera w *Simulation of critical infrastructures.* Prezentuje on szereg typów modeli infrastruktury krytycznej zbudowanych do symulacji zagrożeń oraz konsekwencji zakłóceń pracy systemów zaopatrzenia w energię oraz systemów transportowych[177].

Rozwiązania z zakresu monitoringu krytycznych zasobów Łotwy związanych z zaopatrzeniem w energię elektryczną, wodę, siecią ciepłowniczą oraz infrastrukturą transportową są przedmiotem rozważań opracowania *The Problem Issues of Intelligent Monitoring and Control of CIS in Latvia*[178].

Kolejnym opracowaniem ujmującym problematykę bezpieczeństwa systemów zaopatrzenia w wodę jest *Modelling Resilience*

---

174 S. Bologna, T. Beer, *An Integrated Approach to Survivability Analysis of Large Complex Critical Infrastructures* (http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-3.pdf).

175 V. Rosato, V. Artale, G. Pisacane, G. Sannino, M. V. Struglia, A. Tofani, E. Pascucci, *Risk Analysis and Crisis Scenario Evaluation in Critical Infrastructures Protection*, ENEA, Energetic and Environmental Modelling Unit, Casaccia Research Centre, InTech, Roma 2011 (cdn.intechweb.org/pdfs/18806.pdf).

176 *Comparative Evaluation of Modeling and Simulation Techniques for Interdependent Critical Infrastructures, Scientific Report* (www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/publikationen_ski.parsys.87450.DownloadFile.tmp/comparativeevaluation.pdf).

177 K. Niemeyer, *Simulation of critical infrastructures*, INFORMATION & SECURITY. An International Journal, Vol.15, No.2, 2004, 120-143 (www.gcmarshall.bg/KP/2b/3.pdf).

178 A. Zabasta, N. Kunicina, L. Ribickis, *The Problem Issues of Intelligent Monitoring and Control of CIS in Latvia*, Electronics and Electrical Engineering, 2012. No. 2(118), (http://www.ee.ktu.lt/journal/2012/02/12_ISSN_1392-1215_The Problem Issues of Intelligent Monitoring and Control of CIS in Latvia.pdf).

in a Water Supply System: Contrasting conditions of drought and flood. Przedstawiona koncepcja rozpatruje badany element infrastruktury krytycznej jako metasystem będący kombinacją systemu bio-ekologicznego, technicznego i społeczno-technicznego[179].

Problematyka modelowania zależności między elementami infrastruktury krytycznej w odniesieniu do systemów zaopatrzenia w energię, usług telekomunikacyjnych oraz systemów ratownictwa została przedstawiona w *Critical National Infrastructure Reliability Modeling and Analysis*[180].

Modelowanie podatności na zagrożenia sieci energetycznych, rurociągów naftowych, lotnisk oraz łańcuchów zaopatrzeniowych zostało omówione w *Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses Gerald Brown*[181].

Opracowanie *A model with applications for data survivability in Critical Infrastructures* zawiera propozycję budowy mechanizmów zapewniających dopływ i przechowywanie danych funkcjonowania infrastruktury krytycznej na przykładzie systemu zaopatrzenia w ropę naftową[182].

Zintegrowane podejście do modelowania, symulacji i analizy systemów zaopatrzenia w energię elektryczną oraz rynków finansowych zostało zaprezentowane w *An Integrated Approach to Modeling, Simulation, and Analysis of Critical Infrastructure Systems*[183].

Miary ochrony infrastruktury krytycznej, problematyka modelowania i symulacji bezpieczeństwa infrastruktury krytycznej oraz najważniejsze problemy związane z bezpieczeństwem infrastruktury

---

179 P. Barnes, P. Egodawatta, A. Goonetilleke, *Modelling Resilience in a Water Supply System: Contrasting conditions of drought and flood*, Health Faculty, Queensland University of Technology (iiirr.ucalgary.ca/files/iiirr/B4-2_.pdf).

180 S. H. Conrad, R. J. LeClaire, G. P. O'Reilly, H. Uzunalioglu, *Critical National Infrastructure Reliability Modeling and Analysis* (www.sandia.gov/nisac/wp/wp-content/uploads/downloads/2012/03/Critical- National-Infrastructure -Reliability-Modeling-and-Analysis-2006-3442-J.pdf).

181 M. Carlyle, J. Salmerón, K. Wood, *Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses Gerald Brown* (http://faculty.nps.edu/kwood/docs/DefendingCIBrownEtAlTutorialDraft.pdf).

182 M. Albano, S. Chessa, R. Di Pietro, *A model with applications for data survivability in Critical Infrastructures*, Journal of Information Assurance and Security 4 (2009) (www.researchgate.net).

183 S. Ball, M.D. Marshall, S. Schaffer, K. J. Wedeward, *An Integrated Approach to Modeling, Simulation, and Analysis of Critical Infrastructure Systems* (http://www.icasa.nmt.edu/Content/publication/integrated_approach.pdf).

krytycznej zostały przedstawione w cyklu opracowań w *International journal of mathematics and computers in simulation*[184].

Kwantyfikacja stopnia odporności infrastruktury krytycznej na zagrożenia została zaproponowane przez B. Ch. Ezella w pracy *Infrastructure Vulnerability Assessment Model*. Omówiony model został odniesiony do systemu zaopatrzenia w wodę. Autor wskazał również możliwość implementacji swojego rozwiązania do oceny innych zasobów infrastruktury krytycznej[185].

Zniszczenie lub zakłócenie pracy elementów infrastruktury krytycznej niesie ze sobą zwykle duże starty ekonomiczne. Problem ten jest rozważany w opracowaniu *Economic impact assessment of Critical Infrastructure failure in the EU: A combined Systems Engineering – Inoperability Input-Output Model*[186].

Optymalizacja kosztów w poszukiwaniu słabych punktów systemów infrastruktury krytycznej była przedmiotem badań prowadzonych przez F. Baiardi w pracy *Allocating Resources to the Search for Vulnerabilities in Information Infrastructures*[187].

Przykład zastosowania teorii grafów został przedstawiony w opracowaniu E. Kelevedjieva *Computational Approach for Assessment of Critical Infrastructure in Network Systems.* Autor zaproponował model infrastruktury krytycznej do badania zachowań sieci energetycznych oraz systemów zaopatrzenia w wodę w sytuacjach krytycznych[188].

---

184 L. Lukas, L. Necesal, *Measures for Critical infrastructure protection*, International journal of mathematical models and methods in applied sciences, (http://www.naun.org/multimedia/NAUN/m3as/17-138.pdf), L. Lukas, M. Hromada, *Simulation and Modeling in Critical Infrastructure Protection*, International journal of mathematical models and methods in applied sciences, (http://www.naun.org/multimedia/NAUN/mcs/20-871.pdf), L. Lukas, M. Hromada, *Resilience as main part of protection of critical infrastructure*, International journal of mathematical models and methods in applied sciences, (http://www.naun.org/multimedia/NAUN/m3as/20-879.pdf).

185 B. Ch. Ezell, *Infrastructure Vulnerability Assessment Model (I-VAM)* (create.usc.edu/assets/pdf/51834.pdf).

186 O. E. Jonkeren, D. Ward, B. Dorneanu, G. Giannopoulos, *Economic impact assessment of Critical Infrastructure failure in the EU: A combined Systems Engineering – Inoperability Input-Output Model*, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra, Italy, (www.iioa.org/files/conference-3/903.pdf).

187 F. Baiardi, *Allocating Resources to the Search for Vulnerabilities in Information Infrastructures* (www.di.unipi.it/~baiardi/sec/natoARWrisk.pdf).

188 E. Kelevedjiev, *Computational Approach for Assessment of Critical Infrastructure in Network Systems* (www.gcmarshall.bg/KP/2a/6.pdf).

Teoria grafów została również wykorzystana do procesu automatycznej dedukcji informacji niezbędnych do oceny ryzyka w pracy *Hierarchical, Model-Based Risk Management of Critical Infrastructures*[189].

Nowatorskie rozwiązanie dotyczące wykrywania słabych punktów infrastruktury krytycznej przedstawiono w opracowaniu *Ad-Hoc Cloud Networks: A Probabilistic Model for Vulnerability Detection in Critical Infrastructure Using Bayesian Networks*. Autorzy zwrócili uwagę na możliwość wykorzystania sieci bayesa oraz przetwarzania w chmurze do poprawy funkcjonowania serwisów infrastruktury krytycznej i uodpornienia jej na zagrożenia[190].

Możliwości wykorzystania ogólnie dostępnego oprogramowania (AutoCad, Adobe Photoshop, Global Mapper, ArcGIS (ESRI), Di-Guy (Boston Dynamics), Presagis (MultiGen-Paradigm) i AIMSUN.) do modelowania sytuacji kryzysowych mających wpływ na funkcjonowanie infrastruktury krytycznej zostały przedstawione w *Modeling and Simulation of Catastrophic Events Affecting Critical Infrastructure Systems*[191].

Podsumowując treści powyższych materiałów źródłowych należy podkreślić, iż najbardziej znaczące rozwiązania wykorzystują metody modelowania matematycznego, modelowania obiektowego, teorię sieci i grafów, projektowanie procesów oraz wieloagentową symulację. Najczęściej modelowane są zachowania najważniejszych systemów infrastruktury krytycznej, czyli systemów zaopatrzenia w energię elektryczną, systemów zaopatrzenia w wodę, systemów transportowych, systemów telekomunikacyjnych. Modelowane są również pojedyncze obiekty infrastruktury krytycznej takie jak lotniska, dworce kolejowe, elektrownie oraz ropociągi. Nieliczne są opracowania przedstawiające kompleksowe podejście do oceny bezpieczeństwa infrastruktury krytycznej, jako systemu o wielkiej skali złożoności.

---

189 F. Baiardi, C. Telmon, D. Sgandurra, *Hierarchical, Model-Based Risk Management of Critical Infrastructures* (http://eprints.adm.unipi.it/596/1/baiardijournalrevised.pdf).

190 I. O. Idowu, Q. Shi, M. Merabti, K. Kifayat, *Ad-Hoc Cloud Networks: A Probabilistic Model for Vulnerability Detection in Critical Infrastructure Using Bayesian Networks*, School of Computing and Mathematical Sciences, Liverpool John Moores University (http://www.cms.livjm.ac.uk/pgnet2012/Proceedings/Papers/1569607177.pdf).

191 P. D. Scarlatos, E. I. Kaisar, R. Teegavarapu, *Modeling and Simulation of Catastrophic Events Affecting Critical Infrastructure Systems*, Department of Civil, Environmental and Geomatics Engineering Florida Atlantic University (http://www.wseas.us/e-library/conferences/2009/vouliagmeni/ACCMM/ACCMM1-46.pdf).

Ważnym aspektem prowadzonych badań jest również poszukiwanie wspólnych miar bezpieczeństwa oraz kwantyfikacja wskaźników jakościowych infrastruktury krytycznej.

W opracowaniach zwraca się uwagę na konieczność stosowania nowoczesnych technologii, jako niezbędnego oprzyrządowania do analizy zagrożeń, oceny ryzyka, znajdowania słabych punktów w systemach, instalacjach, urządzenia oraz usługach.

4.1. KONCEPCJA MODELOWANIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFRASTRUKTURY KRYTYCZNEJ

Zgodnie z ogólną teorią systemów model matematyczny rozpatrywanego systemu rzeczywistego jest podstawowym narzędziem za pomocą, którego można zbadać zbiór dopuszczalnych rozwiązań i wybrać *rozwiązanie optymalne*, tj. znaleźć taką konfigurację systemu, w której system będzie funkcjonował w sposób najlepszy. Jak podkreśla K. Ficoń[192], znalezione w ten sposób rozwiązanie optymalne jest rozwiązaniem najlepszym jedynie z punktu widzenia modelu, a nie modelowanej rzeczywistości. Biorąc pod uwagę to stwierdzenie, w zaproponowanym poniżej modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej starano się ująć całą jego funkcjonalność jak najwierniej w odniesieniu do rzeczywistości.

Ochrona infrastruktury krytycznej jest jednym z głównych zadań realizowanych w celu zapewnienia bezpieczeństwa państwa i jego obywateli oraz sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorstw[193]. Proces ochrony infrastruktury krytycznej jest złożonym czasoprzestrzennym działaniem systemowym, którego sprawna i niezawodna realizacja polega na:

- zapobieganiu zakłóceniom funkcjonowania infrastruktury krytycznej,

[192] K. Ficoń, *Badania operacyjne stosowane. Modele i aplikacji*, BEL Studio, Warszawa 2006, s. 12.

[193] Ochrona infrastruktury krytycznej w myśl *Ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym* to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie

- przygotowaniu na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,
- reagowaniu w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- odtwarzaniu infrastruktury krytycznej.

Na gruncie państwa ochrona infrastruktury krytycznej może być realizowana za pomocą tzw. Systemu Zarządzania Bezpieczeństwem Infrastruktury Krytycznej (Ψ)[194]. W ujęciu systemowym system ten definiujemy jako spójną, hierarchicznie zbudowaną organizację (strukturę) ukierunkowaną na niezawodne zabezpieczenie różnorodnych potrzeb nadrzędnego systemu jakim jest System Bezpieczeństwa Narodowego (Ξ)[195].

W strukturze Systemu Bezpieczeństwa Narodowego, System Zarządzania Bezpieczeństwem Infrastruktury Krytycznej pełni rolę wspierającą wobec priorytetowych potrzeb i wymagań tego systemu, co formalnie można zapisać, jako:

$$\Psi|\Xi = \langle E_\Psi, E_\Psi \times E_\Psi \rangle = \langle E_\Psi, \{R_\Psi\} \rangle \tag{4.1}$$

gdzie:

Ψ – system zarządzania bezpieczeństwem infrastruktury krytycznej (struktura podrzędna),
Ξ – system bezpieczeństwa narodowego (struktura nadrzędna),
E_Ψ – zbiór elementów struktury organizacyjno-funkcjonalnej systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
R_Ψ – zbiór relacji systemowych i zadań ochrony infrastruktury krytycznej realizowanych na rzecz systemu bezpieczeństwa narodowego.

Funkcjonalnie pojęcie Systemu Zarządzania Bezpieczeństwem Infrastruktury Krytycznej (Ψ) zdefiniujemy jako uporządkowaną

[194] W procesie modelowania przyjęto, że System Zarządzania Bezpieczeństwem Infrastruktury Krytycznej będzie odpowiadał za ochronę infrastruktury krytycznej.
[195] W projekcie *Strategii rozwoju systemu bezpieczeństwa narodowego RP 2012-2022* z kwietnia 2012 roku, ochrona infrastruktury krytycznej traktowana jest jako system wsparcia bezpieczeństwa państwa. Do systemów wsparcia bezpieczeństwa państwa zaliczane są systemy operacyjne takie, jak: system rezerw strategicznych, system ochrony granicy państwowej, system przeciwpowodziowy, system ochrony danych osobowych i informacji niejawnych. Ich rozwijanie służy uzyskaniu odporności na zagrożenia bezpieczeństwa narodowego, w tym na sytuacje nadzwyczajne i nieprzewidywalne zdarzenia.

hierarchicznie organizację składająca się z organów kierowania, właścicieli infrastruktury krytycznej, obiektów, urządzeń i instalacji przeznaczonych do zaopatrzenia i świadczenia różnorodnych usług dla państwa i jego obywateli, administracji publicznej, instytucji i przedsiębiorstw, co symbolicznie zapiszemy jako:

$$\Psi = \{[K_{IK} \subseteq W_{IK} \subseteq O_{IK} \subseteq U_{IK} \subseteq I_{IK}], [D_{IK} \cup U_{IK}]\} \tag{4.2}$$

gdzie:

Ψ – system zarządzania bezpieczeństwem infrastruktury krytycznej,
K_{IK} – organa kierowania,
W_{IK} – właściciele infrastruktury krytycznej,
O_{IK} – obiekty infrastruktury krytycznej,
U_{IK} – urządzenia infrastruktury krytycznej,
I_{IK} – instalacje infrastruktury krytycznej,
D_{IK} – dostawy zaopatrzenia infrastruktury krytycznej,
U_{IK} – usługi infrastruktury krytycznej.

System zarządzania bezpieczeństwem infrastruktury krytycznej jest pragmatycznym systemem sprawnego działania zorientowanym na wykonanie określonych funkcji i zadań z zakresu zapewnienia bezpieczeństwa państwa i jego obywateli, funkcjonowania administracji publicznej, instytucji i przedsiębiorstw. Dokonuje on konwersji możliwości (potencjału) systemu zarządzania bezpieczeństwem infrastruktury krytycznej (M_Ψ) na potrzeby nadrzędnego systemu bezpieczeństwa narodowego (P_Ξ) w jednym z trzech stanów: pokoju, kryzysu oraz wojny.

$$\Psi : M_\Psi \rightarrow P_\Xi = \begin{cases} P_\Xi^P - pokój \\ P_\Xi^K - kryzys \\ P_\Xi^W - wojna \end{cases} \tag{4.3}$$

gdzie:

Ψ – system zarządzania bezpieczeństwem infrastruktury krytycznej,
M_Ψ – możliwości systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
P_Ξ – potrzeby systemu bezpieczeństwa narodowego w zakresie ochrony infrastruktury krytycznej,

P_{Ξ}^{P} – potrzeby systemu bezpieczeństwa narodowego w zakresie ochrony infrastruktury krytycznej w czasie pokoju,
P_{Ξ}^{K} – potrzeby systemu bezpieczeństwa narodowego w zakresie ochrony infrastruktury krytycznej w czasie kryzysu,
P_{Ξ}^{W} – potrzeby systemu bezpieczeństwa narodowego w zakresie ochrony infrastruktury krytycznej w czasie wojny.

Dla potrzeb budowanego modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej (Ψ) wygodnie go będzie przedstawić w konwencji układu cybernetycznego, zapisanego jako iloczyn kartezjański wejść (potrzeb systemu bezpieczeństwa narodowego), wyjść (możliwości systemu zarządzania bezpieczeństwem infrastruktury krytycznej) oraz decyzji.

$$\Psi \subseteq \{P_{\Xi} \times D_{\Psi}^{\Xi} \times M_{\Psi}\} \xrightarrow{P_{\Psi}(t)} F_{\Psi} \tag{4.4}$$

gdzie:

Ψ – system zarządzania bezpieczeństwem infrastruktury krytycznej,
P_{Ξ} – potrzeby systemu bezpieczeństwa narodowego w zakresie ochrony infrastruktury krytycznej,
D_{Ψ}^{Ξ} – decyzje sterujące procesami zarządzania bezpieczeństwem infrastruktury krytycznej,
M_{Ψ} – możliwości wykonawcze systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
$P_{\Psi}(t)$ – funkcja zarządzania bezpieczeństwem infrastruktury krytycznej,
F_{Ψ} – funkcja celu (efektywności) zarządzania bezpieczeństwem infrastruktury krytycznej.

przy czym:

$$\begin{aligned} P_{\Psi}(t) &: P_{\Xi} \times D_{\Psi}^{\Xi} \rightarrow M_{\Psi} \\ F_{\Psi} &: D_{\Psi}^{\Xi} \times M_{\Psi} \rightarrow R^{+} \end{aligned} \tag{4.5}$$

gdzie:

R^{+} – zbiór liczb rzeczywistych (wskaźnik jakości).

System zarządzania bezpieczeństwem infrastruktury krytycznej, jako jeden z systemów wsparcia systemu bezpieczeństwa narodowego odpowiada za podtrzymywanie i wspomaganie funkcjonowania

podstawowych procesów w państwie. Głównym zadaniem systemu zarządzania bezpieczeństwem infrastruktury krytycznej (4.3) w sensie funkcjonalnym jest przygotowanie i utrzymanie wskazanego potencjału bezpieczeństwa infrastruktury krytycznej (*Π(t)*), który w strukturach bezpieczeństwa państwa transformowany jest do postaci potencjału operacyjnego (*Ω(t)*). Równanie bilansowe potencjału operacyjnego *Ω(t)* w aspekcie bezpieczeństwa infrastruktury krytycznej można zapisać, jak poniżej:

$$\Omega(t) = \Omega_0 - \overline{\Pi(t)} + \Pi(t) \tag{4.6}$$

gdzie:

$\Omega(t)$ – aktualny potencjał operacyjny w chwili *t*,
Ω_0 – początkowy potencjał operacyjny w chwili *t*,
$\overline{\Pi(t)}$ – zużyty potencjał bezpieczeństwa infrastruktury krytycznej,
$\Pi(t)$ – odtworzony potencjał bezpieczeństwa infrastruktury krytycznej.

Jak wynika z równania (4.6) funkcja potencjału operacyjnego *Ω(t)* jest funkcją z jednej strony intensywności niszczenia potencjału bezpieczeństwa infrastruktury krytycznej $\overline{\Pi(t)}$ z drugiej zaś, funkcją intensywności jego odtwarzania. Trzecią jej zmienną niezależną (względnie stałą) jest początkowa wartość potencjału operacyjnego Ω_0, czyli:

$$\Omega(t) = f(\Omega_0, \overline{\Pi(t)}, \Pi(t)) \tag{4.7}$$

Potencjał operacyjny struktur bezpieczeństwa państwa *Ω(t)* jest sukcesywnie zużywany w czasie pokoju, kryzysu oraz wojny. We wszystkich tych sytuacjach są zużywane określone zasoby infrastruktury krytycznej, które poprzez proces zarządzania bezpieczeństwem infrastruktury krytycznej muszą być sukcesywnie odtwarzane i uzupełniane do określonych stanów. Proces zarządzania bezpieczeństwem infrastruktury krytycznej jest procesem ciągłym i musi być prowadzony z odpowiednią intensywnością, niezawodnością, skutecznością i przy racjonalnie uzasadnionych nakładach materialnych (N_M), czasowych (N_T) i finansowych (N_F).

Powyższe uwarunkowania i potrzeby nakładają na system zarządzania bezpieczeństwem infrastruktury krytycznej określone wymagania i ograniczenia, które muszą być spełnione często w krytycznych warunkach (np. podczas sytuacji kryzysowych).

Proces zarządzania bezpieczeństwem infrastruktury krytycznej (PR_{Ψ}) można formalnie zdefiniować, jako transformację potencjału infrastruktury krytycznej ($\Pi(t)$) do postaci potencjału operacyjnego ($\Omega(t)$), którego najwyższą formą jest potencjał ($\Lambda(t)$) rozumiany, jako zdolność do wykonania określonych zadań:

$$PR_{\Psi} \mid N_M, N_T, N_F : \Pi(t) \rightarrow \Omega(t) \rightarrow \Lambda(t) \tag{4.8}$$

gdzie:

PR_{Ψ} – proces zarządzanie bezpieczeństwem infrastruktury krytycznej,
N_M – nakłady materiałowe,
N_T – nakłady czasowe,
N_F – nakłady finansowe,
$\Omega(t)$ – potencjał operacyjny infrastruktury krytycznej,
$\Lambda(t)$ – potencjał bezpieczeństwa infrastruktury krytycznej.

