ANDRZEJ ŻEBROWSKI

ZARZĄDZANIE KRYZYSOWE ELEMENTEM BEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ

WYDAWNICTWO NAUKOWE
UNIWERSYTETU PEDAGOGICZNEGO
KRAKÓW

ZARZĄDZANIE KRYZYSOWE ELEMENTEM BEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ

Uniwersytet Pedagogiczny
im. Komisji Edukacji Narodowej
w Krakowie

Prace Monograficzne nr 627

ANDRZEJ ŻEBROWSKI

ZARZĄDZANIE KRYZYSOWE ELEMENTEM BEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ

WYDAWNICTWO NAUKOWE
UNIWERSYTETU PEDAGOGICZNEGO
KRAKÓW 2012

Recenzenci
prof. zw. dr hab. Jan Szreniawski
prof. zw. dr hab. Eugeniusz Zieliński

redaktor prowadzący Zuzanna Czarnecka
projekt okładki Janusz Schneider

ISSN 0239-6025
ISBN 978-83-7271-746-7

Wydawnictwo Naukowe UP
Redakcja/Dział Promocji
30-084 Kraków, ul. Podchorążych 2
tel./faks 12 662-63-83, tel. 12 662-67-56
e-mail: wydawnictwo@up.krakow.pl

Zapraszamy na stronę internetową:
http://www.wydawnictwoup.pl

układ typograficzny, łamanie Jadwiga Czyżowska-Maślak
druk i oprawa Zespół Poligraficzny UP, zam. 63/12

Wstęp

Po upadku bipolarnego podziału świata, w obliczu postępującej globalizacji problem bezpieczeństwa narodowego i zbiorowego wymaga innowacyjnego podejścia, w tym zarządzania kryzysowego z uwzględnieniem zmian położenia geopolitycznego, praktycznie każdego z państw. Tym złożonym i wzajemnie powiązanym procesom towarzyszą zarówno szanse, jak i zagrożenia, z przewagą tych drugich.

Jednobiegunowy układ sił na arenie międzynarodowej z dominującą pozycją Stanów Zjednoczonych, przy jednoczesnym lekceważeniu innych uczestników stosunków międzynarodowych, stanowi zagrożenie dla międzynarodowej społeczności. Rywalizacja na płaszczyźnie naukowej, gospodarczej i wojskowej, której towarzyszy wszechobecna globalizacja i wyścig zbrojeń, w tym produkcji broni masowej zagłady, są przyczyną istotnych zmian i zawirowań w otoczeniu zewnętrznym i wewnętrznym państw. Zwiększający się dystans w rozwoju, przede wszystkim gospodarczym, jest źródłem zależności większości od stanu posiadania mniejszości. Państwa dominujące w procesie decyzyjnym wykorzystują swoją pozycję na arenie międzynarodowej, w tym w gremiach organizacji międzynarodowych (powszechnych i regionalnych), poprzez stosowanie szerokiego wachlarza środków wymuszając na państwach słabych jednostronne podporządkowanie.

> Światowa Organizacja Handlu, Międzynarodowy Fundusz Walutowy, Bank Światowy tworzą faktyczny rząd gospodarczy w świecie podporządkowany USA, który nie podlega kontroli i nie ma nic wspólnego z demokratycznym ładem. Liberalizacja handlu światowego przysparza korzyści krajom bogatym i straty – biednym. Największe zyski osiągają USA i Unia Europejska, bo kraje zależne otworzyły dla nich swoje rynki, a kraje mocarstwowe im je zamknęły. Globalna gospodarka stała się globalną niesprawiedliwością dla świata. Kapitał globalny doprowadza wszędzie do totalnego chaosu gospodarczego przez deregulację rynku, finansów, zatrudnienia (łatwość zwalniania i przyjmowania do pracy, dowolne umowy o pracę), ochrony socjalnej, budżetu państwa, edukacji, zdrowia, kultury, sądownictwa, bezpieczeństwa wewnętrznego i zewnętrznego[1].

Tym samym rola państw silnych pod względem gospodarczym czy organizacji międzynarodowych sprowadza się do stopniowego uzależnienia pod wzglę-

[1] Z. Narski, *O dyktaturze kapitału globalnego*, Toruń 2004, s. 10.

dem politycznym, gospodarczym, finansowym i wojskowym. Istniejący dystans między Bogatą Północą a Biednym Południem jeszcze bardziej się pogłębia, czego efektem jest narastająca bieda i głód, którym niejednokrotnie towarzyszy przemoc i masowe migracje.

Jesteśmy również świadkami

> rozwoju zjawisk paradoksalnie odwrotnych w sferze społecznej, nasiliły się bowiem narodowe tendencje separatystyczne. Powstało wiele państw nowych, z których wiele stanowi zagrożenie dla pokoju w swoich regionach, gdyż nadal żyje w nich konglomerat grup etnicznych i mniejszości narodowych różniących się kulturą, językiem, religią i stanem posiadania. […] Na problemy mniejszości etnicznych i narodowych nakładają się problemy masowych fal uchodźstwa i migracji z powodu suszy, głodu, wojen domowych i innych katastrof[2].
>
> Najbardziej konfliktogennym czynnikiem jest połączenie fanatyzmu religijnego z szowinizmem narodowym, ponieważ […] różnorodność narodowościowa i wyznaniowo-kulturowa staje się zazwyczaj siłą odśrodkową. Jeśli nałoży się na to zróżnicowanie rozwoju przemysłowo-gospodarczego i poziomu życia, wówczas wyraźnie zarysowuje się rozbieżność aspiracji i dążeń, która wcześniej czy później doprowadzi do walki z zastosowaniem przemocy[3].

Źródeł zagrożeń dla bezpieczeństwa państwa należy upatrywać zarówno w jego otoczeniu zewnętrznym, jak i wewnętrznym. Współczesne stosunki międzynarodowe przy znacznym wysiłku zarówno podmiotów państwowych, jak i pozapaństwowych dalekie są od wzajemnego zrozumienia, partnerskiej współpracy, suwerennego traktowania podmiotów i woli poszukiwania consensusu. W tych stosunkach widoczne są sprzeczne dążenia i aspiracje, brak woli zrozumienia i porozumienia stron, niekiedy niechęć, a nawet izolacja, wywieranie nacisku przez zastosowanie przemocy pozamilitarnej, a nawet militarnej. Następstwa tak prowadzonej polityki przez państwa silne (organizacje międzynarodowe) odczuwa przede wszystkim ludność konkretnego państwa, a nawet regionu. Życie codzienne dostarcza dowodów na to, że sytuacja jest bardziej skomplikowana, a chorobliwa chęć dominacji jednostek i urojone posłannictwo poważnie ograniczają wykorzystanie rozsądku i dróg negocjacji[4].

Zagrożeniem dla bezpieczeństwa państwa jest utrudnianie lub utrata warunków dla swobodnego rozwoju. Zagrożenia te mogą powstać w sferach: politycznej, społecznej, ekonomicznej, psychologicznej, kulturowej, etnicznej, wyznaniowej, językowej, ekologicznej, terytorialnej, historycznej, wojskowej. Mogą one występować w dowolnej konfiguracji lub jednocześnie w kilku obszarach. Przyjmuje się, że ta grupa zagrożeń jest nazywana zagrożeniami o charakterze pozamilitarnym. Szczególnym rodzajem zagrożenia dla bezpieczeństwa państwa są zagrożenia militarne, których źródeł należy upatrywać w sferze militarnej i pozamilitarnej, gdzie jedna ze stron broni swoich interesów na drodze zbrojnej.

[2] J. Gołębiewski, *Bezpieczeństwo narodowe RP*, „Towarzystwo Wiedzy Obronnej" 1999, nr 1, s. 12.

[3] S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, s. 24.

[4] Gołębiewski J., op. cit., s. 11.

W związku z powyższym źródła, które stanowią zagrożenia dla bezpieczeństwa państwa, dzieli się na wewnętrzne i zewnętrzne, natomiast ze względu na charakter na pozamilitarne i militarne[5]. Pamiętać należy o tym, że zagrożenia bez względu na źródła i charakter są zawsze ponadczasowe, co oznacza, że występowały w przeszłości, są obecne i będą zaznaczały swoją obecność w przyszłości. Występują one z różnym nasileniem w czasie i przestrzeni, odpowiednio do skali pojawiających się sprzeczności interesów lub wartości uznawanych za nadrzędne[6].

Zmiany cywilizacyjne stanowią zagrożenia dla bezpieczeństwa każdego państwa, w tym i dla Polski. Oczywiście ich skala i dynamika są zróżnicowane. Mogą one powstać na tle napięć i sprzeczności interesów w stosunkach społeczno-politycznych, finansowo-gospodarczych, narodowościowo-etnicznych, religijno-kulturowych, ekologicznych i wojskowych. Przemawia za tym wielopłaszczyznowy splot uwarunkowań zewnętrznych i wewnętrznych:

- negowanie ustaleń traktatowych będących skutkiem zakończenia II wojny światowej, a także eksponowanie zaszłości historycznych,
- postępująca anarchizacja życia społeczno-politycznego w otoczeniu bliższym i dalszym państwa,
- aspiracje mocarstwowe państw silnych pod względem gospodarczym (Chiny, Japonia, RFN),
- aspiracje mocarstwowe państw posiadających broń masowego rażenia,
- brak kontroli międzynarodowej nad proliferacją broni masowego rażenia, technologiami do jej produkcji i środków przenoszenia,
- nasilające się zjawiska nacjonalizmu, szowinizmu i fundamentalizmu religijnego oraz terroryzmu międzynarodowego,
- brak racjonalnych zachowań ze strony grup społecznych, przede wszystkim elit politycznych (spadek ich wiarygodności), wobec zagrożeń bezpieczeństwa państwa,
- brak skuteczności organizacji międzynarodowych w utrzymaniu pokoju i bezpieczeństwa międzynarodowego,
- postępująca erozja systemu obronnego państwa,
- rozwój przestępczości zorganizowanej o charakterze transgranicznym,
- proces prywatyzacji i reprywatyzacji,
- ubożenie społeczeństwa, spadek płac realnych, postępujące bezrobocie,
- nasilanie się dążeń rewindykacyjnych,
- zagrożenia naturalne, klęski żywiołowe, awarie, katastrofy techniczne itp.

Państwa w procesie budowania bezpieczeństwa swoich obywateli patrzą przez pryzmat nie tylko pokoju i wojny, ale i trzeciej formy, jaką jest kryzys. Brak wojny nie oznacza, że mamy do czynienia z pokojem. Współczesne społeczeństwa stoją wobec wielu wyzwań, gdzie szanse i zagrożenia wymuszają przeciwstawienie się tym ostatnim. Oznacza to, że bezpieczeństwo należy przygotować, a w tym celu trzeba konsekwentnie realizować określone zadania, które powinny

[5] S. Dworecki, op. cit., s. 23.

[6] Ibidem, s. 25.

zabezpieczyć spokojny i zrównoważony rozwój w każdej sytuacji. Zadania te obejmują m.in.:

- przygotowanie systemu obronnego państwa,
- przygotowanie sprawnego i skutecznego systemu ochrony ludności (zarządzanie kryzysowe),
- zabezpieczenie sprawnego funkcjonowania struktur państwa w sytuacji zagrożenia (sytuacja kryzysowa, kryzys),
- przygotowanie w zależności od zagrożeń i wyzwań zasobów informacyjnych, ludzkich, materiałowych, finansowych,
- zintegrowanie wszystkich sił politycznych dla realizacji celów bezpieczeństwa.

Służy temu właściwie zbudowany system bezpieczeństwa państwa, czyli skoordynowany wewnętrznie zbiór elementów organizacyjnych, ludzkich i materiałowych, ukierunkowanych na przeciwdziałanie wszelkim zagrożeniom państwa, a w szczególności politycznym, gospodarczym, psychospołecznym, ekologicznym i militarnym[7]. System bezpieczeństwa państwa jest dynamiczny i zależy od zmian zachodzących w otoczeniu zewnętrznym i wewnętrznym. Na jego strukturę składają się systemy (podsystemy) sektorowe, jak system obronny państwa czy system zarządzania kryzysowego.

Monografia niniejsza poświęcona jest problematyce ochrony ludności w obliczu zagrożeń pozamilitarnych u progu XXI wieku. Jej celem jest przybliżenie wieloaspektowej problematyki związanej z zarządzaniem kryzysowym.

W rozdziale *Bezpieczeństwo państwa* poruszone zostały zagadnienia dotyczące istoty i pojęcia bezpieczeństwa, które wraz z zakończeniem tzw. zimnej wojny znacznie się poszerzyło. Nabiera ono ciągle nowego znaczenia, co oznacza, że zwiększa się jego pojemność, a także możliwość interpretacji. Kolejna kwestia to typologia bezpieczeństwa, która obecnie nie odnosi się wyłącznie do czynnika militarnego i realizacji polityki zagranicznej. Wyróżnia się m.in. bezpieczeństwo gospodarcze, finansowe, informacyjne, żywnościowe, energetyczne, dostępu do surowców naturalnych czy słodkiej wody.

Rozdział noszący tytuł *Podstawy zarządzania kryzysowego* poświęcony został rozważaniom na temat terminologii: kryzys, sytuacja kryzysowa, zarządzanie kryzysowe. Omówione również zostały zasady zarządzania kryzysowego, etapy i system zarządzania kryzysowego na wszystkich poziomach bezpieczeństwa państwa.

W rozdziale *Zagrożenia kryzysowe państwa* zwraca się uwagę na pojecie i klasyfikację zagrożeń. Przemiany zachodzące w otoczeniu wewnętrznym i zewnętrznym (bliższym i dalszym) państwa generują szerokie spektrum zagrożeń o charakterze pozamilitarnym (militarnym), które mają zróżnicowane podłoże, a ich skala i dynamika zależy m.in. od wrażliwości i skuteczności podejmowanych przez społeczeństwo działań. Omówione tu zostały zagrożenia naturalne, techniczne, społeczne i militarne.

[7] *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. W. Łepkowski, Warszawa 2009, s. 139.

W rozdziale *Podstawy prawne zarządzania kryzysowego* zaprezentowane zostały przepisy regulujące zarządzanie kryzysowe z uwzględnieniem prawa międzynarodowego, co jest m.in. następstwem przyjęcia Polski do struktur Sojuszu Północnoatlantyckiego i Unii Europejskiej. W procesie dostosowania prawa krajowego do prawa unijnego strona Polska uregulowała kwestie związane z zarządzaniem kryzysowym przy uwzględnieniu położenia geopolitycznego naszego państwa.

W rozdziale *Podsystem informacyjny* omówiono znaczenie informacji dla skutecznego zarządzania, w tym kryzysowego. Informacja wartościowa i dostarczona uprawnionym podmiotom we właściwym czasie pozwala na podjęcie działań wyprzedzających, co m.in. przekłada się na minimalizację ewentualnych negatywnych skutków lub niedopuszczenie do powstania sytuacji kryzysowej. W procesie zarządzania kryzysowego istotne są źródła informacji międzynarodowe i krajowe. Ich stały monitoring stanowi system wczesnego ostrzegania i alarmowania, co ma istotne znaczenie dla prowadzenia skutecznych działań.

W rozdziale *Podsystem planowania* przedstawione zostało znaczenie tego podsystemu dla zarządzania kryzysowego na poziomach krajowym, wojewódzkim, powiatowym i gminnym. Scharakteryzowano poszczególne plany, jak: *Raport o zagrożeniach bezpieczeństwa narodowego*, który stanowi podstawę dalszych przedsięwzięć planistycznych, Narodowy Program Ochrony Infrastruktury Krytycznej, Plany ochrony infrastruktury krytycznej, Krajowy Plan Zarządzania Kryzysowego, plany logistyczne i plany obrony cywilnej.

W rozdziale *Podsystem kierowania* wskazane zostały podmioty uprawnione do kierowania w zarządzaniu kryzysowym, ze szczególnym wskazaniem na zakres realizowanych zadań i posiadane kompetencje. Do tych podmiotów zalicza się: Radę Ministrów i Prezesa Rady Ministrów, ministra właściwego do spraw wewnętrznych, ministrów i kierowników urzędów centralnych, wojewodów, starostów, wójtów (burmistrzów, prezydentów miast).

W rozdziale *Podsystem wykonawczy* omówiono istotę tego podsystemu, a ponadto: System powiadamiania i alarmowania, System powiadamiania ratunkowego, Krajowy System Ratowniczo-Gaśniczy, Państwowe Ratownictwo Medyczne, udział obrony cywilnej i Sił Zbrojnych Rzeczypospolitej Polskiej w zarządzaniu kryzysowym, podstawy prawne i zadania.

W rozdziale *Inni uczestnicy podsystemu wykonawczego* wskazane zostały pozostałe podmioty, które z uwagi na usytuowanie w strukturze władzy wykonawczej, realizowane zadania i posiadane uprawnienia również biorą aktywny udział w zarządzaniu kryzysowym. Do tych uczestników zalicza się: Policję, Żandarmerię Wojskową, Straż Graniczną, Biuro Ochrony Rządu, a także służby specjalne, które z uwagi na realizowaną funkcję informacyjną zajmują szczególną pozycję w procesie zarządzania kryzysowego.

Rozdział *Ochrona infrastruktury krytycznej państwa* ma ścisły związek z postępem naukowo-technicznym, gdzie technika teleinformatyczna obecna jest praktycznie we wszystkich sferach działania państwa i człowieka. Jej wpływ na zdolność realizowania szerokiego spektrum zadań wynikających z funkcji państwa

oznacza ich zależność od sprawnie działającej infrastruktury. W rozdziale tym wskazane zostały elementy infrastruktury krytycznej, organy uprawnione do jej ochrony, ze szczególnym wskazaniem na pozycję Agencji Bezpieczeństwa Wewnętrznego.

Rozdział ostatni, *Ochrona cyberprzestrzeni państwa* nawiązuje do rozdziału poprzedniego, ponieważ sprawne funkcjonowanie infrastruktury krytycznej państwa, to bezpieczna cyberprzestrzeń będąca (obok ziemi, powietrza, wody i przestrzeni kosmicznej) kolejnym obszarem rywalizacji człowieka. Wspomniana technika teleinformatyczna to współzależność od cyberprzestrzeni. Omówione zostały pojęcie i istota cyberprzestrzeni, podstawy prawne i organy właściwe do jej ochrony.

W monografii zostały omówione przepisy prawa międzynarodowego i krajowego, które odnoszą się do zarządzania kryzysowego. Przynależność Polski do Unii Europejskiej uzasadnia dostosowanie prawa krajowego do przepisów unijnych, co zostało uwzględnione w rozdziale 4. Z kolei obowiązujące regulacje prawa krajowego wskazują organy (kierujące i wykonawcze), ich zadania i uprawnienia w realizacji złożonych przedsięwzięć dotyczących zarządzania kryzysowego. Podstawę prowadzonych rozważań stanowiła ustawa z dnia 26 kwietnia 2007 roku *O zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.). Obok aktów prawnych została wykorzystana literatura przedmiotu, która porusza problematykę zarządzania kryzysowego w obliczu zagrożeń pozamilitarnych. Na uwagę zasługują m.in. prace: Stanisława Dworeckiego *Od konfliktu do wojny*, Warszawa 1996; Andrzeja Żebrowskiego *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003)*, Kraków 2005; Krzysztofa Liedela, Jarosława Prońko, Bernarda Wiśniewskiego (red.) *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, Bielsko-Biała–Warszawa 2007; Krzysztofa Ficonia *Inżynieria zarządzania kryzysowego. Podejście systemowe,* Warszawa 2007; Wiesława S. Krzeszowskiego (red.) *Wojsko w niemilitarnych sytuacjach kryzysowych*, Warszawa 2008; Eugeniusza Nowaka *Zarządzanie logistyczne w sytuacjach kryzysowych*, Warszawa 2008; Katarzyny Sienkiewicz-Małyjurek i Zygmunta Niczyporuka *Bezpieczeństwo publiczne. Zarys problematyki*, Gliwice 2010; Witolda Lidwy, Wiesława Krzeszowskiego, Wojciecha Więcka *Zarządzanie w sytuacjach kryzysowych*, Warszawa 2010; Witolda Skomry *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Warszawa 2010; Stanisława Kwiatkowskiego *Zarządzanie bezpieczeństwem w sytuacjach kryzysowych*, Pułtusk 2011; Grzegorza Sobolewskiego (red.) *Organizacja i funkcjonowanie centrum zarządzania kryzysowego*, Warszawa 2011.

Monografia przeznaczona jest dla teoretyków i praktyków zajmujących się problemami zarządzania kryzysowego w państwie.

ROZDZIAŁ 1

Bezpieczeństwo państwa

1.1. Istota i pojęcie bezpieczeństwa państwa

Globalne środowisko bezpieczeństwa międzynarodowego charakteryzuje się chaosem, który objawia się osłabieniem znaczenia państwa narodowego, niestabilną wewnętrzną sytuacją społeczno-polityczną w wielu państwach, nasilaniem się konfliktów o podłożu etnicznym, religijnym i narodowościowym, rozwojem transgranicznej przestępczości zorganizowanej i terroryzmu międzynarodowego, masową migracją ludności (legalną i nielegalną), rozprzestrzenianiem broni masowego rażenia, technologii do jej produkcji i środków przenoszenia, stopniowym uzależnianiem państw słabo rozwiniętych od państw silnych pod względem gospodarczym, powiększającym się biegunem światowej biedy, pojawianiem się nowych aktorów globalnych, dominacją absolutnej mniejszości nad absolutną większością, dla której brak jest alternatywy itp. Zjawiska te i towarzyszące im wydarzenia wymuszają na społeczności międzynarodowej jakościowo nowe spojrzenie na postrzeganie bezpieczeństwa, nie tylko w kategoriach militarnych.

Dla bezpieczeństwa Polski powyższe zjawiska, a także wyjście z systemu państw socjalistycznych i Układu Warszawskiego oraz przemiany systemowe zapoczątkowane pod koniec lat dziewięćdziesiątych XX wieku mają istotne znaczenie. Wymagają zmagania się z wieloma decyzjami i sytuacjami, najczęściej o negatywnym charakterze, na co społeczeństwo nie zostało przygotowane. Stanowi to źródło niezadowolenia społecznego, a występujący partykularyzm partii politycznych przyczynia się m.in. do obniżenia poziomu bezpieczeństwa na wszystkich poziomach zarządzania bezpieczeństwem państwa.

Procesy zachodzące w świecie i w Europie (zwłaszcza w ostatnich latach oraz mogące wystąpić w przyszłości) prowadzą do sytuacji, w której następują przeobrażenia ustrojowe, społeczno-polityczne o trudnych do przewidzenia następstwach.

*

Bez względu na epokę i ustrój zachowaniem państwa na arenie międzynarodowej rządzą dwa dążenia pierwotne, które odzwierciedlają fundamentalne interesy narodowe: pierwszym jest wola przetrwania, zachowania odrębnego istnienia i tożsamości, co w kategoriach bezpieczeństwa oznacza obronę suwerenności i integralności terytorialnej, drugim jest dążenie do rozwoju własnej potęgi, niekoniecznie wojskowej, i nie tylko w stosunku do innych państw. Kryterium naczelnym jest, a przynajmniej powinno być, chronienie i pomnażanie dobra własnego narodu oraz budowa jego potęgi[1].

> Każde państwo i społeczeństwo inaczej odczuwa swoje potrzeby i definiuje interesy, których realizacja jest niezbędna dla zapewnienia bezpieczeństwa. Zależy to od wielu czynników: sytuacji międzynarodowej, stopnia aspiracji i oddziaływania danego podmiotu na stosunki międzynarodowe, uwarunkowań geostrategicznych, historycznych, etnicznych, kulturowych i innych[2].

Aktualnie pojęcie bezpieczeństwa odnosi się prawie do wszystkich dziedzin rozwoju społecznego, gospodarczego, politycznego, naukowego, technicznego, technologicznego, demograficznego, kulturowego itd.[3]

> W literaturze traktującej o stosunkach międzynarodowych i bezpieczeństwie spotyka się wiele definicji dotyczących bezpieczeństwa narodowego i międzynarodowego. Każda z nich wskazuje, że bezpieczeństwo – podobnie jak pokój między narodami czy też pozycja państwa w społeczności międzynarodowej – nie jest stanem, który można osiągnąć, utrzymać raz na zawsze[4].

Oznacza to, że bezpieczeństwo jest procesem, który pod wpływem czynników wewnętrznych i zewnętrznych ewoluuje. Wymaga zaangażowania nie tylko poszczególnych państw, ale i organizacji międzynarodowych, podejmowania działań mających na celu utrzymanie pokoju mimo istnienia wielu zagrożeń.

W najbardziej dosłownym znaczeniu bezpieczeństwo jest właściwie identyczne z pewnością i oznacza brak zagrożenia fizycznego albo ochronę przed nim[5].

> Należy jednak postrzegać bezpieczeństwo jako stan, który daje poczucie pewności i gwarancje jego zachowania oraz szansę na doskonalenie. Jedna z podstawowych potrzeb człowieka to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, np. zdrowia, pracy, szacunku, uczuć, dóbr materialnych[6].

Bezpieczeństwo jest formą istnienia danego stanu rzeczy osiąganą przez eliminowanie, unikanie i przeciwstawianie się zagrożeniom w celu prolongaty jego

1 S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, s. 14.

2 S. Kamiński, *Bezpieczeństwo Polski: problemy i wyzwania*, „Biuletyn Towarzystwa Wiedzy Obronnej" [b.r.wyd.], s. 6.

3 J. Gołębiewski, *Bezpieczeństwo narodowe RP,* „Towarzystwo Wiedzy Obronnej" 1999, nr 1, s. 9.

4 T. Jemioło, A. Dawidczyk, *Wprowadzenie do metodologii badań bezpieczeństwa*, Warszawa 2007, s. 36.

5 J.W. Gould, W.L. Kolb, *A dictionary of the Social Science*, London 1964, s 629.

6 *Słownik terminów z zakresu dowodzenia i zarządzania*, red. W. Łepkowski, Warszawa 2000, s. 17.

istnienia[7]. Bezpieczeństwo można również postrzegać jako stan równowagi między zagrożeniem wywołanym możliwością zaistnienia konfliktu a potencjałem obronnym państwa[8]. W innym ujęciu „jest to stan, którego utrzymanie jest niezbędne z punktu widzenia funkcjonowania […] państwa, mającego zabezpieczyć interesy zarówno jednostki, jak i społeczeństwa, interesy o charakterze publicznym i prywatnym (w określonych okolicznościach)"[9]. W odniesieniu do państwa bezpieczeństwo najczęściej określane jest jako stan gotowości państwa lub zbioru państw do przeciwstawienia się sytuacji kryzysowej[10]. Na bezpieczeństwo składają się dwa zasadnicze elementy: gwarancja nienaruszalnego przetrwania podmiotu, swoboda jego rozwoju. Nie są one jednak absolutnymi determinantami i odnoszą się do podstawowego wymiaru bezpieczeństwa[11].

Nauki społeczne bezpieczeństwo traktują jako zdolność przetrwania, niezależność, tożsamość czy też pewność rozwoju.

> W analizach dotyczących bezpieczeństwa rozpatruje się występowanie dwóch negatywnie wartościowanych zjawisk, do których zalicza się wyzwania i zagrożenia. Przez wyzwania rozumie się pojawienie się nowych sytuacji, w których występują niezbywalne potrzeby wymagające sformułowania odpowiedzi i podjęcia stosownych działań przez państwo w celu zapewnienia określonego stanu bezpieczeństwa. Nierozwiązane wyzwania mogą dopiero przekształcić się w zagrożenia dla bezpieczeństwa państwa[12].

Bezpieczeństwo państwa, pojmowane jako brak zagrożeń oraz ochrona przed zagrożeniami[13], jest bezpośrednio związane z bezpieczeństwem narodowym czy społecznym. „Pojęcia te w wielu aspektach są ze sobą zbieżne, a często nawet stosowane zamiennie. Bezpieczeństwo państwa należy jednak ujmować w sposób całościowy, gdyż obejmuje ono całokształt stosunków zarówno wewnętrznych, jak i zewnętrznych"[14]. Bezpieczeństwo narodowe (państwa) jest jednym z podstawowych wymiarów bytu i rozwoju społeczeństwa, określonym stosunkiem skali zagrożeń do wielkości potencjału obronnego, jaki społeczeństwo może

[7] J. Świniarski, *Filozofia bezpieczeństwa personalnego i strukturalnego próbą kompleksowego ujęcia wyzwań współczesności*, [w:] *Filozofia bezpieczeństwa personalnego i strukturalnego*, red. R. Rosy, Warszawa 1993, s. 188.

[8] W. Stankiewicz, *Konflikt i bezpieczeństwo – kilka uwag teoretycznych*, „Zeszyty Naukowe AON" 1991, nr 3/4, s. 45.

[9] M. Karpiniuk, *Bezpieczeństwo narodowe a bezpieczeństwo międzynarodowe*, [w:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej w świetle prawa wewnętrznego i międzynarodowego*, red. R. Szynowski, M. Karpiuk, Warszawa 2011, s. 281.

[10] T. Jemioło, A. Dawidczyk, op. cit., s. 36.

[11] Lipski S., *Zarządzanie bezpieczeństwem – wybrane kwestie terminologiczne*, [w:] *Próba identyfikacji współczesnych zagrożeń dla bezpieczeństwa i porządku publicznego w Polsce*, red. K. Rajchel, Warszawa 2006, s. 143.

[12] T. Jemioło, A. Dawidczyk, op. cit., s. 36.

[13] Z. Nowakowski, S. Ciepielewski, *Wymiar społeczny bezpieczeństwa państwa*, [w:] *Bezpieczeństwo osobiste obywatela w RP*, red. K. Rajchel, Warszawa 2007, s. 131.

[14] M. Karpiniuk, op. cit., s. 282.

przeciwstawić tym zagrożeniom[15]. Można je zdefiniować jako cechę takiego układu stosunków zewnętrznych i wewnętrznych państwa, w którym nie występują żadne zagrożenia lub są one neutralizowane przez potencjał obronny[16].

Bezpieczeństwo narodowe stanowi wartość nadrzędną pośród innych celów narodowych i warunkuje ich realizację oraz dotyczy wartości narodowych mierzonych w kategoriach:

- interesów życiowych, wartości, które decydują o trwałości państwa, dobrobycie narodowym i rozwoju, jego tożsamości narodowej, poczuciu bezpieczeństwa we wszystkich sferach życia społecznego,
- interesów strategicznych,
- wartości nie mających bezpośredniego wpływu na bezpieczeństwo państwa, lecz stanowiących o przestrzeganiu norm prawa międzynarodowego, tak w wymiarze politycznym, gospodarczym i militarnym, jak i humanitarnym,
- określających poziom swobody w osiąganiu tych celów, który zależy od pozycji państwa na arenie międzynarodowej i możliwości zaspokojenia oczekiwań społeczeństwa w aspekcie materialnym i psychospołecznym oraz od charakteru wyzwań i zagrożeń bezpieczeństwa narodowego,
- procesu obejmującego różnorodne zabiegi w obszarze stosunków międzynarodowych i wewnętrznych oraz przedsięwzięcia ochronne i obronne mające stworzyć korzystne warunki funkcjonowania państwa na arenie międzynarodowej i wewnętrznej oraz przeciwstawić się wyzwaniom i zagrożeniom bezpieczeństwa narodowego[17].

Tym samym bezpieczeństwo państwa będące jego podstawowym celem jest dominujące nad celami cząstkowymi. Dlatego dążenie do celów cząstkowych wymaga poczucia bezpieczeństwa i braku zagrożeń. Jest to cel idealny, praktycznie nie do osiągnięcia. W związku z tym należy mieć świadomość, że bezpieczeństwo nie jest wszystkim, lecz bez bezpieczeństwa wszystko jest niczym[18]. Należy przy tym pamiętać, że jednym z wyznaczników bezpieczeństwa państwa jest środowisko międzynarodowe, które ma istotny wpływ na bezpieczeństwo wewnętrzne poszczególnych państw. Te dwa środowiska państwa, wewnętrzne i zewnętrzne (bliższe i dalsze), pozostają we wzajemnej współzależności, oczywiście w zróżnicowanym stopniu.

Bezpieczeństwo międzynarodowe w tradycyjnym ujęciu odnosi się do relacji między państwami występującymi samodzielnie lub reprezentowanymi w ramach systemów i instytucji międzynarodowych. W niedalekiej przeszłości odnosiło się to do realizacji polityki zagranicznej i bezpieczeństwa militarnego. Obecnie procesy globalizacyjne rozszerzyły spektrum zjawisk, do których może odnosić się to pojęcie. W tym aspekcie bezpieczeństwo międzynarodowe wyraża

[15] R. Wróblewski, *Wybrane problemy diagnozy bezpieczeństwa narodowego*, „Zeszyty Naukowe AON" 1991, nr 3/4, s. 69.

[16] M. Sułek, *Potencjał gospodarczo-obronny – pojęcie, pomiar, decyzje*, Warszawa 1993, s. 135.

[17] B. Ferenc, *O bezpieczeństwie w Europie*, „Myśl Wojskowa" 1996, nr 2 s. 143.

[18] K. Naumann, *Die Bundeswehr in einer Welt im Umbruch*, Berlin 1994, s. 37.

szerszą treść niż bezpieczeństwo narodowe, gdyż określa zarówno zewnętrzne aspekty bezpieczeństwa państwa, jak i przetrwania i funkcjonowania systemu międzynarodowego, którego celem jest zapewnienie bezpieczeństwa i pokoju zarówno w skali regionalnej, jak i globalnej[19].

Bezpieczeństwo międzynarodowe to brak obiektywnie istniejących zagrożeń i subiektywnych obaw oraz zgodne dążenie i działanie społeczności międzynarodowej na rzecz ochrony określonych wartości państwowych i pozapaństwowych (społecznych) za pomocą norm, instytucji i instrumentów zapewniających pokojowe rozstrzyganie sporów oraz tworzenie gospodarczych, społecznych, ekologicznych i innych przesłanek dynamicznej stabilności i eliminowania zagrożeń[20]. Tym samym bezpieczeństwo międzynarodowe ma wielostronny wymiar i odnosi się do innych obszarów bezpieczeństwa, jak bezpieczeństwo ekonomiczne, ekologiczne, energetyczne, informacyjne, walka ze zorganizowaną przestępczością i inne, które oddziałują na bezpieczeństwo poszczególnych państw.

Bezpieczeństwo międzynarodowe jest rezultatem uczestnictwa państw w systemie międzynarodowym, gdzie otoczenie zewnętrzne jest zarówno źródłem zagrożeń dla bezpieczeństwa wewnętrznego państwa, jak i gwarantem jego bezpieczeństwa.

Państwo z uwagi na swoje żywotne interesy tworzy i rozwija określone systemy bezpieczeństwa, które odpowiednio kształtowane i dostosowywane do zmieniającego się otoczenia wewnętrznego i zewnętrznego pozwalają na realizację celów strategicznych (zob. tabela 1).

Tabela 1. Systemy bezpieczeństwa państwa

Systemy bezpieczeństwa	
państwa	to skoordynowany wewnętrznie zbiór elementów: organizacyjnych, ludzkich i materiałowych ukierunkowanych na przeciwdziałanie wszelkim zagrożeniom państwa, a w szczególności politycznym, gospodarczym, psychospołecznym, ekologicznym i militarnym[1],
obronności	to zbiór uporządkowanych wewnętrznie i wzajemnie powiązanych elementów: ludzi, organizacji, urządzeń działających na rzecz zachowania bezpieczeństwa wojskowego (militarnego) państwa[2]; w innym ujęciu jest to wykorzystanie całego potencjału militarnego i niemilitarnego państwa do przeciwdziałania zewnętrznym zagrożeniom polityczno-militarnym, kryzysowym i wojennym[3],
zarządzania kryzysowego	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[4],
bezpieczeństwa i porządku publicznego	przeznaczony jest do zapewnienia ochrony życia, zdrowia, mienia i innych wartości przed bezprawnymi działaniami oraz ochrony zasad współżycia społecznego i stosunków regulowanych normami prawnymi i zwyczajami[5],

[19] D.J. Mierzejewski, *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*, Toruń 2011, s. 43.

[20] *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 14 i 15.

ochrony granic	ma na celu niedopuszczenie do nielegalnego ich przekraczania i przewożenia towarów (bez względu na ich jakość, rodzaj i przeznaczenie) bez zezwolenia, a także zapobieganie przenikaniu przez granice chorób zakaźnych lub materiałów niebezpiecznych[6],
ochrony systemów informacyjnych	służy przeciwdziałaniu zakłóceniom oraz zapewnieniu poprawnego funkcjonowania systemów zarządzania i kierowania w razie zakłócenia systemu obiegiem informacji[7],
ochrony państwa i jego porządku konstytucyjnego	jego celem jest rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa; rozpoznawanie, zapobieganie i wykrywanie przestępstw: szpiegostwa, terroryzmu, naruszenia informacji niejawnych, innych przestępstw godzących w bezpieczeństwo państwa; godzących w podstawy ekonomiczne państwa; korupcji osób pełniących funkcje publiczne; w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa; nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi w obrocie międzynarodowym oraz ściganie sprawców; wykonywanie funkcji krajowej władzy bezpieczeństwa[8].

1 *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 139; zob. też K. Nóżko, *Sztuka tworzenia przewagi w systemie obronnym RP*, Warszawa 1994, s. 16, który przez system obronny RP rozumie elementy potencjału obronnego własnego i ewentualnie sojuszniczego połączone celem politycznym, zapewniającym historycznie uwarunkowaną suwerenność i niepodległość narodu polskiego, jego prawa do integralności terytorialnej i nienaruszalności granic.

2 *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 141.

3 J. Wojnarowski, *System obronności państwa,* Warszawa 2005, s. 7.

4 Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.).

5 D.J. Mierzejewski, op. cit., s. 42.

6 Ibidem, s. 42.

7 Ibidem.

8 Ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (T. j.: Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.); ustawa z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182, poz. 1228) i inne obowiązujące przepisy prawa.

Źródło: Opracowanie własne na podstawie literatury

Wskazane systemy należy postrzegać jako podsystemy, które tworzą system bezpieczeństwa państwa.

Obecnie bezpieczeństwo nie jest postrzegane wyłącznie w kategoriach wojny i pokoju, ale coraz częściej uwzględnia się jego trzecią formę, którą jest kryzys. Kryzys ma zróżnicowane podłoże, co ma wpływ m.in. na jego skalę i negatywne następstwa. Państwa stojące w obliczu zagrożeń o charakterze asymetrycznym dla bezpieczeństwa wewnętrznego, regionalnego, a nawet globalnego, podejmują wiele rozwiązań natury prawno-organizacyjnej i humanitarnej, aby nie dopuścić do wystąpienia kryzysu lub zminimalizować jego negatywne następstwa.

Zdolność do zapewnienia bezpieczeństwa narodowego (państwa), tak jak każdy cel priorytetowy, jest związana ze strukturą i funkcjonowaniem państwa i zależy od ogólnej ich sprawności oraz efektywności. Ogólnie rzecz ujmując, skuteczność realizacji tego celu zależy od racjonalności struktur oraz kompetencyjności i zdolności elit poli-

tycznych do tworzenia, a następnie konsekwentnej realizacji długofalowych koncepcji strategicznego działania na rzecz bezpieczeństwa narodowego, również na płaszczyźnie stosunków międzynarodowych[21].

1.2. Typologia bezpieczeństwa państwa

Współczesna treść bezpieczeństwa odnosi się nie tylko do kwestii militarnych (wojskowych). W niedalekiej przeszłości bezpieczeństwo państwa postrzegane było wyłącznie w kategoriach bezpieczeństwa wojskowego, przez które rozumie się stan uzyskany w rezultacie działań odpowiednio zorganizowanych i wyposażonych sił zbrojnych oraz zawartych sojuszów wojskowych, a także posiadania koncepcji strategicznej wykorzystania będących w dyspozycji sił stosownie do zaistniałej sytuacji[22].

Należy jednak zaznaczyć, że „tradycyjne bezpieczeństwo narodowe (państwa) było utożsamiane przede wszystkim z siłą wojskową według uproszczonego schematu: zagrożenie to agresja (wojna), a bezpieczeństwo to obrona militarna. Jest oczywiste, że w rzeczywistości od niepamiętnych czasów bezpieczeństwo kształtowały również inne czynniki, obecnie coraz szerzej wyróżniane"[23]. Oznacza to, że „rozpatrywanie obecnie bezpieczeństwa narodowego (państwa) i możliwości jego zagrożenia tylko w kategoriach wojskowych (militarnych), nie wyczerpuje istoty problemu. Ma ono bowiem charakter interdyscyplinarny i wieloaspektowy. Można je odnieść do wszystkich dziedzin (funkcjonowania) państwa"[24].

> Czasy współczesne niosą poważne przewartościowania w życiu społecznym, rozwój techniki i jej zastosowania, mentalność ludności i wzrost zagrożeń cywilizacyjnych zmieniły zakres pojmowania bezpieczeństwa. Wspomniany aspekt wojskowy, do niedawna dominujący, ustępuje miejsca powoli innym – niemilitarnym. Funkcja bezpieczeństwa jest już nie tylko wolą przetrwania, ale także ochroną dobrobytu i swobodnego stylu bycia, swobód i tożsamości narodowej, religijnej, etnicznej itd. Świat się skurczył i bezpieczeństwo pod każdym względem stało się kategorią międzynarodową[25].

Obecne składniki bezpieczeństwa, to obok czynników politycznych i militarnych również czynniki gospodarcze i technologiczne, zasoby surowcowe, polityka w zakresie ekologii, demografii, spraw społecznych i humanitarnych. Na uwagę zasługują również czynniki energetyczne, ekonomiczne, społeczne,

[21] S. Dworecki, op. cit., s. 17.

[22] *Słownik terminów z zakresu bezpieczeństwa…*, op. cit., s. 16.

[23] R. Jakubczak, *Obrona narodowa w tworzeniu bezpieczeństwa III RP*, Warszawa 2004, s. 60.

[24] S. Dworecki, op. cit., s. 12.

[25] J. Gołębiewski, op. cit., s. 12 i 13.

żywnościowe, dostępu do słodkiej wody, informacyjne, kulturowe, etniczne, geopolityczne, infrastruktura krytyczna państwa i inne. Współczesne koncepcje bezpieczeństwa należy poszerzyć o sprawy związane z zachowaniem narodowej tożsamości oraz zapewnienia właściwego udziału w rozwoju cywilizacyjnym współczesnego świata[26]. Zyskał na znaczeniu także ludzki wymiar bezpieczeństwa, czyli poszanowanie podstawowych praw i swobód obywatelskich[27]. Bezpieczeństwo współcześnie jest czymś więcej niż synonimem biologicznej egzystencji narodu i istnienia państwa, zawiera w sobie określone osiągnięcia lub aspiracje dotyczące sposobu i poziomu życia, a także kryteria ustrojowe[28].

W Koncepcji Strategicznej Sojuszu Północnoatlantyckiego z kwietnia 1999 roku stwierdza się, że ważnym elementem polityki Sojuszu jest szerokie podejście do problematyki bezpieczeństwa, zgodnie z którym czynniki polityczne, gospodarcze, społeczne i środowiskowe odgrywają ogromne znaczenie, uzupełniając niejako niezmiernie ważny wymiar obronny[29].

Tabela 2. Poziomy identyfikacji bezpieczeństwa

Poziom	Podmiot bezpieczeństwa	Wyzwania i zagrożenia	Najbardziej prawdopodobne wyzwania i zagrożenia
bezpieczeństwo globalne	świat	problemy globalne: – demograficzny, – energetyczny, – ekologiczny,	wojny światowe, w tym jądrowa zdolna doprowadzić do zagłady świata
bezpieczeństwo regionalne	państwa regionu	zaostrzenie sytuacji międzynarodowej i ekologicznej	wystąpienie regionalnych konfliktów i wojen
bezpieczeństwo państwa	państwo	pogorszenie się sytuacji ekonomicznej, socjalnej, politycznej i in.	wystąpienie wojny domowej i rozkład państwa
bezpieczeństwo społeczeństwa	społeczeństwo, grupa socjalna	nierównomierny dostęp do wszelkiego rodzaju dóbr, wzrost bezprawia	postępująca kryminalizacja, konflikty socjalne, w tym także zbrojne
bezpieczeństwo jednostki ludzkiej	człowiek	bieda, bezprawie, brak swobód, głód, choroby	morderstwa, uprowadzenia, grabieże i kradzieże

Źródło: T. Jemioło, A. Dawidczyk, *Wprowadzenie do metodologii badań bezpieczeństwa*, Warszawa 2007, s. 49

Biorąc pod uwagę szerokie rozumienie bezpieczeństwa państwa, możemy wymienić różne jego rodzaje. Podstawą dla typologii są trzy główne kryteria: podmiotowe, przedmiotowe i funkcjonalne (procesualne)[30].

[26] R. Jakubczak, op. cit., s. 60.

[27] A.D. Rotfeld, *Europejski system bezpieczeństwa* in statu nascendi, Warszawa 1990, s. 2.

[28] J. Stefanowicz, *Bezpieczeństwo współczesnego państwa*, Warszawa 1984, s. 5.

[29] Koncepcja Strategii Sojuszu Północnoatlantyckiego z 23–24 kwietnia 1999 roku. – S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo u progu XXI wieku*, Toruń 2006, s. 112.

[30] J. Zając, *Bezpieczeństwo państwa*, [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczk, A. Materska-Sosnowska, Warszawa 2009, s. 18–19.

Kryterium podmiotowe (o czyje bezpieczeństwo chodzi?) obejmuje bezpieczeństwo jednostki, grup społecznych i narodu jako całości, a także państwa jako suwerennej organizacji politycznej.

Kryterium przedmiotowe (treść bezpieczeństwa) to: polityczne, militarne, ekonomiczne, społeczne, kulturowe, ideologiczne, ekologiczne, informacyjne ludzkie.

Kryterium procesualne obejmuje: stan i proces.

Tabela 3. Sfery bezpieczeństwa

Sfery	Podmiot bezpieczeństwa	Podstawowe przyczyny wyzwań i zagrożeń	Największe prawdopodobieństwo zaistnienia
geopolityczna	korporacje transnarodowe państwa	problemy globalne, nieprzestrzeganie prawa międzynarodowego, roszczenia terytorialne	konflikty i wojny, działalność mafijna, terroryzm międzynarodowy, narkobiznes
polityczna	partie, ruchy społeczne, struktury władzy	kryzys władzy, nieprzestrzeganie prawa	korupcja, przestępczość zorganizowana, kryminalizacja społeczeństwa
ekonomiczna	sfera produkcyjna i handlowa	globalizacja, nieprzestrzeganie prawa, brak nadrzędności polityki	porachunki mafijne, pranie brudnych pieniędzy, likwidacja przedsiębiorstw i handlu, nieracjonalne wykorzystanie surowców naturalnych, zanieczyszczenie środowiska
socjalna	grupy socjalne, organizacje społeczne	nierównomierny dostęp do dóbr, bieda, nierówność wobec prawa	kryminalizacja społeczeństwa i jego poszczególnych grup, konflikty socjalne, terroryzm
demograficzna	ludzie	przeludnienie, upadek opieki lekarskiej, choroby, konflikty etniczne	obniżenie się granicy życia ludzkiego, wzrost umieralności
kulturowa	wzorce kulturowe, duch narodu, morale	obniżenie się ducha narodu i jego morale	przyswajanie obcych wzorców kulturowych, narkomania, prostytucja
militarna	siły zbrojne	niedostateczna ochrona uzbrojenia i techniki wojskowej	kradzieże uzbrojenia i materiałów wybuchowych, zanieczyszczenie środowiska skażeniami promieniotwórczymi i chemicznymi
informacyjna	środowisko naturalne	pogorszenie się stanu środowiska naturalnego	brudna produkcja, wzrost fali imigrantów

Źródło: T. Jemioło, A. Dawidczyk, *Wprowadzenie do metodologii badań bezpieczeństwa*, Warszawa 2007, s. 50

Dbałość o bezpieczeństwo kraju jest podstawowym zadaniem państwa. Instrumentami jego realizacji są prawo, silna gospodarka, stabilny ustrój społeczno-polityczny, dobrze wyposażone i wyszkolone siły zbrojne oraz racjonalna polityka zagraniczna[31].

[31] Dworecki S., op. cit., s. 9.

ROZDZIAŁ 2

Istota zarządzania kryzysowego

2.1. Kryzys, sytuacja kryzysowa, zarządzanie kryzysowe

Kryzys

Kryzys jest nie tylko punktem zwrotnym, przełomem, lecz także wyborem między tradycją a utopią, czyli między zachowaniem *status quo* a pragnieniem zmian tak rewolucyjnych, że bliskich utopii[1]. W potocznym odbiorze kryzys postrzegany jest jako zjawisko negatywne, pełne pesymizmu i najczęściej kojarzony z dramatycznymi wydarzeniami. Sama myśl o kryzysie budzi w człowieku lęk i chęć zapomnienia niekiedy bolesnych przeżyć. W świadomości pojedynczego człowieka, grupy społecznej czy całego społeczeństwa kryzys postrzegany jest jako: zanik, rozkład, schyłek, zmierzch, upadek, cofanie się, kataklizm, awaria, katastrofa, zagłada, co ma bezpośredni wpływ na ich zachowania. Bardzo często prowadzi do rezygnacji z określonej decyzji czy działania, poddania się bez walki, a nawet ucieczki. Kryzys to również czas, w którym mają zajść decydujące zmiany.

Współcześnie uznaje się, że kryzys jest stanem rzeczy, ale stanem przejściowym, stanem niestabilności. W ujęciu ogólnym definiuje się go jako fazę funkcjonowania danego podmiotu (układu, organizmu, systemu), której główną cechą jest niestabilność. Istotą kryzysu jest brak stabilności podmiotu, co powoduje zmianę jego funkcji (a nawet całkowite ich ustanie)[2]. Powyższa definicja jest ogólna i obejmuje każdy z układów, organizmów oraz systemów. Układem (systemem), którego dotyczą kryzysy, są organizmy, instytucje, organizacje narodowe i międzynarodowe, systemy społeczne, polityczne, ekonomiczne itd.[3] Kryzys jest pojęciem wieloznacznym i nabiera praktycznego znaczenia, gdy zostanie wskazany obszar, którego dotyczy, wyróżnić wtedy można kryzys społeczny, polityczny, parlamentarny, tożsamości, moralności, ekonomiczny, militarny, w medycynie, małżeński itp.

[1] K. Kozłowska, *Etymologia, pojęcia i typologia kryzysów*, „Myśl Wojskowa" 2001, nr 2, s. 42.

[2] R. Wróblewski, *Państwo w kryzysie*, Warszawa 2001, s. 11–19.

[3] Szerzej na ten temat pisze B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 142.

Nie ma jednej uniwersalnej definicji kryzysu, określany jest on na wiele sposobów, co zaprezentowane zostało w tabeli 4.

Tabela 4. Definicje kryzysu

	Pojęcie kryzysu
Słownik wyrazów obcych PWN, Warszawa 1980, s. 404	Słowo kryzys pochodzi od greckiego słowa *krisis* mającego wiele znaczeń i oznacza: spór, preferencje, oddzielenie, decydowanie się, zmaganie się, walkę, w których konieczne jest działanie pod presją czasu, a także punkt zwrotny, przełomowy, moment rozstrzygający, jakościową zmianę układu lub w układzie. *Crisis* w języku angielskim poszerza znaczenie o takie cechy, jak nagłość, urazowość i subiektywne konsekwencje urazu w postaci negatywnych przeżyć.
W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Warszawa 2000, s. 282	Kryzys definiowany jest jako moment, okres przełomu, przesilenie, decydujący zwrot, okres załamania gospodarczego. Ma ścisły związek z trwałym zakłóceniem działalności i realizacji celów, naruszaniem równowagi funkcjonowania, a w skrajnych przypadkach nawet zagrożeniem istnienia.
R. Wróblewski, *Państwo w kryzysie*, Warszawa 2001, s. 16	Kryzys jako okres funkcjonowania państwa to stan, w którym bezpośrednie zagrożenie żywotnych interesów państwa (w jego wnętrzu lub w bliskim otoczeniu) następuje tak szybko, że wymusza na władzach publicznych natychmiastowe podjęcie nadzwyczajnych działań.
T. Iwanek, *Kryzys i jego odmiany*, Wrocław 2004, s. 9	Kryzys to punkt zwrotny do zmiany na lepsze lub na gorsze; emocjonalne zdarzenie lub radykalna zmiana statusu życia człowieka; chwila, w której decyduje się człowiek, czy dana sprawa lub działanie będzie kontynuowane, ulepszane i modyfikowane, czy też zostanie zakończone; stan cierpienia z towarzyszącymi uczuciami zagrożenia i lęku przeżywanego w związku z jakimiś zdarzeniami.
T. Iwanek, *Kryzys i jego odmiany*, Wrocław 2004, s. 10	Kryzys to siła rozróżniająca, oddzielenie, wybór, spór, preferencja, sąd, kontestacja, potępienie, znalezienie rozwiązania, wyjaśnienie, interpretacja itp. W związku z tym można wskazać kilka charakterystycznych cech kryzysu. Kryzys może być: 1) doświadczeniem pozytywnym (a nie negatywnym), otwierającym przed człowiekiem nowe horyzonty, nowe perspektywy; może być on jednak źle rozwiązany i wtedy powoduje negatywne skutki w osobowości i życiu duchowym. Zależy to od sposobu reagowania na kryzys, sposobu radzenia sobie, ale w znacznej mierze zależy od tego, czy osoba kryzysująca znajdzie pomocną dłoń drugiego człowieka w swojej bezradności, 2) doświadczeniem, przez które przechodzi każdy człowiek; nie ma człowieka, który byłby wolny od przejścia przez kryzys; ludzie różnią się jednak między sobą wrażliwością na kryzys i umiejętnością radzenia sobie z nim. Niektórzy przeżywają wiele kryzysów, a inni niewiele, ale za to bardzo ciężkich, 3) doświadczeniem powiązanym ze światem wartości i światem decyzji człowieka. Pośród kryzysu objawia się ta hierarchia wartości, którą człowiek naprawdę uznaje; w powiązaniu z kryzysem człowiek musi nierzadko podjąć jakąś decyzję. Czasem niepodejmowanie decyzji jest ucieczką przed wyjściem z kryzysu. Oczywiście nie należy się spieszyć z decyzją podczas kryzysu. Nie należy podejmować żadnych decyzji w najbardziej ostrych stadiach kryzysu, 4) doświadczeniem najbardziej głębokim i angażującym, ostrym, przez które przechodzi człowiek, jest miejscem walki człowieka z sobą samym, czasem ludzkich zmagań.

H. Sęk, *Wybrane zagadnienia psychoprofilaktyki*, [w:] *Społeczna psychologia kliniczna*, red. H. Sęk, Warszawa 1991, s. 487.	Zjawisko lub stan, które charakteryzują się takim stopniem dysproporcji i niezrównoważenia elementów, że wymaga to istotnych zmian. Jest to często stan będący punktem zwrotnym w jakimś procesie.
Słownik podstawowych terminów dotyczących bezpieczeństwa, Warszawa 1994, s. 13	Kryzys to forma (faza) konfliktu, w wyniku którego dochodzi do gwałtownego wzrostu napięcia między stronami, w wyniku czego może nastąpić konflikt zbrojny.
Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2009, s. 61	Kryzys to sytuacja będąca następstwem zagrożenia, prowadząca w konsekwencji do zerwania lub znacznego osłabienia więzów społecznych, przy równoczesnym poważnym zakłóceniu funkcjonowania instytucji publicznych, jednak w takim stopniu, że użyte środki niezbędne do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych przewidzianych w art. 228 Konstytucji Rzeczypospolitej Polskiej.
Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2009, s. 61	Kryzys to sytuacja powstała w wyniku załamania się stabilnego dotąd procesu rozwoju, grożąca utratą inicjatywy i koniecznością godzenia się na przyjmowanie niekorzystnych warunków wymagających podjęcia zdecydowanych wszechstronnych kroków zaradczych.
J. Konieczny, *Zarządzanie w sytuacjach kryzysowych. Rola i zadania administracji publicznej,* Inowrocław 2000, s. 8	Kryzys to: punkt zwrotny na lepsze lub gorsze, znaczące emocjonalne zdarzenie lub radykalna zmiana statusu w życiu człowieka, chwila, gdy decyduje się, czy dana sprawa lub działanie będzie postępować dalej, ulegnie modyfikacji czy też zostanie zakończone, stan cierpienia z towarzyszącymi uczuciami zagrożenia i lęku, przeżywanymi w związku z wyżej wymienionymi zdarzeniami.
R. Oldcorn, *Management,* Londyn 1989, s. 237	Kryzys jest wynikiem nieplanowanych zdarzeń zakłócających lub zagrażających normalnemu funkcjonowaniu organizacji.
W. Wawrzyniak, *Odnawianie przedsiębiorstwa. Od kryzysu do sukcesu*, Warszawa 1999, s. 58	Kryzys w przedsiębiorstwie jest traktowany jako sytuacja wielkiego zagrożenia organizacji jako całości, w której na skutek spiętrzania się różnorodnych trudności i nasilania zjawisk konfliktowych zagrożona jest realizacja jej podstawowych funkcji. Jest to przełom między dwoma jakościowo różnymi fazami jakiegoś procesu, ze skutkami mniej lub bardziej dotkliwymi, z różnym zakresem i czasem trwania, ale zawsze kończącym dotychczasowy sposób działania czy rozwoju sytuacji rozpoczynającym nowy etap.
B. Rozwadowska, *Public relations w sytuacjach kryzysowych*, Wrocław 2002, s. 65	Kryzys jest nagłym, nieoczekiwanym i niepożądanym wydarzeniem, które zakłóca równowagę w firmie [organizacji – przyp. autora] i stanowi zagrożenie dla dowolnej sfery jej działalności.
P. Sienkiewicz, P. Górny, *Analiza systemowa sytuacji kryzysowej,* „Zeszyty Naukowe AON" 2005, nr 4, s. 31	Kryzys to stan będący punktem zwrotnym w procesie rozwoju systemu (kluczowy moment, etap lub zdarzenie), po którym następuje zmiana sytuacji systemowej; moment (chwila, okres), który stanowi zapowiedź zmiany sytuacji systemowej.
R. Wróblewski, *Wprowadzenie do strategii wojskowej*, Warszawa 1998.	Kryzys oznacza rozwój wydarzeń wewnętrznych lub zewnętrznych stanowiących bezpośrednie zagrożenie żywotnych interesów społeczeństwa (państwa) i następujących tak szybko, że wymuszają one na władzach politycznych natychmiastowe podjęcie nadzwyczajnych działań.
B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 143.	W sensie ontycznym kryzys jest kulminacją nagromadzonych i skumulowanych konfliktów – konfliktów wciąż obecnych w życiu społecznym, w państwie, w środowisku międzynarodowym.

Źródło: Opracowanie własne

Mając na uwadze powyższe definicje, można przyjąć, że kryzys prowadzi do destabilizacji funkcji każdego układu (systemu). Przykładem mogą być kryzysy: społeczny (destabilizacja funkcji systemu społecznego), polityczny (destabilizacja funkcji systemu politycznego), czy polityczno-militarny (destabilizacja funkcji systemu politycznego ze względu na konflikt militarny w skali poniżej progu wojny)[4].

Kryzys jest jedną z kategorii teorii bezpieczeństwa, w tym bezpieczeństwa państwa, i stanowi:

- kulminację nagromadzonych zdarzeń, stanów rzeczy (zagrożeń, konfliktów, szans) w różnych dziedzinach życia społecznego, działalności państwa (wielu państw) i innych organizacji, krytyczny rezultat negatywnej działalności człowieka przeciwko człowiekowi lub prawom natury, a także zjawisk wynikających z działania sił natury lub awarii technicznych, którym przeciwdziałanie przekracza możliwości rutynowych działań systemu (jednostki, organizacji, układu), prowadząc w konsekwencji do ewolucji (zmiany) istoty jego funkcjonowania, z przejściem do innej sytuacji systemowej włącznie,
- sytuację ekstremalną, jaka powstała w toku działalności organizacji (systemu), powodującą utratę inicjatywy i możliwość zaistnienia zmiany systemowej, wymagającą podjęcia zdecydowanych, wszechstronnych kroków zaradczych.

W związku z powyższym kryzys oznacza:

- sytuację niekorzystną, poważne załamanie, wzrost napięcia, nagłe i gwałtowne przesilenie, moment przełomu ku złemu lub lepszemu,
- punkt zwrotny i przejście do stanu normalnego lub innego stanu kryzysowego,
- jakościową zmianę systemową w funkcjonowaniu jakiegoś obiektu (systemu, organizacji, instytucji itd.),
- specyficzną cechę jakiejkolwiek sytuacji, przełom miedzy dwiema fazami jakiegoś procesu,
- szczególny splot okoliczności (wyzwań, zagrożeń, słabości i szans) w dziedzinie bezpieczeństwa, w tym bezpieczeństwa narodowego[5].

Istotną rzeczą, jaką wyróżnia się w definiowaniu kryzysu, jest fakt przełomu i jakościowej zmiany w funkcjonowaniu jakiegoś podmiotu. W związku z tym należy podkreślić, że kryzys zawsze oznacza: przełom między dwiema jakościowo różnymi fazami jakiegoś procesu, może być bardziej lub mniej dotkliwy, może mieć różny zakres, czas trwania, ale zawsze kończy dotychczasowy sposób działania czy rozwoju sytuacji, kryzys jest naruszeniem stanu równowagi, kryzys rozpoczyna nowy etap działania czy rozwoju sytuacji[6].

Na kryzys składają się trzy elementy: presja czasu, ewentualność zasadniczego zagrożenia i zaskoczenia, a także fakt, że jest on rezultatem zarówno niebez-

[4] *Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 r.*, cz. 2: *Warunki powstania kryzysów polityczno-militarnych i ich charakter*, Program naukowo-badawczy (kryptonim KAPPA) zlecony Akademii Obrony Narodowej, opracowanie zbiorowe, Warszawa 1997, s. 8–20.

[5] J. Gryz, W. Kitler, *System reagowania kryzysowego*, Toruń 2007, s. 18, 19.