System zarządzania bezpieczeństwem infrastruktury krytycznej jest systemem dynamicznym, który musi nadążać za gwałtownie zmieniającymi się potrzebami państwa, stosownie do rzeczywistej sytuacji geopolitycznej. Racjonalne kształtowanie struktury organizacyjno-funkcjonalnej i procedur jego działania jest zadaniem szczególnie złożonym i odpowiedzialnym. Dlatego jego doskonalenie i usprawnianie odbywa się na drodze modelowania tak teoretycznego, jak też praktycznego. Szczególnie przydatne w tym względzie okazuje się modelowanie symulacyjne i specjalistyczne oprogramowanie narzędziowe.

Budowane modele są jedynie pewnym przybliżeniem określonej rzeczywistości i obrazują tylko wycinkowe aspekty ogólnej struktury organizacyjno-funkcjonalnej rzeczywistego systemu ochrony infrastruktury krytycznej. Sukcesywnie rozwijane i coraz bardziej przybliżane do praktycznych systemów działania przyczyniają się po pierwsze do bliższego poznania stanu faktycznego a po drugie do podjęcia prób usprawnienia tego stanu i doskonalenia funkcji i procesów.

Jednym z takich modeli jest model systemu zarządzania bezpieczeństwem infrastruktury krytycznej. Jest to model formalny zapisany w postaci reguł logiczno-matematycznych za pomocą symbolicznych wyrażeń, funkcji i struktur formalnych.

Zgodnie z ogólnymi założeniami analizy systemowej model systemu zarządzania bezpieczeństwem infrastruktury krytycznej (MM_Ψ) został zdekomponowany na dwa modele – opisowy model identyfikacyjny (MI_Ψ) i optymalizacyjny model decyzyjny (MD_Ψ):

$$MM_\Psi = \langle MI_\Psi, MD_\Psi \rangle \tag{4.9}$$

gdzie:

MM_Ψ – matematyczny model systemu zarządzanie bezpieczeństwem infrastruktury krytycznej,

MI_Ψ – model identyfikacyjny systemu zarządzanie bezpieczeństwem infrastruktury krytycznej,

MD_Ψ – model decyzyjny systemu zarządzanie bezpieczeństwem infrastruktury krytycznej.

Model identyfikacyjny (MI_Ψ) rozpoczyna proces modelowania matematycznego systemu zarządzania bezpieczeństwem infrastruktury krytycznej (Ψ), którego ostatecznym celem jest wypracowanie na etapie modelowania decyzyjnego (MD_Ψ) optymalnych strategii i procedur praktycznego działania ze względu na przyjęte kryterium oceny jakości funkcjonowania systemu rzeczywistego. Model decyzyjny (MD_Ψ) dostarcza naukowych metod i narzędzi służących do usprawnienia funkcjonowania modelu identyfikacyjnego (MI_Ψ), a w efekcie końcowym badanego modelu (MM_Ψ) systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

4.2. MODEL IDENTYFIKACYJNY SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFRASTRUKTURY KRYTYCZNEJ

Model identyfikacyjny MI_Ψ systemu zarządzanie bezpieczeństwem infrastruktury krytycznej Ψ formalnie zostanie zapisany w następujący sposób:

$$MI_{\Psi} = \langle C_{\Psi}, \{D_{\Psi}, R_{\Psi}\}, Z_{\Psi} \rangle \tag{4.10}$$

gdzie:

MI_{Ψ} – model identyfikacyjny systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
C_{Ψ} – cel działania systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
D_{Ψ} – dziedzina systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
R_{Ψ} – relacje występujące w systemie zarządzania bezpieczeństwem infrastruktury krytycznej,
Z_{Ψ} – zasady funkcjonowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

Głównym celem działania systemu zarządzania bezpieczeństwem infrastruktury krytycznej jest minimalizacja zagrożeń oraz maksymalizacja standardu bezpieczeństwa infrastruktury krytycznej. Jego misję można rozpatrzeć w trzech płaszczyznach:

$$C_{\Psi} = \langle C_{\Psi}^{S}, C_{\Psi}^{T}, C_{\Psi}^{O} \rangle \tag{4.11}$$

gdzie:

C_{Ψ} – cel działania systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
C_{Ψ}^{S} – cel strategiczny systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
C_{Ψ}^{T} – cel taktyczny systemu zarządzania bezpieczeństwem infrastruktury krytycznej.
C_{Ψ}^{O} – cel operacyjny systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

Celem strategicznym C_{Ψ}^{S} systemu zarządzania bezpieczeństwem infrastruktury krytycznej Ψ jest podtrzymanie potencjału operacyjnego infrastruktury krytycznej we wszystkich zasadniczych działaniach dotyczących bezpieczeństwa państwa i jego obywateli oraz sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorstw. Osiągany jest on poprzez tworzenie i podtrzymanie określonego potencjału infrastruktury krytycznej, który za pomocą procesu zarządzania bezpieczeństwem infrastruktury krytycznej jest transformowany do określonej postaci potencjału operacyjnego systemu bezpieczeństwa narodowego.

$$C_{\Psi}^{S} : \Pi_{IK} \xrightarrow{PR_{\Psi}} \Pi_{\Xi} \tag{4.12}$$

gdzie:

C_{Ψ}^{S} – cel strategiczny systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
Π_{IK} – potencjał operacyjny infrastruktury krytycznej,
PR_{Ψ} – proces zarządzania bezpieczeństwem infrastruktury krytycznej,
Π_{Ξ} – potencjał operacyjny systemu zarządzania bezpieczeństwem narodowym.

Celem taktycznym C_{Ψ}^{T} systemu zarządzania bezpieczeństwem infrastruktury krytycznej jest zapewnienie i permanentne podtrzymywanie pożądanego potencjału operacyjnego infrastruktury krytycznej Π_{IK} do zapobiegania zakłóceniom funkcjonowania lub zniszczenia infrastruktury krytycznej, przygotowania infrastruktury krytycznej na sytuacje kryzysowe, reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej oraz odtwarzaniu infrastruktury krytycznej. Realizacja celu taktycznego została zapisana, jako transformacja możliwości operacyjnych systemu zarządzania bezpieczeństwem infrastruktury krytycznej w potencjał operacyjny Ψ.

$$C_{\Psi}^{T} : M_{\Psi} \rightarrow \Pi_{\Psi} \tag{4.13}$$

gdzie:

C_{Ψ}^{T} – cel taktyczny systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
M_{Ψ} – możliwości operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
Π_{Ψ} – potencjał operacyjny systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

Celem operacyjnym C_{Ψ}^{O} jest realizacja dynamicznych procesów zarządzania bezpieczeństwem infrastruktury krytycznej PR_{Ψ} w trójwymiarowej przestrzeni obejmującej zdarzenia kryzysowe, przestrzeń i czas. Jest to transformacja procesów zarządzania bezpieczeństwem infrastruktury krytycznej do postaci harmonogramów działań operacyjnych w odniesieniu do zdarzeń kryzysowych.

$$C_{\Psi}^{O} : \Pi_{\Psi} \rightarrow H_{\Psi} \subseteq X \times Y \times T \tag{4.14}$$

gdzie:

C_{Ψ}^{O} – cel operacyjny systemu zarządzanie bezpieczeństwem infrastruktury krytycznej,
Π_{Ψ} – potencjał operacyjny systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
H_{Ψ} – harmonogramy procesów zarządzania bezpieczeństwem infrastruktury krytycznej,
$X \times Y \times T$ – przestrzeń zarządzania bezpieczeństwem infrastruktury krytycznej.

Formalnie harmonogram realizacji procesu zarządzania bezpieczeństwem infrastruktury krytycznej będziemy określać, jako zbiór uporządkowanych trójek – zagrożenia kryzysowego, chwil czasowych obejmujących moment rozpoczęcia danego działania ($t(d_i)$) i czasu trwania podjętego działania ($\tau(d_i)$):

$$zd_i \in ZD : H_{\Psi} = \{\langle zk, t(d_i), \tau(d_i)\rangle\}; i = \overline{1, I} \tag{4.15}$$

gdzie:

zd_i – *i-te* działanie (zadanie) związane z ochroną infrastruktury krytycznej,
ZD – zbiór działań ochrony infrastruktury krytycznej,
H_{Ψ} – harmonogramy procesów zarządzania bezpieczeństwem infrastruktury krytycznej,
zk – zdarzenie kryzysowe,
$t(d_i)$ – moment rozpoczęcia realizacji i-tego działania,
$\tau(d_i)$ – czas trwania i-tego działania.

Biorąc pod uwagę powyższe należy stwierdzić, że celem operacyjnym C_{Ψ}^{O} funkcjonowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej jest planowanie i realizacji działań w przestrzeni $X \times Y \times T$ co jest równoznaczne z generowaniem harmonogramów dla poszczególnych procesów zarządzania bezpieczeństwem infrastruktury krytycznej.

Cel działania systemu ochrony infrastruktury krytycznej możemy zdefiniować także w aspekcie funkcjonalnym poprzez określenie szczegółowych funkcji i zadań fizycznych, jakie musi on realizować na

rzecz systemu bezpieczeństwa narodowego. W tym sensie cel ochrony infrastruktury krytycznej obejmuje cztery zasadnicze procesy:

$$C_{\Psi}^{F} = \langle C_{\Psi}^{Z}, C_{\Psi}^{U}, C_{\Psi}^{AP}, C_{\Psi}^{SN} \rangle \tag{4.16}$$

gdzie:

C_{Ψ}^{F} – cel funkcjonalny systemu zarządzanie bezpieczeństwem infrastruktury krytycznej,
C_{Ψ}^{Z} – zarządzanie bezpieczeństwem systemów zaopatrzeniowych,
C_{Ψ}^{U} – zarządzanie bezpieczeństwem systemów usługowych,
C_{Ψ}^{AP} – zarządzanie bezpieczeństwem administracji publicznej,
C_{Ψ}^{SN} – zarządzanie bezpieczeństwem substancji niebezpiecznych.

Realizacja ochrony systemów zaopatrzeniowych obejmuje następujące kategorie:

$$C_{\Psi}^{F} = \left\{ C_{\Psi}^{Z_i}; i = \overline{1,6} \right\} \tag{4.17}$$

gdzie:

C_{Ψ}^{Z} – zarządzanie bezpieczeństwem systemów zaopatrzeniowych,
$C_{\Psi}^{Z_1}$ – zarządzanie bezpieczeństwem zaopatrzenia w energię elektryczną,
$C_{\Psi}^{Z_2}$ – zarządzanie bezpieczeństwem zaopatrzenia w energię cieplną,
$C_{\Psi}^{Z_3}$ – zarządzanie bezpieczeństwem zaopatrzenia w gaz ziemny,
$C_{\Psi}^{Z_4}$ – zarządzanie bezpieczeństwem zaopatrzenia w ropę naftową,
$C_{\Psi}^{Z_5}$ – zarządzanie bezpieczeństwem zaopatrzenia w żywność,
$C_{\Psi}^{Z_6}$ – zarządzanie bezpieczeństwem zaopatrzenia w wodę.

W zakres ochrony systemów usługowych C_{Ψ}^{U} funkcjonujących w ramach infrastruktury krytycznej wchodzą:

$$C_{\Psi}^{U} = \left\{ C_{\Psi}^{U_i}; i = \overline{1,6} \right\} \tag{4.18}$$

gdzie:

C_{Ψ}^{U} – zarządzanie bezpieczeństwem systemów usługowych,
$C_{\Psi}^{U_1}$ – zarządzanie bezpieczeństwem łączności,
$C_{\Psi}^{U_2}$ – zarządzanie bezpieczeństwem systemów teleinformatycznych,
$C_{\Psi}^{U_3}$ – zarządzanie bezpieczeństwem ochrony zdrowia,

$C_{\Psi}^{U_4}$ – zarządzanie bezpieczeństwem systemów finansowych,
$C_{\Psi}^{U_5}$ – zarządzanie bezpieczeństwem transportu i komunikacji,
$C_{\Psi}^{U_6}$ – zarządzanie bezpieczeństwem systemów ratowniczych.

Zarządzanie bezpieczeństwem administracji publicznej ma na celu zabezpieczenie ciągłości pracy administracji publicznej i obejmuje:

$$C_{\Psi}^{AP} = \left\{C_{\Psi}^{AP_i}; i = \overline{1,3}\right\} \tag{4.19}$$

gdzie:

C_{Ψ}^{AP} – zarządzanie bezpieczeństwem administracji publicznej,
$C_{\Psi}^{AP_1}$ – zarządzanie bezpieczeństwem administracji rządowej,
$C_{\Psi}^{AP_2}$ – zarządzanie bezpieczeństwem administracji samorządowej,
$C_{\Psi}^{AP_3}$ – zarządzanie bezpieczeństwem administracji państwowej.

Ostatnią analizowaną grupą są systemy substancji niebezpiecznych, których obszarem działania jest produkcja, składowanie, przechowywanie i stosowanie substancji chemicznych i promieniotwórczych oraz nadzór nad rurociągami substancji niebezpiecznych:

$$C_{\Psi}^{SN} = \left\{C_{\Psi}^{SN_i}; i = \overline{1,4}\right\} \tag{4.20}$$

gdzie:

C_{Ψ}^{SN} – zarządzanie bezpieczeństwem systemów substancji niebezpiecznych,
$C_{\Psi}^{SN_1}$ – zarządzanie bezpieczeństwem produkcji substancji niebezpiecznych,
$C_{\Psi}^{SN_2}$ – zarządzanie bezpieczeństwem składowania substancji niebezpiecznych,
$C_{\Psi}^{SN_3}$ – zarządzanie bezpieczeństwem przechowywania i stosowania substancji niebezpiecznych,
$C_{\Psi}^{SN_4}$ – zarządzanie bezpieczeństwem rurociągów substancji niebezpiecznych.

Pojęcie dziedziny systemu zarządzania bezpieczeństwem infrastruktury krytycznej D_{Ψ} będzie rozpatrzone w kilku aspektach, wg różnych kryteriów klasyfikacyjnych. Najogólniej dziedziną modelu D_{Ψ} jest zbiór elementów tworzących dany system, wyodrębnionych ze

względu na przyjęte zasady podziału topologicznego. Z uwagi na dynamiczny i interaktywny charakter analizowanego systemu dokonano podziału dziedziny modelu na dwie klasy dotyczące odpowiednio otoczenia zewnętrznego i wewnętrznego.

$$D_\Psi = \{D_\Psi^Z, D_\Psi^W\} \tag{4.21}$$

gdzie:

D_Ψ – dziedzina systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
D_Ψ^Z – otoczenie zewnętrzne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
D_Ψ^W – otoczenie wewnętrzne systemu zarządzania bezpieczeństwem infrastruktury krytycznej (wewnętrzna struktura organizacyjno-funkcjonalna).

W skład zewnętrznego otoczenia systemowego D_Ψ^Z wchodzą wszystkie elementy zewnętrzne środowiska gospodarczego, społecznego, politycznego oraz militarnego mające wpływ na realizację procesu zarządzania bezpieczeństwem infrastruktury krytycznej. Do zbioru elementów otoczenia zewnętrznego systemu zarządzania bezpieczeństwem infrastruktury krytycznej przykładowo można zaliczyć:

$$D_\Psi^Z = \left\{D_\Psi^{Z_i}; i = \overline{1,7}\right\} \tag{4.22}$$

gdzie:

D_Ψ^Z – otoczenie zewnętrzne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
$D_\Psi^{Z_1}$ – system ochrony infrastruktury krytycznej Unii Europejskiej,
$D_\Psi^{Z_2}$ – system ochrony infrastruktury krytycznej państw sąsiadujących,
$D_\Psi^{Z_3}$ – system bezpieczeństwa narodowego,
$D_\Psi^{Z_4}$ – system rezerw strategicznych,
$D_\Psi^{Z_5}$ – system ochrony granicy państwowej,
$D_\Psi^{Z_6}$ – system przeciwpowodziowy,
$D_\Psi^{Z_7}$ – system ochrony danych osobowych i informacji niejawnych.

Elementy zewnętrznego otoczenia systemowego $D_\Psi^{Z_i} \in D_\Psi^Z$ mogą być wykorzystane przez system zarządzania bezpieczeństwem

infrastruktury krytycznej do potęgowania możliwości ochrony infrastruktury krytycznej, a tym samym do wzrostu jego potencjału operacyjnego. Dalsze rozważania nad dziedziną modelu zostaną skoncentrowane na analizie elementów wewnętrznej struktury organizacyjno-funkcjonalnej.

Zgodnie z definicją strukturalną (*4.2*) systemu zarządzania bezpieczeństwem infrastruktury krytycznej, jego podstawowymi elementami są:

$$D_{\Psi}^{W} = \left\{ D_{\Psi}^{W_i}; i = \overline{1,5} \right\}$$

gdzie:

D_{Ψ}^{W} – otoczenie wewnętrzne systemu zarządzania bezpieczeństwem infrastruktury krytycznej (wewnętrzna struktura organizacyjno-funkcjonalna),
$D_{\Psi}^{W_1}$ – organa kierowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
$D_{\Psi}^{W_2}$ – właściciele infrastruktury krytycznej,
$D_{\Psi}^{W_3}$ – obiekty infrastruktury krytycznej,
$D_{\Psi}^{W_4}$ – urządzenia infrastruktury krytycznej,
$D_{\Psi}^{W_5}$ – instalacje infrastruktury krytycznej.

Powyższa definicja obrazuje sposób organizacji systemu zarządzania bezpieczeństwem infrastruktury krytycznej ze względu na kryterium sprawnego zarządzania, w którym dominuje nadrzędny system kierowania $D_{\Psi}^{W_1}$ nad właścicielami $D_{\Psi}^{W_2}$, obiektami $D_{\Psi}^{W_3}$, urządzeniami $D_{\Psi}^{W_4}$ i instalacjami $D_{\Psi}^{W_5}$ infrastruktury krytycznej.

Organa kierowania $D_{\Psi}^{W_1}$ odpowiadają za sprawność i niezawodność procesu ochrony infrastruktury krytycznej. W skład organów kierowania $D_{\Psi}^{W_1}$ wchodzą:

$$D_{\Psi}^{W_1} = \left\{ D_{\Psi}^{W_{1i}}; i = \overline{1,8} \right\} \tag{4.23}$$

gdzie:

$D_{\Psi}^{W_1}$ – organa kierowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
$D_{\Psi}^{W_{11}}$ – Prezes Rady Ministrów,
$D_{\Psi}^{W_{12}}$ – Dyrektor Rządowego Centrum Bezpieczeństwa,

$D_{\Psi}^{W_{13}}$ – Ministrowie,
$D_{\Psi}^{W_{14}}$ – kierownicy urzędów centralnych,
$D_{\Psi}^{W_{15}}$ – wojewodowie,
$D_{\Psi}^{W_{16}}$ – starostowie,
$D_{\Psi}^{W_{17}}$ – wójtowie (burmistrzowie, prezydenci miast),
$D_{\Psi}^{W_{18}}$ – pełnomocnicy ds. ochrony infrastruktury krytycznej.

Za całokształt procesów ochrony infrastruktury krytycznej państwa odpowiada Prezes Rady Ministrów. Dyrektor Rządowego Centrum Bezpieczeństwa oraz ministrowie i kierownicy urzędów centralnych zajmują się głównie planowaniem, organizowaniem i kontrolowaniem procesu ochrony infrastruktury krytycznej na poziomie państwa zgodnie z zaleceniami Prezesa Rady Ministrów. Wojewodowie, starostowie oraz wójtowie (burmistrzowie, prezydenci miast) pełnią funkcje podrzędne warunkujące należytą sprawność procesu kierowania w systemie zarządzania bezpieczeństwem infrastruktury krytycznej na poziomie regionalnym. Pełnomocnicy ds. ochrony infrastruktury krytycznej są przedstawicielami właścicieli infrastruktury krytycznej i odpowiadają za realizację zadań z zakresu ochrony infrastruktury krytycznej.

Właściciele infrastruktury krytycznej $D_{\Psi}^{W_2}$ w systemie zarządzania bezpieczeństwem infrastruktury krytycznej są zobowiązani do realizacji powierzonych im zadań z zakresu ochrony infrastruktury krytycznej. Właściciel infrastruktury krytycznej można podzielić na dwie grupy ze względu na prawo własności:

$$D_{\Psi}^{W_2} = \{D_{\Psi}^{W_{2i}}; i = \overline{1,2}\} \tag{4.24}$$

gdzie:

$D_{\Psi}^{W_2}$ – właściciele infrastruktury krytycznej,
$D_{\Psi}^{W_{21}}$ – państwowi właściciele infrastruktury krytycznej,
$D_{\Psi}^{W_{22}}$ – prywatni właściciele infrastruktury krytycznej.

Innym podziałem właścicieli infrastruktury krytycznej może być podział oparty o kryterium przynależności do odpowiednich systemów infrastruktury krytycznej:

$$D_{\Psi}^{W_2} = \{D_{\Psi}^{W_{2i}}; i = \overline{1,14}\} \tag{4.25}$$

gdzie:

$D_{\Psi}^{W_2}$ – właściciele infrastruktury krytycznej,
$D_{\Psi}^{W_{21}}$ – właściciele systemów zaopatrzenia w energię elektryczną,
$D_{\Psi}^{W_{22}}$ – właściciele systemów zaopatrzenia w energię cieplną,
$D_{\Psi}^{W_{23}}$ – właściciele systemów zaopatrzenia w gaz ziemny,
$D_{\Psi}^{W_{24}}$ – właściciele systemów zaopatrzenia w ropę naftową,
$D_{\Psi}^{W_{25}}$ – właściciele systemów zaopatrzenia w żywność,
$D_{\Psi}^{W_{26}}$ – właściciele systemów zaopatrzenia w wodę,
$D_{\Psi}^{W_{27}}$ – właściciele systemów łączności,
$D_{\Psi}^{W_{28}}$ – właściciele systemów teleinformatycznych,
$D_{\Psi}^{W_{29}}$ – właściciele systemów ochrony zdrowia,
$D_{\Psi}^{W_{210}}$ – właściciele systemów finansowych,
$D_{\Psi}^{W_{211}}$ – właściciele systemów transportowych i komunikacyjnych,
$D_{\Psi}^{W_{212}}$ – właściciele systemów ratowniczych,
$D_{\Psi}^{W_{213}}$ – właściciele systemów administracji publicznej,
$D_{\Psi}^{W_{214}}$ – właściciele systemów substancji niebezpiecznych.