[6] C. Rutkowski, A. Kasprzewski, *Wojskowe aspekty sytuacji kryzysowej. Zadania obronne Polski*, Warszawa 1996.

pieczeństwa, jak i okoliczności, w jakich ono występuje. Wzajemne oddziaływanie trzech elementów, czyli czasu, zagrożenia i zaskoczenia, tworzy definicję kryzysu[7].

Należy podkreślić, że

> wszystkie cechy opisujące kryzys pozwalają stwierdzić, że po to, aby zjawisko było postrzegane jako kryzys, musi zaistnieć nagłe, realne i nieakceptowane przez dany podmiot zagrożenie jego interesów i celów, którego skutki zmieniają lub prowadzą do zmiany istniejącej sytuacji. Istotne znaczenie ma również dostrzeganie bliskości zagrożenia. Jeżeli jest ono oddalone w czasie lub przestrzeni, to może dojść do sytuacji o charakterze kryzysowym o niższym stopniu oddziaływania. […] jeżeli dane zagrożenie jest małe lub zaistniała sytuacja jest jakąś szansą lub ma mały stopień intensywności, to mamy do czynienia z kryzysem o niskim stopniu oddziaływania[8].

W literaturze przedmiotu spotyka się próby klasyfikacji kryzysów według różnych kryteriów i cech. Jednak precyzyjna klasyfikacja kryzysów jest bardzo trudna, co wynika m.in. z faktu, że przyczyny zagrożeń kryzysowych mogą mieć różną konfigurację – zob. tabela 5.

Tabela 5. Kryteria kryzysów w obszarze bezpieczeństwa państwa

Kryteria	Kryteria szczegółowe
podmiotowe	wewnętrzne, zewnętrzne
przedmiotowe	polityczne, społeczne, polityczno-militarne, ekonomiczne, kulturalne, religijne, etniczne, ekologiczne, fizjologiczne, psychologiczne
przestrzenne	lokalne, regionalne, krajowe, międzynarodowe, globalne
czas trwania	incydentalne, krótkotrwałe, średnioterminowe, długoterminowe, permanentne
usytuowanie źródeł	wewnętrzne, zewnętrzne
częstotliwości	jednorazowe, sporadyczne, powtarzające się, cykliczne
symptomy zagrożenia	przewidywalne, nieprzewidywalne, oczekiwane, nieoczekiwane
istnienie konfliktów interesów	konfliktowy, niekonfliktowy

Źródło: J. Gryz, W. Kitler, *System reagowania kryzysowego*, Toruń 2007, s. 19, 20

Typologia jest to szeregowanie i logiczne porządkowanie elementów danego zbioru (przedmiotów, zjawisk itp.) według zasady porównywania ich cech z cechami elementów uznanych za typy w obrębie określonego zbioru. Działania typologiczne są elementem składowym procesu decyzyjnego i stanowią etap wstępny strategii postępowania w rozwiązywaniu sytuacji kryzysowej[9]. Na podstawie posiadanych informacji typologia pozwala na dokonanie wstępnej selekcji i zaszeregowania kryzysu do danej grupy lub typu. Ma to szczególne znaczenie

[7] M. Clarke, *Charakterystyka zachowania się w kryzysie*, Bruksela 1995 (maszynopis), przeł. E. Jendraszczak.

[8] E. Nowak, *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Warszawa 2007, s. 32.

[9] K. Korzecki, *Typologia zagrożeń kryzysowych*, Warszawa 1998.

dla usprawnienia procesu podejmowania decyzji oraz poprawności oceny i analizy informacji. Podstawę typologii kryzysów stanowią informacje pochodzące z własnych oraz innych źródeł. Znajomość typologii kryzysów może usprawnić pracę uprawnionych podmiotów zarządzania kryzysowego w procesie wypracowywania decyzji.

Obok powyższej klasyfikacji wśród kryzysów można wyodrębnić dwie zasadnicze klasy zdarzeń – zob. tabela 6.

Tabela 6. Klasyfikacja kryzysów i towarzyszących im zdarzeń

Kryzysy	Zdarzenia
z dominacją czynników wewnętrznych	zamieszki lub strajki o znaczeniu państwowym, naruszające podstawy obronności, duże klęski żywiołowe, katastrofy ekologiczne, kryzysy ekonomiczne, zbrojne przewroty polityczne, powstania, które nie przerodziły się w wojnę domową, kryzysy polityczne zagrażające porządkowi demokratycznemu, zdarzenia godzące w porządek konstytucyjny, terror itp.
z dominacją czynników zewnętrznych	masowe migracje, prowokacyjne zbrojne starcia (incydenty) graniczne nieprzekraczające progu wojny, interwencje zbrojne, jawne przygotowania państwa sąsiedniego do inwazji na dane państwo, wojna domowa lub wojna między państwami sąsiadującymi z danym państwem, konflikty zbrojne, wojny między państwami z dalszego otoczenia danego państwa, zagrażające wprost lub pośrednio jego bezpieczeństwu i angażujące to państwo po jednej z walczących stron, interwencje militarne z zaangażowaniem znacznych sił, sytuacje wewnętrzne innych państw wymuszające uznanie konieczności wojskowej interwencji humanitarnej danego państwa

Źródło: R. Wróblewski, *Wprowadzenie do strategii wojskowej*, Warszaw 1998, s. 145–146

Do specyficznych zdarzeń krytycznych należy zaliczyć katastrofy cywilizacyjne i klęski żywiołowe. Zmniejszają one poczucie bezpieczeństwa, wiarę w sprawiedliwość, poczucie własnej wartości, wolę życia, optymizm. Różne oblicza tych zdarzeń niszczą bezcenne zasoby przyrodnicze, kulturalne, materialne i psychologiczne, niezbędne do utrzymania zdrowego, spokojnego i bezpiecznego funkcjonowania człowieka[10].

W każdej sytuacji kryzys oznacza nasilenie pewnych zjawisk i procesów negatywnych, prowadzących z reguły do pewnego przełomu i najczęściej bardziej radykalnych i mniej bezpiecznych stanów. Kryzys może ewoluować w stronę narastania zagrożeń i niebezpieczeństw, może też mieć tendencje zanikające, prowadzące do wzrostu bezpieczeństwa. W złożonych sytuacjach społecznych i politycznych, za wyjątkiem stanu permanentnego kryzysu, jest on niestabilnym stanem przejściowym, który albo narasta prowadząc do dalszej destabilizacji,

[10] M. Dobosz, *Zarządzanie kryzysowe. Kryzys – termin*, www.obronacywilna.pl [pobrano 19.04.2012].

konfliktu czy katastrofy, albo zanika, umożliwiając powrót do stanu przedkryzysowego. Oprócz wymienionej wyżej klasyfikacji kryzysów można przyjąć inną klasyfikację, kierując się takimi kryteriami, jak zdolność przystosowania się do zmian wywołanych kryzysem, procesowy charakter zarządzania kryzysowego w organizacji, faza cyklu życia organizacji, czas ostrzegania (jest to okres pomiędzy pierwszymi symptomami pojawiania się problemu do czasu wystąpienia kryzysu), miejsce powstawania problemu, przyczyny sytuacji kryzysowej, sfera organizacji, na którą kryzys oddziałuje, wielość i różnorodność symptomów sytuacji kryzysowej[11]. Wybrane rodzaje kryzysów w organizacji i ich charakterystykę przedstawiono w tabeli 7.

Tabela 7. Podział kryzysów w organizacji

Kryterium podziału	Rodzaj kryzysu i jego charakterystyka
Zdolność przystosowania się do zmian	– *kryzys adaptacji*, jego przejawem są kłopoty z przystosowaniem się do zagrożeń. Niemożność zastosowania rozwiązań i metod stosowanych w przeszłości do zmienionych warunków działania – *kryzys ciągłości*, polega na braku inercji, spowodowany jest rozregulowaniem procesu zarządzania na skutek stałych zmian; o ile zmiany są potrzebne, to organizacja potrzebuje, aby jej rdzeń zarządzania, kulturowy, proceduralny był zestandaryzowany i posiadał stabilność niezależnie od potrzeby zmian. Problem w tym, by stworzyć takie procedury zarządzania, aby zmiany można było wprowadzić elastycznie i etapami
Procesowy charakter zarządzania kryzysowego w organizacji	– *kryzys potencjalny*, zagrożenie dla działalności przedsiębiorstwa i realizowanie celów wynikających z niekorzystnych oddziaływań różnorodnych zjawisk zewnętrznych i wewnętrznych; jeżeli na tym wczesnym etapie nie zostaną podjęte radykalne działania identyfikujące źródła niepokoju, kryzys potencjalny przechodzi w kryzys ukryty – *kryzys ukryty*, trudności w realizowaniu celów przedsiębiorstwa i gospodarowaniu zasobami, często utożsamiane z tzw. trudnościami przejściowymi, które nie są żadną patologią, a zdarzają się wszystkim przedsiębiorstwom i stanowią immanentną cechę działalności gospodarczej; brak działań w celu zneutralizowania szkodliwych efektów kryzysu ukrytego prowadzi do rozwoju tzw. kryzysu jawnego – *kryzys jawny*, pojawienie się trudności w funkcjonowaniu firmy, które z całą konsekwencją zagrażają jej bytowi ekonomicznemu
Faza cyklu życia organizacji	– *kryzys przywództwa*, rozrost rozmiarów przedsięwzięcia do takiej skali, że wykracza poza kontrolę inicjatora, pomysłodawcy; najczęściej utrata kontroli nad rosnącą skalą działalności i rozmiarami organizacji – *kryzys autonomii*, pojawienie się chaosu w utrwalonej strukturze organizacyjnej, utrata kontroli nad nadzorowanymi odcinkami działalności firmy na poszczególnych szczeblach kierowniczych; niezbędne są procesy restruktyzacji, polegające na delegacji uprawnień w dół, czyli na niższe szczeble zarządzania, co z kolei może się zakończyć kryzysem decentralizacji

[11] A. Zelek, *Zarządzanie kryzysowe w przedsiębiorstwie – perspektywa strategiczna*, Warszawa 2003, s. 65.

	– *kryzys decentralizacji*, zmusza do lepszej koordynacji zdecentralizowanych działań i może oznaczać kolejną fazę wzrostu organizacji, efektem zaś takiego rozwoju jest najczęściej kryzys biurokratyzacji – *kryzys biurokratyzacji*, zmniejszenie efektywności funkcjonowania dużych organizacji gospodarczych ze względu na ich naturalną skłonność do wzrostu biurokracji i tym samym wzrostu kosztów stałych – *kryzys dojrzałości*
Czas ostrzegania	– *kryzys nagły*, definiowany jako zaburzenia działalności, który pojawia się bez ostrzeżenia i wzbudza zainteresowanie mediów oraz może mieć niepomyślny wpływ zarówno na bieżącą działalność firmy, jak i na jej dalszy rozwój; bezpośrednim jego efektem jest najczęściej szokowa atmosfera wewnątrz i na zewnątrz przedsiębiorstwa, która w efekcie wpływa na pogorszenie relacji rynkowych i czasowych, nagły spadek wartości rynkowej firmy – *kryzys tlący się*, definiowany jako każdy narastający w czasie problem biznesowy, niezależnie od źródła jego pochodzenia (z zewnątrz czy wewnątrz); kryzys tlący się może trwać długookresowo, ujawniając stopniowo kolejne symptomy zagrożenia
Miejsce powstawania problemu	– *kryzys wewnątrz organizacji*, stanowiący podsystem zarządzania, spowodowany jest czynnikami występującymi wewnątrz przedsiębiorstwa, takimi jak niewłaściwe zarządzanie czy błędna polityka finansowa firmy – *kryzys na zewnątrz organizacji*, przyczynami są przede wszystkim procesy makroekonomiczne, nowe zjawiska społeczne, postęp technologiczny, globalizacja rynków
Tempo przebiegu i czas trwania	– *kryzys nagły*, charakteryzuje go brak czasu na badanie i planowanie; decyzje muszą być podejmowane błyskawicznie – *kryzys przewlekły*, może trwać miesiącami, a nawet latami; długi okres nie sprzyja podjęciu skutecznych działań w celu opanowania kryzysu, zazwyczaj zarządy firm i dyrekcja przyjmują postawę biernego wyczekiwania, licząc na to, że kryzys sam przeminie; wywołują go plotki, pogłoski, spekulacje przekazywane z ust do ust lub nagłaśniane przez media
Przyczyny wywołujące	– *kryzys rzeczywisty*, spowodowany jest różnymi czynnikami i prowadzi zwykle do wielu problemów w przedsiębiorstwie – *kryzys wirtualny* jest sztucznie wytworzony w celu doprowadzenia do zmian, a w konsekwencji do rozwoju i zwiększenia przychodów przedsiębiorstwa

Źródło: A. Zelek, *Zarządzanie kryzysowe w przedsiębiorstwie – perspektywa strategiczna*, Warszawa 2003, s. 43–46

Powyższy podział kryzysów, które w różnych okolicznościach mogą wystąpić w przedsiębiorstwach, mogą mieć miejsce w państwie, województwie, powiecie czy gminie. Takim przykładem są m.in. kryteria, jak miejsca powstania (wewnętrzne, zewnętrzne), przyczyny występowania, procesowy charakter zarządzania kryzysowego w organizacji, tempo przebiegu i czasu trwania.

Kryzys w Sojuszu Północnoatlantyckim

Kryzys jest pojęciem, którym posługują się również państwa członkowskie Sojuszu Północnoatlantyckiego. Dla jego oznaczenia stosuje się takie pojęcia, jak: *powaga kryzysu* i *intensywność kryzysu*.

„Powaga kryzysu oznacza [...] rozmiar i bliskość zagrożenia dla priorytetowych wartości, interesów oraz celów strategicznych strony zagrożonej kryzysem lub znajdującej się w sytuacji kryzysowej”[12]. Stopień powagi kryzysu zależny jest od charakteru (wielkości, powagi) zagrożenia oraz jego bliskości (w czasie, w przestrzeni). Powagę kryzysu stosuje się zwykle jako zmienny wskaźnik wyrażający decyzje polityczne służące przejściu ze stanu normalnego do stanu nadzwyczajnego. Oznacza to, że po podjęciu określonej decyzji o działaniu czynnik powagi kryzysu przestaje się liczyć, a ważniejszym przedmiotem zainteresowania staje się intensywność kryzysu (poziom gwałtowności kryzysu). Intensywność kryzysu nie jest wprost proporcjonalna do jego powagi i zależy od jakości i wielkości sił i środków zaangażowanych w działaniach antykryzysowych[13].

Tabela 8. Stopień powagi kryzysu w zależności od rozmiaru i bliskości zagrożenia

Bliskość zagrożenia	Stopnie powagi kryzysu		
natychmiastowe	niski stopień powagi	średni stopień powagi	wysoki stopień powagi
opóźnione	niski stopień powagi	średni/niski stopień powagi	średni stopień powagi
odległe	niski stopień powagi	niski stopień powagi	niski stopień powagi
	Rozmiar zagrożenia		
	małe	średnie	duże

Źródło: E. Jendraszczak, W. Kozłowski, *Zarządzanie w sytuacjach kryzysowych* – opracowanie na podstawie podręcznika *Generic Crisis Management Handbook (GCMH)* wydanego przy Radzie ds. Operacji i Komitecie ds. ćwiczeń NATO (17.05.1997), MON – DSO, Warszawa 1997, s. 9

W koncepcjach Sojuszu Północnoatlantyckiego przeciwdziałanie kryzysom i ich opanowanie dzieli się według kryterium geograficznego na występujące w strefie bezpieczeństwa (obszarze) NATO oraz poza strefą bezpieczeństwa (obszarem) NATO[14].

Zaangażowanie państw członkowskich i sił zbrojnych Sojuszu Północnoatlantyckiego w rozwiązywanie i opanowanie kryzysu zależy od jego charakteru, skali i przewidywanych skutków. Do pomiaru stopnia zaangażowania sił zbrojnych w sytuacjach kryzysowych stosuje się metody scenariuszowe.

Tabela 9. Przeciwdziałanie i opanowywanie kryzysów

Przeciwdziałanie i opanowywanie kryzysów	
Strefa bezpieczeństwa (obszar) NATO	Poza strefą bezpieczeństwa (obszarem) NATO
duży rozruch, kryzys społeczno-polityczny w państwie NATO	wojny domowe

[12] E. Jendraszczak, W. Kozłowski, *Zarządzanie w sytuacjach kryzysowych* – opracowanie na podstawie podręcznika *Generic Crisis Management Handbook (GCMH)* wydanego przy Radzie ds. Operacji i Komitecie ds. ćwiczeń NATO (17.05.1997), MON – DSO, Warszawa 1997, s. 9.

[13] Ibidem, s. 9.

[14] R. Wróblewski, *Zagrożenia kryzysowe i wojenne Polski w kontekście jej członkostwa w NATO*, Warszawa 1998.

operacja antyterrorystyczna, wynikająca z zagrożenia państwa NATO z zewnątrz	napięcia między państwami grożące wybuchem konfliktu zbrojnego, przywracanie porządku wewnętrznego po wygaśnięciu konfliktu zbrojnego, załamanie się władzy publicznej w państwie lub/i sytuacja, w której dochodzi do nadmiernych cierpień ludności, sytuacja zagrożenia katastrofą nuklearną, wywołana zarówno środkami wojskowymi, jak i awariami w elektrowniach jądrowych, a także poważnymi katastrofami ekologicznymi, zagrożenie licznych grup obywateli państwa, znajdujących się poza granicami, konieczność ochrony morskich szlaków komunikacyjnych, międzynarodowa interwencja zbrojna przeciwko innemu państwu – udział w konflikcie lokalnym

Źródło: B. Balcerowicz, *Sojusz a obrona narodowa*, Warszawa 1999, s. 167

Sytuacja kryzysowa

W teorii kryzysu (w ujęciu ogólnym) rozważanym układem (systemem) jest organizm, instytucja, organizacja, w tym społeczeństwo (system polityczny, społeczny, ekonomiczny itp.). W sensie przedmiotowym kryzys jest zerwaniem istniejącego układu (systemu), polegającym na zmianie jego struktury lub funkcji albo obu tych elementów łącznie. Zjawisko zerwania układu (systemu) rozciąga się w czasie i zachodzi w określonych warunkach jego funkcjonowania. Jest niejako wkomponowane w proces przechodzenia układu (systemu) od stabilności – przez niestabilność – do stabilności o jakościowo innych własnościach, czyli w sytuację kryzysową[15].

Kryzys w potocznym rozumieniu utożsamiany jest z sytuacją kryzysową. Między tymi dwoma pojęciami istnieją jednak znaczące różnice, i tak: kryzys jest elementem sytuacji kryzysowej, każdy kryzys jest sytuacją kryzysową, lecz nie każda sytuacja kryzysowa zawiera w sobie element kryzysu (fazę kryzysu), pojawienie się symptomów kryzysu nie musi wywoływać zmian w istocie organizacji, lecz stanowi wyzwanie dla subiektywnego poczucia normalności jej funkcjonowania[16].

Należy zaznaczyć, że sytuacja kryzysowa jest pojęciem nadrzędnym wobec pojęcia kryzysu i obejmuje oprócz niego fazę występującą przed nim i fazę po nim. Dlatego kryzys stanowi element sytuacji kryzysowej i jest kulminacją nagromadzonych zdarzeń. Jest jedną z faz w rozwoju sytuacji kryzysowej, a zatem każdy kryzys jest także sytuacją kryzysową. Sytuacja kryzysowa w odróżnieniu od kryzysu – by zaistnieć – nie musi stwarzać istotnego zagrożenia dla życia ludzkiego, lecz stanowi swoiste wyzwanie dla społecznego poczucia moralności, tradycji, wartości i bezpieczeństwa[17]. Oznacza to, że sytuacja kryzysowa występuje wówczas, gdy naruszony zostanie akceptowany stan bezpieczeństwa.

15 R. Wróblewski, *Wprowadzenie do strategii wojskowej*, Warszawa 1998.

16 B. Kosowski, *Sprawne i elastyczne zarządzanie w kryzysie*, Warszawa 2008, s. 24.

17 K. Kozłowska, *Etymologia, pojęcia i typologia kryzysów*, „Myśl Wojskowa" 2001, nr 2, s. 46.

Istnieje wiele definicji sytuacji kryzysowej, co przedstawiono w tabeli 10.

Tabela 10. Definicje sytuacji kryzysowej

Autor	Definicje
R. Wróblewski, *Zarys teorii kryzysu. Zagadnienia prewencji i zarządzania kryzysami*, Warszawa 1996, s. 10	Sytuacja kryzysowa to zespół okoliczności zewnętrznych i wewnętrznych wpływających na dany system w ten sposób, iż zaczyna się i jest w nim kontynuowany proces zmian; rezultatem tej zmiany może być jakościowo nowy system lub nowa struktura i funkcja w układzie istniejącym.
E. Jendraszczak, W. Kozłowski, *Zarządzanie w sytuacjach kryzysowych*, Warszawa 1997, s. 7	Sytuacja kryzysowa to zespół gwałtownie zachodzących wydarzeń, który wywołuje oddziaływanie sił destabilizujących na ogólny stan międzynarodowy lub jakikolwiek jego podsystem zasadniczo powyżej normalnego (średniego) poziomu i powoduje tym wzrost prawdopodobieństwa narastania zjawisk negatywnych istniejących już w systemie. Sytuacja kryzysowa to ciąg wzajemnych oddziaływań pomiędzy rządami dwóch lub więcej suwerennych państw uwikłanych w poważny konflikt, tuż na granicy wybuchu wojny, które są świadome niebezpieczeństwa. Sytuacja kryzysowa to zmiana sytuacji pomiędzy dwiema lub więcej przeciwstawnymi stronami, charakteryzująca się wzrostem intensywności negatywnych oddziaływań z wysokim prawdopodobieństwem wystąpienia starć zbrojnych.
P. Sienkiewicz, P. Górny, *Analiza systemowa sytuacji kryzysowych*, „Zeszyty Naukowe AON" 2001, nr 4, s. 31	Sytuacja kryzysowa to sytuacja systemowa charakteryzująca się kulminacją zagrożeń (wewnętrznych i/lub zewnętrznych) powodujących utratę stanu normalności i możliwość zakłócenia podstawowych cech systemowych (stabilności, równowagi, sterowalności, efektywności itp.).
Z. Kral, A. Zabłocka-Kluczka, *Sposób postrzegania kryzysów w polskich przedsiębiorstwach*, „Ekonomika i Organizacja Przedsiębiorstw" 2004, nr 11, s. 48	Sytuacja kryzysowa to taki stan organizacji, który prowadzi do naruszenia jej stabilności lub wręcz opóźnienia rozwoju w stosunku do zmian zachodzących w otoczeniu, a w przypadku utrzymywania się w dłuższym czasie – zagrożenia egzystencji.
J. Gryz, W. Kitler, *System reagowania kryzysowego*, Toruń 2007, s. 22, 23	Sytuacja kryzysowa to zespół okoliczności zewnętrznych i wewnętrznych, w jakich znajduje się dany podmiot (układ, organizacja, system), wpływających na jego funkcjonowanie w taki sposób, że zaczyna się w nim, jest kontynuowany proces zmiany, w rezultacie czego dochodzi do zachwiania równowagi i utraty możliwości kontroli nad przebiegiem wydarzeń albo eskalacji zagrożenia jego interesów. Jeżeli za podmiot rozważań przyjmiemy państwo (lub jego część), to definicja sytuacji kryzysowej może przyjąć następującą postać: sytuacja kryzysowa oznacza zespół warunków zewnętrznych i/lub wewnętrznych, w jakich znajduje się państwo, jego część lub określona dziedzina jego funkcjonowania, wpływających na jego funkcjonowanie w taki sposób, iż zaczyna się w nim i jest kontynuowany proces zmienny, w rezultacie czego dochodzi do zachwiania równowagi i utraty możliwości kontroli nad przebiegiem wydarzeń albo eskalacji zagrożenia interesów narodowych, w tym: integralności terytorialnej, interesów ekonomicznych, politycznych i społecznych oraz zagrożenia życia, zdrowia, mienia, dziedzictwa kulturowego, środowiska lub infrastruktury krytycznej.

K. Kozłowska, *Etymologia, pojęcia i typologia kryzysów*, „Myśl Wojskowa" 2001, nr 2, s. 46	Sytuacja kryzysowa to taka sytuacja, w której coś już nie może być dłużej takie, jakie było do tej pory, nie może być dalej niezmienne, ponieważ ze swej natury nie jest trwałe. Wymaga pielęgnowania i ciągłego dostosowywania się, uaktualniania.
W. Kitler, *Podstawowa terminologia zarządzania kryzysowego,* [w:] *Zarządzanie kryzysowe w sytuacji klęski żywiołowej*, red. E. Nowak, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 2006, nr 1, s. 30	Sytuacja kryzysowa to zespół takich okoliczności zewnętrznych i wewnętrznych, w jakich znajduje się podmiot, czyli system, organizacja, układ, wpływających na jego funkcjonowanie w taki sposób, że zaczyna się w nim, jest kontynuowany proces zmian. Z tego też powodu dochodzi do zachwiania równowagi, a następnie jej przywrócenia dzięki podjętym środkom regulacji, jakie zostaną zastosowane.
E. Nowak, *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Warszawa 2007, s. 39	Sytuacja kryzysowa to sytuacja będąca następstwem zagrożenia i prowadzącą w konsekwencji do zerwania lub znacznego naruszenia więzów społecznych przy równoczesnym poważnym zakłóceniu w funkcjonowaniu instytucji publicznych, jednak w takim stopniu, że użyte środki do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych, o których jest mowa w art. 228 ust. 1 Konstytucji Rzeczypospolitej Polskiej.
Art. 3 ust. 1 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.)	Sytuacja kryzysowa to sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołując znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.

Źródło: Opracowanie własne

W wielu definicjach sytuację kryzysową traktuje się jako wynik konfliktów między państwami, konfliktów zbrojnych, ataku terrorystycznego, i tak:

- sytuacja kryzysowa to ciąg wzajemnych oddziaływań pomiędzy rządami dwóch lub więcej suwerennych państw, uwikłanych w poważny konflikt, tuż na granicy wybuchu wojny, które są świadome niebezpieczeństw;
- sytuacja kryzysowa to stan narastającej destabilizacji, niepewności i napięcia społecznego, charakteryzujący się naruszeniem więzi społecznych, możliwością utraty kontroli nad przebiegiem wydarzeń oraz eskalacji zagrożenia, a w szczególności stwarzający zagrożenie dla życia, zdrowia, mienia, dziedzictwa kulturowego lub infrastruktury krytycznej, w tym spowodowany zdarzeniem terrorystycznym.

Tym samym sytuacja kryzysowa jest zespołem okoliczności zewnętrznych i wewnętrznych powodujących zmiany w danym układzie. Rozpoczyna się z chwilą pojawienia się jej symptomów. Jest niepożądanym zdarzeniem lub ciągiem zdarzeń. Sytuacje kryzysowe mogą spowodować zagrożenia związane z działalnością człowieka, jak również w wyniku awarii, katastrofy czy klęski żywiołowej. Gdy określona organizacja nie jest w stanie reagować na wydarzenia i opanować kryzysu, może dojść do utraty kontroli i w następstwie tego doprowadzić do wystąpienia sytuacji kryzysowej.

Sytuacje kryzysowe są zjawiskami nieoczekiwanymi, nagłymi i destabilizującymi funkcjonowanie społeczności. Aby daną sytuację uznać za kryzysową, konieczne jest wystąpienie takich czynników, jak ograniczenia standardowego

funkcjonowania społeczeństwa i organów administracji publicznej, nieadekwatność posiadanych sił i środków do skali zagrożenia.

Na istotę sytuacji kryzysowej składają się następujące cechy:

- każdy kryzys jest sytuacją kryzysową,
- pojęcie sytuacji kryzysowej jest nadrzędne wobec pojęcia kryzysu,
- kulminacyjnym elementem sytuacji kryzysowej, jeżeli nie zdoła się zaradzić jej czynnikom na etapie eskalacji, jest kryzys,
- sytuacja kryzysowa rozpoczyna się z chwilą pojawienia się jej symptomów, które charakteryzują się przekroczeniem subiektywnie postrzeganego poziomu ryzyka, stanowiącego dla danego podmiotu granicę akceptowalnego poziomu bezpieczeństwa,
- sytuacja kryzysowa obejmuje: etap przedkryzysowy, etap kryzysu, etap pokryzysowy,
- niepodjęcie stosownych działań zaradczych może doprowadzić, w zależności od charakteru sytuacji, do wojny, całkowitego upadku organizacji lub innego stanu jej funkcjonowania, także do innej sytuacji kryzysowej,
- sytuacja kryzysowa, w jakiej się znajduje dany podmiot, stwarza nie tylko zagrożenie, lecz może być również szansą jego rozwoju[18].

Sytuacja kryzysowa pojawia się z reguły jeszcze w czasie pokoju, a kończy w okresie ostrego kryzysu, kiedy następuje wprowadzenie stanów nadzwyczajnych.

Tabela 11. Sytuacja kryzysowa

Zdarzenie (niepokoje) społeczne	Zdarzenia terrorystyczne
SYTUACJA KRYZYSOWA	
Katastrofy naturalne	Awarie techniczne

Źródło: Opracowanie własne

Tabela 12. Umiejscowienie sytuacji kryzysowej w systemie bezpieczeństwa państwa

Stan bezpieczeństwa państwa		
Pokój	Kryzys	Wojna
Sytuacja kryzysowa	Stany nadzwyczajne	
niepokoje społeczne zdarzenia terrorystyczne katastrofa naturalna awaria techniczna	stan klęski żywiołowej stan wyjątkowy stan wojenny	

Źródło: Opracowanie własne

Zarządzanie kryzysowe

Zarządzanie kryzysowe w państwie stanowi integralny element zarządzania jego bezpieczeństwem wewnętrznym i zewnętrznym. Pełni rolę usługową w sto-

[18] J. Gryz, W. Kitler, op. cit., s. 23.

sunku do społeczeństwa. W jego ramach podejmowane są działania mające na celu przeciwdziałanie zagrożeniom, przygotowanie uprawnionych podmiotów (w tym i ludności) na sytuację ich wystąpienia oraz utrzymania lub przywrócenia stanu stabilizacji. Jest działaniem celowym, realizowanym przez uprawnione podmioty na wszystkich poziomach zarządzania bezpieczeństwem państwa (krajowym, resortowym, wojewódzkim, powiatowym, gminnym). Uczestniczą w nim nie tylko podmioty zarządzające, ale także wyspecjalizowane organizacje, służby, straże, inspekcje i społeczeństwo.

Podstawę rozważań na temat zarządzania kryzysowego stanowi nauka o organizacji i zarządzaniu, na podstawie której konstruowane są mechanizmy planowania, podejmowania i realizacji decyzji. Wymiar narodowy zarządzania kryzysowego ma ścisły związek z działaniami politycznymi, ekonomicznymi, społecznymi, kulturowymi, wojskowymi na rzecz budowy, mobilizacji i wykorzystywania możliwości w stanach zagrożenia. Dlatego mówienie o zarządzaniu kryzysowym należy poprzedzić prezentacją pojęcia zarządzania organizacją stosowanego w naukach o organizacji i zarządzaniu – zob. tabela 13.