Obiekty, urządzenia i instalacje infrastruktury krytycznej $D_{\Psi}^{W_3}, D_{\Psi}^{W_4}, D_{\Psi}^{W_5}$ obejmują bardzo dużą klasę różnorodnych budowli, środków urządzeń technicznych warunkujących sprawne i niezawodne działanie infrastruktury krytycznej. Według kryterium funkcjonalnego rodzajów infrastruktury krytycznej techniczne systemy infrastruktury krytycznej można podzielić na następujące klasy:

$$D_{\Psi}^{W_3} = \{D_{\Psi}^{W_{3i}}; i = \overline{1,14}\} \tag{4.26}$$

gdzie:

$D_{\Psi}^{W_3}$ – obiekty infrastruktury krytycznej,
$D_{\Psi}^{W_{31}}$ – obiekty systemów zaopatrzenia w energię elektryczną,
$D_{\Psi}^{W_{32}}$ – obiekty systemów zaopatrzenia w energię cieplną,
$D_{\Psi}^{W_{33}}$ – obiekty systemów zaopatrzenia w gaz ziemny,
$D_{\Psi}^{W_{34}}$ – obiekty systemów zaopatrzenia w ropę naftową,
$D_{\Psi}^{W_{35}}$ – obiekty systemów zaopatrzenia w żywność,
$D_{\Psi}^{W_{36}}$ – obiekty systemów zaopatrzenia w wodę,
$D_{\Psi}^{W_{37}}$ – obiekty systemów łączności,

$D_{\Psi}^{W_{38}}$ – obiekty systemów teleinformatycznych,
$D_{\Psi}^{W_{39}}$ – obiekty systemów ochrony zdrowia,
$D_{\Psi}^{W_{310}}$ – obiekty systemów finansowych,
$D_{\Psi}^{W_{311}}$ – obiekty systemów transportowych i komunikacyjnych,
$D_{\Psi}^{W_{312}}$ – obiekty systemów ratowniczych,
$D_{\Psi}^{W_{313}}$ – obiekty systemów administracji publicznej,
$D_{\Psi}^{W_{314}}$ – obiekty systemów substancji niebezpiecznych.

$$D_{\Psi}^{W_4} = \{D_{\Psi}^{W_{4i}}; i = \overline{1,14}\} \tag{4.27}$$

gdzie:

$D_{\Psi}^{W_4}$ – urządzenia infrastruktury krytycznej,
$D_{\Psi}^{W_{41}}$ – urządzenia systemów zaopatrzenia w energię elektryczną,
$D_{\Psi}^{W_{42}}$ – urządzenia systemów zaopatrzenia w energię cieplną,
$D_{\Psi}^{W_{43}}$ – urządzenia systemów zaopatrzenia w gaz ziemny,
$D_{\Psi}^{W_{44}}$ – urządzenia systemów zaopatrzenia w ropę naftową,
$D_{\Psi}^{W_{45}}$ – urządzenia systemów zaopatrzenia w żywność,
$D_{\Psi}^{W_{46}}$ – urządzenia systemów zaopatrzenia w wodę,
$D_{\Psi}^{W_{47}}$ – urządzenia systemów łączności,
$D_{\Psi}^{W_{48}}$ – urządzenia systemów teleinformatycznych,
$D_{\Psi}^{W_{49}}$ – urządzenia systemów ochrony zdrowia,
$D_{\Psi}^{W_{410}}$ – urządzenia systemów finansowych,
$D_{\Psi}^{W_{411}}$ – urządzenia systemów transportowych i komunikacyjnych,
$D_{\Psi}^{W_{412}}$ – urządzenia systemów ratowniczych,
$D_{\Psi}^{W_{413}}$ – urządzenia systemów administracji publicznej,
$D_{\Psi}^{W_{414}}$ – urządzenia systemów substancji niebezpiecznych.

$$D_{\Psi}^{W_5} = \{D_{\Psi}^{W_{5i}}; i = \overline{1,14}\} \tag{4.28}$$

gdzie:

$D_{\Psi}^{W_5}$ – instalacje infrastruktury krytycznej,
$D_{\Psi}^{W_{51}}$ – instalacje systemów zaopatrzenia w energię elektryczną,
$D_{\Psi}^{W_{52}}$ – instalacje systemów zaopatrzenia w energię cieplną,
$D_{\Psi}^{W_{53}}$ – instalacje systemów zaopatrzenia w gaz ziemny,
$D_{\Psi}^{W_{54}}$ – instalacje systemów zaopatrzenia w ropę naftową,
$D_{\Psi}^{W_{55}}$ – instalacje systemów zaopatrzenia w żywność,

$D_{\Psi}^{W_{56}}$ – instalacje systemów zaopatrzenia w wodę,
$D_{\Psi}^{W_{57}}$ – instalacje systemów łączności,
$D_{\Psi}^{W_{58}}$ – instalacje systemów teleinformatycznych,
$D_{\Psi}^{W_{59}}$ – instalacje systemów ochrony zdrowia,
$D_{\Psi}^{W_{510}}$ – instalacje systemów finansowych,
$D_{\Psi}^{W_{511}}$ – instalacje systemów transportowych i komunikacyjnych,
$D_{\Psi}^{W_{512}}$ – instalacje systemów ratowniczych,
$D_{\Psi}^{W_{513}}$ – instalacje systemów administracji publicznej,
$D_{\Psi}^{W_{514}}$ – instalacje systemów substancji niebezpiecznych.

Powyższa klasyfikacja nie wyczerpuje ogromnej złożoności obiektów, urządzeń i instalacji w procesie funkcjonowania i ochrony infrastruktury krytycznej, a jedynie przedstawia najbardziej typowe ich kategorie wymienione zgodnie z definicją infrastruktury krytycznej.

Ze względów organizacyjnych i technicznych wyodrębnione organa kierowania, właściciele, obiekty, urządzenia i instalacje infrastruktury krytycznej działają w określonych strukturach organizacyjno-funkcjonalnych, które można utożsamiać z autonomicznymi systemami infrastruktury krytycznej.

W strukturze podsystemów zarządzania bezpieczeństwem infrastruktury krytycznej wyróżnia się następujące systemy funkcjonalne:

$$\Psi = S_K \cup \begin{Bmatrix} S_{ZEE}, S_{ZEC}, S_{ZGZ}, S_{ZRN}, S_{ZZ}, S_{ZW}, S_L, \\ S_{ST}, S_{OZ}, S_F, S_{TK}, S_R, S_{AP}, S_{SN} \end{Bmatrix} \tag{4.29}$$

gdzie:
Ψ – system zarządzania bezpieczeństwem infrastruktury krytycznej,
S_K – system kierowania bezpieczeństwem infrastruktury krytycznej,
S_{ZEE} – systemy zaopatrzenia w energię elektryczną,
S_{ZEC} – systemy zaopatrzenia w energię cieplną,
S_{ZGZ} – systemy zaopatrzenia w gaz ziemny,
S_{ZRN} – systemy zaopatrzenia w ropę naftową,
S_{ZZ} – systemy zaopatrzenia w żywność,
S_{ZW} – systemy zaopatrzenia w wodę,
S_L – systemy łączności,
S_{ST} – systemy sieci teleinformatycznych,
S_{OZ} – systemy ochrony zdrowia,

S_F – systemy finansowe,
S_{TK} – systemy transportowe i komunikacyjne,
S_R – systemy ratownicze,
S_{AP} – systemy administracji publicznej,
S_{SN} – systemy substancji niebezpiecznych.

Jednym z podstawowych determinant systemu zarządzania bezpieczeństwem infrastruktury krytycznej jest zbiór relacji $\boldsymbol{R}$ określający powiązania i zależności między obiektami, instalacjami, urządzeniami i usługami infrastruktury krytycznej. Wielka złożoność systemu zarządzania bezpieczeństwem infrastruktury krytycznej Ψ i bardzo obszerny zakres dziedziny $\boldsymbol{D_\Psi}$ powodują, że zbiór relacji i powiązań występujących między jego elementami jest złożony i skomplikowany.

Zbiór relacji $\boldsymbol{R}$ występujących w systemie zarządzania bezpieczeństwem infrastruktury krytycznej można zdefiniować, jako:

$$R_\Psi = \begin{Bmatrix} E_\Psi \times E_\Psi = \{< E_\Psi^{ij}, E_\Psi^{ij} > I \times J\} \\ D_\Psi \times D_\Psi = \{< D_\Psi^{ij}, D_\Psi^{ij} > I \times J\} \end{Bmatrix} \tag{4.30}$$

gdzie:

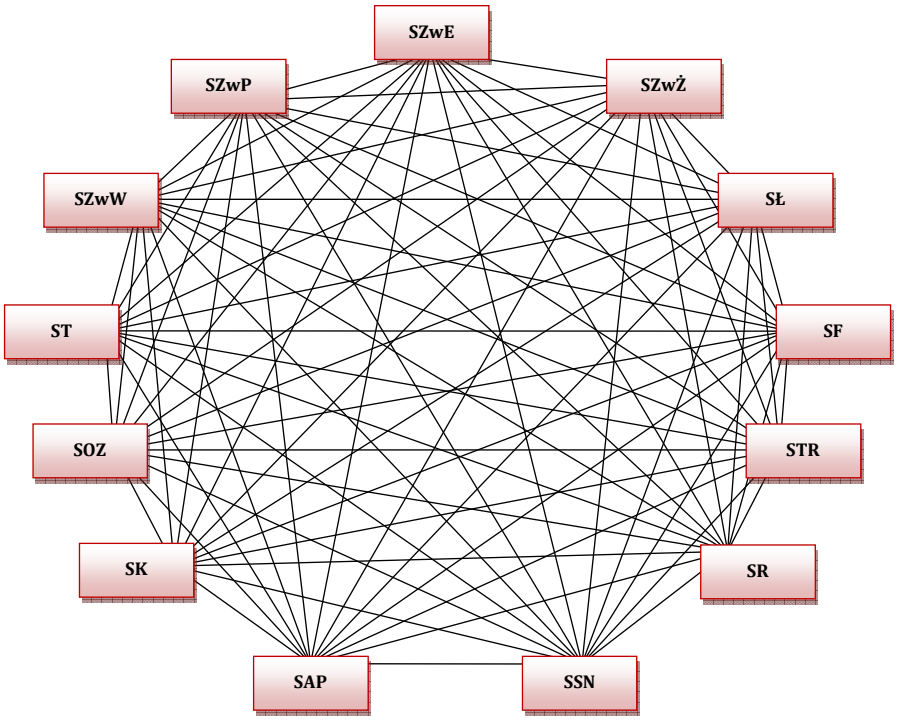
R_Ψ – zbiór relacji w systemie zarządzania bezpieczeństwem infrastruktury krytycznej,
E_Ψ – zbiór elementów struktury organizacyjno-funkcjonalnej systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
D_Ψ – zbiór elementów dziedziny systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

Relacje występujące w systemie zarządzania bezpieczeństwem infrastruktury krytycznej można podzielić na dwie grupy:

$$\mathrm{R}_\Psi = \{R_S, R_I\} \tag{4.31}$$

gdzie:

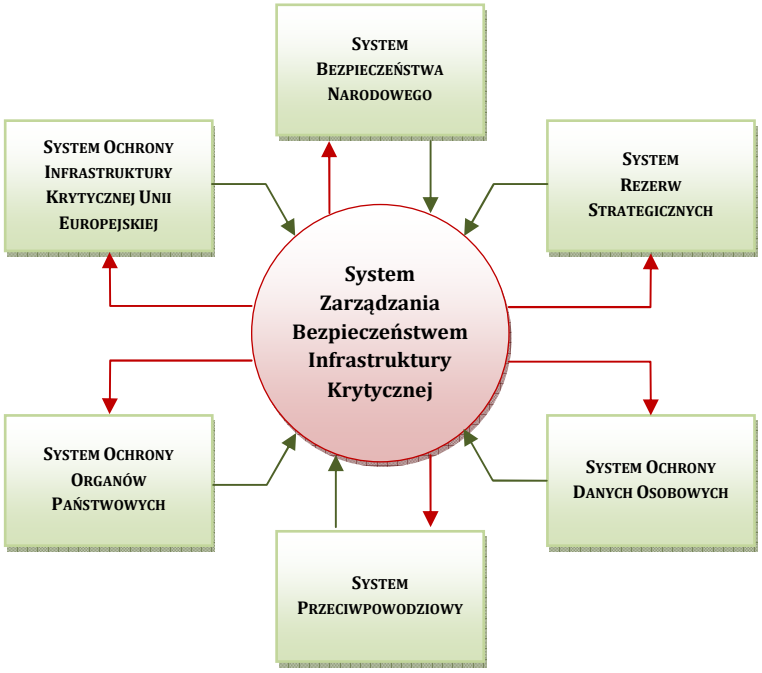
R_S – zbiór relacji systemowych obejmujących zależności wewnętrzne i zewnętrzne,
R_I – zbiór relacji zarządzania bezpieczeństwem infrastruktury krytycznej.



Rys. 4.1. Zbiór relacji wewnętrznych w systemie zarządzania bezpieczeństwem infrastruktury krytycznej

Powyższy rysunek przedstawia relacje występujące między systemami infrastruktury krytycznej:

- SZwE - systemy zaopatrzenia w energię,
- SZwP - systemy zaopatrzenia w paliwa,
- SZwŻ - systemy zapatrzenia w żywność,
- SZwW - systemy zaopatrzenia w wodę,
- SŁ - systemy łączności,
- ST - systemy teleinformatyczne,
- SF - systemy finansowe,
- SOZ - systemy ochrony zdrowia,
- STR - systemy transportowe,
- SK - systemy komunikacji,
- SR - systemy ratownictwa,
- SAP - systemy ciągłości działania administracji publicznej,
- SSN - systemy substancji niebezpiecznych.



Rys. 4.2. Przykładowe relacje systemu zarządzania bezpieczeństwem infrastruktury krytycznej z otoczeniem

Do najbliższego otoczenia zewnętrznego systemu zarządzania bezpieczeństwem infrastruktury krytycznej należą:

- system ochrony infrastruktury krytycznej Unii Europejskiej,
- system ochrony infrastruktury krytycznej państw sąsiadujących,
- system bezpieczeństwa narodowego,
- system rezerw strategicznych,
- system ochrony granicy państwowej,
- system przeciwpowodziowy,
- system ochrony danych osobowych i informacji niejawnych.

4.3. MODEL DECYZYJNY SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFRASTRUKTURY KRYTYCZNEJ

Głównym celem modelowania decyzyjnego MD_Ψ jest podniesienie efektywności działania systemu zarządzania bezpieczeństwem infrastruktury krytycznej, poprzez wskazanie optymalnego wariantu jego funkcjonowania wynikającego z ekstremalizacji przyjętej funkcji kryterium (4.4). Docelowym, praktycznym elementem budowy modelu systemu zarządzania bezpieczeństwem infrastruktury krytycznej jest generowanie scenariuszy działania, pozwalających na czasoprzestrzenną transformacje statycznych zasobów w dynamiczne procesy ochrony infrastruktury krytycznej.

Model decyzyjny systemu zarządzania bezpieczeństwem infrastruktury krytycznej MD_Ψ formalnie zostanie zdefiniowany za pomocą wyrażenia:

$$MD_\Psi = \langle Z_\Psi \rightarrow P_\Psi | O_\Psi, F_\Psi, S_\Psi \rangle \tag{4.32}$$

gdzie:

Z_Ψ – zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
P_Ψ – procesy ochrony infrastruktury krytycznej,
O_Ψ – zbiór ograniczeń ochrony infrastruktury krytycznej,
F_Ψ – funkcja kryterium systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
S_Ψ – scenariusze ochrony infrastruktury krytycznej.

Zasoby operacyjne Z_Ψ systemu zarządzania bezpieczeństwem infrastruktury krytycznej odnoszą się do zasadniczych kategorii materialnych i niematerialnych wykorzystywanych przez system Ψ. Stanowią one rodzaj mediów operacyjnych, które są istotą procesów ochrony infrastruktury krytycznej w dynamice działań operacyjnych. Formalnie zasoby operacyjne Z_Ψ są dzielone na następujące kategorie:

$$Z_\Psi = \{Z_\Psi^M, Z_\Psi^N\} \tag{4.33}$$

gdzie:

Z_Ψ – zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,

Z_{Ψ}^{M} – materialne zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
Z_{Ψ}^{N} – niematerialne zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

Zasoby materialne dotyczą wszelkich materiałów, środków i elementów będących przedmiotem zapotrzebowania materiałowego sił biorących udział w procesie ochrony infrastruktury krytycznej. Należą do nich materiały zaopatrzeniowe, medyczne, techniczne, eksploatacyjne, specjalistyczny sprzęt techniczno-ratunkowy oraz różne urządzenia i systemy techniczne służące do neutralizacji i ograniczania zagrożeń.

$$Z_{\Psi}^{M} = \{Z_{\Psi}^{M1}, Z_{\Psi}^{M2}, Z_{\Psi}^{M3}, Z_{\Psi}^{M4}, Z_{\Psi}^{M5}, \} \tag{4.34}$$

gdzie:
Z_{Ψ}^{M} – materialne zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
Z_{Ψ}^{M1} – zasoby zaopatrzeniowe,
Z_{Ψ}^{M2} – zasoby medyczne,
Z_{Ψ}^{M3} – zasoby techniczne,
Z_{Ψ}^{M4} – zasoby eksploatacyjne,
Z_{Ψ}^{M5} – zasoby ratownicze.

Zasoby niematerialne obejmują przede wszystkim kadry i specjalistyczny personel, ich wiedzę, doświadczenie i umiejętności, a także zasadnicze elementy infrastruktury społecznej systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

$$Z_{\Psi}^{N} = \{Z_{\Psi}^{N1}, Z_{\Psi}^{N2}, Z_{\Psi}^{N3}, Z_{\Psi}^{N4}, Z_{\Psi}^{N5}, \} \tag{4.35}$$

gdzie:
Z_{Ψ}^{N} – niematerialne zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,
Z_{Ψ}^{N1} – zasoby osobowe,
Z_{Ψ}^{N2} – zasoby eksperckie,
Z_{Ψ}^{N3} – zasoby informacyjne,
Z_{Ψ}^{N4} – infrastruktura społeczna.

Skuteczna ochrona infrastruktury krytycznej wymaga efektywnego wykorzystania zarówno zasobów materialnych jak i niematerialnych do zapobiegania sytuacjom kryzysowym, przygotowania się na niekorzystne zdarzenia, reagowania podczas zniszczenia lub zakłócenia pracy infrastruktury krytycznej, a także podczas przywracania zasobów infrastruktury krytycznej do działania.

Wszystkie te działania prowadzą do osiągnięcia gotowości przez system zarządzania bezpieczeństwem infrastruktury krytycznej i uruchamiają procesy operacyjne ochrony kluczowych elementów dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej:

$$Z_{\Psi}^{M} \times Z_{\Psi}^{N} \rightarrow P_{\Psi} \tag{4.36}$$

gdzie:

Z_{Ψ}^{M} – materialne zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,

Z_{Ψ}^{N} – niematerialne zasoby operacyjne systemu zarządzania bezpieczeństwem infrastruktury krytycznej,

P_{Ψ} – procesy ochrony infrastruktury krytycznej.

Zbiór procesów gwarantujących realizację zadań z zakresu ochrony infrastruktury krytycznej można ogólnie podzielić na cztery kategorie:

$$P_{\Psi} \subset \{P_{\Psi}^{Z}, P_{\Psi}^{P}, P_{\Psi}^{R}, P_{\Psi}^{O}\} \tag{4.37}$$

gdzie:

P_{Ψ} – procesy ochrony infrastruktury krytycznej,

P_{Ψ}^{Z} – procesy zapobiegania zakłóceniom infrastruktury krytycznej,

P_{Ψ}^{P} – procesy przygotowania infrastruktury krytycznej na sytuacje kryzysowe,

P_{Ψ}^{R} – procesy reagowania na sytuacje kryzysowe,

P_{Ψ}^{O} – procesu odbudowy infrastruktury krytycznej.

Realizacja procesów ochrony infrastruktury krytycznej wymaga spełnienia szeregu warunków koniecznych i dostatecznych, mających swoje odniesienie, zarówno do otoczenia wewnętrznego, jak też zewnętrznego systemu zarządzania bezpieczeństwem infrastruktury

krytycznej. Zbiór ograniczeń i warunków systemowych można podzielić na trzy grupy, obejmujące odpowiednio:

$$O_\Psi \subset \{O_\Psi^S, O_\Psi^Z, O_\Psi^W\} \tag{4.38}$$

gdzie:

O_Ψ – zbiór ograniczeń ochrony infrastruktury krytycznej,
O_Ψ^S – zbiór ograniczeń systemowych,
O_Ψ^Z – zbiór ograniczeń generowanych przez otoczenie zewnętrzne systemu,
O_Ψ^W – zbiór ograniczeń generowanych przez otoczenie wewnętrzne systemu.

Do ograniczeń systemowych należy zaliczyć deficyt czasu, danych i informacji, zasobów operacyjnych. Stanowią one istotne, systemowe ograniczenia w procesie optymalizacji systemu zarządzania bezpieczeństwem infrastruktury krytycznej.

Grupa ograniczeń zewnętrznych definiuje przede wszystkim czasoprzestrzeń operacyjną zarządzania bezpieczeństwem infrastruktury krytycznej, na którą składają się oprócz klasycznych elementów, takich jak czas i miejsce, również inne elementy typu: czas i moment wystąpienia zdarzenia kryzysowego, aktualne warunki klimatyczno-meteorologiczne, trend rozwojowy sytuacji kryzysowej, prognozowany czas zwalczania sytuacji kryzysowej, rozległość przestrzenna miejsca zdarzenia, dostępność komunikacyjna i transportowa miejsca zdarzenia, warunki do ewakuacji i prowadzenia akcji ratowniczych, możliwość wykorzystania zasobów miejscowych, prognozowane skutki i konsekwencje.

Ograniczenia wewnętrzne wynikają przede wszystkim z możliwości wykonawczych systemu zarządzania bezpieczeństwem infrastruktury krytycznej w stosunku do rzeczywistych potrzeb ochrony infrastruktury krytycznej w odniesieniu do zidentyfikowanych potrzeb.

Funkcja kryterium systemu zarządzania bezpieczeństwem infrastruktury krytycznej stanowi rodzaj pewnego miernika, z reguły mającego postać analityczną, przy pomocy, którego ocenia się funkcjonowanie danego systemu. W przypadku prakseologicznych systemów działania, jakim jest m.in. rozpatrywany system zarządzania bezpieczeństwem infrastruktury krytycznej, zasadniczym parametrem

jego funkcjonalności jest kryterium skuteczności, niezawodności i bezpieczeństwa działania w odniesieniu do zidentyfikowanych zagrożeń.

W zakres pojęcia funkcjonalności (F_Ψ) systemu zarządzania bezpieczeństwem infrastruktury krytycznej zaliczane są następujące elementy:

$$F_\Psi \subset \left\{F_\Psi^1, F_\Psi^2, F_\Psi^3 \middle| O_\Psi^S \cup O_\Psi^Z \cup O_\Psi^W\right\} \tag{4.39}$$

gdzie:

F_Ψ – funkcjonalność systemu zarządzania bezpieczeństwem ochrony infrastruktury krytycznej,
F_Ψ^1 – skuteczność działania,
F_Ψ^2 – niezawodność działania,
F_Ψ^3 – bezpieczeństwo działania,
O_Ψ^S – ograniczenia systemowe,
O_Ψ^Z – ograniczenia zewnętrzne,
O_Ψ^W – ograniczenia wewnętrzne.

Głównym celem modelowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej jest przygotowanie takich procedur działania, które pozwolą optymalnie kierowanie tym systemem, w sensie przyjętego wskaźnika jakości – funkcji kryterium.

W ujęciu praktycznym optymalne decyzje polegają na wyznaczeniu szczegółowych planów i procedur ochrony infrastruktury krytycznej w odniesieniu do zidentyfikowanych zagrożeń, przy spełnieniu rzeczywistych ograniczeń systemowych i bieżących warunków brzegowych.

W wyniku prognozowania stanu zagrożeń i oceny stopnia bezpieczeństwa systemowego, w oparciu o ustaloną funkcję kryterium i szerokie spektrum różnych uwarunkowań i ograniczeń, podejmowane są decyzje do działań operacyjnych. Fizycznym obrazem tych decyzji będą np. szczegółowe plany ochrony infrastruktury krytycznej, a ich nośnikiem informacyjnym są tzw. scenariusze ochrony infrastruktury krytycznej.

* * *

Proces modelowania systemu zarządzania bezpieczeństwem infrastruktury krytycznej został zdekomponowany na dwa etapy konceptualne dotyczące odpowiednio budowy modelu indentyfikacyjnego i na jego bazie modelu optymalizacyjnego (decyzyjnego). Przedstawiono również ogólne podejście do formalnego modelowania prakseologicznego systemu działania, jakim jest system zarządzania bezpieczeństwem infrastruktury krytycznej państwa.

Na początku zdefiniowano zadania i strukturę modelu identyfikacyjnego, który zgodnie z ogólną teorią systemów został opisany przy pomocy uporządkowanej trójki obejmującej: cel działania i podstawowe funkcje, składowe elementy struktury organizacyjnej oraz topologiczne relacje i różnorodne powiązania między tymi elementami. Tak przedstawiony model identyfikacyjny determinuje strukturę funkcjonalno-organizacyjną systemu zarządzania bezpieczeństwem infrastruktury krytycznej, która w ujęciu prakseologicznym składa się z następujących roboczych systemów zarządzania bezpieczeństwem:

- zaopatrzenia w energię,
- zaopatrzenia w paliwa,
- zapatrzenia w żywność,
- zaopatrzenia w wodę,
- łączności,
- sieci teleinformatycznych,
- systemów finansowych,
- ochrony zdrowia,
- transportu,
- komunikacji,
- ratownictwa,
- ciągłości działania administracji publicznej,
- systemów substancji niebezpiecznych[196].

Wyodrębnione elementy składowe systemu zarządzania bezpieczeństwem infrastruktury krytycznej zostały przedstawione

[196] Pod pojęciem systemów substancji niebezpiecznych ujęto systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

w jednolitej konwencji za pomocą aparatu analizy i topologii matematycznej.

Budując model decyzyjny starano się ustalić zbiór ograniczeń oraz funkcję kryterium, determinującą proces zarządzania bezpieczeństwem infrastruktury krytycznej. Modelowanie decyzyjne ujmuje system zarządzania bezpieczeństwem infrastruktury krytycznej w dynamice działań, jako ciąg kolejno podejmowanych decyzji, sterujących procesem zarządzania bezpieczeństwem infrastruktury krytycznej.

Sposób zarządzania bezpieczeństwem infrastruktury krytycznej powinien być optymalny ze względu na przyjęte kryterium oceny jego efektywności, którym jest postulat minimalizacji zagrożeń oraz maksymalizacji standardu bezpieczeństwa infrastruktury krytycznej. Poszukiwanie optymalnych strategii prowadzących do realizacji tego kryterium jest głównym zadaniem zaproponowanego powyżej procesu modelowania opartego na metodyce K. Ficonia[197].

[197] K. Ficoń, *Badania operacyjne stosowane. Modele i aplikacji*, BEL Studio, Warszawa 2006.

ROZDZIAŁ 5
MODEL KONCEPTUALNY SYSTEMU OCENY BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ

Ostatnim zadaniem procedury badawczej jest opracowanie modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej. Model ten został zbudowany w oparciu o taksonomiczną formułę potencjałową wykorzystaną do oceny poziomu przygotowania zasobów infrastruktury krytycznej do sytuacji kryzysowych. Formuła ta z powodzeniem była stosowana do oceny potencjału złożonych systemów broni[198], potencjału morskiego państwa[199] oraz poziomu zagrożeń w aglomeracjach miejskich[200].

5.1. OGÓLNA KONCEPCJA TAKSONOMICZNEJ FORMUŁY POTENCJAŁOWEJ

Taksonomia definiowana jest, jako nauka o zasadach porządkowania i podziału na grupy jednostek różnych zbiorowości. Jej metody i narzędzia badawcze są stosowane do pomiarów zjawisk (systemów) złożonych, których nie można wyrazić ani opisać za pomocą jednej zmiennej. Dzięki oryginalnym narzędziom i efektywnym procedurom badawczym, metody taksonomiczne mogą być wykorzystane do badania dowolnie złożonych zjawisk (systemów)

[198] K. Ficoń, *Badania operacyjne stosowane. Modele i aplikacje*, BEL Studio, Warszawa 2006, s. 276.
[199] K. Ficoń, T. Szubrycht, G. Krasnodebski, *Wykorzystanie metod taksonomicznych do określenia potencjału morskiego państwa*, [w:] *Gry i symulacje jako przedmiot i metoda badań w naukach społecznych*, Collegium Civitas, Warszawa 2009.
[200] G. Krasnodebski, *Wykorzystanie taksonomicznej formuły potencjałowej do oceny poziomu zagrożeń w aglomeracjach miejskich*, [w:] *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, Wyd. WSAiB, Gdynia 2011.

zarówno jakościowych, jak też ilościowych[201]. Zasadniczą zaletą badań taksonomicznych i stosowanych tam metod i narzędzi jest:

- możliwość wymiernego oceniania (porządkowania) zjawisk, procesów, systemów dowolnie złożonych,
- wykorzystanie w procesie badawczym najbardziej charakterystycznych zbiorów cech i parametrów opisowych,
- klasyfikowanie ocenianych zjawisk, obiektów czy systemów na podstawie wymiernych, ilościowych wskaźników oceny.

Metody taksonomiczne należą do grupy metod numerycznych, bazujących na statystycznej analizie porównawczej. Zasadniczo służą one do rozwiązywania problemów porównywalności oraz porządkowania danej zbiorowości, ze względu na poziom przyjętego miernika, będącego syntezą wielocechowego kryterium jakości. Pozwalają klasyfikować (porządkować, grupować) obiekty w wielowymiarowej przestrzeni ich charakterystyk (cech). Głównym celem badania taksonomicznego jest porządkowanie zbioru obiektów ze względu na poziom wielocechowego zjawiska (wskaźnika).

Podstawowym pojęciem taksonomii jest pojęcie obiektu (Q), będącego przedmiotem badań klasyfikacyjnych i zbioru cech (X) określających specyficzne właściwości rozpatrywanych obiektów. Najważniejsze są cechy ocenianych obiektów, które są istotne w świetle analizowanego zjawiska złożonego. Obiektami są badane jednostki (zjawiska, procesy, systemy) podlegające klasyfikacji.

$$Q = \{Q_k \; ; k = \overline{1, K}\} \tag{5.1}$$

gdzie:

$Q_k \in Q$ – zbiór badanych obiektów,
K – liczność zbioru obiektów Q.

Przedmiotem klasyfikacji jest zbiór wyodrębnionych obiektów {Q} ze względu na przedmiot (kryterium) badań. Pojęcie obiektu może obejmować dowolne elementy (zbiory) typologiczne, będące przedmiotem badań. Obiektami mogą być zarówno elementy proste (jednorodne), jak również złożone systemy społeczne czy zjawiska naturalne. Szczególnym przykładem zbiorowości badań

[201] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, BEL Studio, Warszawa 2007, s. 120.

taksonomicznych może być zbiór zagrożeń opisany za pomocą pewnych charakterystyk (cech), odzwierciedlających najbardziej istotne właściwości tych zagrożeń z punktu widzenia pożądanych standardów bezpieczeństwa.

Cechami są właściwości obiektów (jednostek) badanego zbioru Q, wyodrębnione specjalnie ze względu na przyjęte kryterium klasyfikacji obiektów. Zbiór cech przyjętych do opisu klasyfikowanych obiektów Q jest oznaczany symbolem X:

$$X = \{X_i \ ; i = \overline{1, I}\} \tag{5.2}$$

gdzie:

$X_i \in X$ – zbiór cech opisujących badane obiekty,
I – liczność zbioru cech.

W zależności od rodzaju i klasy rozpatrywanego obiektu (zjawiska, systemu) należy zdefiniować odpowiedni zbiór cech (zmiennych) opisujących właściwości tych obiektów z punktu widzenia potrzeb badawczych. Wyodrębnione dla potrzeb procesu badawczego cechy, odzwierciedlające istotne właściwości obiektów nazywane są cechami diagnostycznymi. Liczbowe reprezentacje cech diagnostycznych służą do wyznaczania analitycznej miary podobieństwa badanych obiektów w sensie przyjętego kryterium jakości.

Metody taksonomiczne służą do rozwiązywania problemów relatywizacji i porównywalności oraz porządkowania określonej zbiorowości ze względu na poziom przyjętego miernika, będącego syntezą wielocechowego kryterium jakości. W procedurze badania taksonomicznego wyróżnia się następujące zasadnicze etapy[202]:

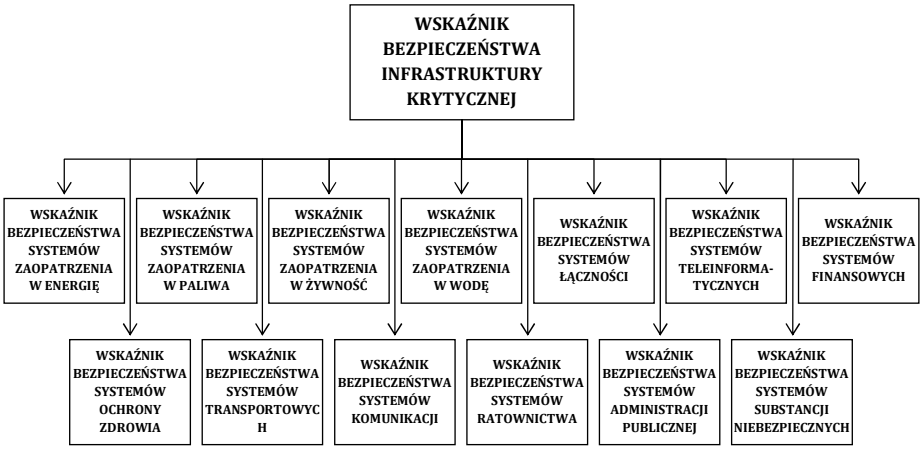
- wstępną analizę badanego problemu,
- dobór cech diagnostycznych i skal ich pomiaru,
- zgromadzenie danych statystycznych,
- wybór metody klasyfikacji,
- klasyfikacja badanych obiektów,
- weryfikacja i interpretacja wyników,
- interpretacja wyników.

[202] A. Becla, A. Zielińska, *Elementy statystyki i metod ilościowych*, I-Bis, Wrocław 2003, s. 141.

Przedstawiona powyżej koncepcja badań taksonomicznych jest podstawą do budowy modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej.

5.2. MODEL SYSTEMU OCENY BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ

Zastosowanie przedstawionej powyżej procedury badawczej pozwoliło stworzyć model systemu oceny poziomu przygotowania zasobów infrastruktury krytycznej do sytuacji kryzysowych. Podstawą budowy modelu była przyjęta na potrzeby badań klasyfikacja sektorowa infrastruktury krytycznej, zdefiniowana w *Ustawie o zarządzaniu kryzysowym z 26 kwietnia 2007 r.,* informacje branżowe oraz informacje dostępne na stronach *U.S. Department of Homeland Security.*



Rys. 5.1. Struktura oceny bezpieczeństwa infrastruktury krytycznej[203]

Ogólnie infrastruktura krytyczna została podzielone na następujące systemy:

- zaopatrzenia w energię,
- zaopatrzenia w paliwa,
- zapatrzenia w żywność,
- zaopatrzenia w wodę,

[203] Struktury oceny wskaźników składowych wskaźnika bezpieczeństwa infrastruktury krytycznej zamieszczone zostały w załączniku nr 1.

- łączności,
- teleinformatyczne,
- finansowe,
- ochrony zdrowia,
- transportowe,
- komunikacji,
- ratownictwa,
- ciągłości działania administracji publicznej,
- substancji niebezpiecznych.

5.3. WSKAŹNIK BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ

Bezpieczeństwo infrastruktury krytycznej wyznaczane jest na podstawie wskaźników bezpieczeństwa poszczególnych sektorów infrastruktury krytycznej zgodnie z regułą:

$$B_{IK} = f\begin{pmatrix} W_{SE}, W_{SP}, W_{SZ}, W_{SW}, W_{SL}, W_{ST}, W_{SF}, \\ W_{SOZ}, W_{ST}, W_{SK}, W_{SR}, W_{SAP}, W_{SSN} \end{pmatrix} \tag{5.3}$$

gdzie:

B_{IK} – wskaźnik bezpieczeństwa infrastruktury krytycznej,
W_{SE} – wskaźnik bezpieczeństwa zaopatrzenia w energię,
W_{SP} – wskaźnik bezpieczeństwa zaopatrzenia w paliwa,
W_{SZ} – wskaźnik bezpieczeństwa zapatrzenia w żywność,
W_{SW} – wskaźnik bezpieczeństwa zaopatrzenia w wodę,
W_{SL} – wskaźnik bezpieczeństwa systemów łączności,
W_{ST} – wskaźnik bezpieczeństwa systemów teleinformatycznych,
W_{SF} – wskaźnik bezpieczeństwa systemów finansowych,
W_{SOZ} – wskaźnik bezpieczeństwa ochrony zdrowia,
W_{ST} – wskaźnik bezpieczeństwa systemów transportowych,
W_{SK} – wskaźnik bezpieczeństwa systemów komunikacji,
W_{SR} – wskaźnik bezpieczeństwa ratownictwa,
W_{SAP} – wskaźnik bezpieczeństwa administracji publicznej,
W_{SSN} – wskaźnik bezpieczeństwa systemów substancji niebezpiecznych.

5.4. WSKAŹNIK BEZPIECZEŃSTWA ZAOPATRZENIA W ENERGIĘ

Sektor energii elektrycznej obejmuje wytwarzanie, przesyłanie oraz dystrybucję energii elektrycznej. Ze względu na duże uzależnienie funkcjonowania pozostałych systemów infrastruktury krytycznej od energii elektrycznej, sektor ten pełnią kluczową rolę w całym systemie i stanowi jego czuły punkt[204].

W sektorze energii elektrycznej wyróżniamy następujące elementy:

- systemy wytwarzania (elektrownie konwencjonalne, elektrownie jądrowe, elektrownie wodne, elektrownie słoneczne, elektrownie wiatrowe),
- systemy przesyłania (stacje energetyczne, linie przesyłowe, centra kontroli),
- systemy dystrybucji (stacje energetyczne, linie przesyłowe, centra kontroli).

Wskaźnik bezpieczeństwa systemów zaopatrzenia w energię będzie wyznaczany na podstawie wartości trzech wskaźników składowych:

$$W_{SE} = f\left(W_{SE_1}, W_{SE_2}, W_{SE_3}\right) \tag{5.4}$$

gdzie:

W_{SE} – wskaźnik bezpieczeństwa systemów zaopatrzenia w energię,
W_{SE_1} – wskaźnik bezpieczeństwa systemów wytwarzania energii elektrycznej,
W_{SE_2} – wskaźnik bezpieczeństwa systemów przesyłania energii elektrycznej,
W_{SE_3} – wskaźnik bezpieczeństwa systemów dystrybucji energii elektrycznej.

[204] Homeland Security, *Energy Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf).

Wskaźnik bezpieczeństwa systemów wytwarzania energii elektrycznej będzie odzwierciedlał stopień przygotowania pięciu typów elektrowni na sytuacje kryzysowe. Wyznaczany będzie jak następująca funkcja:

$$W_{SE_1} = f\left(W_{SE_{11}}, W_{SE_{12}}, W_{SE_{13}},, W_{SE_{14}},, W_{SE_{15}}\right) \tag{5.5}$$

gdzie:

W_{SE_1} – wskaźnik bezpieczeństwa systemów wytwarzania energii elektrycznej,
$W_{SE_{11}}$ – wskaźnik bezpieczeństwa elektrowni konwencjonalnych,
$W_{SE_{12}}$ – wskaźnik bezpieczeństwa elektrowni jądrowych,
$W_{SE_{13}}$ – wskaźnik bezpieczeństwa elektrowni wodnych,
$W_{SE_{14}}$ – wskaźnik bezpieczeństwa elektrowni słonecznych,
$W_{SE_{15}}$ – wskaźnik bezpieczeństwa elektrowni wiatrowych.

Odporność na zniszczenia oraz zakłócenia pracy systemów przesyłania energii elektrycznej będzie wyrażana przy pomocy następującego wskaźnika:

$$W_{SE_2} = f\left(W_{SE_{21}}, W_{SE_{22}}, W_{SE_{23}}\right) \tag{5.6}$$

gdzie:

W_{SE_2} – wskaźnik bezpieczeństwa systemów przesyłania energii elektrycznej,
$W_{SE_{21}}$ – wskaźnik bezpieczeństwa stacji energetycznych w systemie przesyłania energii elektrycznej,
$W_{SE_{22}}$ – wskaźnik bezpieczeństwa linii przesyłowych w systemie przesyłania energii elektrycznej,
$W_{SE_{23}}$ – wskaźnik bezpieczeństwa centrów kontroli w systemie przesyłania energii elektrycznej.

Ostatnim wskaźnikiem składowym oceny bezpieczeństwa sektora energetycznego jest wskaźnik bezpieczeństwa systemów dystrybucji energii elektrycznej. Wyznaczany on będzie zgodnie z regułą:

$$W_{SE_3} = f\left(W_{SE_{31}}, W_{SE_{32}}, W_{SE_{33}}\right) \tag{5.7}$$

gdzie:

W_{SE_2} – wskaźnik bezpieczeństwa systemów dystrybucji energii elektrycznej,

$W_{SE_{31}}$ – wskaźnik bezpieczeństwa stacji energetycznych w systemie dystrybucji energii elektrycznej,

$W_{SE_{32}}$ – wskaźnik bezpieczeństwa linii przesyłowych w systemie dystrybucji energii elektrycznej,

$W_{SE_{33}}$ – wskaźnik bezpieczeństwa centrów kontroli w systemie dystrybucji energii elektrycznej.

5.5. WSKAŹNIK BEZPIECZEŃSTWA ZAOPATRZENIA W PALIWA

Sektor zaopatrzenia w paliwa obejmuje wydobycie, przetwarzanie, przesyłanie, składowanie oraz dystrybucję ropy naftowej i gazu ziemnego. Sektor paliwowy podobnie jak energetyczny należy do grupy sektorów strategicznych, wobec czego pełni on rolę pierwszoplanową w procesie zarządzania bezpieczeństwem infrastruktury krytycznej[205]. Zaliczamy do niego następujące elementy:

- system zaopatrzenia w ropę naftową,
- system zaopatrzenia w gaz ziemny.

Do systemu zaopatrzenia w ropę naftową należą:

- instalacje wydobywcze na lądzie i w morzu,
- terminale przeładunkowe ropy naftowej i paliw,
- rurociągi przesyłowe ropy naftowej i paliw,
- instalacje składowanie ropy naftowej i paliw,
- instalacje przetwarzania ropy naftowej i paliw,
- instalacje dystrybucji ropy naftowej i paliw.

W skład systemu zaopatrzenia w gaz ziemny wchodzą następujące elementy:

- instalacje wydobywcze na lądzie i w morzu,
- rurociągi przesyłowe gazu ziemnego,

[205] Homeland Security, *Energy Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf), *Dams Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-dams-2010.pdf).

- instalacje składowanie gazu ziemnego,
- instalacje przetwarzania gazu ziemnego,
- instalacje dystrybucji gazu ziemnego.

Wskaźnik bezpieczeństwa systemów zaopatrzenia w paliwa będzie wyznaczany na podstawie wartości dwóch wskaźników składowych określających bezpieczeństwo systemów zaopatrzenia w ropę naftową oraz gaz ziemny:

$$W_{SP} = f\left(W_{SP_1}, W_{SP_2}\right) \tag{5.8}$$

gdzie:

W_{SP} – wskaźnik bezpieczeństwa systemów zaopatrzenia w paliwa,
W_{SP_1} – wskaźnik bezpieczeństwa systemów zaopatrzenia w ropę naftową,
W_{SP_2} – wskaźnik bezpieczeństwa systemów zaopatrzenia w gaz ziemny.

Poziom zabezpieczeń systemów zaopatrzenia w ropę naftową będzie wyrażany za pomocą funkcji:

$$W_{SP_1} = f\left(W_{SP_{11}}, W_{SP_{12}}, W_{SP_{13}}, W_{SP_{14}}, W_{SP_{15}}, W_{SP_{16}}\right) \tag{5.9}$$

gdzie:

W_{SP_1} – wskaźnik bezpieczeństwa systemów zaopatrzenia w ropę naftową,
$W_{SP_{11}}$ – wskaźnik bezpieczeństwa instalacji wydobywczych na lądzie i w morzu,
$W_{SP_{12}}$ – wskaźnik bezpieczeństwa terminali ropy naftowej i paliw,
$W_{SP_{13}}$ – wskaźnik bezpieczeństwa rurociągów przesyłowych ropy naftowej i paliw,
$W_{SP_{14}}$ – wskaźnik bezpieczeństwa instalacji składowania ropy naftowej i paliw,
$W_{SP_{15}}$ – wskaźnik bezpieczeństwa instalacji przetwarzania ropy naftowej i paliw,
$W_{SP_{16}}$ – wskaźnik bezpieczeństwa instalacji dystrybucji ropy naftowej i paliw.