Tabela 13. Pojęcie zarządzania organizacją

Autor	Pojęcie
J. Penc, *Leksykon biznesu*, Warszawa 1997, s. 506	Zarządzanie to układ działań regulujących funkcjonowanie danej organizacji, zgodnie z wytyczonymi celami.
A.K. Koźmiński, *Zarządzanie tu i teraz*, Warszawa 1996, s. 14	Zarządzanie jest swego rodzaju wędrówką przez chaos, konstruowaniem rzeczywistości z dostępnych zarządzającemu elementów: pomysłów, ludzi i relacji między nimi, instytucji formalno-prawnych, środków materialnych i pieniężnych, a także praw do dysponowania nimi.
L. Krzyżanowski, *Podstawy nauk o organizacji i zarządzaniu*, Warszawa 1998, s. 207	Zarządzanie to taki rodzaj kierowania, w którym tytuł do wywierania wpływu na hierarchię i systemy wartości, interesy, dążenie oraz postawy i organizacyjne zachowania kierowanych wynika głównie, choć nie wyłącznie, z władania lub z faktu dysponowania przez kierującego zasobami materialno-energetycznymi lub nominalnymi i informacyjnymi o szczególnym znaczeniu dla funkcjonowania i rozwoju organizacji bądź z samego przeświadczenia kierowanych, że kierujący ma możliwość pozyskiwania tych zasobów.
Twórcy naukowych podstaw organizacji, red. J. Kurnal, Warszawa 1972, s. 16	Zarządzanie to szczególny rodzaj kierowania, w którym podstawą oddziaływania na przedmiot kierowania jest sformalizowana hierarchiczna nadrzędność podmiotu kierowania (władza wynikająca z formalnej hierarchii).
Teoria organizacji i zarządzania, red. J. Kurnal, Warszawa 1979, s. 16	Zarządzanie umownie można rozumieć jako szczególny rodzaj kierowania, w którym podstawą oddziaływania na przedmiot kierowania jest sformalizowana, hierarchiczna nadrzędność podmiotu kierowania (władza wynikająca z formalnej hierarchii).
L.H. Haber, *Management. Zarys zarządzania małą firmą,* Kraków 1998, s. 19	Zarządzanie należy traktować jako formę praktycznej działalności związanej z procesem podejmowania decyzji dotyczących jak najlepszego wykorzystania posiadanych zasobów rzeczowych, kapitałowych i ludzkich w celu realizacji założonych zadań, zapewniających stały rozwój organizacji.

Encyklopedia biznesu, cz. II, Warszawa 1995, s. 1138	Zarządzanie to ustawiczny proces tworzenia reguł ładu w danym układzie w postaci norm, planów i instrukcji i innych jeszcze dokumentów. Ze swego założenia mają one być instrumentami koordynacji w pozyskiwaniu rzeczowych i osobowych składników działalności, ich rozmieszczeniu i stosowaniu do określonych w tej działalności celów.
R.W. Griffin, *Podstawy zarządzania organizacjami*, Warszawa 1996, s. 38	Zarządzanie to zestaw działań (obejmujących planowanie i podejmowanie decyzji, organizowanie, przewodzenie, tj. kierowanie ludźmi i kontrolowanie) skierowanych na zasoby organizacji (ludzkie, finansowe, rzeczowe oraz informacyjne) i wykonywanych z zamiarem osiągnięcia celów organizacji w sposób sprawny i skuteczny.
F.E. Kast, J.E. Rosenzweig, *Organization and Management*, New York 1979, s. 339	Zarządzanie to proces koordynowania zbiorowych wysiłków ludzi działających w zorganizowanych strukturach dla osiągnięcia założonych celów w oparciu o wyznaczone zadania i przy pomocy techniki.
W.A. Shrode, D. Voich, *Organization and Management: Basic systems concepts*, Illinois 1974, s. 7	Zarządzanie to zespół działań lub proces mający na celu koordynację i integrację użytkowania zasobów dla osiągnięcia celu organizacji (wydajności i satysfakcji) poprzez ludzi przy użyciu techniki w zorganizowanych strukturach.
W.J. Stanton, M.J. Etzel, B.J. Walker, *Fundamentals of Marketing*, New York 1994, s. 661	Zarządzanie to proces planowania, nadawania mocy i oceniania starań (wysiłków) zespołów ludzkich pracujących dla wspólnego celu.
A. Zawiślak, *Pułapy i pułapki zarządzania*, Warszawa 1982, s. 44	Zarządzanie to proces decyzyjny realizowany na wielu poziomach organizacji, który ma zapewnić eliminację wykrytych zagrożeń, wykorzystywanie zarysowujących się szans oraz efektywne spełnianie przez organizację wszystkich funkcji niezbędnych do osiągania postawionego celu.
B. Mikuła, *Organizacje oparte na wiedzy*, Kraków 2006, s. 119	Zarządzanie […]: jest to sposób będący postępowaniem normującym i dyspozycyjnym, który ma powodować osiągnięcie założonych celów przez podmiot gospodarczy (instytucję) i jego podsystemy. proces ten zachodzi w układzie uzależnienia organizacyjnego (jako relacji nadrzędności – podporządkowania) kierownictwa i wykonawstwa oraz jest zdeterminowany przez spełnienie następujących funkcji: decydowania, identyfikacji, planowania, organizacji, motywacji, kontroli, funkcje zarządzania są uporządkowane i zintegrowane w formach organizacyjnych, do których należą: system decyzyjny zarządzania: zarządzanie strategiczne, zarządzanie zasobami ludzkimi, zarządzanie marketingowe, zarządzanie finansami, zarządzanie operacyjne i inne, systemy funkcjonalne, to procedury i procesy ukierunkowane na realizację prac administracyjnych, ekonomiczno-zarządczych, badawczych i innych w poszczególnych dziedzinach działalności firmy, systemy techniczne procesu zarządzania (systemy łączności, komputerowe systemy obliczeniowe, monitoring), układy zintegrowane, funkcje zarządzania są spełniane przy wykorzystaniu określonych instrumentów, np. ekonomiczno-finansowych, prawnych, motywacyjnych przez techniki negocjacji, metody rachunkowe i inne.

Źródło: Opracowanie własne

Powyższe definicje uprawniają do stwierdzenia, że zarządzanie jest działalnością kierowniczą stanowiącą zestaw przemyślanych działań, które polegają na ustaleniu celów organizacji i powodowaniu ich realizacji dzięki skoordynowaniu wysiłków (starań)

wszystkich jej uczestników oraz wykorzystaniu posiadanych przez nią zasobów, procesów i informacji w sposób sprawny i skuteczny oraz zgodny ze społeczną racjonalnością działań gospodarczych. Innymi słowy, zarządzanie organizacją to zespół działań zapewniających koordynację i integrację użytkowania zasobów w zorganizowanych strukturach oraz współpracę z jej otoczeniem zewnętrznym w taki sposób, aby przyjęte przez nią cele mogły być osiągane skutecznie oraz sprawnie i zapewniać jej reputację i prestiż w otoczeniu. Zarządzanie jest wielką sztuką pobudzania przy wykorzystaniu posiadanych środków, technologii i własnych umiejętności, energii i inwencji twórczej wszystkich, którzy przyczyniają się do wartości (dóbr, usług, informacji). Oznacza ono zatem sterowanie (przy wykorzystaniu stosownych technik i informacji) wszystkimi elementami systemu w sposób zintegrowany, aby we wzajemnym powiązaniu i oddziaływaniu przyczyniały się do powodzenia organizacji, tj. urzeczywistnianiu jej celów. Odnosi się ono przede wszystkim do ludzi, do organizowania ich pracy i wyposażenia jej w niezbędne środki oraz tworzenia takich warunków i motywacji, aby mogli oni i chcieli w pełni angażować się w swoją pracę i obowiązki służbowe[19].

Zarządzanie tworzy określony porządek ekonomiczny, przenosi obowiązujące w społeczeństwie normy i wartości do praktyki, utrwala pożądane zachowania ludzi, ich postawy i nastawienia, czyli gotowość do realizacji postawionych przed nimi zadań oraz selekcji kryteriów doboru sposobów i środków prowadzących do ich rozwiązania[20].

W nowej technologii zarządzania, rozumianej jako całokształt wiedzy, umiejętności i gotowości ich stosowania przez podmioty zarządzania połączone w zorganizowany sposób z materialnymi środkami zarządzania, umiejętnie łączy się w spójną całość elementy twarde (technika zarządzania), miękkie (koncepcje zarządzania) i organizacyjne (organizacja zarządzania)[21]. Mówiąc o zarządzaniu, należy pamiętać, że opiera się ono na formalnych zależnościach, które pozwalają na dokonanie podziału zadań i kompetencji oraz koordynację działań. Nakreśla również ramy do współdziałania jednostek w trakcie prowadzenia działań i określa sposoby ich aktywizacji. Zarządzanie ma ścisły związek z funkcjonowaniem organizacji, która traktowana jest jako grupa ludzi mających wspólny cel, zadania, plany oraz program działania, w swej istocie jest ono także procesem tworzenia i przekształcania organizacji w coraz sprawniej i skuteczniej działający system.

Wyznacznikiem zarządzania jest posiadanie przez zarządzającego władzy, której podstawę stanowi prawo do dysponowania zasobami pozwalającymi na funkcjonowanie organizacji. Głównym zadaniem organu zarządzającego jest wypracowanie takiej strategii oddziaływania na członków organizacji, która w danych warunkach będzie optymalna, czyli zapewni rozwój i zyski organizacji bez względu na osobiste strategie realizowane przez poszczególnych jej człon-

[19] J. Penc, *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Kraków 1998, s. 59 i 60.

[20] B. Wawrzyniak, *Przedsiębiorczość – klucz do przyszłości*, „Przegląd Organizacji" 1988, nr 7, s. 7.

[21] J.K. Solarz, *Narodowe style zarządzania. Mity czy fakty*, Wrocław 1984, s. 25.

ków[22]. Odzwierciedleniem strategii organu zarządzającego są ustanowione zasady funkcjonowania organizacji, czyli zbiór przepisów, regulujących:

- podział zadań i kompetencji pomiędzy poszczególnych członków tej organizacji,
- sposób doboru, opiniowania i wynagrodzenia jej członków,
- sposób rozstrzygania sporów zaistniałych wewnątrz organizacji,
- zasady współdziałania członków (komórek) organizacji w czasie rozwiązywania problemów obejmujących swoim obszarem kompetencje kilku członków (komórek) organizacji,
- sposób oddziaływania na poszczególnych członków w celu zwiększenia ich zaangażowania na rzecz realizacji celów organizacji, czyli przekonanie ich, że najlepszą strategią działania jest przyjęta przez tę organizację[23].

Zarządzający określa cele, jakie ma osiągnąć dana organizacja (państwo, województwo, powiat, gmina), co jest równoznaczne z określeniem stanu, w jakim powinna się ona znaleźć po ich realizacji. W procesie planowania wykonawstwa przyjętych celów zarządzający musi uwzględniać zagrożenia, jakie mogą pojawić się w otoczeniu zewnętrznym organizacji (państwa, województwa, powiatu, gminy), co nie oznacza, że nie musi monitorować ich otoczenia wewnętrznego. Środowisko bezpieczeństwa międzynarodowego jest bowiem złożone i nieprzewidywalne, co w określonych sytuacjach można odnieść do środowiska narodowego. Oznacza to, iż organizacja i jej otoczenie zawsze może znaleźć się w innym stanie, niż to zarządzający przewidywał. Stany przejściowe organizacji i jej otoczenia można podzielić na:

- pożądane, zgodne z przewidywaniami zarządzającego,
- korzystniejsze od przewidywanych, stanowią wtedy szanse na szybsze realizowanie naszych celów,
- obojętne, nieprzewidywalne, ale nie mające zasadniczego wpływu na realizację założonych celów,
- niekorzystne, stwarzające zagrożenia w osiągnięciu przyjętego celu,
- bardzo niekorzystne (kryzysowe), stwarzające zagrożenie nie tylko dla realizacji zadań, ale również dla przetrwania samej organizacji[24].

Zarządzający organizacją muszą mieć świadomość tego, że prawdopodobieństwo wystąpienia poszczególnych stanów jest zróżnicowane, jednak żadnego z nich nie można wykluczyć.

Zaprezentowane definicje mają istotny wpływ na rozumienie terminologii zarządzania kryzysowego, a ponadto przekładają się one na jego pojęcie.

22 E. Nowak, op. cit., s. 41.

23 Ibidem.

24 Ibidem.

Tabela 14. Pojęcia zarządzania kryzysowego

Źródło	Pojęcie
Leksykon zarządzania, Warszawa 2004, s. 674	Zarządzanie kryzysowe to szczególna forma zarządzania polegająca na możliwie wczesnym rozpoznaniu ukrytych sytuacji kryzysowych oraz zaplanowaniu i podjęciu działań zapobiegawczych i zmniejszających ostre kryzysy. Celem jest wyprowadzenie organizacji z kryzysu oraz stworzenie trwałych podstaw do jej dalszej egzystencji i rozwoju. Zarządzanie w kryzysie zależy od rodzaju kryzysu i fazy kryzysu.
R. Wróblewski, *Zarys teorii kryzysu, zagadnienia prewencji i zarządzania kryzysami*, Warszawa 1996, s. 39	Zarządzanie kryzysowe to proces kierowania w państwie mający na celu zapobieganie sytuacjom kryzysowym, a w wypadku ich zaistnienia – zawrócenie kierunku rozwoju nagłych i niebezpiecznych wydarzeń, zagrażających żywotnym interesom społeczeństwa.
M. Amstrong, *Jak być dobrym menadżerem*, Warszawa 1997, s. 150	Zarządzanie kryzysowe to proces rozwiązywania napiętych sytuacji w sposób, w którym szereg współzależnych operacji jest planowany, organizowany, kierowany i kontrolowany. Wytyczany jest także kierunek procesu decyzyjnego dla osób odpowiedzialnych za podejmowanie decyzji w celu uzyskania szybkiego, lecz nie pochopnego rozwiązania problemu, w obliczu którego znalazła się organizacja. W ujęciu prakseologicznym zarządzanie kryzysowe to nic innego jak dobre zarządzanie pod presja.
E. Nowak, *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Warszawa 2007, s. 43	Zarządzanie kryzysowe to uporządkowana działalność polegająca na zapobieganiu sytuacjom kryzysowym lub przejmowaniu nad nimi kontroli i kształtowaniu ich przebiegu w drodze zaplanowanych działań oraz na odtworzeniu zasobów lub przywróceniu im ich pierwotnego charakteru. Zarządzanie kryzysowe 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.
P. Sienkiewicz, P. Górny, *Analiza systemowa sytuacji kryzysowych*, Warszawa 2001, s. 32	Zarządzanie kryzysowe to 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.
M. Cieślarczyk, R. Kuriata, *Kryzysy i sposoby radzenia sobie z nimi*, Łódź 2005, s. 103	Zarządzanie kryzysowe to całokształt rozwiązań systemowych w zakresie ochrony ludności, realizowanych przez władze publiczne wszystkich szczebli we współdziałaniu z wyspecjalizowanymi organizacjami i instytucjami, celem zapobiegania sytuacjom trudnym, niebezpiecznym, stwarzającym zagrożenia dla życia, zdrowia, mienia, środowiska, infrastruktury, przygotowania systemu reagowania, a w razie wystąpienia zagrożeń, kształtowanie, kontrolowanie ich przebiegu (reagowanie) w sposób zapewniający minimalizowanie strat, a także odbudowę struktur po katastrofie.
Słownik z zakresu terminów bezpieczeństwa narodowego, Warszawa 2009, s. 166	Zarządzanie kryzysowe to reagowanie na nadciągający lub trwający kryzys i usuwanie jego skutków w cyklu zdarzeń i czynności, od przewidywania i planowania antykryzysowego wraz z reagowaniem na codzienne zdarzenia, aż po zakończeniu odbudowy ze zniszczeń (przygotowanie, reagowanie, odbudowa).

Elementarne pojęcia pedagogiki społecznej i pracy socjalnej, red. D. Ladek, T. Pilch, Warszawa 1999, s. 72	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 likwidacja skutków zaistniałej sytuacji.
J. Gołębiewski, *Zarządzanie kryzysowe*, „Wiedza Obronna" 2001, nr 1, s. 76	Zarządzanie kryzysowe to całokształt rozwiązań systemowych w zakresie ochrony ludności, realizowanych przez władze publiczne wszystkich szczebli, we współdziałaniu z wyspecjalizowanymi organizacjami i instytucjami, celem zapobiegania sytuacjom trudnym, niebezpiecznym, stwarzającym zagrożenie dla życia, zdrowia, mienia, środowiska i infrastruktury; przygotowania systemu reagowania, a w razie wystąpienia zagrożeń kształtowanie i kontrolowanie ich przebiegu (reagowanie) w sposób zapewniający minimalizowanie strat i akceptowany poziom bezpieczeństwa oraz odbudowy struktur społecznych po katastrofie.
K. Zieliński, *Bezpieczeństwo obywateli podczas kryzysów niemilitarnych oraz reagowanie w razie katastrof i klęsk żywiołowych,* Warszawa 2004, s. 29	Zarządzanie kryzysowe to całokształt rozwiązań systemowych w sferze ochrony ludności, wypełnianych przez władze publiczne wszystkich szczebli, we współdziałaniu z wyspecjalizowanymi organizacjami i innymi instytucjami w celu zapobiegania sytuacjom niebezpiecznym, stwarzającym zagrożenie dla życia, zdrowia obywateli oraz środowiska.
J. Gryz, W. Kitler, *System reagowania kryzysowego*, Toruń 2007, s. 33 i 34	Zarządzanie kryzysowe 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. Zarządzanie kryzysowe jest zatem: integralną częścią zarządzania organizacją (systemem) w ogóle, dziedziną zarządzania bezpieczeństwem w ogóle, w tym bezpieczeństwem państwa, zarządzaniem organizacją pod presją, w stanie ryzyka, rozwiązywaniem sytuacji napiętych, działaniem na rzecz obniżenia napięć i przeciwdziałania konfliktom lub sytuacjom trudnym o charakterze niekonfliktowym, przeciwdziałaniem eskalacji kłopotliwych zjawisk, działalnością polegająca na przywracaniu stanu normalnego lub utrzymaniu tego stanu mimo wystąpienia symptomów sytuacji kryzysowej, działaniem celowym – podczas zarządzania kryzysowego odrzucamy problemy marginalne i wątpliwe, przekazując je instytucjom niezajmującym się sytuacją kryzysową.
Art. 2 ustawy z dnia 17 lipca 2009 roku *o zmianie ustawy o zarządzaniu kryzysowym* (Dz. U. z 2009 r. Nr 131, poz. 1073)	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 odtworzeniu zasobów i infrastruktury krytycznej.

Źródło: Opracowanie własne

Uwzględniając powyższe definicje, zarządzanie jest szczególnym przypadkiem organizowania, polegającym na łączeniu ze sobą w skoordynowany sposób

jednostek i zasobów dla osiągnięcia pożądanego celu[25]. Występująca „koordynacja może przybierać formy tak zindywidualizowane, jak i zbiorowe. Zarządzać może zespół albo jedna osoba. Punktem wyjścia powstania zarządzania jest postrzegana niepewność, ponieważ zarządzanie jest radzeniem sobie z niepewnością"[26]. Takie ujęcie zarządzania w pełni odnosi się do zarządzania kryzysowego na wszystkich poziomach zarządzania bezpieczeństwem państwa, które w aspekcie występowania szerokiego spektrum zagrożeń jest coraz bardziej złożone oraz wymagające m.in. wyspecjalizowanej wiedzy. Skuteczne wykonawstwo zadań przez uprawnione podmioty w trakcie zarządzania kryzysowego na poziomie państwa, województwa, powiatu i gminy wymaga nie tylko czytelnych przepisów prawa, profesjonalizmu osób, służb, instytucji, wyposażenia w odpowiedni sprzęt, ale i odpowiednich nakładów finansowych, które rzutują na realizowane zadania w czasie trwania kryzysu.

W celu niedopuszczenia lub zminimalizowania negatywnych skutków kryzysu ważny jest sprawnie działający system informacji, m.in. o symptomach pojawiających się zagrożeń kryzysowych. W stanie poprzedzającym wystąpienie kryzysu, w czasie jego trwania oraz odtwarzania stanu przedkryzysowego istotny jest przepływ informacji. Posiadanie właściwych informacji w zarządzaniu kryzysowym jest sprawą o zasadniczym znaczeniu. Są one traktowane jako podstawowy element, który niejednokrotnie decyduje o skuteczności i jakości zarządzania. Taką rolę spełnia system informacyjny, który powinien zapewniać dostęp do informacji uprawnionym odbiorcom, we właściwym czasie i w sposób czytelny. Powinien również wspierać proces monitorowania zagrożeń na poziomie państwa, województwa, powiatu i gminy.

Mając na uwadze powyższe rozważania, zarządzanie kryzysowe jest:

- integralną częścią zarządzania organizacją (systemem),
- dziedziną zarządzania bezpieczeństwem w ogóle, w tym bezpieczeństwem narodowym,
- zarządzaniem organizacją pod presją w stanie ryzyka,
- rozwiązywaniem napiętych sytuacji,
- przeciwdziałaniem eskalacji kłopotliwych zjawisk[27].

Działania podejmowane w ramach zarządzania kryzysowego powinny sprowadzać się do obniżania napięć i przeciwdziałania konfliktom lub sytuacjom trudnym o charakterze niekonfliktowym, a także do przywracania stanu normalnego lub utrzymania tego stanu mimo wystąpienia symptomów sytuacji kryzysowej.

[25] S.E. Sjöstrand, *Företagsledning (Zarządzanie),* [in:] *Organisationsteori på svenska (Teoria organizacji po szwedzku),* ed. B. Czarniawska, Malmö 1998.

[26] M. Kostera, *Współczesne koncepcje zarządzania*, Warszawa 2008, s. 9, 10.

[27] E. Nowak, op. cit., s. 43.

2.2. Zasady zarządzania kryzysowego

Zarządzanie ma ścisły związek z działalnością organizacji, która rozumiana jest jako grupa ludzi posiadających wspólny cel, zadania, plany oraz program działania. Zarządzanie jest również procesem tworzenia i przekształcania organizacji w sprawny i skutecznie działający system.

Podstawowym zadaniem podmiotów zarządzających na poziomie kraju, województwa, powiatu i gminy jest wypracowanie i praktyczne wdrożenie takiej strategii oddziaływania na członków organizacji, która w określonych warunkach umożliwi rozwój organizacji. Wyznacznikiem strategii podmiotu zarządzającego jest określenie zasad działania organizacji, czyli przepisów regulujących: podział zadań i kompetencji pomiędzy poszczególnych członków, sposób doboru, opiniowania i wynagradzania jej członków, rozstrzygania sporów zaistniałych wewnątrz organizacji, zasady współdziałania członków organizacji w czasie rozwiązywania problemów obejmujących swoim obszarem kompetencje kilku członków, sposób oddziaływania na poszczególnych członków w celu zwiększenia ich zaangażowania na rzecz realizacji celów organizacji, czyli przekonania ich, że najlepszą strategią działania jest strategia organizacji[28]. Wskazanie i przestrzeganie określonych zasad i umiejętności leży u podłoża skutecznego zarządzania. Zasady obowiązujące w zarządzaniu organizacją zestawiono w tabeli 15.

Tabela 15. Czternaście zasad zarządzania organizacją

Zasada	Treść
podział pracy	Im bardziej ludzie się wyspecjalizują, tym sprawniej mogą wykonywać swoją pracę.
autorytet	Kierownicy muszą wydawać polecenia, aby prace były wykonywane. Autorytet formalny daje im prawo rozkazywania, ale nie zawsze zapewnia posłuszeństwo, jeżeli nie będzie mu towarzyszyć także autorytet osobisty (na przykład wynikający z potrzebnej wiedzy).
dyscyplina	Członkowie organizacji powinni przestrzegać przepisów i uzgodnień nią rządzących. Dyscyplina wynika z dobrego przywództwa na wszystkich szczeblach organizacji.
jednolitość rozkazodawstwa	Każdy pracownik powinien otrzymywać polecenia od jednej tylko osoby. Podporządkowanie pracownika więcej niż jednemu bezpośredniemu przełożonemu prowadzi niekiedy do sprzecznych poleceń i zakłócenia autorytetu.
jednolitość kierowania	Jeden kierownik powinien kierować operacjami prowadzącymi w organizacji do jednego celu i realizowanymi według jednego planu.
podporządkowanie interesu osobistego interesowi ogółu	W żadnym przedsięwzięciu interesy poszczególnych pracowników nie powinny przeważać nad interesami organizacji jako całości.
wynagrodzenie	Płaca za wykonaną pracę powinna być sprawiedliwa zarówno z punktu widzenia pracownika, jak i pracodawcy.

[28] Ibidem, s. 41.

centralizacja	Ograniczenie roli podwładnych w podejmowaniu decyzji oznacza centralizację, zwiększenie zaś ich roli decentralizację. Ostateczna odpowiedzialność za podejmowanie decyzji należy do kierowników, ale jednocześnie powinni oni przekazywać podwładnym dostateczne uprawnienia decyzyjne, aby mogli oni właściwie wykonywać swoje zadania.
hierarchia	Linie podporządkowania w organizacji, przebiegające od głównego kierownika do najniższego szczebla w organizacji.
ład	Każdy człowiek i każda rzecz powinny być na właściwym miejscu we właściwym czasie. Ludzie powinni zajmować te stanowiska, które są dla nich najodpowiedniejsze.
odpowiednie traktowanie pracowników	Kierownicy powinni się odnosić do podwładnych w sposób przychylny i sprawiedliwy.
stabilność personelu	Duża fluktuacja pracowników niekorzystnie wpływa na sprawność funkcjonowania organizacji.
inicjatywa	Podwładni powinni mieć swobodę tworzenia i realizacji swoich planów, nawet jeżeli to może prowadzić do pewnych błędów.
harmonia	Praca zespołowa, poczucie jedności i przynależności do jednej grupy powinny być popierane i podtrzymywane.

Źródło: J.A. F. Stoner, R.E. Freeman, D.R. Gilbert, *Kierowanie*, Warszawa 1999, s. 52

Można przyjąć, że przedstawione wyżej ogólne zasady zarządzania są również zestawem reguł dla zarządzania kryzysowego. Zasady zarządzania kryzysowego umożliwiają podmiotom na poziomach krajowym, wojewódzkim, powiatowym i gminnym na realizowanie zadań wynikających z ustawy z dnia 26 kwietnia 2007 roku *O zarządzaniu kryzysowym*[29] i innych ustaw szczegółowych. Ponadto zasady te pozwalają na dostosowanie prowadzonej działalności do przepisów prawa regulujących problematykę związaną z zarządzaniem kryzysowym, co pozwala na skuteczne realizowanie ustawowych zadań. Zasady zarządzania kryzysowego przedstawiono w tabeli 16.

Tabela 16. Podstawowe zasady zarządzania kryzysowego

Zasada	Treść
jednoosobowego kierownictwa	Polega na powierzeniu kompetencji decyzyjnych jednoosobowym organom, które sprawują władzę ogólną w danym zakresie kompetencji. Organami takimi są: premier, wojewoda, starosta, wójt, burmistrz, prezydent miasta.
odpowiedzialności organów władzy publicznej	Reguła określająca odpowiedzialność za zarządzanie w sytuacjach kryzysowych przez funkcjonujące w państwie organy administracji rządowej i samorządowej. Wiąże się ze stałą, historycznie uwarunkowaną, podstawową rolą administracji, która sprowadza się do usuwania zagrożeń i zapewnienia bezpieczeństwa w powierzonym jej zakresie władzy administracyjnej.
prymatu układu terytorialnego	Oznacza, że podstawę działania organów władzy stanowi podział terytorialny państwa i dostosowanie planu działania do warunków miejscowych.

[29] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

powszechności	Zobowiązuje wszystkie podmioty prawa państwowego do uczestnictwa w działaniach antykryzysowych, stosownie do ich statusu prawnego i organizacyjnego.
funkcjonalnego podejścia	Polega na określeniu względnie stałych, zwykle powtarzalnych, typowych i sformalizowanych proceduralnie działań, wyodrębnionych ze względu na ich rodzaj i charakter, ukierunkowanych na realizację celów bezpieczeństwa państwa.
zespolenia	Nadaje się władztwo organom władzy ogólnej (wojewoda, starosta, wójt) według zasad określonych w ustawach (nad wszelkimi pozostałymi formami administracji zarówno zespolonej, jak i niezespolonej).
ciągłości funkcjonowania państwa	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.
pomocowości	Wzajemna pomoc.

Źródło: W. Kitler, *Zarządzanie bezpieczeństwem narodowym jako podstawa organizacji zarządzania kryzysowego*, [w:] *Zarządzanie kryzysowe w sytuacji klęski żywiołowej*, red. E. Nowak, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 2006, nr 1, s. 52–62

Warto również mieć na uwadze zasadę adekwatności, która nakazuje podjęcie zarządzania kryzysowego (w pierwszej kolejności) na najniższym poziomie terytorialnym.

> Oznacza to, że jeżeli skutki jakiegoś zagrożenia nie przekraczają granic gminy, to całość działań antykryzysowych należeć będzie do kompetencji wójta (burmistrza, prezydenta, miasta). Natomiast gdy skutki, na przykład katastrofy, przekroczą granicę gminy, to główną rolę zarządzającego działaniami ratowniczymi przejmuje starosta. Podobnie rola jest wypełniana przez wojewodę (gdy skutki jakiegoś zdarzenia przekroczą granicę jednego powiatu) i ministra (gdy skutki urzeczywistnionego lub potencjalnego zagrożenia wykraczają poza jedno województwo). Zaznaczenia wymaga też obowiązkowa gotowość organów wyższego szczebla do udzielenia pomocy organom niższego szczebla[30].

Oprócz wymienionych zasad obowiązujących w zarządzaniu kryzysowym, skuteczne i jednolite działania w sytuacjach kryzysowych wszelkich organów władzy wymagają przy tym spełnienia czterech elementarnych warunków:

- posiadania odpowiednio szerokich kompetencji, czyli prawa do egzekwowania władzy nad innymi w sytuacjach kryzysowych (w przypadku kryzysów wewnętrznych) – spełnienie tego warunku wymaga istnienia odpowiedniego systemu prawnego; prawo powinno regulować wszelkie kwestie obowiązków władz i organizacji, zarówno tych wchodzących w skład administracji publicznej, specjalnie przez nią powołanych z powodu szczególnego stanu nadzwyczajnego, jak i utworzonych z inicjatywy społecznej;
- posiadanie możliwości oddziaływania na przebieg oraz skutki kryzysów zewnętrznych, których wpływ na stan bezpieczeństwa wewnętrznego państwa w dobie globalizacji będzie się sukcesywnie powiększał;

[30] *Zarządzanie kryzysowe a media i granice państw w erze globalizacji*, red. M. Koziński, Słupsk 2010, s. 34.