Bezpieczeństwo systemów zaopatrzenia w gaz ziemny będzie wyznaczane w następujący sposób:

$$W_{SP_2} = f\left(W_{SP_{21}}, W_{SP_{22}}, W_{SP_{23}}, W_{SP_{24}}, W_{SP_{25}}\right) \tag{5.10}$$

gdzie:

W_{SP_2} – wskaźnik bezpieczeństwa systemów zaopatrzenia w gaz ziemny,

$W_{SP_{21}}$ – wskaźnik bezpieczeństwa instalacji wydobywczych na lądzie i w morzu,

$W_{SP_{22}}$ – wskaźnik bezpieczeństwa rurociągów przesyłowych gazu ziemnego,

$W_{SP_{23}}$ – wskaźnik bezpieczeństwa instalacji składowania gazu ziemnego,

$W_{SP_{24}}$ – wskaźnik bezpieczeństwa instalacji przetwarzania gazu ziemnego,

$W_{SP_{25}}$ – wskaźnik bezpieczeństwa instalacji dystrybucji gazu ziemnego.

5.6. WSKAŹNIK BEZPIECZEŃSTWA ZAPATRZENIA W ŻYWNOŚĆ

Sektor zaopatrzenia w żywność obejmuje produkcję, przetwarzanie, magazynowanie, transport oraz dystrybucję żywności. Przykładami produktów żywnościowych są zboża, owoce, warzywa, mięso, ryby, nabiał, napoje, wyroby piekarnicze, przetwory rolno-spożywcze. Rozważając problematyką bezpieczeństwa systemów zaopatrzenia w żywność należy bezwzględnie wziąć pod uwagę zamierzone działania człowieka związane z celowym skażeniem żywności czynnikami biologicznymi, chemicznym i radiologicznymi[206].

W sektorze zaopatrzenia w żywność wyróżniamy następujące systemy:

- produkcji żywności,
- przetwarzania żywności,
- magazynowania żywności,
- transportu żywności,
- dystrybucji żywności.

[206] Homeland Security, *Food and Agriculture Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf).

Wskaźnik bezpieczeństwa systemów zaopatrzenia w żywność będzie wyznaczany na podstawie wartości pięciu wskaźników składowych określających bezpieczeństwo systemów zaopatrzenia w żywność:

$$W_{SZ} = f\left(W_{SZ_1}, W_{SZ_2}, W_{SZ_3}, W_{SZ_4}, W_{SZ_5}\right) \tag{5.11}$$

gdzie:

W_{SZ} – wskaźnik bezpieczeństwa systemów zaopatrzenia w żywność,
W_{SZ_1}– wskaźnik bezpieczeństwa systemów produkcji żywności,
W_{SZ_2}– wskaźnik bezpieczeństwa systemów przetwarzania żywności,
W_{SZ_3}– wskaźnik bezpieczeństwa systemów magazynowania żywności,
W_{SZ_4}– wskaźnik bezpieczeństwa systemów transportu żywności,
W_{SZ_5}– wskaźnik bezpieczeństwa systemów dystrybucji żywności.

5.7. WSKAŹNIK BEZPIECZEŃSTWA ZAOPATRZENIA W WODĘ

System zaopatrzenia w wodę obejmuje obiekty, instalacje, urządzenia oraz usługi związane dostarczeniem wody pitnej oraz prowadzeniem gospodarki ściekowej. Zakłócenia pracy tego systemu mogą nieść dotkliwe skutki dla zdrowia ludzi, gospodarcze, psychologiczne a także mieć negatywny wpływ na środowisko naturalne[207].

W skład systemu zaopatrzenia w wodę należą:

- ujęcia wody,
- instalacje poboru wody,
- zbiorniki retencyjne,
- instalacje uzdatniania wody,
- instalacje przechowywania wody,
- instalacje dystrybucji wody,
- instalacje kontroli jakości wody.

System gospodarki ściekowej zawiera:

- instalacje odbioru ścieków,

[207] Homeland Security, *Water Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/ xlibrary/assets/nipp-ssp-water-2010.pdf).

- przepompownie ścieków,
- oczyszczalnie ścieków,
- spusty oczyszczonej wody.

Wskaźnik bezpieczeństwa systemów zaopatrzenia w wodę będzie wyznaczany na podstawie wartości dwóch wskaźników składowych określających bezpieczeństwo systemów zaopatrzenia w wodę oraz bezpieczeństwo systemów gospodarki ściekowej:

$$W_{SW} = f\left(W_{SW_1}, W_{SW_2}\right) \tag{5.12}$$

gdzie:

W_{SW} – wskaźnik bezpieczeństwa systemów zaopatrzenia w wodę,
W_{SW_1} – wskaźnik bezpieczeństwa systemów zaopatrzenia w wodę pitną,
W_{SW_2} – wskaźnik bezpieczeństwa systemów gospodarki ściekowej.

Ocena bezpieczeństwa systemów zaopatrzenia w wodę będzie wyznaczana w następujący sposób:

$$W_{SW_1} = f\left(W_{SW_{11}}, W_{SW_{12}}, W_{SW_{13}}, W_{SW_{14}}, W_{SW_{15}}, W_{SW_{16}}, W_{SW_{17}}\right) \tag{5.13}$$

gdzie:

W_{SW_1} – wskaźnik bezpieczeństwa systemów zaopatrzenia w wodę pitną,
$W_{SW_{11}}$ – wskaźnik bezpieczeństwa ujęć wody,
$W_{SW_{12}}$ – wskaźnik bezpieczeństwa instalacji poboru wody,
$W_{SW_{13}}$ – wskaźnik bezpieczeństwa zbiorników retencyjnych,
$W_{SW_{14}}$ – wskaźnik bezpieczeństwa instalacji uzdatniania wody,
$W_{SW_{15}}$ – wskaźnik bezpieczeństwa instalacji przechowywania wody,
$W_{SW_{16}}$ – wskaźnik bezpieczeństwa instalacji dystrybucji wody,
$W_{SW_{17}}$ – wskaźnik bezpieczeństwa instalacji kontroli jakości wody.

Ocena bezpieczeństwa systemów gospodarki ściekowej wyznaczana będzie zgodnie z regułą:

$$W_{SW_2} = f\left(W_{SW_{21}}, W_{SW_{22}}, W_{SW_{23}}, W_{SW_{24}}\right) \tag{5.14}$$

gdzie:

W_{SW_2} – wskaźnik bezpieczeństwa systemów gospodarki ściekowej,
$W_{SW_{21}}$ – wskaźnik bezpieczeństwa instalacji odbioru ścieków,
$W_{SW_{22}}$ – wskaźnik bezpieczeństwa przepompowni ścieków,
$W_{SW_{23}}$ – wskaźnik bezpieczeństwa oczyszczalni ścieków,
$W_{SW_{24}}$ – wskaźnik bezpieczeństwa spustów oczyszczonej wody.

5.8. WSKAŹNIK BEZPIECZEŃSTWA SYSTEMÓW ŁĄCZNOŚCI

Sektor łączności należy do najszybciej rozwijających się elementów infrastruktury krytycznej razem z sektorem teleinformatycznym. Oba sektory są ze sobą ściśle powiązane ze względu na udostępniane usługi. Należy podkreślić, że rozwój technologii komunikacyjnych spowodował, że pozostałe warstwy infrastruktury krytycznej są uzależnione od łączności. Usługi oferowane lub świadczone przez sektor łączności są kluczowymi składnikami procesów biznesowych i rządowych, mających fundamentalne znaczenie dla naszego codziennego życia. Szczególnie istotne są usługi łączności świadczone na rzecz sektora energii elektrycznej, finansów, systemów ratownictwa i systemów administracji publicznej[208].

Sektor łączności obejmuje następujące podsystemy:

- łączności przewodowej,
- łączności bezprzewodowej,
- łączności satelitarnej,
- łączności radiowej,
- łączności telewizyjnej.

Wskaźnik bezpieczeństwa systemów łączności będzie wyznaczany na podstawie wartości pięciu wskaźników składowych określających bezpieczeństwo systemów łączności:

$$W_{SL} = f\left(W_{SL_1}, W_{SL_2}, W_{SL_3}, W_{SL_4}, W_{SL_5}\right) \tag{5.15}$$

[208] Homeland Security, *Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf).

gdzie:

W_{SL} – wskaźnik bezpieczeństwa systemów łączności,

W_{SL_1} – wskaźnik bezpieczeństwa systemów łączności przewodowej,

W_{SL_2} – wskaźnik bezpieczeństwa systemów łączności bezprzewodowej,

W_{SL_3} – wskaźnik bezpieczeństwa systemów łączności satelitarnej,

W_{SL_4} – wskaźnik bezpieczeństwa systemów łączności radiowej,

W_{SL_5} – wskaźnik bezpieczeństwa systemów łączności telewizyjnej.

5.9. WSKAŹNIK BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH

Rozwój nowoczesnych technologii sprawił, że sektor technologii informacyjnych i komunikacyjnych stał się ważnym obszarem działalności gospodarczej i społecznej. Działalność człowieka jest w dużym stopniu uzależniona od elementów krytycznej infrastruktury teleinformatycznej.

Zarządzanie elementami krytycznej infrastruktury teleinformatycznej jest dość problematyczne w gospodarce rynkowej i wymaga współpracy publiczno-państwowej. Wynika to głównie z tego, że większość tych elementów należy do prywatnych właścicieli.

Sektor teleinformatyczny infrastruktury krytycznej obejmuje głównie sieci i systemy teleinformatyczne. W jego skład również wchodzi dostarczenia produktów technologii informacyjnych oraz świadczenie usług serwisowych, tworzenie oprzyrządowania do wykrywania zagrożeń w sieciach komputerowych i radzenia sobie z incydentami zagrażającymi bezpieczeństwu narodowemu, usługi zarządzanie domenami, serwisy identyfikacji i autentykacji, sieciowe usługi komunikacyjne oraz infrastruktura zapewniająca funkcjonowanie Internetu.

Sektor teleinformatyczny obejmuje następujące elementy:

- dostawcy sprzętu IT,
- dostawcy oprogramowania,
- dostawcy Internetu,
- dostawcy usług internetowych,

- dostawcy usług sieci szkieletowych,
- dostawcy bezpiecznych usług sieciowych,
- instytucje bezpieczeństwa sieciowego.

Wskaźnik bezpieczeństwa systemów teleinformatycznych będzie wyznaczany na podstawie wartości siedmiu wskaźników składowych określających bezpieczeństwo systemów i sieci teleinformatycznych:

$$W_{ST} = f\left(W_{ST_1}, W_{ST_2}, W_{ST_3}, W_{ST_4}, W_{ST_5}, W_{ST_6}, W_{ST_7}\right) \tag{5.16}$$

gdzie:

W_{ST} – wskaźnik bezpieczeństwa systemów teleinformatycznych,
W_{ST_1} – wskaźnik bezpieczeństwa dostawców sprzętu IT,
W_{ST_2} – wskaźnik bezpieczeństwa dostawców oprogramowania,
W_{ST_3} – wskaźnik bezpieczeństwa dostawców Internetu,
W_{ST_4} – wskaźnik bezpieczeństwa dostawców usług internetowych,
W_{ST_5} – wskaźnik bezpieczeństwa dostawców usług komputerowych sieci szkieletowych,
W_{ST_6} – wskaźnik bezpieczeństwa dostawców bezpiecznych usług sieciowych,
W_{ST_7} – wskaźnik bezpieczeństwa instytucji bezpieczeństwa sieciowego.

5.10. WSKAŹNIK BEZPIECZEŃSTWA SYSTEMÓW FINANSOWYCH

System finansowy to złożony mechanizm systemu ekonomicznego odpowiedzialny za współtworzenie siły nabywczej oraz świadczenie usług pozwalających na jej krążenie w gospodarce[209]. Jego elementami są:

- rynkowy system finansowy,
- publiczny system finansowy.

Rynkowy system finansowy obejmuje:

- instytucje finansowe,
- rynki finansowe,

[209] B. Pietrzak, Z. Polański, B. Woźniak, *System finansowy w Polsce*, Wydawnictwo Naukowe PWN, Warszawa 2003. Homeland Security, Banking and Finance Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, Washington 2010 (http://www.dhs.gov/sites/default/files/publications/nipp-ssp-banking-and-finance-2010.pdf).

- infrastrukturę systemu,
- regulacje i zasady określające sposób ich funkcjonowania.

Publiczny system finansowy składa się z:

- instytucji budżetowych,
- instrumentów fiskalnych,
- publicznych instrumentów finansowych,
- instytucji fiskalnych.

System finansowy powinien realizować swoje funkcje w sposób ciągły i efektywny, posiadając odporność na nieoczekiwanych i niekorzystnych zaburzeń o znacznej skali. Zakłócenia w pracy systemu finansowego i zaburzenia efektywności świadczenia usług pośrednictwa finansowego negatywnie wpływają na sytuację przedsiębiorstw i gospodarstw domowych.

Wskaźnik bezpieczeństwa systemów finansowych będzie wyznaczany na podstawie wartości dwóch wskaźników składowych określających bezpieczeństwo rynkowego i publicznego systemu finansowego:

$$W_{SF} = f\left(W_{SF_1}, W_{SF_2}\right) \tag{5.17}$$

gdzie:

W_{SF} – wskaźnik bezpieczeństwa systemów finansowych,
W_{SF_1} – wskaźnik bezpieczeństwa rynkowego systemu finansowego,
W_{SF_2} – wskaźnik bezpieczeństwa publicznego systemu finansowego.

Ocena bezpieczeństwa rynkowego systemu finansowego jest dokonywana za pomocą następującej funkcji:

$$W_{SF_1} = f\left(W_{SF_{11}}, W_{SF_{12}}, W_{SF_{13}}, W_{SF_{14}}, W_{SF_{15}}, W_{SF_{16}}\right) \tag{5.18}$$

gdzie:

W_{SF_1} – wskaźnik bezpieczeństwa rynkowego systemu finansowego,
$W_{SF_{11}}$ – wskaźnik bezpieczeństwa systemów bankowych,
$W_{SF_{12}}$ – wskaźnik bezpieczeństwa funduszy inwestycyjnych,
$W_{SF_{13}}$ – wskaźnik bezpieczeństwa towarzystw ubezpieczeniowych,
$W_{SF_{14}}$ – wskaźnik bezpieczeństwa rynku pieniężnego,
$W_{SF_{15}}$ – wskaźnik bezpieczeństwa rynku akcji,

$W_{SF_{16}}$ – wskaźnik bezpieczeństwa rynku obligacji.

Wskaźnik bezpieczeństwa publicznego systemu finansowego będzie wyznaczany z godnie z regułą:

$$W_{SF_2} = f\left(W_{SF_{21}}, W_{SF_{22}}, W_{SF_{23}}, W_{SF_{24}}\right) \tag{5.19}$$

gdzie:

W_{SF_2} – wskaźnik bezpieczeństwa publicznego systemu finansowego,
$W_{SF_{21}}$ – wskaźnik bezpieczeństwa instytucji budżetowych,
$W_{SF_{22}}$ – wskaźnik bezpieczeństwa instrumentów fiskalnych,
$W_{SF_{23}}$ – wskaźnik bezpieczeństwa instrumentów finansowych,
$W_{SF_{24}}$ – wskaźnik bezpieczeństwa instytucji fiskalnych.

5.11. WSKAŹNIK BEZPIECZEŃSTWA OCHRONY ZDROWIA

System ochrony zdrowia to zbiór instytucji państwowych i prywatnych odpowiedzialnych za świadczenie usług leczniczych, dostarczanie leków, szczepionek, środków medycznych oraz sprzętu medycznego[210]. W jego skład wchodzą:

- publiczne zakłady opieki zdrowotnej,
- prywatne zakłady opieki zdrowotnej,
- ambulatoria,
- praktyki lekarskie,
- firmy farmaceutyczne,
- instytucje ubezpieczenia zdrowotnego,
- instytucje kontroli i nadzoru.

Wskaźnik bezpieczeństwa systemu ochrony zdrowia będzie wyznaczany na podstawie wartości siedmiu wskaźników składowych określających stopień przygotowania systemu na sytuacje kryzysowe:

$$W_{SOZ} = f\left(W_{SOZ_1}, W_{SOZ_2}, W_{SOZ_3}, W_{SOZ_4}, W_{SOZ_5}, W_{SOZ_6}, W_{SOZ_7}\right) \tag{5.20}$$

[210] Homeland Security, *Healthcare and Public Health Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf).

gdzie:

W_{SOZ} – wskaźnik bezpieczeństwa systemu ochrony zdrowia,

W_{SOZ_1} – wskaźnik bezpieczeństwa publicznych zakładów opieki zdrowotnej,

W_{SOZ_2} – wskaźnik bezpieczeństwa prywatnych zakładów opieki zdrowotnej,

W_{SOZ_3} – wskaźnik bezpieczeństwa ambulatoriów,

W_{SOZ_4} – wskaźnik bezpieczeństwa praktyk lekarskich,

W_{SOZ_5} – wskaźnik bezpieczeństwa firma farmaceutycznych,

W_{SOZ_6} – wskaźnik bezpieczeństwa instytucji ubezpieczenia zdrowotnego,

W_{SOZ_7} – wskaźnik bezpieczeństwa instytucji kontroli i nadzoru.

5.12. WSKAŹNIK BEZPIECZEŃSTWA SYSTEMÓW TRANSPORTOWYCH

Wskaźnik bezpieczeństwa systemów transportowych przeznaczony będzie do prezentacji stopnia przygotowania na sytuacje kryzysowe elementów infrastruktury krytycznej państwa przeznaczonych do transportu towarów[211]. Obejmował on będzie następujące rodzaje transportu:

- transport samochodowy,
- transport kolejowy,
- transport lotniczy,
- transport rurociągowy,
- żeglugę śródlądową,
- żeglugę morską.

Wskaźnik bezpieczeństwa systemów transportowych będzie wyznaczany na podstawie wartości sześciu wskaźników składowych określających bezpieczeństwo obiektów, instalacji, urządzeń oraz usług transportowych:

[211] Homeland Security, *Transportation Systems Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/ assets/nipp-ssp-transportation-systems-2010.pdf).

$$W_{STR} = f\left(W_{STR_1}, W_{STR_2}, W_{STR_3}, W_{STR_4}, W_{STR_5}, W_{STR_6}\right) \tag{5.21}$$

gdzie:

W_{STR} – wskaźnik bezpieczeństwa systemów transportowych,
W_{STR_1} – wskaźnik bezpieczeństwa transportu samochodowego,
W_{STR_2} – wskaźnik bezpieczeństwa transportu kolejowego,
W_{STR_3} – wskaźnik bezpieczeństwa transportu lotniczego,
W_{STR_4} – wskaźnik bezpieczeństwa transportu rurociągowego,
W_{STR_5} – wskaźnik bezpieczeństwa żeglugi śródlądowej,
W_{STR_6} – wskaźnik bezpieczeństwa żeglugi morskiej.

5.13. WSKAŹNIK BEZPIECZEŃSTWA SYSTEMÓW KOMUNIKACJI

System komunikacji obejmuje elementy infrastruktury krytycznej odpowiedzialne za transport osób. Podobnie jak omówiony powyżej system transportowy, obejmuje on:

- transport samochodowy,
- transport kolejowy,
- transport lotniczy,
- żeglugę śródlądową,
- żeglugę morską.

Efektywnie funkcjonujący system komunikacyjny jest jednym z najważniejszych czynników wpływających na bezpieczeństwo transportu osobowego.

Wskaźnik bezpieczeństwa systemów komunikacji będzie wyznaczany na podstawie wartości pięciu wskaźników składowych określających bezpieczeństwo transportu osobowego:

$$W_{SK} = f\left(W_{SK_1}, W_{SK_2}, W_{SK_3}, W_{SK_4}, W_{SK_5}\right) \tag{5.22}$$

gdzie:

W_{SK} – wskaźnik bezpieczeństwa systemów komunikacji,
W_{SK_1} – wskaźnik bezpieczeństwa transportu samochodowego,
W_{SK_2} – wskaźnik bezpieczeństwa transportu kolejowego,
W_{SK_3} – wskaźnik bezpieczeństwa transportu lotniczego,
W_{SK_4} – wskaźnik bezpieczeństwa żeglugi śródlądowej,

W_{SK_5} – wskaźnik bezpieczeństwa żeglugi morskiej.

5.14. WSKAŹNIK BEZPIECZEŃSTWA RATOWNICTWA

System ratownictwa obejmuje wszystkie instytucje oraz organizacje realizujące zadania związane z ratowaniem zdrowia i życia ludzi, ratowaniem mienia i środowiska oraz prognozowaniem, rozpoznawaniem i likwidacją skutków zdarzeń kryzysowych[212]. Bardzo ważną funkcją jest również powiadamianie i alarmowanie o zagrożeniach ludności cywilnej. W skład systemu wchodzą:

- Krajowy System Ratowniczo-Gaśniczy,
- Państwowe Ratownictwo Medyczne,
- System Powiadamiania Ratunkowego,
- ratownictwo górskie,
- ratownictwo morskie,
- ratownictwo górnicze,
- Wodne Ochotnicze Pogotowie Ratunkowe,
- Krajowy System Wykrywania Skażeń i Alarmowania.

Wskaźnik bezpieczeństwa systemów ratownictwa będzie wyznaczany na podstawie wartości ośmiu wskaźników składowych określających przygotowanie poszczególnych elementów do wykonywania działań związanych z bezpieczeństwem infrastruktury krytycznej:

$$W_{SR} = f\left(W_{SR_1}, W_{SR_2}, W_{SR_3}, W_{SR_4}, W_{SR_5}, W_{SR_6}, W_{SR_7}, W_{SR_8}\right) \tag{5.23}$$

gdzie:

W_{SR} – wskaźnik bezpieczeństwa systemów ratownictwa,

W_{SR_1} – wskaźnik bezpieczeństwa Krajowego Systemu Ratowniczo-Gaśniczy,

W_{SR_2} – wskaźnik bezpieczeństwa Państwowego Ratownictwa Medycznego,

[212] Homeland Security, *Emergency Services Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf).

W_{SR_3} – wskaźnik bezpieczeństwa Systemu Powiadamiania Ratunkowego,
W_{SR_4} – wskaźnik bezpieczeństwa ratownictwa górskiego,
W_{SR_5} – wskaźnik bezpieczeństwa ratownictwa morskiego,
W_{SR_6} – wskaźnik bezpieczeństwa ratownictwa górniczego,
W_{SR_7} – wskaźnik bezpieczeństwa Wodnego Ochotniczego Pogotowia Ratunkowego,
W_{SR_8} – wskaźnik bezpieczeństwa Krajowego Systemu Wykrywania Skażeń i Alarmowania.

5.15. WSKAŹNIK BEZPIECZEŃSTWA ADMINISTRACJI PUBLICZNEJ

System administracji publicznej obejmuje organy administracji rządowej oraz samorządowej odpowiedzialne za zaspakajanie indywidualnych oraz zbiorowych potrzeba obywateli we wszystkich dziedzinach życia. Skuteczność funkcjonowania systemu zarządzania kryzysowego jest uzależniona w dużej mierze od funkcjonowania systemu administracji publicznej, stąd też niezwykle ważnym przedsięwzięciem jest solidne przygotowanie mechanizmów zapewniających ciągłość działania tego systemu.

Rozpatrując problem bezpieczeństwa systemów administracji publicznej należy wziąć pod uwagę przygotowanie na sytuacje kryzysowe:

- administracji rządowej,
- urzędów centralnych,
- administracji samorządowej,
- administracji zespolonej,
- administracji niezespolonej.

Wskaźnik bezpieczeństwa administracji publicznej będzie wyznaczany na podstawie wartości pięciu wskaźników składowych określających przygotowanie poszczególnych jednostek systemu do sytuacji kryzysowych:

$$W_{SAP} = f\left(W_{SAP_1}, W_{SAP_2}, W_{SAP_3}, W_{SAP_4}, W_{SAP_5}\right) \tag{5.24}$$

gdzie:
W_{SAP} – wskaźnik bezpieczeństwa systemów administracji publicznej,

W_{SAP_1} – wskaźnik bezpieczeństwa administracji rządowej,
W_{SAP_2} – wskaźnik bezpieczeństwa urzędów centralnych,
W_{SAP_3} – wskaźnik bezpieczeństwa administracji samorządowej,
W_{SAP_4} – wskaźnik bezpieczeństwa administracji zespolonej,
W_{SAP_5} – wskaźnik bezpieczeństwa administracji niezespolonej.

5.16. WSKAŹNIK BEZPIECZEŃSTWA SYSTEMÓW SUBSTANCJI NIEBEZPIECZNYCH

Sektor infrastruktury krytycznej substancji niebezpiecznych obejmuje produkcję, składowanie, przechowywania i stosowanie substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych, a także ich recykling[213]. W skład systemu wchodzą:

- zakłady produkcyjne,
- systemy transportowe,
- systemy magazynowania,
- odbiorców substancji niebezpiecznych,
- zakłady utylizacji substancji niebezpiecznych.

Wskaźnik bezpieczeństwa systemów substancji niebezpiecznych będzie wyznaczany na podstawie wartości pięciu wskaźników składowych określających bezpieczeństwo poszczególnych elementów systemu:

$$W_{SSN} = f\left(W_{SSN_1}, W_{SSN_2}, W_{SSN_3}, W_{SSN_4}, W_{SSN_5}\right) \tag{5.25}$$

gdzie:

W_{SSN} – wskaźnik bezpieczeństwa systemów substancji niebezpiecznych,
W_{SSN_1} – wskaźnik bezpieczeństwa zakładów produkcyjnych,
W_{SSN_2} – wskaźnik bezpieczeństwa systemów transportowych,
W_{SSN_3} – wskaźnik bezpieczeństwa systemów magazynowania,

[213] Homeland Security, *Chemical Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-chemical-2010.pdf), *Nuclear Reactors, Materials, and Waste Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-nuclear-2010.pdf).

W_{SSN_4} – wskaźnik bezpieczeństwa odbiorców substancji niebezpiecznych,

W_{SSN_5} – wskaźnik bezpieczeństwa zakładów utylizacji substancji niebezpiecznych.

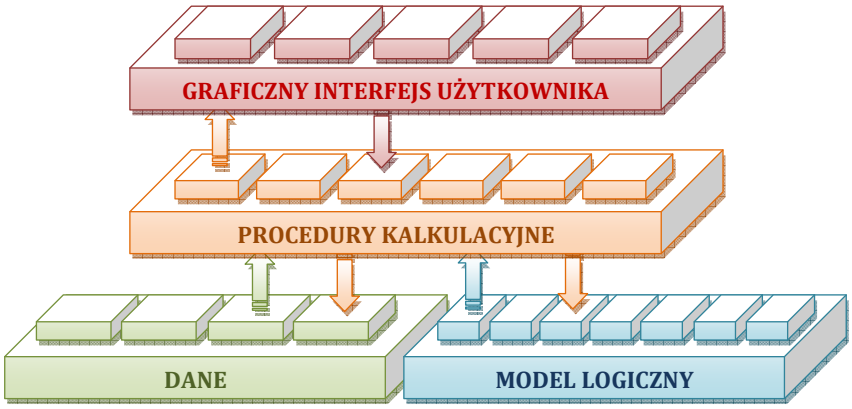
* * *

Zmiana charakteru współczesnych zagrożeń oraz ich zmienność w czasie spowodowała, że coraz więcej miejsca poświęca się problemom zarządzania kryzysowego. Formalne zagadnienia bezpieczeństwa cywilnego, ochrony infrastruktury technicznej oraz współpracy cywilno-wojskowej są przedmiotem wielu konferencji oraz badań naukowych. Postrzeganie kryzysu, jako klęski żywiołowej ustępuje miejsca nowej definicji, która obejmuje również zagrożenia terrorystyczne oraz zagrożenia odnoszące się do infrastruktury krytycznej państwa.

Zmiany te wymuszają konieczność prowadzenia prac nad modyfikacją narodowego systemu bezpieczeństwa w kierunku tworzenia kompleksowych i zintegrowanych narzędzi zarządzania kryzysowego umożliwiających efektywne wykorzystanie wszelkich dostępnych komponentów reagowania kryzysowego. Budowa i usprawnienie systemu zarządzania kryzysowego jest jednym z pilniejszych zadań, jakie stoją obecnie przed naszą administracją państwową. Jednym z istotnych elementów w systemie zarządzania kryzysowego jest właściwa ochrona infrastruktury krytycznej państwa odpowiedzialnej za przebieg procesów gospodarczych i społecznych.

Opracowanie modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej, wykorzystującego taksonomiczną formułę potencjałową, jako główną procedurę kalkulacyjną, posłużyło zbudowaniu prototypowej aplikacji komputerowej do oceny bezpieczeństwa infrastruktury krytycznej na poziomie regionalnym.

Zaprojektowana aplikacja komputerowa posiada budowę trójwarstwową (Rys. 5.2). Zasoby informacyjne (dane) oraz model logiczny wyznaczania wskaźników bezpieczeństwa poszczególnych elementów infrastruktury krytycznej zaimplementowany został w bazie danych (załącznik 4).



Rys. 5.2. Struktura aplikacji komputerowej oceny bezpieczeństwa infrastruktury krytycznej

Warstwa procedur kalkulacyjnych składa się z algorytmów obliczeniowych tworząc w ten sposób maszynę obliczeniową całego systemu (załącznik 3). Maszyna obliczeniowa budowana jest również w oparciu o przechowywany w bazie danych logiczny model wyznaczania wskaźników bezpieczeństwa zawierający sieć zależności pomiędzy wskaźnikami bezpieczeństwa oraz zmienne decyzyjne ustalające znaczenie wskaźników w modelu.

Graficzny interfejs użytkownika stanowi część systemu odpowiedzialną za bezpośredni kontakt z użytkownikiem. Zawiera on interfejsy niezbędne do wykonywania operacji w bazie danych oraz przeprowadzania obliczeń (załącznik 2). Graficzny interfejs użytkownika działa w środowisku sytemu operacyjnego Windows i został zaimplementowany z wykorzystaniem obowiązujących standardów komponentów wizualnych oprogramowania.

ZAKOŃCZENIE

Doświadczenia z ostatnich lat pokazują, że ludzkość staje coraz częściej w obliczu poważnych awarii technicznych, gwałtownych zjawisk klimatycznych, wzrostu zagrożenia atakami terrorystycznymi oraz niebezpieczeństw w cyberprzestrzeni. Czynniki te powodują, że bardzo istotnym zadaniem realizowanym przez systemy bezpieczeństwa narodowego, a w szczególności przez systemy zarządzania kryzysowego jest ochrona infrastruktury krytycznej obejmująca wszelkie przedsięwzięcia zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności kluczowych obiektów, instalacji, urządzeń oraz usług dla bezpieczeństwa oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców.

Przeprowadzone badania wykazały, że odpowiedzialność za budowę i nadzorowanie skutecznych mechanizmów podnoszących poziom bezpieczeństwa w odniesieniu do zwiększającej się liczby zagrożeń, leży na barkach głownie władzy publicznej. Administratorzy państw demokratycznych, w tym również i Polski, mają konstytucyjny obowiązek kształtowania wielowymiarowego bezpieczeństwa zewnętrznego, wewnętrznego i globalnego na maksymalnym poziomie, zgodnie ze światowymi standardami i zasadami prawno-międzynarodowymi.

Analiza historyczna wykazała, że postrzeganie bezpieczeństwa przez społeczność międzynarodową cały czas ewoluuje. Przestało już ono dotyczyć tylko kwestii związanych z naruszeniem integralności terytorialnej państwa, ale również bierze pod uwagę szeroki zakres problemów począwszy od stabilności ekonomicznej a skończywszy na degradacji środowiska naturalnego człowieka.

Wyraźnie widać, że definicja pojęcia pokoju i bezpieczeństwa ulega poszerzeniu. Pokój oznacza dużo więcej niż brak wojny, natomiast bezpieczeństwo przestaje być rozumiane przez ludzi tylko w kategoriach czysto wojskowych. Wymaga się, aby bezpieczeństwo zapewniało warunki do rozwoju gospodarczego, sprawiedliwości społecznej,

ochrony środowiska, demokratyzacji, rozbrojenia, a także poszanowanie praw człowieka i państwa.

Bezpieczeństwo, w jego najszerszym znaczeniu, obejmuje znacznie więcej niż brak konfliktów. Obejmuje ono poszanowanie praw człowieka, dobre zarządzanie, dostęp do edukacji i opieki zdrowotnej oraz zapewnienie każdej osobie możliwości do rozwoju osobowości.

Przeprowadzone badania wykazały również dualny charakter bezpieczeństwa. Może być ono rozpatrywane jako stan spokoju, pewności, wolności od zagrożeń, strachu lub ataku oraz jako losowy proces, w którym stan bezpieczeństwa i jego organizacja podlegają permanentnym, dynamicznym zmianom stosownie do zewnętrznych oddziaływań i uwarunkowań. Bezpieczeństwo jako proces oznacza natomiast ciąg działań wykonywanych przez jednostki, społeczności lokalne, państwa, organizacje międzynarodowe w celu tworzeniu pożądanego stanu równowagi.

Bardzo ważnym kierunkiem badań była konieczność przeanalizowania zasad funkcjonowania systemu zarządzania kryzysowego. Uzyskane na tej drodze informacje pozwoliły zrozumieć istotę i celu zarządzania kryzysowego, jako działalności prowadzonej dla zapewnienia stanu bezpieczeństwa w obliczu zagrożeń militarnych i niemilitarnych.

Realizacja tego etapu badań obejmowała również wnikliwą analizę regulacji formalno-prawnych oraz rozwiązań organizacyjno-funkcjonalnych systemu zarządzania kryzysowego w celu określenia miejsca systemu ochrony infrastruktury krytycznej w systemie zarządzania kryzysowego.

Poddano obserwacji również zmiany podejścia organów administracji publicznej do zagadnień związanych z ochroną kluczowych obiektów, instalacji, urządzeń oraz usług dla bezpieczeństwa oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców.

Wyniki przeprowadzonych badań zostały wykorzystane jako materiał wejściowy do skonstruowania procesu ochrony infrastruktury krytycznej, obejmującego podprocesy:

- zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej,
- przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,

- reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- odtwarzania infrastruktury krytycznej.

Określono, że zapobieganie zakłóceniom pracy infrastruktury krytycznej polega na podejmowaniu działań, zmierzających do wskazania głównych celów ochrony infrastruktury krytycznej, identyfikacji infrastruktury krytycznej w ramach państwa oraz Unii Europejskiej, identyfikacji zagrożeń, oceny ryzyka, określenia sieci powiązań w ramach systemu infrastruktury krytycznej oraz relacji pomiędzy poszczególnymi systemami.

Przygotowanie infrastruktury krytycznej na sytuacje kryzysowe obejmuje działania zmierzające do budowy mechanizmów służących zapewnieniu ciągłości działania najważniejszych dla społeczeństwa i gospodarki obiektów, instalacji, urządzeń i usług. Wykazano, że głównym celem podejmowanych przedsięwzięć jest zwiększenie odporności infrastruktury krytycznej na zidentyfikowane zagrożenia. Przygotowanie do sytuacji kryzysowych może odbywać się poprzez odpowiednie przydzielenie sił i środków oraz zapewnienie alternatywnych systemów zabezpieczających wszystkie potrzeby.

Reagowanie w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej to szereg przedsięwzięć podejmowanych przede wszystkim w celu zapewnienia ciągłości działania. Proces reagowania na sytuacje kryzysowe podzielono na następujące podprocesy:

- monitorowanie i prognozowanie rozwoju sytuacji kryzysowej,
- neutralizacja i ograniczanie zdarzeń kryzysowych,
- uruchamianie mechanizmów ciągłości działania zasobów infrastruktury krytycznej.

Odtwarzanie (odbudowa) pracy infrastruktury krytycznej polega na przywróceniu jej możliwości funkcjonalnych do stanu sprzed zaistnienia sytuacji kryzysowej. Głównymi działaniami, podejmowanymi niezwłocznie po zniszczeniu bądź zakłóceniu pracy infrastruktury krytycznej są przedsięwzięcia zapewniające jej ciągłość działania przynajmniej w minimalnym stopniu.

Zgromadzony materiał badawczy z pierwszych etapów procedury badawczej pozwolił przystąpić do budowy modelu matematycznego systemu zarządzania bezpieczeństwem infrastruktury krytycznej. Zgodnie z teorią systemów oraz zasadami analizy

systemowej proces modelowania został zdekomponowany na dwa etapy konceptualne dotyczące odpowiednio budowy modelu indentyfikacyjnego i na jego bazie modelu decyzyjnego. Przedstawiono również ogólne podejście do formalnego modelowania prakseologicznego systemu działania, jakim jest system zarządzania bezpieczeństwem infrastruktury krytycznej państwa.

Na początku zdefiniowano zadania i strukturę modelu identyfikacyjnego, który zgodnie z ogólną teorią systemów został opisany przy pomocy uporządkowanej trójki obejmującej: cel działania i podstawowe funkcje, składowe elementy struktury organizacyjnej oraz topologiczne relacje i różnorodne powiązania między tymi elementami.

Wyodrębnione elementy składowe systemu zarządzania bezpieczeństwem infrastruktury krytycznej zostały przedstawione w jednolitej konwencji za pomocą aparatu analizy i topologii matematycznej.

Budując model decyzyjny starano się ustalić zbiór ograniczeń oraz funkcję kryterium, determinującą proces zarządzania bezpieczeństwem infrastruktury krytycznej. Modelowanie decyzyjne zostało wykorzystane do przedstawienia systemu zarządzania bezpieczeństwem infrastruktury krytycznej w dynamice działań, jako ciągu kolejno podejmowanych decyzji, sterujących procesem zarządzania bezpieczeństwem infrastruktury krytycznej.

Ostatnim zadaniem procedury badawczej było opracowanie modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej. Model ten został zbudowany w oparciu o taksonomiczną formułę potencjałową wykorzystaną do oceny poziomu przygotowania zasobów infrastruktury krytycznej do sytuacji kryzysowych.

Stworzony modelu konceptualnego systemu oceny bezpieczeństwa infrastruktury krytycznej, został wykorzystany do budowy prototypowej aplikacji komputerowej oceny bezpieczeństwa infrastruktury krytycznej na poziomie regionalnym.

Podjęcie problemu badawczego w formie rozprawy naukowej stanowi dobry asumpt do prowadzenia dalszych badań naukowych oraz specjalistycznych prac analityczno-wdrożeniowych zmierzających docelowo do zaprojektowania i zbudowania kompleksowego systemu zarządzania bezpieczeństwem infrastruktury krytycznej wykorzystującego szerokie wsparcie nowoczesnych technologii z sektora IT.

BIBLIOGRAFIA

Opracowania zwarte:

1. Antonowicz L., Guz T., Pałubska M. R. (red.), *Bezpieczeństwo Polski. Historia i współczesność,* KUL, Lublin 2010.
2. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Adam Marszałek, Toruń 2005.
3. Becla A., Zielińska A., *Elementy statystyki i metod ilościowych*, I-Bis, Wrocław 2003.
4. Cempel C., *Teoria i inżynieria systemów*, Politechnika Poznańska, Poznań 2004.
5. Chrabkowski M., Tatarczuk C., Tomaszewski J., *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, WSAiB, Gdynia 2011.
6. Cieślarczyk M., *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wyd. AP, Siedlce 2009.
7. Ficoń K., *Badania operacyjne stosowane. Modele i aplikacji*, BEL Studio, Warszawa 2006.
8. Ficoń K., *Inżynieria zarządzania kryzysowego. Podejście systemowe*, BEL Studio, Warszawa 2007.
9. Ficoń K., *Logistyka kryzysowa. Procedury, potrzeby, potencjał*, BEL Studio, Warszawa 2011.
10. Gryz J., Kitler W., *System reagowania kryzysowego*, Adam Marszałek, Toruń 2007.
11. Haliżak E., Kuźniar R., Michałowska G., Parzymies S., Symonides J., Zięba R., *Stosunki międzynarodowe w XXI wieku. Księga jubileuszowa z okazji 30-lecia Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego*, WN Scholar, Warszawa 2006.
12. *Koncepcja systemu zarządzania kryzysowego*, Komenda Główna Policji, Warszawa 1998.
13. Konieczny J., *Zarządzanie w sytuacjach kryzysowych*, wypadkach i katastrofach, Wydawnictwo Garmond, Poznań-Warszawa, 2001.
14. Ladak D., Pilch T. (red.), *Elementarne pojęcia pedagogiki społecznej i pracy socjalnej*, Wydawnictwo ŻAK, Warszawa 1999.

15. Nowak E., *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Akademia Obrony Narodowej, Warszawa 2007.
16. Ostrokólski A., *Problemy zapewnienia bezpieczeństwa regionalnego*, Olsztyn 2008.
17. Pawłowski J., *Słownik terminów z zakresu bezpieczeństwa narodowego,* Warszawa 2002.
18. Rosa R., *Filozofia bezpieczeństwa*, Bellona, Warszawa 1995.
19. Santayana G., *The Life of Reason*, 1905-1906.
20. Sienkiewicz P., Górny P., *Analiza systemowa sytuacji kryzysowych*, Wydawnictwo AON, Warszawa 2001.
21. Sienkiewicz-Małyjurek K., Krynojewski F., *Zarządzanie kryzysowe w administracji publicznej*, Wydawnictwo Difin, Warszawa 2010.
22. Skrzypek E., Hofman M., *Zarządzanie procesami w przedsiębiorstwie*, Oficyna a Wolters Kluwer business, Warszawa 2010.
23. *Słownik języka polskiego,* t. 1, Wydawnictwo PWN, Warszawa 1978.
24. Sołkiewicz H. (red.), *Operacyjno-taktyczny leksykon morski*, Tom 1, AMW, Gdynia 2012.
25. Stankiewicz W. (red.), *Ekonomika obrony*, AON, Warszawa 1994.
26. Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Wydawnictwo ISP PAN, Warszawa 1996.
27. Stawnicka J., Wiśniewski B., Socha R., *Zasadnicze problemy zarządzania kryzysowego w organizacjach zhierarchizowanych*, KWP, Katowice 2011.
28. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2007.
29. Sulęta W. R., *System zarządzania kryzysowego województwa pomorskiego*, AMW, Gdynia 2010.
30. Szubrycht T. (red.), *Leksykon bezpieczeństwa morskiego*, AMW, Gdynia 2008.
31. Świniarski J., *Filozoficzne podstawy edukacji dla bezpieczeństwa*, MON, Warszawa 1999.
32. Tyburska A. (red.), *Ochrona infrastruktury krytycznej*, WSPol, Szczytno 2010.
33. Tyrała P. (red.), *Zarządzanie bezpieczeństwem*, Kraków 2000.
34. Wiliams P. D., Studia bezpieczeństwa, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2012.
35. Wróblewski R., *Zarys teorii kryzysu, zagadnienia prewencji i zarządzania kryzysowego*, Wydawnictwo AON, Warszawa 1996.

36. *Założenia projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym*, MSWiA, Warszawa 2011.
37. Ziarko J., Walas-Trębacz J., *Podstawy zarządzania kryzysowego. Część 1. Zarządzanie kryzysowe w administracji publicznej*, Krakowska Szkoła Wyższa, Kraków 2009.
38. Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje-struktury-funkcjonowanie*, Scholar, Warszawa 1999.

Artykuły:

1. Dudek D., *Bezpieczeństwo Rzeczypospolitej jako wartość konstytucyjna,* [w]: Antonowicz L., Guz T., Pałubska M. R. (red.), *Bezpieczeństwo Polski. Historia i współczesność,* KUL, Lublin 2010.
2. Ficoń K., *Bezpieczeństwo jako systemowa kategoria ontologiczna*, BELLONA, 2012.
3. Ficoń K., *Wykorzystanie funkcji potęgowo-wykładniczej w procesie zarządzania bezpieczeństwem*, ZN AMW, Nr 1, AMW, Gdynia 2009.
4. Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Kwartalnik bezpieczeństwo Narodowe, Nr 18, BBN, Warszawa 2011.
5. Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Kwartalnik bezpieczeństwo Narodowe, Nr 18, BBN, Warszawa 2011.
6. Krasnodębski G., *Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informacyjnego*, [w:] *Problemy zapewnienia bezpieczeństwa regionalnego*, Olsztyn 2008.
7. Kukułka J., *Bezpieczeństwo a współpraca europejska: współzależności i sprzeczności interesów. Sprawy międzynarodowe*, nr 7, Warszawa 1982.
8. Kundzewicz Z. W., Matczak P., *Zagrożenia naturalnymi zdarzeniami ekstremalnymi*, Nauka Nr 4, Warszawa 2010.
9. Mazur M., *Pojęcie systemu i rygory jego stosowania*. [w:] Materiały Szkoły Podstaw Inżynierii Systemów nr 2, Komitet Budowy Maszyn PAN, Orzysz1976.
10. Stachowiak Z., *Bezpieczeństwo ekonomiczne*, [w:] W. Stankiewicz (red.), *Ekonomika obrony*, AON, Warszawa 1994.

11. Sulęta R., Krasnodębski G., *Podstawy prawne zarządzania kryzysowego w Polsce*, [w:] *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, WSAiB, Gdynia 2011.
12. Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] P. Tyrała (red.), *Zarządzanie bezpieczeństwem*, Kraków 2000.
13. Trejnis Z., *Infrastruktura krytyczna – koncepcje i zakres*, [w:] A. Tyburska (red.), *Ochrona infrastruktury krytycznej*, WSPol, Szczytno 2010.
14. Zięba R., *Teoria ogólna bezpieczeństwa państwa w stosunkach międzynarodowych*, [w:] *Stosunki międzynarodowe w XXI wieku. Księga jubileuszowa z okazji 30-lecia Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego*, WN Scholar, Warszawa 2006.