- posiadania dostępu do baz danych zapewniających otrzymywanie pełnych, aktualnych i wiarygodnych informacji; wiąże się to nie tylko z możliwością przetwarzania tych informacji, ale przede wszystkim podejmowania wynikających z nich natychmiastowych decyzji wdrażanych w życie; spełnienie tego założenia wymaga funkcjonowania odpowiedniego systemu stanowisk operacyjno-koordynacyjnych oraz procedur;
- posiadania planów zarządzania kryzysowego w skali państwa, województw, powiatów, gmin na wypadek potencjalnych, zidentyfikowanych i prognozowanych sytuacji kryzysowych; dzięki nim, a także prowadzonym na ich podstawie przygotowaniom, np. ćwiczeń, możliwe jest określenie: kto i za co odpowiada, co i kiedy będzie robił, za pomocą jakich sił i środków oraz na jakiej podstawie prawnej[31].

2.3. Etapy zarządzania kryzysowego

Ustawa z dnia 26 kwietnia 2007 roku *O zarządzaniu kryzysowym* w art. 2 stanowi, że 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 odtwarzania zasobów i infrastruktury krytycznej[32]. Wymaga to ze strony uprawnionych podmiotów zarządzających bezpieczeństwem państwa podejmowania wielu wzajemnie powiązanych przedsięwzięć, które pozwolą na niedopuszczenie do wystąpienia sytuacji kryzysowej lub zminimalizowania jej negatywnych następstw.

Zarządzanie kryzysowe składa się z dwóch podstawowych okresów stabilizacji i realizacji. W okresie stabilizacji podejmowane są przedsięwzięcia poprzedzające wystąpienie sytuacji kryzysowej, obejmują one etap zapobiegania i etap przygotowania – to szereg przedsięwzięć natury organizacyjnej na poziomach: krajowym, wojewódzkim, powiatowym i gminnym, których celem jest przygotowanie i wdrożenie wypracowanych decyzji skutkujących niedopuszczeniem do wystąpienia zagrożenia lub zminimalizowania wystąpienia jego negatywnych następstw. Ponadto uprawnione podmioty zarządzające i wykonawcze realizują czynności bez konieczności uruchamiania procedur alarmowych.

W okresie realizacji wykonywane są przedsięwzięcia związane ze zwalczaniem zagrożeń i ich skutków, a także odtwarzaniem zniszczonej infrastruktury. Są one wykonywane na podstawie wypracowanych i wdrożonych procedur po-

[31] J. Gryz, W. Kitler, op. cit., s. 202.

[32] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

stępowania przez uprawnione podmioty zarządzające, specjalistyczne podmioty wykonawcze i w uzasadnionych sytuacjach społeczeństwo. Okres ten obejmuje etapy reagowania i odbudowy.

Tabela 17. Proces zarządzania kryzysowego

Okres zarządzania kryzysowego	Etapy zarządzania kryzysowego
STABILIZACJA, okres przed wystąpieniem zagrożenia i po jego przezwyciężeniu, a przed następną sytuacją kryzysową	ZAPOBIEGANIE, działania, które mają eliminować lub redukować prawdopodobieństwo wystąpienia kryzysu i ograniczać jego negatywne skutki dla ludzi i środowiska. PRZYGOTOWANIE, działalność planistyczno-organizacyjna, która obejmuje: opracowywanie planów i scenariuszy na wypadek wystąpienia określonej sytuacji kryzysowej; działania mające na celu zwiększanie sił i środków potrzebnych do efektywnego działania. Działania przygotowawcze obejmują również praktyczne przygotowanie podmiotów zarządzających i ratowniczych oraz ludności pod kątem postępowania na wypadek zaistnienia sytuacji kryzysowej.
REALIZACJA, okres eskalacji, przesilenia i deeskalacji sytuacji kryzysowej	REAGOWANIE, przedsięwzięcia podejmowane po wystąpieniu określonej sytuacji kryzysowej. Celem działań w tej sferze jest dostarczanie pomocy poszkodowanym oraz ograniczenie bezpośrednich i wtórnych zniszczeń i strat. Podmioty wykonawcze zarządzania kryzysowego to podstawowe siły reagowania. ODBUDOWA, końcowy etap procesu zarządzania kryzysowego, którego podstawowym zadaniem jest przywrócenie stanu poprzedniego i odtworzenie infrastruktury krytycznej mniej wrażliwych na następne sytuacje kryzysowe.

Źródło: Opracowanie własne na podstawie J. Gołębiewski, *Zarządzanie kryzysowe metodą rozwiązywania problemów bezpieczeństwa*, [w:] *Zarządzanie kryzysowe w transporcie lądowym na Pomorzu. Materiały konferencyjne*, Szczecin 2003, s. 10–20

Zarządzanie kryzysowe wymaga wypracowania i praktycznego wdrożenia przedsięwzięć mieszczących się w czterech etapach, do których zalicza się zapobieganie, przygotowanie, reagowanie, odbudowę.

Tabela 18. Etapy zarządzania kryzysowego

Etapy zarządzania	Treść etapów
Zapobieganie	działania legislacyjne, przygotowanie systemu zarządzania i dowodzenia, przygotowanie i gospodarowanie budżetem, określanie priorytetów działania dla etapu zapobiegania, monitorowanie zagrożeń, analiza i ocena zagrożeń, analiza źródeł i symptomów zagrożeń, ocena wrażliwości społeczeństwa na zagrożenia i jego przygotowania do działań antykryzysowych, planowanie i opracowywanie scenariuszy działań zapobiegawczych, planowanie zagospodarowania przestrzennego, prognozowanie strat ludzkich, mienia i infrastruktury krytycznej w określonej sytuacji kryzysowej,

	edukacja dla bezpieczeństwa, transfer technologii, bilans zasobów, określenie zasad i sposobów kontroli i nadzoru.
Przygotowanie	opracowanie planu zarządzania kryzysowego, budowa centrum zarządzania kryzysowego, określenie zasad komunikacji, określenie systemów monitorowania, organizacja systemu alarmowania i ostrzegania, określenie procedur zwracania się o pomoc i jej udzielania, określenie zasad stosowania przymusu prawnego w stosunku do ludności, organizacji pozarządowych i sektora prywatnego, tworzenie baz magazynowych oraz baz danych o możliwości pozyskania środków i materiałów, opracowanie baz danych, edukacja społeczeństwa, doskonalenie służb ratowniczych, stworzenie i utrzymanie warunków przetrwania ludności w sytuacjach kryzysowych, w zakresie dostaw wody, energii, żywności, odzieży, lekarstw, środków czystości i tymczasowych miejsc zakwaterowania dla osób ewakuowanych, stworzenie warunków, zapewniających ciągłość funkcjonowania administracji publicznej i infrastruktury krytycznej, uaktualnianie elementów przygotowania.
Reagowanie	uruchomienie procedur kierowania (dowodzenia) i współdziałania działań ratowniczych, uruchomienie procesu ciągłej informacji, zorganizowanie punktu kontaktowego (informowanie ludności), uruchomienie systemów ostrzegania i alarmowania, uruchomienie procedur adekwatnych do zagrożeń, uruchomienie struktur ratowniczych, uruchomienie procesu ewakuacji, neutralizowanie ognisk zagrożeń, organizowanie samopomocy społecznej, wsparcie operacji przez siły zbrojne, udział organizacji społecznych i humanitarnych, uruchomienie ochrony psychologicznej ofiar, stworzenie doraźnych warunków do przetrwania osób poszkodowanych.
Odbudowa	szacowanie szkód i strat powstałych w następstwie sytuacji kryzysowej, zapewnienie pomocy ludności, leczenie i rehabilitacja, wypłacanie odszkodowań poszkodowanym, informowanie o prawach i obowiązkach, odtwarzanie i uzupełnianie zapasów (gotowości) służb ratowniczych, przywrócenie równowagi i bezpieczeństwa ekologicznego, odbudowa i przywrócenie sprawności infrastruktury, odtwarzanie baz materiałowych, nowe inicjatywy legislacyjne, sprawne administrowanie, realizacja zobowiązań (rozliczenie kosztów reagowania), podsumowanie i wnioski, modyfikacja i aktualizacja planów reagowania, prace dokumentacyjne (sprawozdania) raporty itp.

Źródło: Opracowanie własne na podstawie K. Sienkiewicz-Małyjurek, F.R. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej,* Warszawa 2010, s. 21

Należy podkreślić, że granice pomiędzy poszczególnymi etapami są czasem płynne i wzajemnie się przenikają, co oznacza, że zarządzanie kryzysowe jest procesem, a nie przedsięwzięciem jednorazowym.

Przeniesienie wymienionych etapów na zadania podmiotów uczestniczących w zarządzaniu kryzysowym w świetle obowiązującej ustawy z dnia 26 kwietnia 2007 roku *O zarządzaniu kryzysowym* przedstawia się następująco:

- do zadań wojewody w sprawach zarządzania kryzysowego należy: kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa (art. 14 ust. 2),
- do zadań starosty w sprawach zarządzania kryzysowego należy kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie powiatu (art. 17 ust. 2),
- do zadań wójta, burmistrza, prezydenta miasta w sprawach zarządzania kryzysowego należy kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie gminy (art. 19 ust. 2).

Należy podkreślić, że we wskazanych zadaniach został pominięty etap zapobiegania. Na etapie przygotowania uwzględniono jedynie dwa zadania, które polegają na monitorowaniu zagrożeń i przedsięwzięciach planistycznych. Natomiast etapy reagowania i usuwania skutków zdarzeń wymieniono jako realizowane pod kierownictwem wymienionych wyżej podmiotów.

Zgodnie z art. 21 ustawy z dnia 26 kwietnia 2007 roku *O zarządzaniu kryzysowym*, obowiązek podjęcia działań w zakresie zarządzania kryzysowego spoczywa na tym organie właściwym w sprawach zarządzania kryzysowego, który pierwszy otrzymał informację o wystąpieniu zagrożenia. Organ ten niezwłocznie informuje o zaistniałym zdarzeniu organy odpowiednio wyższego i niższego szczebla, przedstawiając jednocześnie swoją ocenę sytuacji oraz informacje o zamierzonych działaniach.

Na podstawie ustawy można określić praktyczne zadania systemu zarządzania kryzysowego, które będą wypadkową treści z zadań przewidzianych do realizacji przez wszystkie szczeble administracji określone w tym dokumencie:

- Na etapie zapobiegania: doradzanie w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych, dostarczanie niezbędnych informacji dotyczących aktualnego stanu bezpieczeństwa państwa niższym szczeblom zarządzania kryzysowego, monitorowanie, analizowanie i prognozowanie rozwoju zagrożeń;
- Na etapie przygotowania: planowanie finansowania zadań własnych z zakresu zarządzania kryzysowego w ramach własnych budżetów, tworzenie w budżecie jednostek samorządu terytorialnego rezerwy celowej na realizację zadań własnych z zarządzania kryzysowego w wysokości do jednego procenta bieżących wydatków budżetowych, gromadzenie i przekazywanie informacji, nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności, opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej, organizowanie

współdziałania ze związkami ochotniczych straży pożarnych w sytuacjach kryzysowych, planowanie i wnioskowanie o użycie Sił Zbrojnych RP oraz innych organów w zakresie zarządzania kryzysowego, planowanie wsparcia przez organy administracji publicznej na rzecz realizacji zadań Sił Zbrojnych RP, przygotowywanie propozycji działań i przedstawianie wniosków dotyczących wykonania, zmiany lub zaniechania działań ujętych w planach zarządzania kryzysowego, a także w zakresie użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych, przygotowywanie, opracowywanie, aktualizowanie, opiniowanie i przedkładanie do zatwierdzenia oraz zatwierdzanie planów zarządzania kryzysowego i planów ochrony infrastruktury krytycznej, wydawanie organom podległym zaleceń do planów zarządzania kryzysowego, zapewnienie funkcjonowania administracji publicznej oraz możliwości odtworzenia infrastruktury krytycznej, zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym, zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego;

- Na etapie reagowania: kierowanie działaniami związanymi z monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń, przekazywanie do wiadomości publicznej informacji związanych z zagrożeniami, realizacja zadań z zakresu ochrony infrastruktury krytycznej, planowania cywilnego oraz zaleceń i wytycznych do planów zarządzania kryzysowego (wynikających z dokumentów planistycznych), współdziałanie na wszystkich szczeblach administracji rządowej w zakresie informowania i przekazywania poleceń do wykonania w systemie całodobowym dla jednostek ochrony zdrowia w przypadkach awaryjnych, losowych, jak również zaburzeń funkcjonowania systemu, współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej, współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne, współpraca z podmiotami realizującymi monitoring środowiska, z zespołami zarządzania kryzysowego, między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie ochrony, współpraca z komórkami i jednostkami organizacyjnymi NATO i Unii Europejskiej oraz innych organizacji międzynarodowych, dokumentowanie działań podejmowanych przez centra zarządzania kryzysowego, pełnienie całodobowego dyżuru (w tym dyżuru lekarza koordynatora ratownictwa medycznego) w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego i podwyższenia gotowości obronnej państwa oraz w ramach gotowości obronnej państwa, przeciwdziałanie skutkom zdarzeń o charakterze terrorystycznym, racjonalne gospodarowanie siłami i środkami w sytuacjach kryzysowych, w czasie stanów nadzwyczajnych i w czasie wojny;
- Na etapie odbudowy: odtworzenie infrastruktury lub przywrócenie jej pierwotnego charakteru, opiniowanie potrzeb w zakresie odtworzenia infrastruk-

tury lub przywrócenia jej pierwotnego charakteru, opiniowanie sprawozdań końcowych z działań podejmowanych w związku z zarządzaniem kryzysowym[33].

Logistyka

W systemie ochrony ludności i środowiska na każdym poziomie zarządzania kryzysowego znaczące miejsce zajmuje zabezpieczenie logistyczne.

> Szczególność zarządzania logistycznego w sytuacjach kryzysowych wynika z faktu, że realizowane jest ono pod presją. W czasie pokoju (w tzw. stanie normalnym) presję tę stanowią oczekiwania społeczeństwa formułowane jako żądania zapewnienia mu warunków przetrwania na wypadek zaistnienia sytuacji kryzysowej, natomiast w sytuacjach kryzysowych są nią zagrożenia i wynikające z nich ryzyko utraty zdrowia i życia[34].

Od zarządzania logistycznego oczekuje się wysokiej skuteczności realizacji strategii logistycznej, która wyraża się w misji i celu działań logistycznych[35]. Ma to ścisły związek ze sprawnym przepływem zasobów informacyjnych, ludzkich, rzeczowych, finansowych zgodnie z potrzebami i celami zarządzania kryzysowego. Funkcją logistyki w zarządzaniu kryzysowym jest koordynacja przepływów zaopatrzenia, usług logistycznych, w tym medycznych, która przebiega pod presją czasu. Celem działań realizowanych w sferze zarządzania kryzysowego i bezpieczeństwa publicznego jest organizacja przepływów posiadanych zasobów w jak najkrótszym czasie, aby zminimalizować możliwości wystąpienia zagrożeń lub ich skutków.

Oznacza to, że misją działań logistycznych podejmowanych w sytuacjach kryzysowych jest dotarcie (z dostawami zaopatrzenia i usługami logistycznymi oraz medycznymi) do wszystkich osób poszkodowanych w możliwie najkrótszym czasie, natomiast celem działań logistycznych w sytuacjach kryzysowych jest zapewnienie wszystkim osobom poszkodowanym niezbędnych warunków przetrwania oraz ochrony zdrowia i życia[36].

Zarządzanie logistyczne w zarządzaniu kryzysowym przedstawia tabela 19.

Zabezpieczenia logistyczne jest niezbędne na wszystkich etapach zarządzania kryzysowego. Przejawia się ono w koordynacji sił i środków oraz działań organów administracji publicznej, organizacji społecznych i humanitarnych, przedsiębiorców i samego społeczeństwa.

Warto pamiętać, że zasoby logistyczne powinny być dostosowane do zagrożeń występujących na danym obszarze i powinny zależeć przede wszystkim od sił i środków tworzących możliwości wykonywania zadań związanych z realizacją dowozu zaopatrzenia i świadczenia usług logistycznych, zadań, czynności

[33] *Zarządzanie kryzysowe…*, op. cit., s. 44–46.

[34] E. Nowak, *Zarządzanie logistyczne w sytuacjach kryzysowych*, Warszawa 2008, s. 7.

[35] Ibidem, s. 7.

[36] Ibidem.

i przedsięwzięć, które muszą być realizowane w sytuacjach kryzysowych oraz specyficznych uwarunkowań zabezpieczenia logistycznego poszkodowanych w sytuacjach kryzysowych.

Tabela 19. Zarządzanie logistyczne w zarządzaniu kryzysowym

Etapy	Treści
Zapobieganie	prognozowanie sytuacji logistycznej, w tym medycznej, określenie źródeł zaopatrzenia oraz potencjału usługowego, bilansowanie zasobów logistycznych z prognozowanymi potrzebami ludności poszkodowanej, planowanie realizacji zadań logistycznych na wypadek sytuacji kryzysowych
Przygotowanie	weryfikowanie i planowanie realizacji zadań logistycznych, polegające na: a) weryfikowaniu opracowanych załączników funkcjonalnych do planów zarządzania kryzysowego, w tym planowaniu zasobów realizacji zadań logistycznych, b) tworzeniu warunków organizacyjnych i technicznych do sprawnego zarządzania logistycznego, c) tworzeniu warunków do realizacji zadań logistycznych dotyczących pomocy medycznej, dostaw wody, energii, żywności, odzieży, pościeli, lekarstw, środków sanitarnych i higieny osobistej oraz organizacji tymczasowych miejsc zakwaterowania na wypadek ewakuacji ludności, szkolenie i doskonalenie organów i jednostek wykonawczych przewidzianych do realizacji zadań logistycznych
Reagowanie	Organizacja: pomocy medycznej poszkodowanym w strefach zagrożeń, dostaw zaopatrzenia ludności poszkodowanej, ewakuacji ludzi i mienia ze strefy zagrożenia, usług gospodarczo-bytowych i specjalistycznych na rzecz osób poszkodowanych, tymczasowych miejsc zakwaterowania, przedsięwzięć sanitarno-higienicznych i przeciwepidemiologicznych w strefach zagrożenia i tymczasowych miejsc zakwaterowania, opieki psychologicznej, ratowania i ewakuacji zwierząt ze stref zagrożonych, opieki i pomocy weterynaryjnej dla zwierząt, ratowanie zasobów dziedzictwa kulturowego, środowiska i infrastruktury krytycznej
Odbudowa	udział organów logistycznych w szacowaniu szkód i strat, uruchomienie programów pomocy indywidualnej i zbiorowej dla osób poszkodowanych, udział w odtwarzaniu usług publicznych, w tym zaopatrzenia w media komunalne, organizacja odtworzenia zasobów logistycznych

Źródło: E. Nowak, *Zarządzanie logistyczne w sytuacjach kryzysowych*, Warszawa 2008, s. 38

W zarządzaniu kryzysowym za zabezpieczenie logistyczne odpowiadają bezpośrednio na poziomie centralnym – kierownik grupy planowania wsparcia i analizy zasobów oraz kierownik grupy koordynacji pomocy humanitarnej, na poziomie: województwa, powiatu, gminy – kierownicy grup zabezpieczenia logistycznego oraz grup opieki zdrowotnej i pomocy socjalno-bytowej.

2.4. System zarządzania kryzysowego

Każda organizacja jako całość powinna odznaczać się tym, że wszystkie jej składniki (elementy) są tak ze sobą połączone, iż współprzyczyniają się do powodzenia przedsięwzięcia[37]. Należy podkreślić, że sposób powiązania ze sobą różnych elementów organizacji decyduje o jej strukturze, dzięki której układ tych elementów tworzy spójną całość, czyli system[38].

Tabela 20. Pojęcie systemu według różnych autorów

Źródło	Pojęcie systemu
Słownik języka polskiego PWN, t. VIII, Warszawa 1996, s. 983	System to: – skoordynowany układ elementów, zbiór tworzący pewną całość, uwarunkowany stałością i uporządkowaniem jego części, – uporządkowany zbiór twierdzeń, poglądów, tworzących jakąś teorię, – zasady organizacji czegoś, ogół przepisów, reguł obowiązujących, według których coś jest wykonywane, także forma ustrojowa państwa, – określony sposób, metoda postępowania, wykonywanie jakieś czynności.
J. Penc, *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Kraków 1998, s. 21	System jest to zbiór elementów wzajemnie na siebie oddziaływujących, wymieniających z otoczeniem materię, energię i informację.
W. Kieżun, *Sprawne zarządzanie organizacją*, Warszawa 1997, s. 13	System jest to wyodrębniona część otaczającej nas rzeczywistości, mająca pewną wewnętrzną strukturę, a więc składająca się z części uporządkowanych według ustalonych reguł, określających ich wzajemne relacje.
P. Sienkiewicz, *Teoria efektywności systemów kierowania*, t. I: *Wstęp do systematologii,* Warszawa 1979, s. 82	Systemem nazywamy każdy obiekt złożony, wyróżniony z badanej rzeczywistości, przedstawiony jako pewna całość i tworzony przez zbiór obiektów elementarnych (elementów) i powiązań (relacji) pomiędzy nimi.
L. Krzyżanowski, *Podstawy nauk o organizacji i zarządzaniu*, Warszawa 1998, s. 128	System, SYS, to zbiór elementów, e, wyróżnionych w jakimkolwiek przedmiocie, P, ze względu na zachodzące miedzy nimi stosunki, Sup, wyrażające jakieś uporządkowanie: SYS=[{e(P)},Sup].
J. Gryz, W. Kitler, *System reagowania kryzysowego*, Toruń 2007, s. 202	Dany fragment rzeczywistości (obiekt złożony) można określić systemem, jeżeli spełni następujące warunki: – stanowi pewną całość i da się precyzyjnie wydzielić z otoczenia, czyli posiada ściśle określone granice, – da się podzielić na pewne stałe elementy (które mogą być również obiektami złożonymi) wraz z możliwością określenia ich miejsca w systemie, czyli musi istnieć możliwość określenia jego struktury wewnętrznej, – musi istnieć możliwość wyspecyfikowania reguł opisujących funkcjonowanie poszczególnych elementów rozpatrywanego fragmentu rzeczywistości, a przede wszystkim wzajemnych powiązań i zależności między nimi.

Źródło: Opracowanie własne

[37] T. Kotarbiński, *Traktat o dobrej robocie*, Wrocław 1969, s. 74.

[38] J. Penc, *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Kraków 1998, s. 21.

W skład systemu wchodzą:

- receptory, czyli układy doprowadzające do systemu informacje o występujących konfiguracjach układu: system – jego otoczenie, niezbędne dla działania systemu (np. Rządowe Centrum Bezpieczeństwa, Agencja Bezpieczeństwa Wewnętrznego),
- efektory, czyli układy wykonawcze, przy pomocy których system dokonuje zmian w konfiguracjach układu: system – jego otoczenie (np. straż pożarna, pogotowie ratunkowe, policja, siły zbrojne),
- centralny układ sterujący, który przekształca odbierane przez system sygnały z otoczenia w działanie efektorów,
- układ pamięciowy, umożliwiający gromadzenie informacji i wykorzystywanie ich w przyszłości (np. bazy danych o zagrożeniach kryzysowych)[39].

System, który jest zdolny do wykonywania długotrwałej pracy, będąc w stanie wymiany materii, energii i informacji z otoczeniem i dążąc do zachowania równowagi dynamicznej, nazywa się systemem otwartym[40].

> System otwarty dzięki umiejętności dokonywania zmian w różnych elementach i sposobie działania na podstawie danych, które były odbierane w przeszłości, jest zdolny do dostosowania się do zmian występujących w otoczeniu. Oznacza to, że posiada on umiejętność uczenia się i doskonalenia sposobów swojego działania. Organizacja jest takim systemem otwartym zachowującym się rozmyślnie, tzn. systemem, który nie tylko dobiera środki do osiągania celów, ale także samodzielnie określa cele, które następnie realizuje[41].

Każdy system posiada pewne cechy, które można sformułować następująco:

- elementy systemu są współzależne i powiązane relacjami,
- system rozpatruje się zawsze jako spójną całość,
- systemy w pewnym sensie dążą do realizacji celu i ich elementy osiągają stan końcowy będący stanem równowagi,
- systemy posiadają wejścia i wytwarzają wyjścia niezbędne dla funkcjonowania innych systemów,
- wszystkie systemy dokonują transformacji wejścia w wyjście,
- systemy zamknięte dążą do entropii (przetwarzanie informacji jest warunkiem przetrwania systemu),
- system musi mieć możliwość regulacji swoich elementów dla osiągnięcia złożonych celów (planowanie, kontrola),
- systemy zwykle składają się z mniejszych podsystemów usytuowanych hierarchicznie,
- złożone systemy charakteryzuje znaczne zróżnicowanie (dywersyfikacja funkcji i zadań),

[39] L. Michnowski, *Sieć informatyczna jako warunek intensywnego rozwoju organizacji gospodarczej*, „Przegląd Organizacji" 1981, nr 9, s. 362.

[40] J. Penc, op. cit., s. 22.

[41] Ibidem, s. 22 i 23.

- systemy dążą do stanu końcowego (ekwifinalności), który może być osiągnięty różnymi metodami[42].

Powyższe elementy wzajemnie ze sobą powiązane tworzą strukturę systemu.

Należy podkreślić, że każda organizacja jest systemem, ponieważ spełnia powyższe warunki, czyli stanowi wyodrębnioną część społeczeństwa, posiada określona strukturę wewnętrzną oraz określone zasady działania.

> System zarządzania to uporządkowany zbiór reguł, norm i praktycznych umiejętności kadry kierowniczej, określający zasady i sposoby zachowania przedsiębiorstw oraz instytucji, które kreują te zasady i sposoby, a także egzekwują zastosowanie się do nich podmiotów gospodarczych. System ten realizowany jest przez cztery podstawowe funkcje (planowanie, organizowanie, motywowanie i kontrolowanie), a sprawność jego funkcjonowania zależy od właściwości (cech) dobranej struktury organizacyjnej, obsady kadrowej i sposobu podejmowania decyzji[43].

W innym ujęciu system zarządzania należy rozumieć jako dający się wyodrębnić z organizacji układ organów zarządzających, powiązań informacyjnych niezbędnych do realizacji procesu zarządzania, metod i działań regulujących sposób i zasady funkcjonowania danej organizacji zgodnie z wytyczonymi celami, przy czym jest to układ dynamicznie zmieniający się w czasie, a motorem wprowadzanych zmian, dotyczących wszystkich jego elementów, są organy zarządzające[44].

Jeżeli do pojęcia „system zarządzania" dodamy określenie wskazujące sytuację, w jakiej ma przebiegać kierowanie, to w przypadku kryzysu otrzymamy termin system zarządzania kryzysowego. W związku z tym należy przyjąć, że „system zarządzania kryzysowego" stanowi integralną część systemu zarządzania organizacją i służy przygotowaniu, a następnie zapewnieniu jej sprawnego funkcjonowania w czasie występowania sytuacji kryzysowych (w tym kryzysów).

Przez analogię do struktury systemu zarządzania system zarządzania kryzysowego można określić jako 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[45].

[42] J. Penc, *Leksykon biznesu*, Warszawa 1997, s. 434.

[43] Ibidem, s. 438.

[44] W. Kitler, *Podstawowa terminologia zarządzania kryzysowego*, [w:] *Zarządzanie kryzysowe w sytuacji klęski żywiołowej,* red. E. Nowak, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 2006, nr 1, s. 41 i 42.

[45] E. Nowak, *Zarządzanie kryzysowe…*, s. 46; zob. też W. Kitler, *Podstawowa terminologia zarządzania kryzysowego*, [w:] *Zarządzanie kryzysowe w sytuacji klęski żywiołowej,* red. E. Nowak, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 2006, nr 1, s. 139.

System zarządzania kryzysowego można również zdefiniować jako złożony, częściowo mobilny system społeczno-gospodarczo-administracyjny, którego zadaniem jest skuteczne przeciwdziałanie wszelkim kategoriom zagrożeń kryzysowych za pomocą dostępnych sił i środków materialnych na bazie przyjętej struktury organizacyjno-funkcjonalnej, w ramach obowiązującego porządku prawnego[46]. System ten oparty jest na czterech podstawowych filarach: porządku prawnym i zobowiązaniach instytucji publicznych, specjalistycznej kadrze i kompetencjach organów administracyjnych, strumieniach informacyjnych i organach kierowniczych, przepływach fizycznych, wyposażeniu i zasobach materiałowych.

Tabela 21. Cztery filary systemu zarządzania kryzysowego

System zarządzania kryzysowego			
Akty prawne, rozporządzenia, inne przepisy	Organa administracyjne i jednostki wykonawcze	Strumienie informacyjno-sterujące	Przepływy materiałowo-techniczne
Procedury formalne i rozporządzenia wykonawcze			
Zasoby kadrowe, informacyjne i materiałowo-techniczne			
Jednostki ratownicze, gaśnicze, ewakuacyjne, specjalne, policja, wojsko			

Źródło: K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 228

Funkcjonowanie systemu zarządzania kryzysowego musi być rozpatrywane na tle pewnego hierarchicznego systemu bezpieczeństwa, determinowanego przez spektrum potencjalnych zagrożeń. Przyjmując jako podstawę klasyfikacyjną kryterium zasięgu przestrzennego, ogół potencjalnych zagrożeń można podzielić na: lokalne, sektorowe, regionalne, krajowe, międzynarodowe[47]. Zagrożeniom tym można przypisać odpowiednie kategorie przeciwdziałania, które sprowadzają się do podjęcia działań antykryzysowych w formie wypracowanych procedur zarządzania kryzysowego. Kategorie zarządzania kryzysowego według kryterium przestrzennego przedstawiono w tabeli 22.

Tabela 22. Kategorie zarządzania kryzysowego

Kryterium zarządzania kryzysowego	Zakres
Reagowanie kryzysowe lokalne	Realizowane jest na szczeblu pewnej jednostki administracyjnej, np. reagowanie w skali osiedla, dzielnicy, miasta, wsi, a także w dużych obiektach użyteczności publicznej, na imprezach masowych
Reagowanie kryzysowe sektorowe	Organizowane jest głównie przez specjalistyczne siły i środki określonych branż gospodarczych, a nawet wielkich zakładów głównie przemysłowych oraz niektórych sektorów gospodarki narodowej, np. w zakładach chemicznych, portach lotniczych i morskich, w sektorze gospodarki komunalnej, rolno-spożywczym, górnictwie węglowym

[46] K. Ficoń, op. cit., s. 227.

[47] Ibidem., s. 231.

Reagowanie kryzysowe regionalne	Prowadzone jest przede wszystkim na szczeblu pewnych jednostek podziału administracyjnego kraju i dotyczy najczęściej obszaru gminy, powiatu czy województwa, a także większych jednostek, np. makroregionu czy obszaru objętego np. stanem klęski żywiołowej
Reagowanie kryzysowe krajowe	Odnosi się do zagrożeń różnych aspektów bezpieczeństwa państwa, np. natury gospodarczej, finansowej, społecznej, a także ekologicznej, politycznej lub militarnej
Reagowanie kryzysowe międzynarodowe	Ma z reguły wymiar transgraniczny, kontynentalny i często globalny, może dotyczyć różnych aspektów zagrożenia bezpieczeństwa w wielu państwach jednocześnie, w szczególności mogą to być kwestie związane z zagrożeniami politycznymi, gospodarczymi czy ekologicznymi, a najbardziej ekstremalnym poziomem reagowania są konflikty zbrojne i działania wojenne prowadzone w wymiarze narodowym lub koalicyjnym.