Dokumenty normatywne:

1. *Konstytucji RP z dnia 2 kwietnia 1997 r.*, Dz. U. z 1997 r. Nr 78, poz. 483, ze zm.
2. *Rozporządzenie Ministra Infrastruktury z dnia 7 maja 2004 r. w sprawie sposobu uwzględniania w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa*, Dz. U. z 2004 r. Nr 125, poz. 1309.
3. *Rozporządzenie Ministra Kultury z dnia 25 sierpnia 2004 r. w sprawie organizacji i sposobu ochrony zabytków na wypadek konfliktu zbrojnego i sytuacji kryzysowych*, Dz. U. z 2004 r. Nr 212, poz. 2153.
4. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 grudnia 1999 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego*, Dz. U. z 1999 r. Nr 111, poz. 1311.
5. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2001 r. w sprawie szczegółowych zasad kierowania i współdziałania jednostek ochrony przeciwpożarowej biorących udział w działaniu ratowniczym*, Dz. U. z 2001 r. Nr 82, poz. 895.
6. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2007 r. w sprawie szczegółowej organizacji centrów powiadamiania ratunkowego*, Dz. U. z 2007 r. Nr 178, poz. 1263.

7. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2009 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego i wojewódzkich centrów powiadania ratunkowego*, Dz. U. z 2009 r. Nr 130, poz. 1073 ze zm.
8. *Rozporządzenie Ministra Zdrowia z dnia 15 marca 2007 r. w sprawie szpitalnego oddziału ratunkowego*, Dz. U. z 2007 r. Nr 55, poz. 365.
9. *Rozporządzenie Ministra Zdrowia z dnia 16 kwietnia 2007 r. w sprawie doskonalenia zawodowego dyspozytorów medycznych*, Dz. U. z 2007 r. Nr 77, poz. 525.
10. *Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie wojewódzkiego planu działania systemu Państwowe Ratownictwo Medyczne oraz kryteriów kalkulacji kosztów działalności zespołów ratownictwa medycznego*, Dz. U. z 2011 r. Nr 3, poz. 6.
11. *Rozporządzenie Ministra Zdrowia z dnia 24 lutego 2009 r. w sprawie szczegółowego zakresu uprawnień i obowiązków lekarza koordynatora ratownictwa medycznego*, Dz. U. z 2009 r. Nr 39, poz. 322.
12. *Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*, Dz. U. z 2008 r. Nr 128, poz. 821.
13. *Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*, Dz. U. z 2011 r. Nr 86, poz. 471.
14. *Rozporządzenie Prezesa Rady Ministrów z dnia 14 lipca 2010 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej*, Dz. U. Nr 135, poz. 906.
15. *Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania*, Dz. U. 2009 nr 226 poz. 1810.
16. *Rozporządzenie Rady Ministrów z dnia 16 października 2006 r. w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach*, Dz. U. z 2006 r. Nr 191, poz. 1415.
17. *Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych*, Dz. U. z 2005 r. Nr 20, poz. 169.

18. *Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad udziału pododdziałów i oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu*, Dz. U. z 2003 r. Nr 41, poz. 347.
19. *Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin*, Dz. U. z 2002 r. Nr 96, poz. 850.
20. *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*, Dz. U. Nr 83, poz. 541.
21. *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej*, Dz. U. Nr 83, poz. 542.
22. *Ustawa o zmianie ustawy o zarządzaniu kryzysowym z dnia 29 października 2010 r.*, Dz. U. z 2010 nr 240 poz. 1600.
23. *Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej*, Dz. U. z 2002 r. Nr 62, poz. 558 ze zm.
24. *Ustawa z dnia 18 lipca 2001 r. Prawo wodne*, Dz. U. z 2001 r. Nr 115, poz. 1229.
25. *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*, Dz. U. z 2004 r. Nr 241, poz. 2416.
26. *Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*, Dz. U. z 2004 r. Nr 241, poz. 2416.
27. *Ustawa z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela*, Dz. U. z 2002 r. Nr 233, poz. 1955.
28. *Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw*, Dz. U. z 2009 r. Nr 85, poz. 716.
29. *Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej*, Dz. U. 1991 r. Nr 81 poz. 351, ze zm.
30. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz. U. z 2007 r. Nr 89, poz. 590.
31. *Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska*, Dz. U. z 2001 r. Nr 62, poz. 627.
32. *Ustawa z dnia 5 czerwca 1998 r. o administracji rządowej w województwie*, Dz. U. z 1998 r. Nr 91, poz. 577.

33. *Ustawa z dnia 5 czerwca 1998 r. o administracji rządowej w województwie – teks jednolity*, Dz. U. z 2001 r. Nr 80, poz. 872.
34. *Ustawa z dnia 5 grudnia 2008 r. o zmianie ustawy o ochronie przeciwpożarowej oraz niektórych innych ustaw*, Dz. U. z 2009 r. Nr 11, poz. 59.
35. *Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym*, Dz. U. z 2006 r. Nr 191, poz. 1410 ze zm.

Źródła internetowe:

1. Al Mannai W. I., *Development of a decision support tool to inform resource allocation for critical infrastructure protection in homeland security*, Monterey, California 2008 (http://www.dtic.mil/dtic/tr/fulltext/u2/a483640.pdf).
2. Albano M., Chessa S., Di Pietro R., *A model with applications for data survivability in Critical Infrastructures*, Journal of Information Assurance and Security 4 (2009) (www.researchgate.net).
3. Annan K., *Millenium Report*, Chapter 3 (*www.un.org/millennium/sg/report*).
4. Bagheri E., Ghorbani A., *Towards an MDA-Oriented UML Profile for Critical Infrastructure Modeling* (www.ee.ryerson.ca/~bagheri/papers/pst2.pdf).
5. Baiardi F., *Allocating Resources to the Search for Vulnerabilities in Information Infrastructures* (www.di.unipi.it/~baiardi/sec/natoARWrisk.pdf).
6. Baiardi F., Telmon C., Sgandurra D., *Hierarchical, Model-Based Risk Management of Critical Infrastructures* (http://eprints.adm.unipi.it/596/1/baiardijournalrevised.pdf).
7. Ball S., Marshall M.D., Schaffer S., Wedeward K. J., *An Integrated Approach to Modeling, Simulation, and Analysis of Critical Infrastructure Systems* (http://www.icasa.nmt.edu/Content/publication/integrated_approach.pdf).
8. Barnes P., Egodawatta P., Goonetilleke A., *Modelling Resilience in a Water Supply System: Contrasting conditions of drought and flood*, Health Faculty, Queensland University of Technology (iiirr.ucalgary.ca/files/iiirr/B4-2_.pdf).

9. Bologna S., Beer T., *An Integrated Approach to Survivability Analysis of Large Complex Critical Infrastructures* (http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-3.pdf)
10. Brown G. G., Carlyle W. M., Salmer´on J., K. Wood*, Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses*, Informs 2005, (http://faculty.nps.edu/kwood/docs/DefendingCIBrownEtAlTutorialDraft.pdf).
11. Brown T., *Multiple Modeling Approaches and Insights for Critical Infrastructure Protection* (www.sandia.gov/nisac/downloads288).
12. Carlyle M., Salmerón J., K. Wood, *Analyzing the Vulnerability of Critical Infrastructure to Attack, and Planning Defenses Gerald Brown* (http://faculty.nps.edu/kwood/docs/DefendingCIBrownEtAlTutorialDraft.pdf).
13. *Communication from the Commission to the Council and the European Parliament, Critical Infrastructure Protection in the fight against terrorism*, Brussels, 20.10.2004, COM(2004) 702 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF).
14. *Comparative Evaluation of Modeling and Simulation Techniques for Interdependent Critical Infrastructures*, Scientific Report (http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/publikationen_ski.parsys.87450.DownloadFile.tmp/comparativeevaluation.pdf).
15. Conrad S. H., LeClaire R. J., O'Reilly G. P., Uzunalioglu H., *Critical National Infrastructure Reliability Modeling and Analysis* (http://www.sandia.gov/nisac/wp/wp-content/uploads/downloads/2012/03/Critical-National-Infrastructure-Reliability-Modeling-and-Analysis-2006-3442-J.pdf)
16. *Critical infrastructure resilience strategy*, Australia 2010, (www.tisn.gov.au, 12.2012)
17. *Critical Infrastructure Strategic Roadmap*, Electricity Sub-Sector Coordinating Council, Princeton 2010, (http://www.nerc.com/docs/escc/ESCC_Strat_Roadmap_V4_7_Oct2010_clean.pdf)
18. *Critical Infrastructure Threats and Terrorism*, DCSINT Handbook No. 1.02, 2006, (http://www.fas.org/irp/threat/terrorism/sup2.pdf).
19. *Critical Infrastructure Threats and Terrorism*, DCSINT Handbook No. 1.02, 2006. (http://www.fas.org/irp/threat/terrorism/sup2.pdf).

20. D Dudenhoeffer. D., Permann M. R., Manic M., *CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis*, 2006 (www.inl.gov/technicalpublications/ Documents/3578215.pdf).
21. Ezell B. Ch., *Infrastructure Vulnerability Assessment Model (I-VAM)* (create.usc.edu/assets/pdf/51834.pdf).
22. *Final Report of the National Commission on Terrorist Attacks Upon the United States*, www.c-span.org/pdf/911finalreportexecsum.pdf.
23. Giannopoulos G., Filippini R., Schimmer M., *Risk assessment methodologies for Critical Infrastructure Protection,* Part I: A state of the art, European Commission Joint Research Centre Institute for the Protection and Security of the Citizen, Publications Office of the European Union, 2012 (http://ec.europa.eu/home-affairs/ doc_centre/terrorism/docs/RA-ver2.pdf)
24. *Green Paper on a European Programme for Critical Infrastructure Protection, Brussels*, 17.11.2005, COM(2005) 576 final (http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf).
25. Homeland Security, *Banking and Finance Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/sites/default/files/publications/nipp-ssp-banking-and-finance-2010.pdf).
26. Homeland Security, *Chemical Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-chemical-2010.pdf).
27. Homeland Security, *Commercial Facilities Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf).
28. Homeland Security, *Communications Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf).
29. Homeland Security, *Critical Manufacturing Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-critical-manufacturing-2010.pdf).

30. Homeland Security, *Dams Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-dams-2010.pdf).
31. Homeland Security, *Defense Industrial Base Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf).
32. Homeland Security, *Education Facilities Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf).
33. Homeland Security, *Emergency Services Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf).
34. Homeland Security, *Energy Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf).
35. Homeland Security, *Food and Agriculture Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf).
36. Homeland Security, *Healthcare and Public Health Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf).
37. Homeland Security, *National InfrastructureProtection Plan, Partnering to enhance protection and resiliency*, Washington 2009 (http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).
38. Homeland Security, *National Monuments and Icons Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf).
39. Homeland Security, *Nuclear Reactors, Materials, and Waste Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-nuclear-2010.pdf).

40. Homeland Security, *Transportation Systems Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf).
41. Homeland Security, *Water Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan*, Washington 2010 (http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf).
42. *http://www.dhs.gov/critical-infrastructure-sectors.*
43. Idowu O., Shi Q., Merabti M., Kifayat K., *Ad-Hoc Cloud Networks: A Probabilistic Model for Vulnerability Detection in Critical Infrastructure Using Bayesian Networks*, School of Computing and Mathematical Sciences, Liverpool John Moores University (http://www.cms.livjm.ac.uk/pgnet2012/Proceedings/Papers/1569607177.pdf).
44. International Recovery Platform Secretariat, *Guidance note on recovery: infrastructure*, Japan, www.recoveryplatform.org.
45. Johnson Ch. W., Williams R., *Computational Support for Identifying Safety and Security Related Dependencies between National Critical Infrastructures*, Department of Computing Science, University of Glasgow (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.139.4581).
46. Jonkeren O. E., Ward D., Dorneanu B., Giannopoulos G., *Economic impact assessment of Critical Infrastructure failure in the EU: A combined Systems Engineering – Inoperability Input-Output Model*, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra, Italy, (www.iioa.org/files/conference-3/903.pdf).
47. Kelevedjiev E., *Computational Approach for Assessment of Critical Infrastructure in Network Systems* (www.gcmarshall.bg/KP/2a/6.pdf)
48. Klein R., Rome E., Beyel C., Linnemann R., Reinhardt W., *Information Modelling and Simulation in large interdependent Critical Infrastructures in IRRIIS* (http://www.irriis.org/Filebee4.pdf?lang=2&oiid=9206&pid=952).
49. Lukas L., Hromada M., *Resilience as main part of protection of critical infrastructure*, International journal of mathematical models and methods in applied sciences, (http://www.naun.org/multimedia/NAUN/m3as/20-879.pdf).

50. Lukas L., Hromada M., *Simulation and Modeling in Critical Infrastructure Protection*, International journal of mathematical models and methods in applied sciences, (http://www.naun.org/multimedia/NAUN/mcs/20-871.pdf).
51. Lukas L., Necesal L., *Measures for Critical infrastructure protection*, International journal of mathematical models and methods in applied sciences, (http://www.naun.org/multimedia/NAUN/m3as/17-138.pdf).
52. Malak K., *Typologia bezpieczeństwa. Nowe wyzwania*, stosunki-miedzynarodowe.pl/bezpieczenstwo/954-typologia-bezpieczenstwa-nowe-wyzwania.
53. *National Infrastructure Protection Plan 2009*, http://www.dhs.gov/national-infrastructure-protection-plan.
54. New York State Comprehensive Emergency Management Plan, *Critical Infrastructure and Key Resources Functional Annex*, Prepared by the member agencies of the New York State Critical Infrastructure and Key Resources Branch, 01.2012, (http://www.dhses.ny.gov/planning/documents/cikr-branch-3.2012.pdf)
55. Niemeyer K., *Simulation of critical infrastructures*, INFORMATION & SECURITY. An International Journal, Vol.15, No.2, 2004, 120-143 (www.gcmarshall.bg/KP/2b/3.pdf).
56. Pederson P., Dudenhoeffer D., Hartley S., Permann M., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory 2006 (http://www.inl.gov/technicalpublications/Documents/3489532.pdf).
57. *Protecting Critical Infrastructures –Risk and Crisis Management, A guide for companies and government authorities*, Berlin 2008, www.bmi.bund.de.
58. Pye G., Warren M. J., *Conceptual Modelling: Choosing a Critical Infrastructure Modelling Methodology*, Deakin University (http://ro.ecu.edu.au/isw/16/).
59. Rosato V., Artale V., Pisacane G., Sannino G., Struglia M. V., Tofani A., Pascucci E., *Risk Analysis and Crisis Scenario Evaluation in Critical Infrastructures Protection*, ENEA, Energetic and Environmental Modelling Unit, Casaccia Research Centre, InTech, Roma 2011 (cdn.intechweb.org/pdfs/18806.pdf).

60. Sandia National Laboratories, *Optimal Recovery Sequencing for Critical Infrastructure Resilience Assessment*, New Mexico, USA 2010, (http://prod.sandia.gov/techlib/access-control.cgi/2010/106237.pdf, 12.2012).
61. Satumtira G., Dueñas-Osorio L., *Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research* (http://link.springer.com/chapter/10.1007%2F978-3-642-11405-2_1#page-1).
62. Scarlatos P. D., Kaisar E. I., Teegavarapu R., *Modeling and Simulation of Catastrophic Events Affecting Critical Infrastructure Systems*, Department of Civil, Environmental and Geomatics Engineering Florida Atlantic University (http://www.wseas.us/e-library/conferences/2009/vouliagmeni/ACCMM/ACCMM1-46.pdf).
63. Siaterlis Ch., Genge B., Hohenadel M., Del Pra M., *Enabling the Experimental Exploration of Operating Procedures on Critical Infrastructures* (http://www.thei3p.org/docs/events/ifip2012presentation/hohenadel.pdf).
64. The Heritage Foundation, *One Year Later: Lessons from Recovery after the Great Eastern Japan Earthquake*, special report, Washington 2012, (http://report.heritage.org/sr0108)
65. Tolone W. J., Lee S., Xiang W., McNally R. K., Schumpert A., *Effective Scenario Composition for the Revelation of Blind Spots in Critical Infrastructure Protection Planning*, In Proceedings of the First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (ICCIP '07), Dartmouth College, Hanover, New Hampshire, USA, March 19-21, 2007.
66. Tolone W. J., Lee S., Xiang W., McNally R. K., Schumpert A., *Effective Scenario Composition for the Revelation of Blind Spots in Critical Infrastructure Protection Planning*, In Proceedings of the First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (ICCIP '07), Dartmouth College, Hanover, New Hampshire, USA, March 19-21, 2007
67. Traktat o Unii Europejskiej (http://eur-lex.europa.eu/pl/treaties/index.htm).

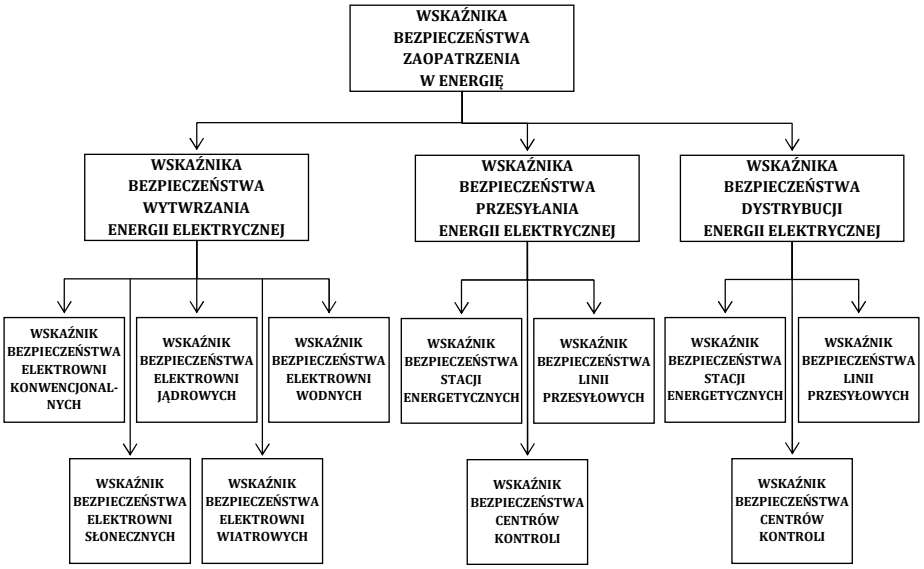
68. Visarraga D. B., *Understanding Complex Systems: Infrastructure Impacts* (http://www.mathaware.org/mam/2011/essays/complexsystemsVisarraga.pdf).
69. www.britannica.com/EBchecked/topic/1279086/Madrid-train-bombings-of-2004.
70. www.britannica.com/EBchecked/topic/1696348/London-bombings-of-2005.
71. www.networkworld.com/news/2012/100812-ponemon-cyberattacks-263113.html.
72. Young-Suk, Spencer B.F., Elnashai Jr. Amr S., *Seismic Loss Assessment and Mitigation for Critical Urban Infrastructure Systems* (https://www.ideals.illinois.edu/bitstream/handle/2142/4603/NSEL.Report.007.pdf?sequence=4).
73. Zabasta A., Kunicina N., Ribickis L., *The Problem Issues of Intelligent Monitoring and Control of CIS in Latvia*, Electronics and Electrical Engineering, 2012. No. 2(118), (http://www.ee.ktu.lt/journal/2012/02/12__ISSN_1392-1215_The Problem Issues of Intelligent Monitoring and Control of CIS in Latvia.pdf).