Źródło: Opracowano na podstawie K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 231–232

Wymienione kategorie zarządzania kryzysowego charakteryzują się odrębnością, zróżnicowaniem w aspekcie wykorzystywanych sił i środków, procedurami, a także zasięgiem przestrzennym i skalą prowadzonych operacji. Podstawowym wyznacznikiem każdego systemu zarządzania kryzysowego jest jego gotowość do natychmiastowego uruchomienia i podjęcia działań adekwatnych do rodzaju zagrożenia. System powinien być zdolny do działania w każdych warunkach: społecznych, środowiskowych, klimatycznych, technicznych. Oznacza to, że powinien on być wysoce mobilny we wszystkich stanach zagrożenia (niemilitarnych i militarnych), o każdej porze dnia i nocy.

Systemy zarządzania kryzysowego (poziom: państwo, województwo, powiat, gmina) funkcjonują w złożonych systemach społecznych i administracyjnych. Skuteczność działania tych systemów zależy od sprawnej infrastruktury systemowej, która określa relacje między podmiotem a przedmiotem działania.

Tabela 23. Otoczenie systemu zarządzania kryzysowego

Kryteria	Elementy
Podmioty	organy administracji publicznej (rządowej i samorządowej), ogół personelu zaliczanego do zasobów kadrowych systemu, specjalistyczne organa decyzyjne i komórki kierownicze, podmioty i jednostki wykonawcze realizujące określone procedury
Przedmioty	podstawy normatywno-prawne i uregulowania legislacyjne, zasoby specjalistycznej wiedzy, informacji i umiejętności, zbiory podejmowanych decyzji, poleceń i strumienie meldunków, zasoby materiałowo-techniczne i logistyczne
Infrastruktura	infrastruktura normatywno-prawna, infrastruktura społeczna, infrastruktura informacyjna, infrastruktura techniczna

Źródło: K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 233–234

Kryterium podmiotowości systemu zarządzania kryzysowego może być również rozpatrywane w węższym aspekcie funkcjonowania i wówczas dzieli się na dwa podsystemy: podsystem kierowania w zarządzaniu kryzysowym i podsystem wykonawczy w zarządzaniu kryzysowym.

- Do elementów podsystemu kierowania zarządzaniem kryzysowym zalicza się m.in. etatowe i nieetatowe podmioty administracyjno-organizacyjne, zasilające w informacje i decyzyjne, które są utożsamiane z następującymi strukturami: nadrzędnym systemem kierowania, etatowym podmiotem kierowania, dyżurną służbą operacyjną systemu, doraźnie powołanym sztabem kryzysowym, centrum monitoringu i łączności, przedstawicielami wybranych służb i jednostek operacyjnych, podrzędnymi organami kierowania w zarządzaniu kryzysowym w terenie.
- Do podmiotów wykonawczych systemu zarządzania kryzysowego zalicza się następujące siły i środki: jednostki ratowniczo-gaśnicze, przede wszystkim Państwowej Straży Pożarnej (Ochotniczej Straży Pożarnej), jednostki ratownictwa medycznego (pogotowie ratunkowe), jednostki ratownictwa technicznego służb profesjonalnych i komunalnych, jednostki ratownictwa specjalistycznego (ekologiczne, chemiczne), pododdziały i odziały policji, sił zbrojnych, Żandarmerii Wojskowej, Straży Granicznej itd.

Dla skutecznego funkcjonowania tego systemu ważna jest również infrastruktura informacyjna i infrastruktura techniczna – zob. tabela 24.

Tabela 24. Infrastruktura informacyjna i techniczna systemu zarządzania kryzysowego

Rodzaj infrastruktury	Elementy infrastruktury
Informacyjna	obowiązujące akty prawne, przepisy wykonawcze, statuty i regulaminy różnych organów i instytucji, publiczne systemy łączności i telekomunikacji, komercyjne centra operatorskie i stacje przekaźnikowe, branżowe, sektorowe i specjalistyczne systemy informatyczne, komputerowe bazy danych i nowoczesne bazy wiedzy, komputerowe systemy wspomagania decyzji i systemy eksperckie, nowoczesne systemy telematyczne
Techniczna	sieć komunikacyjna i transportowa, regiony, państwa, sieć energetyczna państwa, wraz ze wszystkimi urządzeniami, infrastruktura portów morskich, lotniczych i lądowych, różne obiekty i budowle użyteczności publicznej, obiekty i budowle handlowo-magazynowe, systemy transportu przesyłowego i towarzyszące im magazyny, państwowe rezerwy strategiczne paliw, żywności, medykamentów, sieć magazynowo-handlowa i usługowa państwa, wybrane publiczne zakłady produkcyjne i jednostki usługowe, mobilny państwowy system ratownictwa medycznego, system bankowy i depozyty finansowe osób prawnych, naturalne zasoby przyrodnicze przydatne w zarządzaniu kryzysowym

Źródło: K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 235–236

Kiedy skala i dynamika występujących zagrożeń ogranicza lub uniemożliwia skuteczne zarządzanie kryzysowe na określonym poziomie (kraj, województwo, powiat, gmina), wówczas elementy każdego podsystemu są wspierane przez delegowane siły i środki ze szczebla nadrzędnego (siły zbrojne, policja), przez najbliższych terytorialnie sąsiadów (województwo, powiat, gmina), a także instytucje publiczne. System zarządzania kryzysowego musi obejmować wszystkie poziomy zarządzania bezpieczeństwem państwa i jako twór organizacyjno-funkcjonalny jest konieczny dla zapewnienia bezpieczeństwa ludności w sytuacjach stanowiących zagrożenie życia, mienia i środowiska.

Misją systemu zarządzania kryzysowego jest, po pierwsze, zneutralizowanie lub zlikwidowanie zagrożeń, zanim ze zdwojoną siłą wystąpią negatywne skutki, po drugie, w przypadku pojawienia się negatywnych następstw przystąpienie natychmiast do ich neutralizacji i likwidacji we wszystkich sferach, po trzecie, włączenie zdobytej wiedzy i doświadczenia związanego z likwidacja danego zagrożenia i jego skutków do aktualizacji posiadanych scenariuszy i przygotowanie odpowiedniego systemu profilaktyki i prewencji[48]. Celem systemu zarządzania kryzysowego jest ograniczenie strat ludzkich i materialnych, powodowanych przez katastrofy oraz ochrona przed wszystkimi zagrożeniami (naturalnymi, technicznymi, wojennymi) poprzez realizację programów zapobiegawczych, przygotowawczych, reagowania i odbudowy[49].

System zarządzania kryzysowego w Polsce

System Zarządzania Kryzysowego Rzeczypospolitej Polskiej jest przeznaczony do zapobiegania sytuacjom kryzysowym, przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowania w przypadku ich wystąpienia oraz odtwarzania infrastruktury lub przywracania jej pierwotnego charakteru. Jest on zbudowany dla potrzeb działań doraźnych i wyjątkowych, integrujących procesy informacyjno-decyzyjne i przepływy fizyczno-materiałowe na bazie przestrzennej infrastruktury technicznej i aktualnej struktury administracyjnej.

Do zadań systemu zarządzania kryzysowego należy:

- ocena zagrożeń wynikających z zaistniałych sytuacji kryzysowych (militarnych i pozamilitarnych, zewnętrznych i wewnętrznych) oraz przygotowanie propozycji ich rozwiązania w ramach wsparcia procesu decyzyjnego,
- skuteczne reagowanie w tych sytuacjach z uwzględnieniem możliwości płynnego przejścia do procesu osiągania gotowości obronnej państwa czasu wojny,
- planowanie użycia sił militarnego i niemilitarnego podsystemu bezpieczeństwa państwa oraz koordynowanie ich działań,
- prowadzenie monitoringu, informowanie o rozwoju sytuacji kryzysowych oraz współdziałanie w tym zakresie z właściwymi instytucjami i agendami Sojuszu Północnoatlantyckiego, Unii Europejskiej oraz państwami nienależą-

[48] Ibidem, s. 229.

[49] M. Kaliński, *Miejsce gotowości cywilnej i zarządzania kryzysowego we współpracy cywilno-wojskowej,* [w:] *Współpraca cywilno-wojskowa*, Warszawa 1999, s. 173.

cymi do ich struktur. Funkcjonowanie Systemu Zarządzania Kryzysowego RP należy rozpatrywać w dwóch wariantach:

a) w układzie sojuszniczym (koalicyjnym),

b) jako autonomiczny w ramach państwa[50].

System zarządzania kryzysowego jest tworzony przez władze publiczne na wszystkich poziomach zarządzania bezpieczeństwem państwa zgodnie z obowiązującymi przepisami. W jego skład wchodzą wyspecjalizowane jednostki sektora publicznego, prywatnego i obywatele. Z uwagi na charakter wykonywanych zadań posiadają zróżnicowaną strukturę organizacyjną, specjalistyczne wyposażenie, proces szkolenia, a także przypisane kompetencje. Oznacza to, że tworzą wyodrębnione podsystemy w systemie zarządzania kryzysowego i mogą być postrzegane jako samodzielne systemy. W systemie zarządzania kryzysowego jednostki te, co wyraźnie należy podkreślić, są powiązane systemem zależności i wzajemnego oddziaływania, co skutkuje realizacją przypisanych im zadań w sytuacjach kryzysowych.

Elementy systemu zarządzania kryzysowego w RP:

- Organy administracji państwowej wraz z jednostkami wykonawczymi. Administracja państwowa wykonuje zadania związane z przepływem zasobów informacyjnych, osobowych, rzeczowych, kapitałowych i koordynacją działań. Natomiast jednostki wykonawcze zajmują się realizacją ustawowych zadań (Ministerstwo Spraw Wewnętrznych, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Agencja Wywiadu, Służba Wywiadu Wojskowego, Biuro Ochrony Rządu, Generalny Inspektor Informacji Finansowej, Służba Celna, Służba Więzienna, jednostki rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej);
- Podmioty interwencyjno-ratownicze – Policja, Straż Graniczna, Żandarmeria Wojskowa, Siły Zbrojne Rzeczypospolitej Polskiej, Państwowa Straż Pożarna, Ochotnicza Straż Pożarna, inne jednostki ochrony przeciwpożarowej, centra powiadamiania ratunkowego, jednostki Państwowego Ratownictwa Medycznego, dyspozytorzy medyczni, jednostki ochrony zdrowia, Morska Służba Poszukiwania i Ratownictwa, Straż Gminna, a także inne, każdy w zakresie swojej właściwości, państwowe urzędy, agencje, straże, służby, inspekcje;
- Podmioty pozarządowe – Ochotnicza Straż Pożarna (OSP), Wodne Ochotnicze Pogotowie Ratunkowe (WOPR), Górskie Ochotnicze Pogotowie Ratunkowe (GOPR), Tatrzańskie Ochotnicze Pogotowie Ratunkowe (TOPR), Polski Czerwony Krzyż (PCK), Liga Obrony Kraju (LOK);
- Społeczeństwo w ramach samopomocy, pomocy sąsiedzkiej (ewakuacja, pomoc rzeczowa i finansowa poszkodowanym);
- Media – działające jako środki informacji o zagrożeniach, powiadamiania, metodach zabezpieczenia, ewakuacji, potrzebach dla poszkodowanych i realizowanych przedsięwzięć[51].

[50] K. Ficoń, op. cit., s. 229.

[51] K. Sienkiewicz-Małyjurek, F.K. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej*, Warszawa 2010, s. 70.

Powyższe podmioty są integrowane w podsystem zarządzania, który poprzez współdziałanie i koordynowanie prowadzi do sprawnego realizowania założonych celów systemu zarządzania kryzysowego.

Ujęcie systemowe zarządzania kryzysowego pozwala na wskazanie dwóch podstawowych jego podsystemów: podsystemu instytucji zarządzania kryzysowego (zob. tabela 24) i podsystemu narzędzi zarządzania kryzysowego (zob. tabela 25) oraz wskazanie otoczenia systemu, czyli obiektów podlegających zarządzaniu kryzysowemu, czyli społeczeństwo, ugrupowania ratownicze, środowisko gospodarcze i przyrodnicze.

Tabela 25. Podsystem instytucji zarządzania kryzysowego

<table>
<tr><td colspan="2">Instytucje zarządzające</td><td rowspan="9">Narzędzia zarządzania</td><td rowspan="9">Obiekty zarządzania</td></tr>
<tr><td colspan="2">Organy prawodawcze państwa</td></tr>
<tr><td colspan="2">Organy administracji rządowej</td></tr>
<tr><td colspan="2">Samorząd terytorialny</td></tr>
<tr><td rowspan="6">Kierownictwo służb straży i organizacji</td><td>jednostek ratowniczo-gaśniczych,</td></tr>
<tr><td>służb ratowniczych,</td></tr>
<tr><td>porządku publicznego,</td></tr>
<tr><td>pozarządowych,</td></tr>
<tr><td>gospodarczych,</td></tr>
<tr><td>użyteczności publicznej</td></tr>
</table>

Źródło: Opracowano na podstawie B. Poskrobko, *Zarządzanie środowiskiem*, Warszawa 2007, s. 65

Narzędzia zarządzania kryzysowego tworzą środki zarządzania i instrumenty zarządzania. Do środków zarządzania zalicza się: źródła informacji, zasoby wiedzy, doświadczenie, wypracowane procedury podejmowania decyzji i wydawania poleceń, procedury współpracy i współdziałania, system sprawozdawczy, zasoby materiałowe i techniczne[52]. Instrumenty zarządzania pozwalają w sposób ciągły na oddziaływanie bezpośrednie i pośrednie na obiekty zarządzania (obowiązki i uprawnienia, które wynikają z prawa międzynarodowego i prawa krajowego, umów i porozumień dotyczących zaradzania kryzysowego)[53]. Narzędzia zarządzania kryzysowego pozwalają na sprawne działanie, a także oddziaływają na obiekty zarządzania kryzysowego.

Tabela 26. Podsystem narzędzi zarządzania kryzysowego

<table>
<tr><td rowspan="7">Instytucje zarządzania</td><td colspan="2">Narzędzia zarządzania</td><td rowspan="7">Obiekty zarządzania</td></tr>
<tr><td colspan="2">Regulacje prawne</td></tr>
<tr><td rowspan="4">Środki zarządzania</td><td>Polityki i strategie kryzysowe</td></tr>
<tr><td>Planowanie kryzysowe</td></tr>
<tr><td>Procedury informacyjne i decyzyjne</td></tr>
<tr><td>Procesy energetyczno-zasilające</td></tr>
<tr><td colspan="2">Instrumenty zarządzania</td></tr>
</table>

Źródło: Opracowano na podstawie B. Poskrobko, *Zarządzanie środowiskiem*, Warszawa 2007, s. 65

[52] J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego*, Kraków 2010, s. 120.

[53] Ibidem, s. 120.

Tabela 27. Otoczenie podlegające zarządzaniu kryzysowemu

Instytucje zarządzające		
Narzędzia zarządzania		
Obiekty zarządzania		
Społeczeństwo	Ratownictwo	Środowisko
pojedyncze osoby, rodziny, grupy społeczne, społeczność lokalna, system społeczny	system wykrywania zagrożeń i alarmowania, wydzielone siły: Policji, Sił Zbrojnych, Żandarmerii Wojskowej, Straży Granicznej, Straży Gminnej, Straży Ochrony Kolei, jednostki ratowniczo-gaśnicze straży pożarnej, jednostki ratownictwa medycznego pogotowia ratunkowego, szpitalne oddziały ratownicze, szpitale (w tym specjalistyczne), jednostki ratownictwa technicznego (energetyczne, gazowe, wodno-kanalizacyjne, budowlane), jednostki ratownictwa specjalistycznego (chemiczne, ekologiczne, górnicze, morskie, kolejowe, drogowe, wodne, wysokogórskie), formacje obrony cywilnej, Polski Czerwony Krzyż, firmy ochrony osób i mienia	źródła zagrożeń: przyrodnicze – stan zanieczyszczenia powierzchni Ziemi i środowiska wodnego, regulacja rzek i zabudowa ich naturalnych terenów zalewowych, stan lasów, ścieki nieoczyszczone i odprowadzane bezpośrednio do rzek i gleby, nielegalne gromadzenie odpadów, zanieczyszczenie środowiska spowodowane działalnością gospodarczą gospodarcze – obiekty infrastruktury przemysłowej, kulturalnej, komunalnej: zakłady przemysłowe, obiekty handlowe i usługowe, instytucje edukacyjne i kulturalne, sieci przesyłowe, zakłady i magazyny przechowujące środki toksyczne, ujęcia wody pitnej i sieci wodno-kanalizacyjne, drogi, mosty, dworce kolejowe, porty lotnicze i morskie, węzły telekomunikacyjne, zbiorniki i instalacje z materiałami niebezpiecznymi

Źródło: Opracowano na podstawie J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego*, Kraków 2010, s. 121–124

System zarządzania kryzysowego w Polsce jest wieloszczeblowy i składa się z następujących komponentów:

- organów zarządzania kryzysowego,
- organów opiniodawczo-doradczych właściwych w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego,
- centrów zarządzania kryzysowego, utrzymujących 24-godzinną gotowość do podjęcia działań.

Tabela 28. System zarządzania kryzysowego w Polsce

System zarządzania kryzysowego			
Szczebel administracyjny	Organ zarządzania kryzysowego	Organ opiniodawczo-doradczy	Centrum Zarządzania Kryzysowego
Krajowy	Rada Ministrów, Prezes Rady Ministrów	Rządowy Zespól Zarządzania Kryzysowego	Rządowe Centrum Bezpieczeństwa
Resortowy	minister kierujący działem administracji rządowej kierownik organu centralnego	Zespół Zarządzania Kryzysowego (ministra, urzędu centralnego)	Centrum Zarządzania Kryzysowego (ministra, urzędu centralnego)
Wojewódzki	wojewoda	Wojewódzki Zespół Zarządzania Kryzysowego	Wojewódzkie Centrum Zarządzania Kryzysowego
Powiatowy	starosta powiatu	Powiatowy Zespół Zarządzania Kryzysowego	Powiatowe Centrum Zarządzania Kryzysowego
Gminny	wójt, burmistrz, prezydent miasta	Gminny Zespół Zarządzania Kryzysowego	Gminne (Miejskie) Centrum Zarządzania Kryzysowego

Źródło: M. Kolińska, *Prawnoorganizacyjne uwarunkowania funkcjonowania Rządowego Centrum Bezpieczeństwa*, Warszawa 2010, s. 26

ROZDZIAŁ 3

Zagrożenia kryzysowe państwa

3.1. Pojęcie i klasyfikacja zagrożeń

Zmiany cywilizacyjne, które zostały poprzedzone upadkiem bipolarnego podziału świata i Związku Radzieckiego, stanowią zarówno wyzwania, jak i zagrożenia, szanse oraz ryzyko dla każdej organizacji (podmiotu, społeczności narodowej, narodu, państwa), a nawet pojedynczego człowieka. Są to dylematy współczesnego świata, który wkracza w erę wszechobecnej globalizacji i społeczeństwa informacyjnego, co z kolei przekłada się na bezpieczeństwo poszczególnych państw i środowiska międzynarodowego.

Obok istniejących zagrożeń pojawiło się wiele nowych, którym towarzyszy pytanie o ich naturę i istotę oraz wynikającą z nich potrzebę zmian w podejściu pojedynczego człowieka i organizacji (państwa) do likwidacji ich skutków lub/i niedopuszczenia do powstania. Nie ulega wątpliwości, że analiza i prognoza zagrożeń staje się jednym z priorytetowych obszarów poznania[1]. Jest to tym bardziej istotne, że systematyczne badanie możliwości wystąpienia zagrożeń pozwala na przygotowanie społeczeństwa, podmiotów właściwych sferze zarządzania kryzysowego (kierujących i wykonawczych) do takiego postępowania, które pozwoli na zapobieganie powstaniu sytuacji kryzysowej i/lub niedopuszczenia do jej rozprzestrzeniania.

Przebieg dotychczasowych zjawisk czy wydarzeń, które były źródłem zagrożeń o zróżnicowanym podłożu, pozwala przyjąć, że będziemy świadkami (uczestnikami) sytuacji kryzysowych będących następstwem katastrof i klęsk żywiołowych spowodowanych przez siły natury, ale także celowe lub przypadkowe działania człowieka.

Wyzwaniem staje się w tych okolicznościach sprawne rozwiązywanie spraw związanych z bezpieczeństwem. W określonych warunkach stanowią szanse i/lub zagrożenia. W innym ujęciu wyzwanie to sytuacja nowa i trudna, wymagająca określonej postawy i podjęcia stosownych działań[2]. Wyzwanie jest zatem sygnałem do podjęcia działań, najczęściej wyrażających określone stanowisko w relacjach militarnych, gospodarczych czy politycznych (również związanych

[1] G. Sobolewski, *Reagowanie kryzysowe w środowisku miejskim. Aspekt militarny*, Warszawa 2009, s. 72.

[2] B. Balcerowicz, *Pokój i nie-pokój na progu XXI wieku*, Warszawa 2002, s. 185.

z podjęciem działań w ramach zarządzania kryzysowego), artykułowanie ostrzeżeń i pokazywanie możliwości reagowania.

> Wyzwanie możemy traktować jako możliwość pojawienia się problemu, przy czym waga tego problemu w początkowej fazie nie jest istotna. Można więc przyjąć, że jest to sytuacja wymagająca rozwiązań, w której istnieje małe prawdopodobieństwo wystąpienia zakłóceń funkcjonowania danego podmiotu. […] Bardzo często zagrożenie to wyzwanie, któremu nie przeciwdziałano skutecznie we właściwym czasie i które nie zostało rozwiązane. Jeżeli wyzwanie zostanie w porę dostrzeżone, a działania podjęte, to nie przekształci się ono w zagrożenia[3].
>
> W związku z powyższym nie należy używać obu terminów zamiennie, ponieważ istnieje istotna różnica w ich znaczeniu. O ile zagrożenie wymaga podejmowania działań przez dany podmiot celem ich neutralizacji dla zachowania stabilności, o tyle wyzwanie może być tylko sygnałem do podjęcia takich działań. Często zaniechanie działań w przypadku pojawienia się wyzwań może się przekształcić w zagrożenie. Dlatego można wyróżnić cechę łączącą oba zjawiska – przechodzenie z kategorii wyzwań do zagrożeń[4].

Innymi słowy, wyzwania mogą przerodzić się w zagrożenia. Jest to ostrzeżenie wskazujące na konieczność wczesnego reagowania na pojawiające się sygnały o możliwym niebezpiecznym rozwoju sytuacji w organizacji lub w jej otoczeniu.

Pojęcie zagrożenia jest wieloznaczne i jest rozpatrywane z punktu widzenia wielu dyscyplin naukowych, ponadto jest analizowane w sytuacjach jednostkowych i grupowych, a także w układach obejmujących społeczne procesy w skali makro i mikro, w okolicznościach i uwarunkowaniach uwzględniających aspekt subiektywny i obiektywny danego zjawiska (grupy zjawisk). Zróżnicowane podejście do pojęcia zagrożenia uzasadnia w aspekcie prowadzonych rozważań związanych z zarządzaniem kryzysowym przedstawienie kilku jego definicji (tabela 29).

Tabela 29. Definicje zagrożenia

Źródło	Definicja
Leksykon wiedzy wojskowej, Warszawa 1979, s. 510	Zagrożenie to sytuacja, w której istnieje zwiększone prawdopodobieństwo utraty życia, zdrowia, wolności albo dóbr materialnych.
R. Wróblewski, *Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej,* Warszawa 1993	Zagrożenie to możliwość powstania takiej sytuacji, w której społeczeństwo (państwo) nie ma warunków do swobodnego bytu i rozwoju lub są one w istotnym stopniu utrudnione.
S. Korycki, *System bezpieczeństwa Polski*, Warszawa 1994, s. 54	Zagrożenie jest definiowane na różne sposoby, i tak: – stan psychiczny lub świadomościowy wywołany postrzeganiem zjawisk, które subiektywnie ocenia się jako niekorzystne lub niebezpieczne, – czynniki obiektywne powodujące stany niepewności i obawy: mogą to być rzeczywiste działania innych uczestników życia społecznego, niekorzystne i niebezpieczne

[3] M. Wrzosek, *Identyfikacja zagrożeń organizacji zhierarchizowanej*, Warszawa 2010, s. 20.

[4] *Zagrożenia kryzysowe*, red. G. Sobolewski, Warszawa 2011, s. 26 i 27.

	dla żywotnych interesów i podstawowych wartości danego podmiotu (jednostkowego lub zbiorowego), – sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia.
S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, s. 21	Zagrożeniem dla bezpieczeństwa podmiotu (państwa, narodu, organizacji, instytucji, związku) będzie utrudnienie lub utrata warunków do swobodnego bytu i rozwoju. Zagrożenia takie mogą powstać w dziedzinach: politycznej (np. izolacja polityczna, szantaż polityczny), społecznej (np. ograniczenie lub zerwanie współpracy kulturalnej, naukowo-technicznej, turystycznej), gospodarczej (np. ograniczenie lub zerwanie wymiany handlowej, pomocy finansowej lub jednocześnie w kilku dziedzinach – w dowolnej konfiguracji).
J. Penc, *Leksykon biznesu*, Warszawa 1997, s. 505	Zagrożenie to wszystkie czynniki zewnętrzne, które są postrzegane przez firmę [organizację – przyp. Autora] jako bariery, utrudnienia, niebezpieczeństwa, dodatkowe koszty, wysiłki, wyrzeczenia itp.
Z. Ratajczak, *Oblicza ludzkiej zaradności*, [w:] *Człowiek w sytuacji zagrożenia. Kryzysy, katastrofy, kataklizmy*, red. K. Popiołek, Poznań 2001, s. 16	Zagrożenie to wzrost prawdopodobieństwa pogorszenia się dotychczasowej sytuacji człowieka. Pogorszenie to polega na gwałtownej dekompozycji układu między wartościami człowieka a jego możliwościami, ponieważ w nim samym lub w jego otoczeniu zaszły określone zmiany.
J. Ziarko, *Orientowanie się i funkcjonowanie jednostki w sytuacji zagrożenia. Aspekty psychologiczno-dydaktyczne,* [w:] *Administracja, zarządzanie i handel zagraniczny w warunkach integracji, Materiały konferencyjne – zarządzanie bezpieczeństwem,* red. K. Budzowski, Kraków 2002, s. 419	Zagrożenie oznacza pogorszenie się relacji sytuacyjnych, gdzie w sposób względnie gwałtowny zostaje naruszona równowaga między elementami otoczenia a cechami i aktualnym stanem jednostki, zakłócająca mechanizmy regulacji jej zachowania.
J. Kunikowski, *Słownik terminów z zakresu wiedzy i edukacji dla bezpieczeństwa*, [w:] *Bezpieczeństwo człowieka i zbiorowości społecznych*, red. W.J. Maliszewski, Bydgoszcz 2005, s. 189	Zagrożenie to sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia.
K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe,* Gdynia 2007, s. 76	Przez zagrożenie należy rozumieć zdarzenie spowodowane przyczynami losowymi (naturalnymi) lub nielosowymi (celowymi), które wywiera negatywny wpływ na funkcjonowanie danego systemu lub powoduje niekorzystne (niebezpieczne) zmiany w jego otoczeniu wewnętrznym lub zewnętrznym. Kumulowane i nierozwiązane na czas zagrożenia mogą prowadzić do zaistnienia sytuacji kryzysowej zarówno w rozpatrywanym systemie, jak też określonym środowisku systemowym.
Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2009, s. 162	Zagrożenie – sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia.
W. Lidawa, W. Krzeszowski, W. Więcek, *Zarządzanie w sytuacjach kryzysowych*, Warszawa 2010, s. 7	Zagrożenie to zdarzenie powstające losowo lub wywołane celowo, które wywiera negatywny wpływ na funkcjonowanie politycznych i gospodarczych struktur państwa, na warunki bytowania ludności oraz stan środowiska naturalnego.
Zagrożenia kryzysowe, red. G. Sobolewski, Warszawa 2011, s. 26	Zagrożenie określane jest jako sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia.

Źródło: Opracowanie własne

Podstawą klasyfikacji zagrożeń są pierwotne źródła i przyczyny je generujące. Kryterium przyczynowe wyodrębnia cztery główne kategorie:

- zagrożenia naturalne spowodowane fizyczno-chemicznymi zjawiskami natury, przyrody, kosmosu, do niedawna jeszcze bez udziału człowieka,
- zagrożenia techniczne związane z racjonalną (głównie gospodarczą) działalnością człowieka, rozwojem cywilizacyjnym i postępem naukowo-technicznym,
- zagrożenia społeczne generowane w sposób mniej lub bardziej celowy przez człowieka, postęp kulturalno-cywilizacyjny, a także różne teorie naukowe i poglądy społeczne jednostek, grup i organizacji społecznych,
- inne przyczyny obejmujące różne kompilacje powyższych źródeł o zróżnicowanym stopniu ich udziału oraz nowe, nieznane dotychczas kategorie[5].

Ponadto zgodnie ze stanem przygotowania podmiotu (państwa, organizacji, firmy) do sytuacji zagrożenia można zaliczyć zagrożenia nieprzewidywalne (nieuświadomione) i przewidywalne (uświadomione)[6].

W przypadku zagrożenia bezpieczeństwa państwa dzielą się na wewnętrzne i zewnętrzne, źródła przyczyn do niego prowadzących natomiast ze względu na charakter na militarne i pozamilitarne:

- za zagrożenie wewnętrzne bezpieczeństwa państwa uważa się zespół przyczyn, których źródłem są elementy jego struktury prowadzące do destabilizacji sytuacji lub naruszenia podstawowych wartości, takich jak: wola przetrwania (państwa, narodu), terytorialna integralność, niezależność polityczna, suwerenność wyboru ustroju społeczno-politycznego oraz swoboda w podejmowaniu decyzji dotyczących polityki wewnętrznej i zewnętrznej, jakość i warunki życia (zachowanie odpowiedniego standardu życiowego społeczeństwa i perspektyw wszechstronnego rozwoju);
- za zagrożenie zewnętrzne bezpieczeństwa można uznać naruszenie przez inne państwo jednej z następujących zasad: suwerennej równości, poszanowania praw nieodłącznych dla suwerenności, powstrzymania się od groźby użycia siły lub samego jej użycia, nienaruszalności granic, integralności terytorialnej, pokojowego załatwiania sporów; nieingerencji w sprawy wewnętrzne, poszanowania praw człowieka i podstawowych rodzajów wolności, łącznie z wolnością myśli, sumienia, wyznania lub przekonań, równouprawnienia i prawa narodów do samostanowienia, partnerskiej współpracy między państwami, wypełniania w dobrej wierze zobowiązań wynikających z prawa międzynarodowego;
- zagrożenie militarne państwa to splot zdarzeń polityczno-militarnych, w którym może nastąpić utrudnienie lub utrata warunków do niezakłóconego bytu i rozwoju narodu (państwa) albo naruszenie bądź utrata jego suwerenności i integralności terytorialnej w wyniku oddziaływania militarnego (napaści zbrojnej);

[5] K. Ficoń, op. cit., s. 76 i 77.