WYKAZ RYSUNKÓW

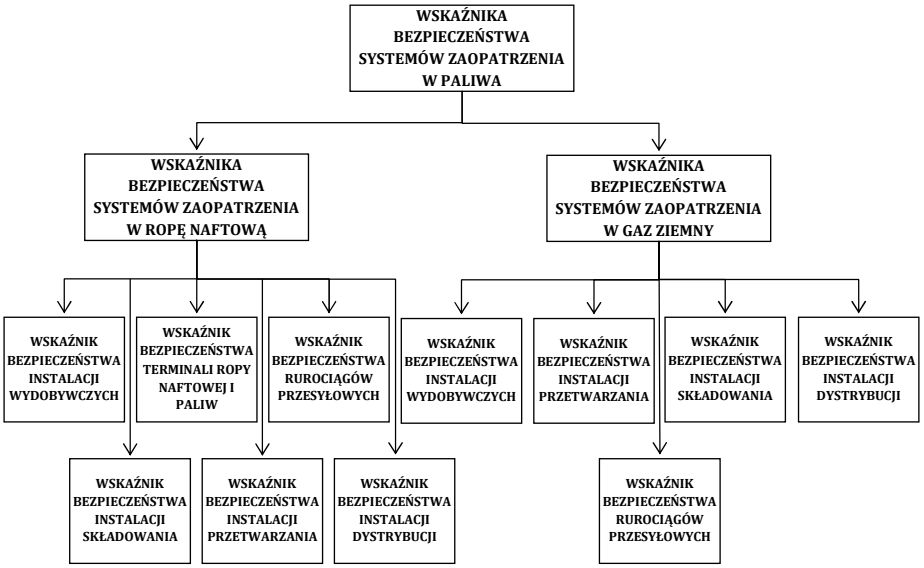
ZAŁĄCZNIKI

ZAŁĄCZNIK 1.
STRUKTURY WSKAŹNIKÓW BEZPIECZEŃSTWA

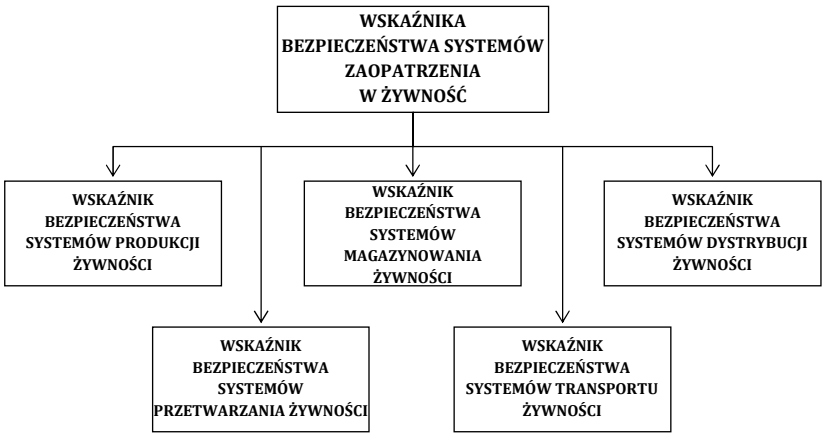
1. Struktura oceny wskaźnika bezpieczeństwa systemów zaopatrzenia w energię



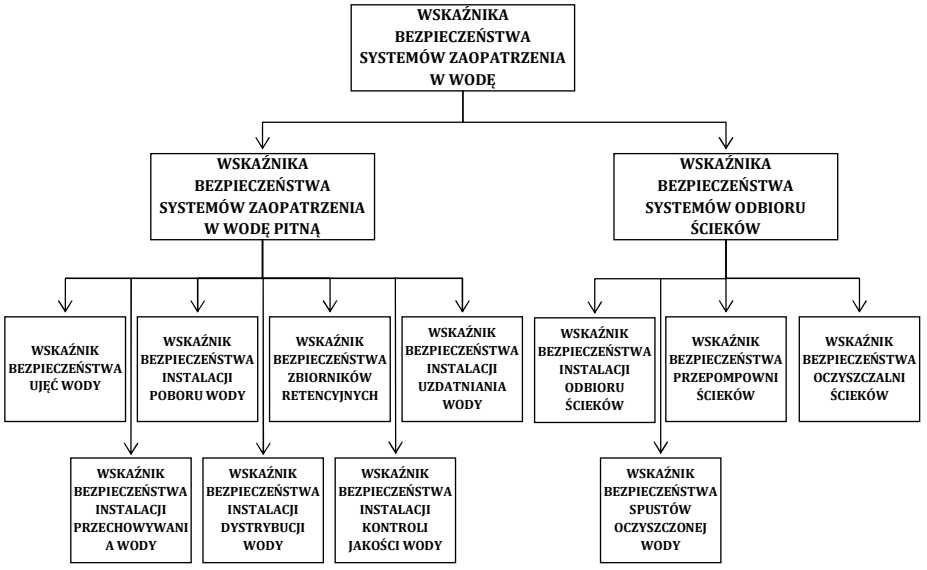
2. Struktura oceny wskaźnika bezpieczeństwa systemów zaopatrzenia w paliwa



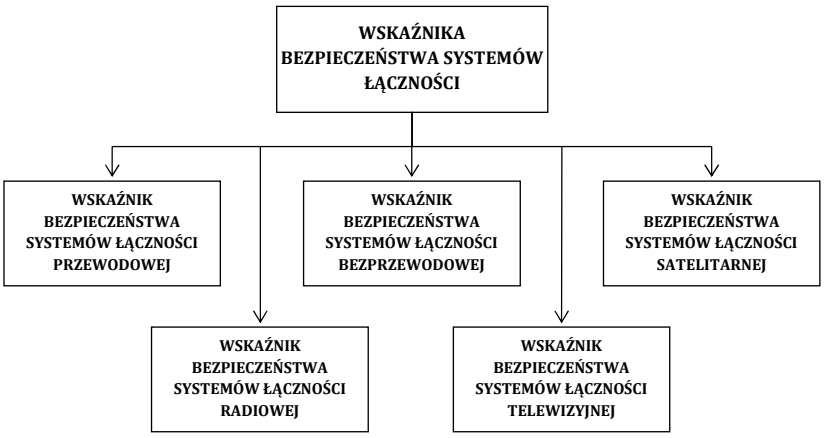
3. Struktura oceny wskaźnika bezpieczeństwa systemów zaopatrzenia w żywność



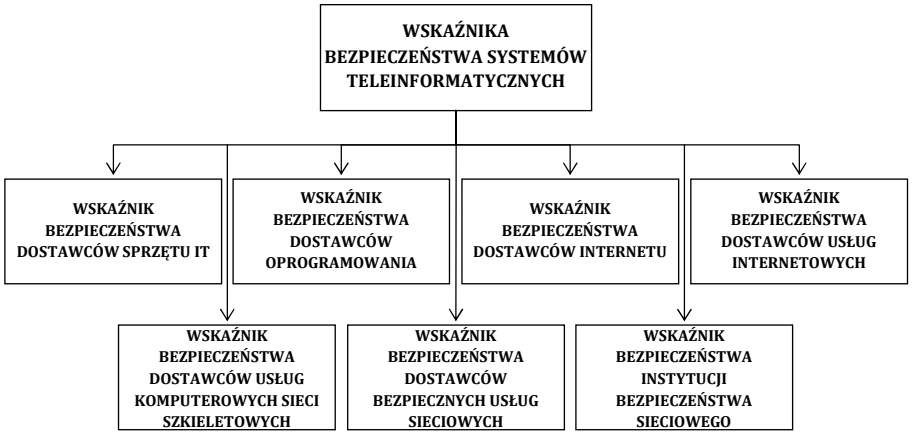
4. Struktura oceny wskaźnika bezpieczeństwa systemów zaopatrzenia w wodę



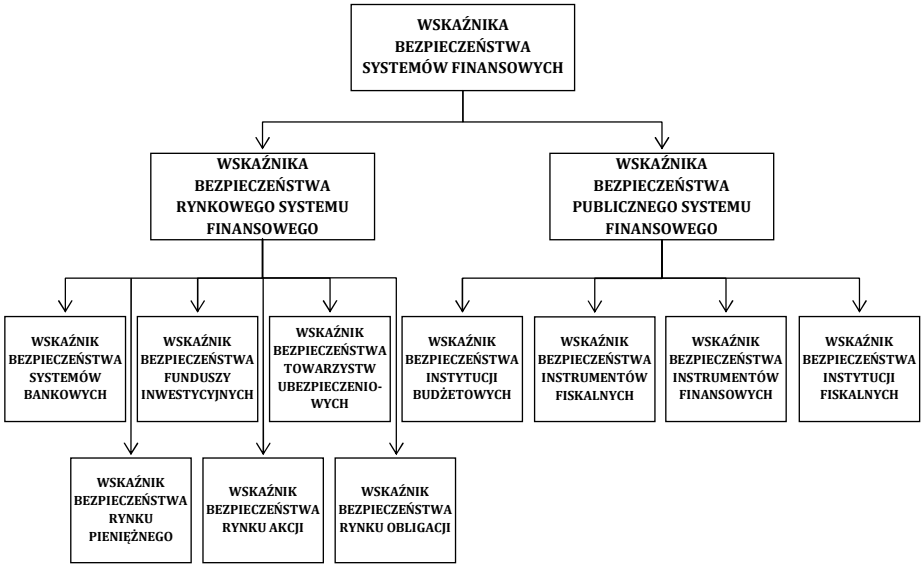
5. Struktura oceny wskaźnika bezpieczeństwa systemów łączności



6. Struktura oceny wskaźnika bezpieczeństwa systemów teleinformatycznych

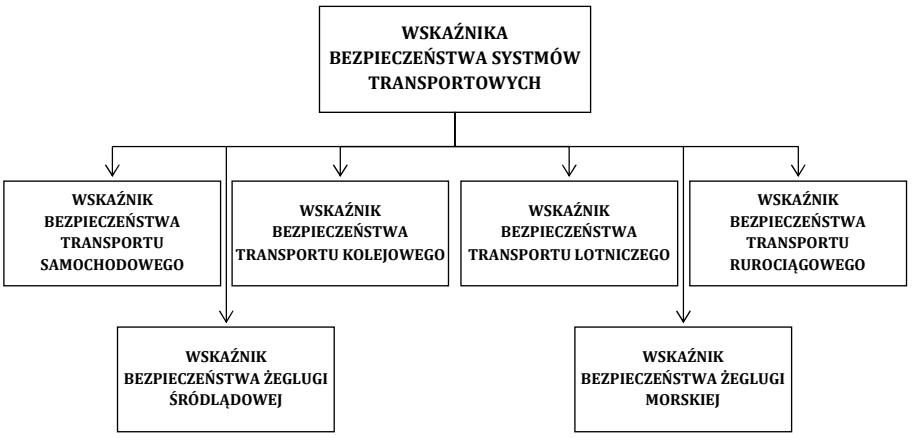


7. Struktura oceny wskaźnika bezpieczeństwa systemów finansowych

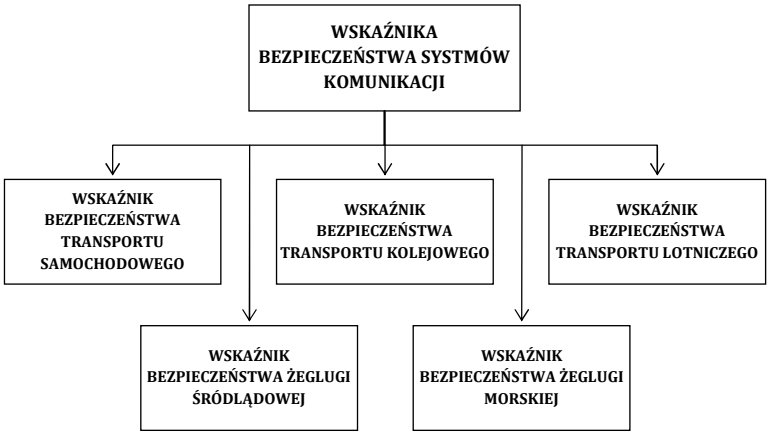


8. Struktura oceny wskaźnika bezpieczeństwa systemu ochrony zdrowia

9. Struktura oceny wskaźnika bezpieczeństwa systemów transportowych

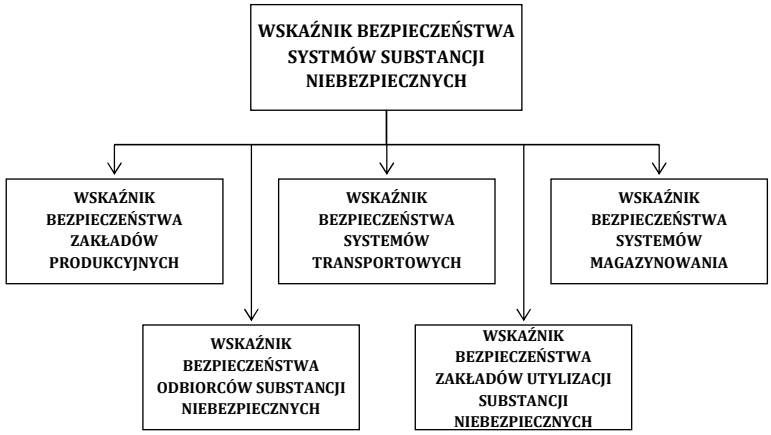


10. Struktura oceny wskaźnika bezpieczeństwa systemów transportowych



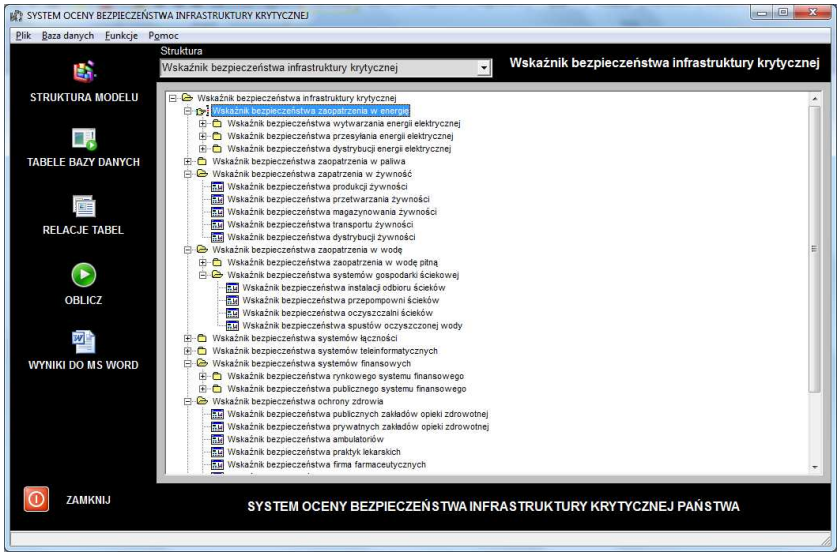
11. Struktura oceny wskaźnika bezpieczeństwa systemów administracji publicznej

12. Struktura oceny wskaźnika bezpieczeństwa systemów substancji niebezpiecznych

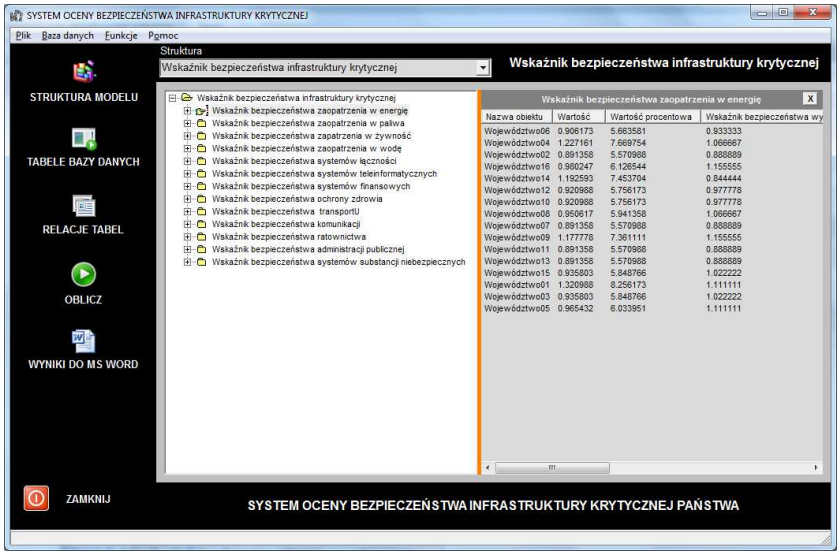


ZAŁĄCZNIK 2.
GRAFICZNE INTERFEJSY UŻYTKOWNIKA SYSTEMU INFORMATYCZNEGO OCENY BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ

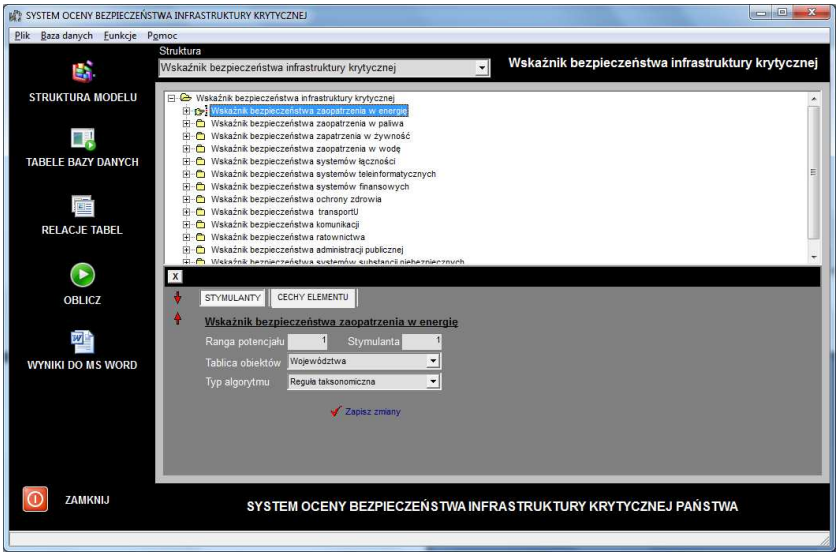
1. Główny interfejs użytkownika



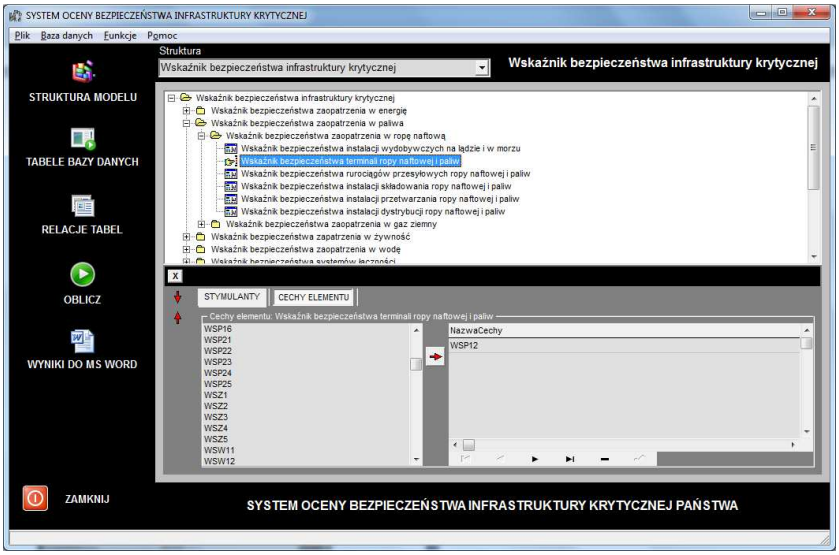
2. Wyniki obliczeń



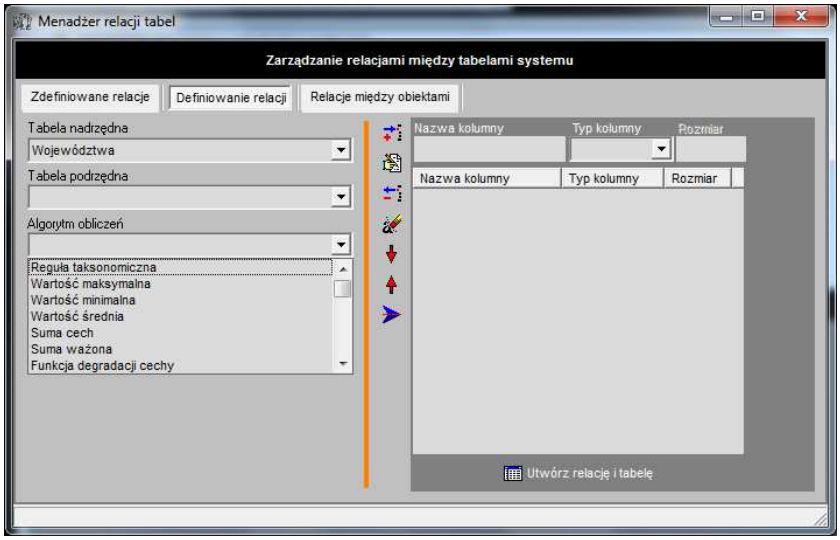
3. Okno zmiennych decyzyjnych



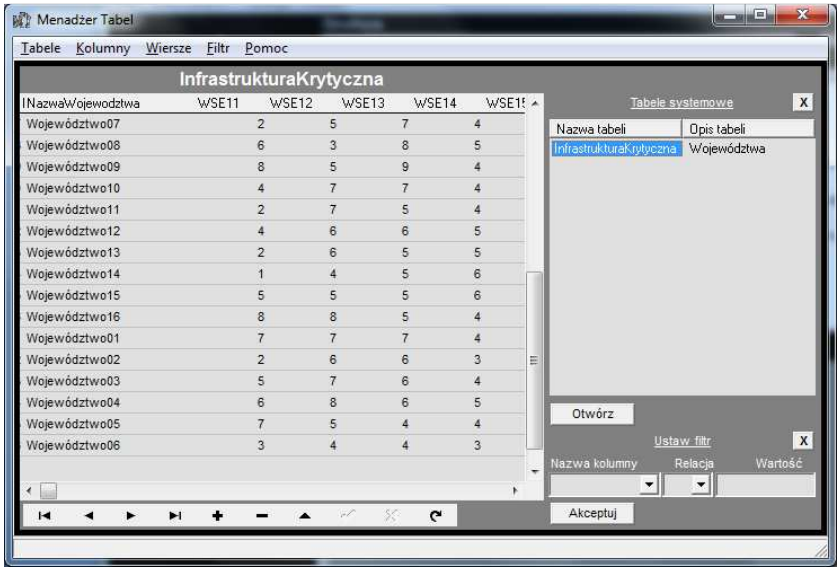
4. Menadżer relacji systemowych



5. Menadżer relacji tabel



6. Menadżer tabel z ocenami eksperckimi



ZAŁĄCZNIK 3.
PROCEDURY KALKULACYJNE

1. Wycinek kodu źródłowego modułu kalkulacyjnego

```
TList * POT_FunkcjaTAX(TList *aKO,TList *aKZD)
{

  float lSuma;
  float lSrednia;
  float lSumaRP;
  int   i,j;
  float *lWSO;
  TList *lKolekcjaWyjsciowa;

  lKolekcjaWyjsciowa = new TList();
  if (aKO->Count==0)
   return lKolekcjaWyjsciowa;

  for (i=0;i< (((TCechyObiektu*)aKO->Items[0]))->cCechy->Count;i++) {
   lSuma = 0;
   for (j=0;j<aKO->Count;j++){
    lSuma =lSuma + ((TWartoscCechy*)((TCechyObiektu*)aKO->Items[j])->cCechy->Items[i])->cWartoscCechy;
   }
   lSrednia = lSuma / aKO->Count;
   for (j=0;j<aKO->Count;j++){
    if (lSrednia == 0)
       ((TWartoscCechy*)((TCechyObiektu*)aKO->Items[j])->cCechy->Items[i])->cWyliczonaCechaUnormowana = 0;
    else{
     if (((TWartoscCechy*)((TCechyObiektu*)aKO->Items[j])->cCechy->Items[i])->cWartoscCechy == 0)
       ((TWartoscCechy*)((TCechyObiektu*)aKO->Items[j])->cCechy->Items[i])->cWyliczonaCechaUnormowana = 0;
     else
       ((TWartoscCechy*)((TCechyObiektu*)aKO->Items[j])->cCechy->Items[i])->cWyliczonaCechaUnormowana =
       ((TWartoscCechy*)((TCechyObiektu*)aKO->Items[j])->cCechy->Items[i])->cWartoscCechy / lSrednia;
    }
   }
  }

  lSumaRP = 0;
  for (j=0;j<aKZD->Count;j++){
   lSumaRP = lSumaRP + ((TZmienneDecyzyjne*)aKZD->Items[j])->cRP;
  }
  for (i=0;i<aKO->Count;i++){
   lWSO = new float;
   *lWSO = 0;
   for(j=0;j< ((TCechyObiektu*)aKO->Items[i])->cCechy->Count;j++){
    if(((TWartoscCechy*)((TCechyObiektu*)aKO->Items[i])->cCechy->Items[j])->cWyliczonaCechaUnormowana == 0)
     *lWSO = *lWSO + 0;
    else
     *lWSO = *lWSO + ((TZmienneDecyzyjne*)aKZD->Items[j])->cRP * pow(((TWartoscCechy*)
     ((TCechyObiektu*)aKO->Items[i])->cCechy->Items[j])->cWyliczonaCechaUnormowana ,
      (float)((TZmienneDecyzyjne*)aKZD->Items[j])->cSDN);
   }
   *lWSO = *lWSO / lSumaRP;
   lKolekcjaWyjsciowa->Add(lWSO);
  }
  return lKolekcjaWyjsciowa;
}
```

ZAŁĄCZNIK 4.
MODEL DANYCH