[6] M. Wrzosek, op. cit., s. 21.

- zagrożenie pozamilitarne państwa jest splotem zdarzeń (występujących w stanie kryzysu), w wyniku którego może nastąpić utrudnienie lub utrata warunków do niezakłóconego bytu i rozwoju państwa (narodu) lub naruszenie bądź utrata jego suwerenności i integralności terytorialnej. Przy czym cel działania (wymuszenie uległości lub ustępstw) zamierza się osiągnąć przez wywieranie nacisku i stosowanie sankcji politycznych lub ekonomicznych, bez uciekania się do stosowania przemocy fizycznej (siły zbrojnej)[7].

  Kryteria klasyfikacji źródeł zagrożeń kryzysowych przedstawiono w tabeli 30.

Tabela 30. Kryteria klasyfikacji zagrożeń kryzysowych

Kategorie	Podkategorie
źródła powstania	naturalne, techniczne, społeczne, cywilizacyjne, ekologiczne
podział rodzajowy	zdarzenia, katastrofy, klęski, kataklizmy
czas eliminacji	krótkoterminowe, średnioterminowe, długoterminowe, bezterminowe
dziedzina działania	sektorowe, religijne, polityczne, uniwersalne
poziom destrukcji	minimalny, średni, wysoki, totalny
zasięg przestrzenny	lokalny, regionalny, krajowy, międzynarodowy, ogólnoświatowy
determinizm przyczyn	celowe, losowe, mieszane, przyrodnicze
możliwości antycypacji	kontrolowane, prognozowane, nieprzewidywalne

Źródło: Opracowano na podstawie K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe,* Gdynia 2007, s. 78

Klasyfikacja zagrożeń kryzysowych[8]:

- ze względu na rodzaj i skalę negatywnych następstw:
  - o niskiej skali intensywności oddziaływania i małym poziomie szkodliwości (zdarzenia, incydenty, przypadki), tzw. zagrożenia niskopoziomowe,
  - o średniej skali intensywności oddziaływania i średnim poziomie szkodliwości (awarie, wypadki, zjawiska), tzw. zagrożenia średniopoziomowe,
  - o wysokiej skali intensywności i wysokim poziomie szkodliwości (klęski, katastrofy, krachy, plagi), tzw. zagrożenia wysokopoziomowe,
  - o bardzo wysokiej, katastroficznej intensywności i bardzo dużym poziomie szkodliwości (kataklizmy, epidemie, wojny), zaliczane do kategorii zagrożeń ekstremalnych.
- ze względu na prognozowany czas neutralizacji i usuwania ich skutków:
  - zagrożenia, których skutki są krótkotrwale i szybko przemijające, z reguły o niskim poziomie destrukcji i stosunkowo dużej prognozowalności,
  - generujące następstwa średniookresowe trwające pewien ograniczony czas, których rezultaty są zdeterminowane i możliwe do usunięcia w realnym czasie,
  - generujące długotrwałe skutki, których czas neutralizacji jest relatywnie długi i trudny do oszacowania, gdyż ich następstwa są mało prognozowalne i trudno przewidywalne,

[7] S. Dworecki, op. cit., s. 23–25.

[8] K. Ficoń, op. cit., s. 78–91.

- zagrożenia, których negatywne skutki nie są możliwe do usunięcia w realnie określonym czasie i nie można racjonalnie ustalić żadnego terminu bez narażenia się na popełnienie zbyt dużego błędu;

- ze względu na obszar kryzysowego oddziaływania:
  - określonych dziedzin życia gospodarczo-ekonomicznego,
  - wybranych form życia społeczno-obyczajowego (społeczne, religijne, etniczne, kulturowe),
  - porządku publicznego i ładu światowego (narodowe, polityczne, cywilizacyjne),
  - naturalne i przyrodnicze, mające często olbrzymie konsekwencje społeczne, gospodarcze i ekologiczne,
  - totalne, obejmujące wszystkie wymiary i dziedziny życia społecznego, gospodarczego,politycznego,cywilizacyjnego,klimatycznego,ekologicznego;
- ze względu na ich negatywne skutki:
  - powodujące skutki doraźne, mniej groźne i relatywnie łatwiejsze do usunięcia,
  - poważne i groźne, których negatywne skutki cechuje wyższy poziom destrukcji, a ich usunięcie wymaga zaangażowania większych sił i środków,
  - bardzo groźne i potężne, które powodują szkodliwe i niebezpieczne następstwa trudne do szybkiego usunięcia,
  - totalne, generujące katastrofalne następstwa, ogromne straty i najwyższe wieloaspektowe niebezpieczeństwo;
- ze względu na rodzaj i naturę przyczyn je wywołujących:
  - z przyczyn zależnych, spowodowanych mniej lub bardziej celowym i świadomym oddziaływaniem człowieka i jego wytworów technicznych, społecznych i cywilizacyjnych,
  - z przyczyn losowych, niezależnych od czynników, na które przy obecnym poziomie rozwoju cywilizacyjnego nie można racjonalnie i celowościowo oddziaływać,
  - z przyczyn mających charakter mieszany (losowo-celowościowy), których źródła są mniej lub bardziej rozpoznane i poddające się w różnym stopniu oddziaływaniom sterowniczym człowieka,
  - z przyczyn przyrodniczych, ekologicznych i kosmicznych, na które człowiek praktycznie nigdy nie będzie miał wpływu czy możliwości oddziaływania;
- ze względu na zakres i obszar ich oddziaływania przestrzennego:
  - miejscowe i lokalne (środowiskowe),
  - regionalne (często przygraniczne),
  - państwowe (narodowe, etniczne),
  - międzynarodowe (transgraniczne),
  - globalne;
  -

- ze względu na możliwości antycypowania ich rezultatów, jeśli chodzi o zasięg, intensywność i szkodliwość:
  - zagrożenia, które kształtują się stopniowo i mogą być prognozowane i racjonalnie kontrolowane oraz redukowane do minimalnego poziomu, gwarantującego względne bezpieczeństwo,
  - zagrożenia, których obszar działania, skalę intensywności i ewentualne następstwa można dość wiarygodnie antycypować, ale przy obecnym stanie wiedzy i technologii brakuje skutecznych mechanizmów i możliwości sterowania nimi,
  - nie dające się przewidzieć czy w jakimkolwiek stopniu prognozować, rozumiane inaczej jako zagrożenia losowe i całkowicie nieuniknione,
  - spowodowane tzw. siłą wyższą, których nie można ani przewidzieć, ani prognozować ich skutków, wobec których człowiek pozostaje całkowicie bezsilny.

Klasyfikację zagrożeń kryzysowych ze względu na skalę intensywności i możliwości zwalczania przedstawiono w tabeli 31.

Tabela 31. Klasyfikacja i charakterystyka zagrożeń kryzysowych ze względu na skalę intensywności i możliwości zwalczania

Kryteria podziału	Kategorie zagrożeń	Skala intensywności	Możliwości zwalczania
Źródła powstania zagrożeń	naturalne techniczne społeczne cywilizacyjne ekologiczne	zróżnicowana zróżnicowana zróżnicowana zróżnicowana zróżnicowana	względne względne względne względne względne
Podział rodzajowy zagrożeń	zdarzenia, incydenty katastrofy, awarie klęski, katastrofy kataklizmy, wojny	mała średnia duża wielka	duże średnie małe brak
Prognozowany czas usuwania skutków	krótkoterminowe średnioterminowe długoterminowe bezterminowe	mała średnia duża nieznana	duże średnie małe brak
Obszar zagrożeń kryzysowych	sektory, branże społeczeństwo stosunki polityczne przyroda i ekologia wszystkie dziedziny	mała średnia duża wielka globalna	duże średnie średnie małe względne
Poziom destrukcji bezpieczeństwa	ograniczone wysokie nieznane totalne	mała średnia duża wielka	duże średnie małe brak
Determinizm przyczyn	celowe losowe mieszane terroryzm przyrodnicze	zróżnicowana zróżnicowana zróżnicowana zróżnicowana zróżnicowana	względne względne względne względne względne

Prognozowany zasięg przestrzenny	lokalne regionalne krajowy międzynarodowe ogólnoświatowe	mała średnia duża wielka globalna	duże średnie małe ograniczone żadne
Możliwości zwalczania zagrożenia	kontrolowane prognozowane nieprzewidywalne brak możliwości	mała średnia duża totalna	duże średnie małe brak

Źródło: K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe*, Gdynia 2007, s. 82

Należy podkreślić, że zagrożenie może być bezpośrednią przyczyną rozpoczęcia i rozwoju procesu zmiennego w czasie i przestrzeni, który może doprowadzić do naruszenia równowagi, powstania sytuacji kryzysowej, utraty możliwości kontroli nad przebiegiem konkretnego wydarzenia, a w konsekwencji do powstania kryzysu[9]. Dlatego zagrożenie wymaga podejmowania działań, których celem jest niedopuszczenie do powstania i rozwoju sytuacji kryzysowej. Z kolei wyzwanie informuje podmioty realizujące zadania związane z zarządzaniem kryzysowym o konieczności zajęcia stanowiska, które pozwoli w przyszłości na skuteczne reagowanie.

Zagrożenie jest pojęciem, które jest używane w rozważaniach prowadzonych na temat szeroko rozumianego bezpieczeństwa. Tym samym zagrożenie oznacza możliwe niebezpieczeństwo, przewidywanie, iż określone zjawiska będą przebiegały w sposób stanowiący pewne ryzyko[10]. Ma to ścisły związek z wystąpieniem niepowodzenia planowanych działań lub też utraty posiadanych wartości materialnych, a w określonych sytuacjach nawet intelektualnych. Oznacza to, że zagrożenia stanowią istotny element procesu decyzyjnego organizacji, co wymaga dokonania wyboru skutecznego działania prowadzącego do obniżenia poziomu zagrożenia lub niedopuszczenia do jego powstania. Obniżenie poziomu zagrożenia polega na wyodrębnieniu w nim wielu elementów składowych jako czynników lub symptomów.

> Zagrożenia mogą być zarówno niespodziewane, jako produkt uboczny działań podjętych w celu osiągnięcia konkretnych pozytywnych korzyści, jak i zamierzone, jako wytwór podmiotu dla wykorzystania ich jako instrumentów do umyślnego oddziaływania na inny podmiot, celem osiągnięcia konkretnych negatywnych dla niego zjawisk. Zagrożenia mogą mieć także charakter ciągły, np. zjawiska przyrodnicze lub elementy programu pewnej grupy społecznej przekazywanego z pokolenia na pokolenie. W takiej sytuacji społeczeństwo często akceptuje zagrożenia jako zjawiska niepożądane, ale realnie istniejące, niemożliwe do wyeliminowania[11].

Zagrożenie jako zjawisko można w zależności od jego charakteru (militarne i/lub pozamilitarne) przy zastosowaniu takich samych wyznaczników, jak czas,

[9] *Zagrożenia kryzysowe*, op. cit., s. 26.

[10] M. Wrzosek, op. cit., s. 21.

[11] Ibidem, s. 22.

przestrzeń czy skala oddziaływania, opisać i wskazać z dużym prawdopodobieństwem poziom mogących wystąpić szkód. Wymaga to ciągłego monitorowania miejsc o podwyższonym ryzyku, analizy symptomów wystąpienia negatywnego zjawiska (zdarzenia), jego oceny, podjęcia decyzji i uruchomienia posiadanych sił i środków.

Nie zawsze jednak należy traktować zjawiska zagrażające bezpieczeństwu jako zagrożenie.

> Część z nich nie zawsze jest groźna i nie zawsze wypełnia termin zagrożenie. Jeśli stan zagrożenia jest związany ze świadomością podmiotu będącego jego obiektem, to można wnioskować, że tylko brak należytej wiedzy o istocie zjawiska zagrożenia prowadzi do określonego stanu psychicznego. Zatem poznanie i zrozumienie zjawiska zagrożenia powoduje ograniczenie poziomu niebezpieczeństwa. Wówczas zamiast terminu zagrożenie trafniej wydaje się określać zaistniały stan jako ryzyko, które należy eliminować, lub jako wyzwanie […], które można lub trzeba podejmować[12].

Ryzyko ma ścisły związek z działalnością tak pojedynczego człowieka, jak i organizacji (państwa, narodu, firmy) i jej następstwami. Ryzyko jest określane jako sytuacja, gdy co najmniej jeden z elementów składających się na nią nie jest znany, ale znane jest prawdopodobieństwo jego wystąpienia (lub ich, jeżeli tych elementów jest więcej)[13]. Prawdopodobieństwo to może być albo wymierne, albo tylko odczuwalne przez podejmującego decyzje. Warunki ryzyka występują tylko wówczas, kiedy posiadane doświadczenia pozwalają na porównanie występującego w danej chwili zjawiska (zdarzenia). Problemy występujące w sytuacji ryzykownej można w przypadku wymierności jej elementów rozwiązać, wykorzystując rachunek prawdopodobieństwa lub metody statystyczne[14]. W odniesieniu do państwa lub społeczności stan ryzyka to sytuacja, w której dostępność poszczególnych możliwości i związane z każdą z nich potencjalne korzyści są znane z pewnym szacunkowym prawdopodobieństwem[15]. W innym ujęciu

> ryzyko to prawdopodobieństwo poniesienia strat przez organizację w następstwie podjęcia określonej decyzji; działanie, w którym nie wszystkie zmienne dają się oszacować na podstawie rachunku prawdopodobieństwa. Ryzyko różni się od niepewności. Pojęcie niepewności stosuje się wtedy, gdy w badaniu określonego zjawiska lub tendencji nie da się zastosować rachunku prawdopodobieństwa. Ryzyko natomiast dotyczy zdarzeń powtarzalnych [co ma często miejsce w sytuacjach uzasadniających uruchomienie procedur związanych z zarządzaniem kryzysowym – przyp. Autora], których możliwość zaistnienia można obliczyć statystycznie, czyli można je skalkulować. Często mówi się, że ryzyko to dobrze skalkulowana niepewność[16].

[12] Ibidem, s. 23.

[13] Ibidem, s. 24.

[14] *Encyklopedia organizacji i zarządzania*, Warszawa 1981, s. 564.

[15] R.W. Gryffin, *Podstawy zarządzania organizacjami*, Warszawa 2001, s. 271.

[16] J. Penc, op. cit., s. 388–389.

Takim przykładem jest możliwość skalkulowania częstotliwości występowania w ściśle określonych rejonach Polski powodzi. Prawdopodobieństwo wystąpienia lub niewystąpienia określonych zdarzeń może być wymierne albo tylko odczuwane przez podejmującego ryzyko, przy czym percepcja tego ryzyka jest nieodłącznie związana z systemem emocjonalnym decydenta[17].

Ryzyko dotyczy praktycznie każdej działalności, w tym ma ścisły związek z bezpieczeństwem wewnętrznym i zewnętrznym państwa. Występuje również w procesie zarządzania kryzysowego, z którym decydenci i podmioty wykonawcze zawsze muszą się liczyć i wkalkulować w proces decyzyjny.

Monitorowanie środowiska o podwyższonym ryzyku, przygotowanie pod względem merytorycznym podmiotów uczestniczących w zarządzaniu kryzysowym, dysponowanie odpowiednim wyposażeniem, znajomość procedur – daje możliwość niedopuszczenia do wystąpienia określonego zagrożenia lub zminimalizowania jego negatywnych następstw. Szansą dla podmiotu uczestniczącego w zarządzaniu kryzysowym są okoliczności, które sprzyjają realizacji założonych celów. Szansą dla tych podmiotów są zmiany, których wprowadzenie uzasadniają zjawiska (zdarzenia). Ich zaangażowanie związane ze sferą zarządzania kryzysowego ma wpływ na racjonalne wykorzystanie posiadanych sił i środków, niedopuszczenie do uaktywnienia się zagrożenia (zagrożeń) lub minimalizowanie wystąpienia ich negatywnych następstw, co bezpośrednio przekłada się na bezpieczeństwo ludności.

3.2. Zagrożenia naturalne

Zagrożenia naturalne wywoływane są przez czynniki fizyczne, siły i zjawiska przyrodnicze. Okazuje się, że mimo iż są one zidentyfikowane i zbadane przez człowieka, to jednak ich skala i siła niszczenia sprawiają, że nauka, technika i technologie oraz człowiek są bezradni. Przyroda, gdzie widoczna jest nadmierna ingerencja człowieka, powoli staje się jego przeciwnikiem, a człowiek często znajduje się na pozycji przegranej. Również dążenie ludzkości do poznania i zagospodarowania przestrzeni otaczającej Ziemię wiąże się ze zmianami fizycznymi i chemicznymi, co oznacza, że człowiek musi się liczyć z zagrożeniami kosmicznymi. Prowadzone badania z udziałem nielicznych państw wykazują, że wpływ kosmosu na życie na Ziemi jest wbrew pozorom bardzo znaczący. Stawarza to podstawę do prognozowania zagrożeń, których źródłem jest kosmos.

Zagrożenia naturalne obejmują zdarzenia związane z działaniem sił natury, zwłaszcza z wyładowaniami atmosferycznymi, wstrząsami sejsmicznymi, silnymi wiatrami, intensywnymi opadami atmosferycznymi, długotrwałym wystę-

[17] Ibidem, s. 389.

powaniem ekstremalnych temperatur, osuwiskami ziemi, pożarami, suszami, powodziami, zjawiskami lodowymi na rzekach i morzu oraz jeziorach i innych zbiornikach wodnych, masowym występowaniem szkodników, chorób roślin, zwierząt, chorób zakaźnych ludzi albo działaniem innego żywiołu[18].

Podział zagrożeń naturalnych przedstawiono w tabeli 32.

Tabela 32. Podział zagrożeń naturalnych

Zagrożenia naturalne	
Klimatyczne	intensywne opady powodzie, lawiny susze, upały oblodzenie, zaspy huragany, tornada burze i wyładowania atmosferyczne efekt cieplarniany pożary
Tektoniczne	trzęsienia ziemi erupcja wulkanów fale tsunami zakłócenia magnetyczne ziemi
Biologiczne	choroby zakaźne epidemie, pandemie choroby klimatyczne skażenie wody skażenie żywności
Kosmiczne	promieniowanie słoneczne promieniowanie kosmiczne kolizja kosmiczna obca cywilizacja obce formy życia

Źródło: K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe*, Gdynia 2007, s. 84

Zagrożenia klimatyczne

Zagrożenia klimatyczne (zwane również atmosferycznymi) mają ścisły związek nie tylko ze zjawiskami występującymi w przyrodzie, ale nadmierną ingerencją człowieka, czego następstwem są m.in. zmiany klimatu. Do powszechnych kategorii zagrożeń klimatycznych zalicza się: powodzie i lawiny błotne, susze i upały, śnieżyce, zaspy i oblodzenia, silne wiatry i ulewy, wyładowania atmosferyczne, efekt cieplarniany. W następstwie zakłócenia naturalnego obiegu wody na powierzchni i w atmosferze ziemskiej powstają długotrwałe, traktowane w kategoriach katastrof susze oraz intensywne upały i powodzie.

Powodzie są na terytorium Polski najczęściej występującym zagrożeniem naturalnym. Powódź to czasowe pokrycie przez wodę terenu, który w normalnych warunkach nie jest pokryty wodą, powstałe na skutek wezbrania wody w ciekach naturalnych, zbiornikach wodnych, kanałach oraz od strony morza,

[18] Ustawa z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej* (Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.). art. 3 ust. 1 pkt 2.

powodujące zagrożenie dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej[19]. Niszczące działanie wody jest widoczne nie tylko w czasie wielkich powodzi, ale również tych, które występują kilka razy w roku na terenie Polski i mają mniejszy zasięg.

Tabela 33. Powodzie i susze

Powodzie (lawiny) i susze (upały)	
Nadmiar wody	
Powodzie	Lawiny
opadowe roztopowe zimowe sztormowe	śnieżne błotne osuwiska ziemi potokowe i rumowiskowe
Niedobór wody	
Susze/Upały	
meteorologiczne (atmosferyczne) hydrologiczne rolnicze stulecia	obniżenie poziomu wody zanieczyszczenie gleby erozja gleby zakłócony bilans wodny

Źródło: Opracowano na podstawie K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe,* Gdynia 2007, s. 86

Obszarami szczególnego zagrożenia powodzią są tereny pomiędzy wałem przeciwpowodziowym, naturalnym wysokim brzegiem a linią brzegu, obszary pasa nadbrzeżnego oraz strefy przepływów wezbrań powodziowych. Obszarami potencjalnego zagrożenia są natomiast tereny narażone na powódź w przypadku przelania się wód przez wał przeciwpowodziowy, zniszczenia bądź uszkodzenia wałów przeciwpowodziowych lub budowli piętrzących[20].

Ten rodzaj klęski żywiołowej jest szczególnie groźny z uwagi na to, iż nie ma możliwości precyzyjnego określenia czasu, miejsca i wielkości tego zjawiska[21]. Należy podkreślić, że charakter powodzi jest zdecydowanie inny na rzekach nizinnych i potokach górskich.

Takie sytuacje wymagają udziału znacznych sił i środków koniecznych zarówno do prowadzenia akcji przeciwpowodziowej, jak i do przywrócenia stanu pierwotnego.

Opady atmosferyczne to ciekłe lub stale produkty kondensacji pary wodnej spadającej z chmur na powierzchnię ziemi[22]. Zalicza się do nich mżawki, deszcze, a także śnieg i grad. Okres zimy to niekiedy intensywne opady śniegu i towa-

[19] Ustawa z dnia 18 lipca 2001 r. *Prawo wodne* (Dz. U. z 2001 r. Nr 115, późn. 1229 z późn. zm.), art. 9 ust. 1 pkt 10.

[20] *Zagrożenia kryzysowe*, op. cit., s. 31.

[21] W. Lidawa, W. Krzeszowski, W. Więcek, *Zarządzanie w sytuacjach kryzysowych*, Warszawa 2010, s. 8.

[22] *Zagrożenia kryzysowe*, op. cit., s. 33.

rzyszące im niskie temperatury. W skrajnych wypadkach dochodzi do zakłócenia życia społeczeństwa, co wiąże się z brakiem dostawy wody (zimnej i ciepłej), energii elektrycznej, gazu. Ponadto występują trudności w transporcie i komunikacji, uszkodzenia linii przesyłowych energii elektrycznej, linii telekomunikacyjnych itp. Niebezpieczne jest także zaleganie śniegu na budynkach mieszkalnych i użyteczności publicznej. Jego nieusuwanie może doprowadzić do katastrof budowlanych. Skala i liczba takich katastrof świadczy m.in. o nieprzestrzeganiu przepisów regulujących użytkowanie obiektów budowlanych.

> Do opadów atmosferycznych zalicza się także grad, który jest opadem zamarzniętej wody. Zazwyczaj opad gradu związany jest z chmurami deszczowymi, dlatego gradobicie występuje przeważnie ze zjawiskiem burzy. Zjawisko gradobicia trwa stosunkowo krótko, jednak bryły lodu mogą być tak duże, że z dużą siłą niszczą zboża, gałęzie drzew, kwiaty, pąki roślin. W skrajnych przypadkach mogą skutkować śmiercią drobnego ptactwa czy zwierząt. Przynoszą również szkody w innych dziedzinach gospodarki, mogą być przyczyną zniszczenia budynków czy samochodów[23].

Należy podkreślić, iż mimo wiedzy dotyczącej fizyki atmosfery człowiek nie jest w stanie określić czasu i miejsca wystąpienia gradobicia, co oznacza, że nie może uprzedzić ludności o jego nadejściu.

Obfite opady śniegu i jego zaleganie w górach są przyczyną występowania lawin śnieżnych. Utrata stabilności i spadanie, ześlizgiwanie się ze stoku mas śniegu, lodu, skał i gleby to potężna energia niszczycielska. Jej skutki to zniszczona infrastruktura komunikacyjna i transportowa, zniszczone budynki mieszkalne i użyteczności publicznej, śmierć ludzi i zwierząt. Do czynników sprzyjających powstawaniu lawin zalicza się: rzeźbę terenu, pokrywę śnieżną, jednorazowy opad śniegu (powyżej 20 cm), nawis śnieżny, odwilż, wiatr, duże dobowe wahania temperatury.

Tabela 34. Charakterystyka lawin i ich skutki

Wielkość lawiny	Klasyfikacja przemieszczania	Klasyfikacja zniszczeń	Klasyfikacja ilościowa
zsuw	przesunięcie śniegu bez niebezpieczeństwa zasypania (niebezpieczeństwo upadku)	stosunkowo mało niebezpieczne dla ludzi	tor lawiny <50 m objętość <100 m
mała	zatrzymuje się na stoku	może zasypać, zranić lub zabić człowieka	tor lawiny <100 m objętość <1000 m
średnia	dobiega do końca stoku	może zasypać, zniszczyć samochód, uszkodzić ciężarówkę, może zburzyć mały budynek, połamać kilka drzew	tor lawiny < 1000 m objętość <10 000 m
duża	osiąga dno doliny, a nawet przeciwstok	może zniszczyć wagon kolejowy, dużą ciężarówkę, kilka budynków lub fragment lasu	tor lawiny > 1000 m objętość > 10 000 m

Źródło: *Zagrożenia kryzysowe*, red. G. Sobolewski, Warszawa 2011, s. 35

[23] Ibidem, s. 34.

Obok lawin śnieżnych poważnymi zagrożeniami są lawiny błotne, potoki błotno-rumowiskowe i osuwiska, które powstają w następstwie długotrwałych i intensywnych opadów deszczu. Niszczącą siłę potoku cechuje olbrzymia energia, zdolność transportowa, objętość oraz wartość rumowiska. Napotkane przeszkody nie obniżają jej energii, a nawet powodują jej wzrost. Potoki błotno-rumowiskowe powodują rozległe spustoszenia, niszcząc wszystko na swojej drodze (drogi, mosty, zabudowę, grunty rolne).

Susze to długotrwały okres niedoboru opadów atmosferycznych w stosunku do średnich sum opadów w danym okresie[24]. Przyczyn suszy należy upatrywać w anomaliach klimatycznych wywołanych zmianami w układzie mas powietrza. Susza powoduje przesuszenie gleby, zmniejszenie lub całkowite zniszczenie upraw roślin alimentacyjnych a co za tym idzie klęski głodu, zmniejszenie zasobów wody pitnej, a także zwiększone prawdopodobieństwo katastrofalnych pożarów. W Europie Środkowej susza występuje sporadycznie i nie stanowi zagrożenia dla zdrowia i życia, ale w szczególnych okolicznościach może być przyczyną poważnych strat materialnych, przede wszystkim w rolnictwie i leśnictwie. Do skutków suszy zalicza się m.in. drastyczne obniżenie dochodów z produkcji rolnej, znaczny wzrost cen żywności, obniżenie zasobów wody pitnej, pogorszenie jakości wody pitnej, możliwość powstania epidemii lub wzrost zachorowalności, konflikty społeczne.

Silne wiatry – w Polsce istnieje małe prawdopodobieństwo powstania huraganów, lecz należy liczyć się z zagrożeniami powodowanymi silnymi wichurami, których prędkość przekracza 100 km/h[25]. W związku ze zmieniającym się klimatem zjawisko to staje się coraz powszechniejsze w rejonach, w których do tej pory huragany nie występowały, na przykład w Europie Środkowej i Zachodniej. W Polsce coraz częściej występują także trąby powietrzne, które pojawiają się najczęściej na wiosnę i latem.

Tabela 35. Klasyfikacja maksymalnych prędkości wiatru i ich skutki

Prędkość wiatru w km/h na wysokości 10 m	Charakterystyka wiatru	Skutki działania wiatru
62–74	wiatr gwałtowny	łamie gałęzie drzew, chodzenie pod wiatr jest utrudnione
75–88	wichura	powoduje uszkodzenia budynków, zrywa dachówki, łamie całe drzewa
89–102	silna wichura	powoduje duże uszkodzenia budynków, wyrywa drzewa z korzeniami
103–117	gwałtowna wichura	powoduje rozległe uszkodzenia
> 118	wiatr huraganowy lub trąba powietrzna	powoduje zniszczenia i spustoszenia, możliwe są wypadki śmiertelne

Źródło: J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Warszawa 2005, s. 298

[24] E. Nowak, *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Warszawa 2007, s. 22.

[25] T. Szmidka, *Charakterystyka zagrożeń mogących powodować zaistnienie sytuacji kryzysowych (zagrożenia niemilitarne)*, [w:] *Łączność w sytuacjach kryzysowych o charakterze niemilitarnym na obszarze kraju*, *Materiały z konferencji Zakładu Systemów Łączności i Informatyki AON*, Warszawa 2004, s. 70.

Występujące obecnie silne wiatry, orkany i huragany stanowią poważne zagrożenie. Prawdopodobieństwo ich występowania na terytorium Polski jest coraz większe[26]. Należy mieć świadomość tego, że wiatr wiejący z dużą prędkością stanowi zagrożenie nie tylko dla ludzi, ale też dla budynków prywatnych i użyteczności publicznej, a także infrastruktury krytycznej państwa. Do czynników destrukcyjnych w przypadku huraganów i silnych wiatrów zalicza się: wiatr jako siłę niszczącą, zrywającą dachy, wyrywającą drzewa z korzeniami, niszcząca budynki, opady, które temu towarzyszą i mogą powodować liczne powodzie, nasiąkanie ziemi wodą, osuwiska, fale przypływowe na terenach nadbrzeżnych[27]. Klimatolodzy zakładają znaczący wzrost ich mocy, co oznacza konieczność rozszerzenia skali poprzez dodanie nowego zjawiska o nazwie hiperkan. Będzie się on charakteryzował dużo większą prędkością, niższym ciśnieniem i większą energią niż normalne huragany[28].

Mając na uwadze charakter powyższych negatywnych zjawisk, trudno jest mówić o jakiejkolwiek ochronie, można jedynie minimalizować skutki poprzez wczesne wykrywanie i ostrzeganie ludności. Wykryte zagrożenie oraz wiedza o nadejściu silnego wiatru nie pozwala jednak na uniknięcie ofiar w ludziach i strat materialnych.

W Polsce szczególnie narażone na występowanie silnych wiatrów są wybrzeże Bałtyku, Beskid Żywiecki, Karkonosze, okolice Wrocławia oraz Podhale.

Burze – gwałtownym skokom temperatury i ciśnienia towarzyszą burze i wyładowania atmosferyczne, których siła rażenia jest trudna do prognozowania i skutecznego przeciwdziałania. Należą do najbardziej gwałtownych zjawisk pogodowych występujących na terytorium Polski. Zagrożeniem dla zdrowia, życia ludzi i zwierząt są wyładowania atmosferyczne z uwagi na zgromadzoną energię, której nie można opanować. Wyróżnia się dwa rodzaje wyładowań atmosferycznych: chmurowe i chmura–ziemia, przy czym najgroźniejsze jest wyładowanie drugie. Mimo że nie trwa nawet sekundę, to jednak nagromadzona energia jest najbardziej niszczycielska, począwszy od zniszczenia pojedynczego obiektu, do spustoszenia bardzo rozległych obszarów włącznie. Szczególnie wrażliwe obiekty to urządzenia i systemy energetyczne, transformatory i linie przesyłowe wysokiego napięcia.

[26] Nie ulega wątpliwości, że zjawiska huraganów i orkanów w coraz większym stopniu zaczynają dotykać Polskę. Egzemplifikacją tych zjawisk może być huragan *Kyrill* w dniach 16–19 stycznia 2007 roku, który 18 stycznia dotarł do Polski, miejscami wiejąc z prędkością 150 km/h. Najwyższa prędkość tego huraganu została odnotowana na Śnieżce, gdzie zabrakło podziałki na wiatromierzu, a maksymalne możliwe wychylenie wyniosło 250 km/h. Innym przykładem jest orkan *Emma*, który w dniach 29 lutego – 2 marca 2008 roku dotarł do Polski z Wysp Owczych, pustosząc wcześniej Niemcy, Austrię i Czechy. Kolejny przykład to orkan *Xynthia*, który przeszedł nad Polską w dniach 28 lutego – 1 marca 2010 roku, wiejąc z prędkością ponad 140 km/h, *Zagrożenia kryzysowe*, op. cit., s. 39.

[27] *Zagrożenia kryzysowe,* op. cit., s. 39.

[28] Ibidem, s. 40.

Tabela 36. Silne wiatry jako zagrożenie klimatyczne

Wiatry, tornada
sztormowe fale
powalone drzewa
latające przedmioty
uszkodzone budowle
wypadki komunikacyjne
zablokowane szlaki komunikacyjne
zerwane linie energetyczne

Tabela 37. Burze jako zagrożenie klimatyczne

Burze atmosferyczne
wyładowania elektryczne
awarie urządzeń technicznych
pożary budowli i urządzeń
pożary obszarów leśnych
porażenie piorunem
złe samopoczucie
ograniczone bezpieczeństwo

Źródło: K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe*, Gdynia 2007, s. 88

Katastrofy naturalne są zaliczane do miejscowych zagrożeń, które w Polsce rejestruje Państwowa Straż Pożarna. Dominują wśród nich silne wiatry i opady deszczu. Średnią liczbę katastrof naturalnych występujących na terenie Polski w ciągu roku (lata 2003–2007) przedstawiono w tabeli 38.

Tabela 38. Średnia liczba katastrof naturalnych w ciągu roku w Polsce

Zagrożenie	Średnia liczba zdarzeń
silne wiatry	18 612
opady deszczu	10 119
przybory wód	5 415
opady śniegu	4 564

Źródło: K. Sienkiewicz-Małyjurek, Z.T. Niczyporuk, *Bezpieczeństwo publiczne. Zarys problemu*, Gliwice 2010, s. 65

Zagrożenia tektoniczne

Przyczyną ok. 90% trzęsień ziemi są ruchy tektoniczne. Przez pojęcie trzęsienia ziemi rozumie się wstrząsy podziemne oraz drgania powierzchni ziemi spowodowane przyczynami naturalnymi (procesami tektonicznymi, wybuchami wulkanów, tzw. ruchami zapadowymi)[29]. Trzęsienia ziemi stanowią zagrożenia dla zdrowia i życia ludzkiego, a także dla infrastruktury, powodują poważne zniszczenia.

Ze względu na źródło powstania trzęsienia ziemi można je podzielić na:

- wulkaniczne, o stosunkowo niewielkim zasięgu, poprzedzające wybuch wulkanu lub mu towarzyszące,
- zapadowe, o zasięgu lokalnym, powstające wskutek zapadania się jaskiń na obszarze krasu, wymywania otworów gipsowych lub solnych oraz eksploatacji wyrobisk górniczych (zjawisko tąpania),
- tektoniczne, stanowiące najczęstsze zjawisko, wywołane nagłymi przesunięciami mas skalnych w skorupie ziemskiej[30].

[29] T. Szmidka, op. cit., s. 70.

[30] *Zagrożenia kryzysowe*, op. cit., s. 47 i 48.

Pod względem zjawisk sejsmicznych Polska jest krajem, w którym trzęsienia ziemi zdarzają się bardzo rzadko, a nawet jeśli do nich dochodzi, to nie są silne. Według danych Instytutu Geofizyki Polskiej Akademii Nauk w ostatnim tysiącleciu na terytorium Polski zanotowano 76 trzęsień ziemi. Najbardziej aktywne sejsmicznie rejony kraju to Karpaty i Sudety. Wiele trzęsień ziemi odczuwalnych w kraju ma swoje epicentrum poza granicami Polski, jak to miało miejsce 16 grudnia 2008 roku, gdy wystąpiło trzęsienie ziemi w południowej Szwecji, a wszystkie stacje sejsmologiczne w Polsce zarejestrowały to zjawisko. Z punktu widzenia sejsmologii 2004 rok był w Polsce wyjątkowo aktywny. Doszło wtedy do dwóch trzęsień ziemi na terenie kraju: 21 września w obwodzie kaliningradzkim miało miejsce szczególnie silne promieniowanie fal sejsmicznych, co spowodowało odczucie zjawiska na Suwalszczyźnie, 30 listopada na Podhalu, o sile 4,9 w skali Richtera, którego przyczyną były ruchy tektoniczne[31].

Należy podkreślić, że niezależnie od trzęsień ziemi w Polsce występują także wstrząsy wywołane działalnością górniczą. Zjawiska tego rodzaju pojawiają się najczęściej na obszarach Zagłębia Górnośląskiego i Zagłębia Bełchatowskiego.

Zagrożenia biologiczne

Współczesne środowisko człowieka mimo postępu w naukach medycznych, chemicznych i naukach pokrewnych nie jest wolne od zagrożeń dla zdrowia i życia człowieka, zwierząt oraz roślin. „Stoimy u progu globalnego kryzysu związanego z chorobami zakaźnymi. Żaden kraj nie jest bezpieczny. Żaden kraj nie może już dłużej pozwolić sobie na ignorowanie tego zagrożenia"[32].

W 2002 roku brytyjski Raport rządowy zaczynał się od przerażającej uwagi, że optymistyczne przeświadczenie o rychłym zwycięstwie nad chorobami zakaźnymi okazało się głęboko nieuzasadnione. Na początku XXI wieku – dowodzi Raport – choroby zakaźne są nadal poważnym globalnym zagrożeniem dla ludzkiego zdrowia, dobrobytu, stabilizacji społecznej i poczucia bezpieczeństwa. Obawy spowodowane były faktem, iż stanowią one 41% wszystkich chorób na całym świecie, łącznie z takimi jak HIV/AIDS, gruźlica i malaria, z których każda zabija miliony ludzi[33].

Potwierdzeniem tej diagnozy było

podjęcie w 2005 roku działań związanych z pojawieniem się nowej wersji grypy, która zabrała się w podróż wraz z ptakami wędrownymi i przybyła z Dalekiego Wschodu do Europy. Kiedy zjawiła się w Rosji, wywołała zdziwione miny; przybywając do Rumunii, wzbudziła zaniepokojenie. Lecz dopiero gdy wirus wywołujący chorobę zabił ptaki w Grecji, dziennikarze umieścili tę historię na pierwszych stronach gazet, politycy natomiast zaczęli plątać się w zeznaniach. Okazało się nagle, że mają w ręku biologiczną bombę, która w każdej chwili może wybuchnąć. Pomimo ogromnej wiedzy naukowej, umiejętności praktycznych i zaawansowanej technologii w dziedzinie medycyny trzęśliśmy się ze strachu przed jedną z najprostszych form biologicznych – wirusem[34].

31 W. Lidawa, W. Krzeszowski, W. Więcek, op. cit., s. 48–49.

32 Wypowiedź Gro Harlem Brundtland, gdy zajmowała stanowisko Dyrektora Generalnego Światowej Organizacji, WHO, *Annual Report*, 1996.

33 P. Moore, *Tajemnicze choroby współczesnego świata. Nowe zagrożenia – wirusy, bakterie, zarazki*, Warszawa 2009, s. 7.

34 Ibidem, s. 7–8.

Oznacza to, że epidemie, epizootie czy epifizie stanowią poważne zagrożenie dla człowieka i jego środowiska. Masowe rozprzestrzenianie się zachorowań na chorobę (choroby) zakaźną wśród ludzi, zwierząt i roślin może doprowadzić do stanu, który należy traktować w kategoriach stanu klęski żywiołowej na znacznych obszarach. Do czynników, które przyczyniają się do rozwoju tego typu zagrożeń, zalicza się: swoistość czynników sprawczych (etiologicznych): biotycznych (bakterie, wirusy, grzyby), rezerwuarowych (ludzie, zwierzęta, powietrze, gleba, woda), nosicieli choroby (owady, stawonogi, gryzonie, ptaki), wrażliwość organizmów, wzajemne oddziaływanie środowiska[35]. Istotą problemu dotyczącego rozprzestrzeniania się chorób u progu XXI wieku jest łatwe przenoszenie patogenów. Procesowi temu sprzyja rozwój globalizacji, której towarzyszy m.in. swobodny przepływ ludzi (ich wzajemne kontakty), zwierząt, żywności czy też komponentów do jej produkcji. Tym samym choroby mogą przemieszczać się praktycznie w czasie rzeczywistym, adaptować się do nowych warunków w poszukiwaniu swoich ofiar.

Ponadto niekorzystne zmiany w środowisku naturalnym, starzenie się społeczeństwa, a co za tym idzie wzrost podatności na zachorowanie, nabywanie przez drobnoustroje nowych cech, jaką jest odporność na antybiotyki, pojawianie się nowych wirusów posiadających zdolności do transmisji i wywoływania choroby, będą powodem wysokiej zachorowalności w więcej niż jednym kraju i rozprzestrzeniania się wirusów. W społeczeństwie dużą grupę będą stanowili ludzie podatni na nowy szczep, u których wystąpi brak przeciwciał dla nowego wirusa lub też poziom tych przeciwciał będzie bardzo niski[36].

Na uwadze należy mieć również celowe działanie człowieka, który kierując się różnymi pobudkami będzie wykorzystywał dostępne czynniki biologiczne i chemiczne czy łatwość ich produkcji dla realizacji partykularnych strategii, której negatywne skutki są niekiedy trudne do przewidzenia. Pamiętać też trzeba o prowadzeniu badań nad nowymi rodzajami tzw. broni biologicznej i chemicznej, gdzie brak antidotum na jej zastosowanie w niepowołanych rękach stanowi poważne zagrożenie dla człowieka i jego środowiska naturalnego.

Również negatywne zjawiska spowodowane aktywną działalnością człowieka lub sił natury stanowią miejsce wzajemnego przenikania się chorób, które rozwijają się w przyjaznym sobie środowisku. Zagrożenia te, spowodowane skutkami innych zdarzeń katastroficznych, takich jak powodzie, susze, trzęsienia ziemi, fale tsunami, stanowią doskonałe warunki dla rozwoju drobnoustrojów, co może prowadzić do powstania ognisk różnego rodzaju chorób zakaźnych, które przyczynią się do wybuchu epidemii. Rozprzestrzenianie się różnych chorób zakaźnych oraz epidemii jest bezpośrednim wynikiem niezachowania określonych wymogów sanitarno-higienicznych lub migracji innych organizmów zwie-

[35] *Zagrożenia kryzysowe*, op. cit., s. 41.

[36] Szerzej na ten temat pisze L.B. Brydak, *Grypa, pandemia grypy – mit czy realne zagrożenie*?, Warszawa 2008, s. 422.

rzęcych, takich jak np. bakterie, wirusy i różne szczepy chorobowe przenoszone w ostatnich latach przez wędrowne ptaki[37].

W praktyce wyodrębnia się dwa rodzaje źródeł epidemii: punktowe (np. studnie, produkty żywnościowe, nosiciele miejscowi) oraz migracje i kontakty osobiste[38]. Rozprzestrzenianie epidemii w pierwszym przypadku następuje nagle, ma gwałtowny przebieg, w krótkim czasie atakuje bardzo wiele osób. Natomiast migracje ludności i kontakty osobiste stanowią naturalne źródło dla nosicieli, co przy globalnym przemieszczaniu się ludności jest poważnym problemem dla identyfikacji, diagnozowania, a tym bardziej dla profilaktyki.

Do zagrożeń biologicznych zalicza się również skażenie biologiczne wody i żywności. Zanieczyszczenia wody, powietrza i gleby mogą być powodowane zarówno przez czynniki biologiczne, chemiczne, jak i promieniotwórcze.

Należy mieć na uwadze realne zagrożenie wykorzystywania mikroorganizmów chorobotwórczych (wirusów, riketsji, bakterii) do celowego zarażania ludzi, zwierząt, skażenia wody, żywności, płodów rolnych. Wykorzystanie mikroorganizmów chorobotwórczych jako środka bojowego stanowi aktualnie poważne zagrożenie, jednak nie wszystkie mikroorganizmy mogą być zdatne do użycia w ataku biologicznym. Kolejny niezmiernie ważny problem to brak wiedzy i świadomości na temat chorób zakaźnych, dróg przenoszenia, skutków czy profilaktyki. Zagrożenia biologiczne stanowią poważne wyzwanie dla podmiotów zajmujących się zarządzaniem kryzysowym na wszystkich poziomach bezpieczeństwa państwa.

Kryteria potencjału broni biologicznej to:

- udowodniona wcześniej przydatność mikroorganizmu chorobotwórczego jako broni biologicznej,
- wysoki współczynnik zachorowalności, chorobowości i (lub) śmiertelności,
- niskie dawki infekcji,
- duża zakaźalność, krótki okres inkubacji,
- duże straty socjalno-ekonomiczne,
- trudności wykrycia na wczesnym etapie,
- duża dostępność,
- niski koszt produkcji,
- łatwość rozpowszechniania,
- stabilność w środowisku,
- brak lub mała skuteczność profilaktyki, ochrony i leczenia[39].

Zagrożenia kosmiczne

Prowadzone badania nad kosmosem wskazują, że ma on duży wpływ na życie na Ziemi. Stwarza to racjonalne przesłanki do prognozowania licznych zagrożeń dla człowieka i jego naturalnego środowiska.

[37] K. Ficoń, op. cit., s. 89.

[38] Ibidem, s. 89.

[39] J. Kocik, *Kryteria idealnego środka broni biologicznej*, [w:] *Bioterroryzm. Zasady postępowania lekarskiego*, red. K. Chomiczewski, J. Kocik, M.T. Szkoda, Warszawa 2002, s. 54–58.

Do najbardziej powszechnych zagrożeń, których źródłem jest przestrzeń otaczająca Ziemię, można zaliczyć:

- promieniowanie kosmiczne (twarde, miękkie, szkodliwe, przenikliwe, zależne od bardzo wielu czynników nie do końca jeszcze poznanych),
- natężenie promieniowania słonecznego (jego spektrum i przenikliwość oraz wpływy na klimat i warunki życia na Ziemi),
- statystyczną możliwość zderzenia Ziemi z obcym ciałem kosmicznym (wcale nie tak abstrakcyjną jak niegdyś sądzono) i ogromne konsekwencje cywilizacyjne i przyrodnicze takiej kolizji,
- zmianę natężenia magnetyzmu ziemskiego i siły grawitacji (zarówno samej Ziemi, jak też naszej planety w całym Układzie Słonecznym),
- oddziaływanie tzw. plam słonecznych oraz różnych ognisk promieniowania i wybuchów termojądrowych na Słońcu,
- ewentualność spotkania obcej cywilizacji czy przejawów jakiegokolwiek życia pozaziemskiego i związane z tym nieobliczalne konsekwencje biologiczne, społeczne, cywilizacyjne[40].

W procesie monitorowania kosmosu będącego źródłem zagrożenia dla życia na Ziemi należy uwzględniać zjawiska i procesy, które tam zachodzą i są odmienne od warunków panujących na naszej planecie. Przestrzeń otaczająca naszą planetę ma silny wpływ na klimat na Ziemi oraz zjawiska geofizyczne (w tym tektoniczne i magnetyczne). Kolejna istotna kwestia to zupełnie inny zegar czasowy, co oznacza, że procesy, które tam zachodzą, rozgrywają się w odmiennej skali czasoprzestrzennej obejmującej m.in. miliony lat świetlnych, co dla nas jest niewyobrażalne[41]. Ponadto człowiek w celu poprawy swoich warunków życia rozpoczął już penetrację kosmosu, mając nadzieję na jego eksplorację. Szczególna uwaga jest skupiona na opanowywaniu kosmosu nie tylko dla celów militarnych, ale i jego zasobów surowcowych, w tym o znaczeniu strategicznym dla człowieka. W celu niedopuszczenia lub zminimalizowania negatywnych następstw niekontrolowanej eksploracji kosmosu należy dążyć do stworzenia przez społeczność międzynarodową takich warunków prawno-organizacyjnych, które sprawią, że wszechświat będzie nie tylko poznawalny, ale i bezpieczny.

3.3. Zagrożenia techniczne

Zagrożenia o charakterze technicznym mają ścisły związek z postępem cywilizacyjnym, w tym naukowym i technicznym, a przede wszystkim z działalnością gospodarczą człowieka. Totalna, pozbawiona najczęściej skrupułów

[40] Ibidem, s. 83 i 84.

[41] Ibidem, s. 84 i 85.

ingerencja człowieka w środowisko naturalne powoduje zachwianie naturalnych zasad ewolucji i rozwoju, co w początkowym okresie uaktywnia mechanizmy obronne środowiska przyrodniczego. Jednak w skrajnych przypadkach ma miejsce eliminacja wszelkich mechanizmów obronnych i samozachowawczych, co prowadzi do załamania się linii ewolucyjnych całych gatunków przyrodniczych, włącznie z krajobrazami i bezpieczeństwem naturalnej egzystencji człowieka[42].

Niekontrolowany rozwój przemysłu powoduje zatrucie środowiska naturalnego, systematycznie zwiększa się liczba odpadów, a także emisja dwutlenku węgla do atmosfery, przy jednoczesnym zmniejszaniu się obszarów zalesionych, wzroście zjawiska globalnego ocieplenia i anomalii pogodowych. Szczególne zagrożenie stwarzają elektrownie atomowe, zakłady i magazyny przechowujące środki toksyczne oraz pojazdy transportujące te substancje, a także laboratoria przechowujące niebezpieczne substancje biologiczne i chemiczne. Materiały toksyczne, wybuchowe i promieniotwórcze stosowane są przede wszystkim w energetyce, przemyśle chemicznym, paliwowym, hutniczym, motoryzacyjnym. Awarie w takich zakładach i w elektrowniach mogą spowodować zatrucia, pożary, wybuchy, śmierć wielu osób i doprowadzić do skażenia terenu na dziesiątki lat[43].

Tabela 39. Podział zagrożeń technicznych

Zagrożenia techniczne	
Pożary i klęski krajobrazowe	pożary naturalne pożary sztuczne pożary przemysłowe pożary komunalne pożary obszarowe
Skażenie chemiczne	awarie chemiczne skażenia chemiczne skażenia promieniotwórcze zanieczyszczenia biologiczne
Katastrofy budowlane	katastrofy przemysłowe katastrofy instalacyjne katastrofy komunalne szkody górnicze
Katastrofy komunalne	awarie energetyczne awarie wodociągowe awarie gazowe awarie ciepłownicze
Katastrofy komunikacyjne	katastrofy kosmiczne katastrofy lotnicze katastrofy kolejowe katastrofy morskie katastrofy w żegludze śródlądowej katastrofy samochodowe

Źródło: Opracowano na podstawie K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe,* Gdynia 2007, s. 90

[42] Szerzej zob. K. Ficoń, op. cit., s. 90.

[43] K. Sienkiewicz-Małyjurek, Z.T. Niczyporuk, op. cit., s. 46.

Do najbardziej niszczycielskich sił zalicza się pożary, których skala i dynamika to nie tylko ogromna siła destrukcji, ale też niezwykle groźne następstwa, w tym tragedie ludzkie. Przyjmuje się, że około 80% pożarów powstaje z winy działalności ludzkiej, lekkomyślności, braku zdrowego rozsądku, nieprzestrzegania obowiązujących przepisów i zasad ochrony przeciwpożarowej, a także dywersji, sabotażu i celowego podpalenia. Generalnie pożary dzielimy na naturalne i sztuczne. Pierwsze wywoływane są przez siły natury, np. pożary lasów od wyładowań atmosferycznych, spowodowane długotrwałą suszą i wysoką temperaturą, pożary torfowisk i łąk powodowane tzw. samozapaleniem, wyładowaniami atmosferycznymi lub zaprószeniem ognia przez ludzi. Szczególnie niebezpieczne są pożary obiektów mieszkalnych, które stanowią najwyższe zagrożenie dla zdrowia i życia ludzi oraz zwierząt domowych i należą do najczęstszych zdarzeń.

Kolejna grupa to pożary obiektów przemysłowych i komunalnych. W tej kategorii dochodzi nie tylko do utraty życia ludzkiego, ale i do skażenia terenu substancjami łatwopalnymi i toksycznymi. Szczególnie niebezpieczne są pożary obiektów, w których wykorzystywane są środki radioaktywne, np. zakłady przemysłu nuklearnego czy elektrownie atomowe. Pożary tego typu obiektów to promieniotwórcze skażenie nie tylko ludzi bezpośrednio tam się znajdujących, ale i środowiska. To również radioaktywne skażenie obszarów znajdujących się w znacznej odległości od epicentrum, gdyż chmura pyłu radioaktywnego może być przenoszona przez wiatr na znaczne odległości. Przebywanie ludzi w strefie skażonej grozi chorobą popromienną, na którą nadal brak antidotum. Na uwadze należy mieć również neutralizację i utylizację odpadów radioaktywnych oraz wygaszonych reaktorów atomowych. Wypalone stosy atomowe zawierają substancje promieniotwórcze, których aktywność może trwać nawet 50 000 lat[44]. Rozwój energetyki jądrowej oznacza, że będzie przybywało coraz więcej źródeł i odpadów promieniotwórczych.

Ważnym problemem są również awarie techniczne[45] obiektów mieszkalnych, użyteczności publicznej i przemysłowych. Efektem takich awarii mogą być pożary, skażenia i zagrożenie ekologiczne. Ogromną siłą niszczycielską odznaczają się katastrofy wielkich budowli hydrotechnicznych, jak zapory wodne, stopnie i systemy piętrzące wodę, przede wszystkim dla celów energetycznych i rolniczych. Do grupy katastrof technicznych zalicza się także awarie, wypadki i różne zdarzenia związane z transportem i komunikacją (mosty, wiadukty, przeprawy itd.).

Warto zwrócić uwagę na katastrofy górnicze, które mają miejsce w rejonach wydobycia węgla. W kopalniach mogą wystąpić pożary, zawały chodników, podtopienia, tąpnięcia chodników i szybów kopalnianych, wybuchy gazów. Katastrofy górnicze są niebezpieczne nie tylko dla ludzi tam pracujących, w ich następstwie może dojść do osunięcia gruntu, awarii instalacji znajdujących się pod

[44] K. Ficoń, op. cit., s. 93.

[45] „Awaria techniczna to gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie obiektu budowlanego, urządzenia technicznego lub systemu urządzeń technicznych powodujące przerwę w ich używaniu lub utratę ich właściwości" – art. 3 ust. 1 pkt 3 ustawy z dnia 18 kwietnia 2002 roku *O stanie klęski żywiołowej* (Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.).

ziemią, destabilizacji budynków mieszkalnych, użyteczności publicznej, a nawet obiektów przemysłowych.

Istotne miejsce zajmują wypadki i katastrofy komunikacyjne, które są związane z rozwojem cywilizacyjnym i postępem technicznym. Produkcja coraz nowocześniejszych pojazdów o różnym przeznaczeniu ma istotny wpływ na wzrost liczby i skutków wypadków. Wśród zagrożeń komunikacyjnych dominują wypadki drogowe. Do czynników, które mają znaczący wpływ na postępujący wzrost zagrożeń w ruchu drogowym, należy zaliczyć zwiększenie natężenia ruchu drogowego, ubogą infrastrukturę drogową, zły stan techniczny pojazdów biorących udział w ruchu drogowym, działania człowieka (nieprzestrzeganie przepisów ruchu drogowego, alkohol, leki, narkotyki, predyspozycje psychomotoryczne). Pojedyncze wypadki komunikacyjne, a także katastrofy drogowe, kolejowe, lotnicze czy morskie, to zarówno ofiary w ludziach, jak i znaczne starty materialne. Bardzo często następstwem takich katastrof jest skażenie środowiska naturalnego substancjami toksycznymi, promieniotwórczymi, chemicznymi, których neutralizacja jest niezmiernie trudna i długotrwała. Wymienione awarie to nie tylko zmęczenie materiału, wadliwa konstrukcja, ale także celowa działalność człowieka (organizacji), który poprzez stosowanie substancji niebezpiecznych niszczy nie tylko infrastrukturę, a życie ludzi. W Polsce toksycznymi środkami przemysłowymi jest potencjalnie zagrożone 2/3 terytorium kraju i proporcjonalna do tego liczba ludności[46]. Ponadto szacuje się, że w skali kraju występuje rocznie co najmniej 1000–1500 zarejestrowanych przypadków nadzwyczajnych zagrożeń ludzi i środowiska[47].

> Według statystyk prowadzonych przez Państwową Straż Pożarną utrzymuje się wzrost liczby miejscowych zagrożeń, ale spada liczba pożarów w ciągu roku. Do miejscowych zagrożeń zalicza się: zagrożenia drogowe, zagrożenia ekologiczne, awarie infrastruktury komunalnej, zagrożenia chemiczne, zagrożenia budowlane, zagrożenia kolejowe, zagrożenia lotnicze, zagrożenia radiologiczne, a także silne wiatry, powodzie, obfite opady. W pożarach i miejscowych zagrożeniach co roku ginie średnio 3800 osób, a ponad 33 000 zostaje rannych[48].

Należy zaznaczyć, że w Polsce wśród zagrożeń XXI wieku dominują zagrożenia drogowe, ekologiczne, awarie infrastruktury technicznej i zagrożenia chemiczne. Średnioroczną liczbę tych zagrożeń w latach 2003–2009 zestawiono w tabeli 40.

[46] N. Sypion, *Współczesne zagrożenia bezpieczeństwa zbiorowego,* [w:] *Wybrane zagadnienia: propozycje metodyczne*, Toruń 2003, s. 26.

[47] T. Berliński, *Różnorodność postrzegania zagrożeń*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Kraków 2000, s. 68.

[48] K. Sienkiewicz-Małyjurek, Z.T. Niczyporuk, op. cit., s. 51.

Tabela 40. Średnia liczba katastrof i awarii technicznych w Polsce w ciągu roku

Katastrofy i awarie techniczne	Średnia liczba zdarzeń w ciągu roku
Zagrożenia drogowe	43 020
Zagrożenia ekologiczne	2741
Awarie infrastruktury technicznej	1652
Zagrożenia chemiczne	1013
Zagrożenia budowlane	988
Zagrożenia kolejowe	292
Zagrożenia lotnicze	146
Zagrożenia radiologiczne	15

Źródło: K. Sienkiewicz-Małyjurek, Z.T. Niczyporuk, *Bezpieczeństwo publiczne. Zarys problemu*, Gliwice 2010, s. 52

3.4. Zagrożenia społeczne

Zagrożenia społeczne są szczególnymi zagrożeniami, gdzie sprawcą i równocześnie ofiarą jest zarówno pojedynczy człowiek, jak i społeczeństwo znajdujące się w określonym stadium niezadowolenia społecznego, socjalnego, ekonomicznego, politycznego, kulturowo-obyczajowego czy religijnego[49]. Powszechną formą okazywania niezadowolenia przez społeczeństwo są strajki, manifestacje, masowe zgromadzenia, rozruchy uliczne itp. Organizowane na szeroką skalę manifestacje uliczne w określonych sytuacjach mogą się przerodzić w trudny do opanowania ruch anarchistyczny, co wymusza działanie sił porządkowych. W wyniku brutalności władz nasilają się protesty i żądania ofiar o charakterze politycznym, programowym i socjalnym. Doświadczenia wielu państw pokazują, że w skrajnych sytuacjach ma miejsce interwencja sił zbrojnych.

Zjawiska, które destabilizują sytuację wewnętrzną w państwie, powstają w procesach tworzenia warunków socjalno-bytowych: gwarantowania bezpieczeństwa i swobód obywatelskich, prywatyzacji i reprywatyzacji, kreowania polityki przemysłowej, rolnej i usług, rozwoju nauki, techniki i technologii, ochrony środowiska naturalnego, a także tworzenia prawa i jego przestrzegania. Tym procesom sprzyja trwająca transformacja ustrojowa, a także postępująca globalizacja, obecna praktycznie we wszystkich sferach działania państwa (szczególnie jest widoczna w sferze gospodarczej).

Pogłębiający się deficyt budżetu państwa, według dyrektyw kapitału globalnego zmusza kraje do ograniczania osłony socjalnej i innych wydatków na potrzeby zbiorowe, co obniża popyt i pogłębia recesję. Liberalizacja handlu międzynarodowego skutku-

[49] K. Ficoń, op. cit., s. 97.

je przenoszeniem firm produkcyjnych do krajów o niskich płacach i podatkach, co zwiększa bezrobocie w rozwiniętych państwach. W ubogich krajach w obawie przed wzrostem inflacji podnosi się stopy procentowe od kredytu, co obniża poziom inwestycji. Następstwem tego nie jest wzrost gospodarczy, lecz narastająca bieda. Światowa Organizacja Handlu, Międzynarodowy Fundusz Walutowy, Bank Światowy tworzą faktyczny rząd gospodarczy na świecie, podporządkowany USA, który nie podlega kontroli i nie ma nic wspólnego z demokratycznym ładem. Liberalizacja handlu światowego przysparza korzyści krajom bogatym i strat biednym. Największe zyski osiągają USA i Unia Europejska (nie wszystkie państwa), bo kraje zależne otworzyły dla nich swe rynki, a kraje mocarstwowe im je zamknęły. Globalna gospodarka stała się globalną niesprawiedliwością dla świata. Kapitał globalny doprowadza wszędzie do totalnego chaosu gospodarczego i społecznego poprzez deregulację rynku, finansów, zatrudnienia (łatwość zwalniania i przyjmowania do pracy, dowolne umowy o pracę), ochrony socjalnej, budżetu państwa, edukacji, zdrowia, kultury, sądownictwa, bezpieczeństwa wewnętrznego[50].

Społeczeństwo polskie prawdopodobnie nie do końca ma świadomość zachodzących zmian społeczno-politycznych, ze szczególnym wskazaniem na gospodarcze. Niewątpliwie poziom życia znacznie się obniżył, co jest źródłem niezadowolenia społecznego, które przyjmuje różne formy.

Często słyszy się o demokracji i państwie prawa. Przy czym ci przywódcy, którzy o tym najgłośniej mówią, zazwyczaj najmniej tego pragną. Nie wiadomo, czy chcą ustanowić pewien rodzaj despotyzmu, czy dążą tego, by ktoś zrobił za nich to, co sami zrobić powinni. Może to prowadzić do destabilizacji sytuacji społecznej[51].

Jedna z istotniejszych przesłanek stanowiących poczucie zagrożenia przez społeczeństwo, to zagrożenie bezpieczeństwa i swobód obywatelskich. Przejawia się to w niestabilnym i niespójnym prawie, przypadkach działania prawa wstecz, bezkarności przestępców, aferach gospodarczych i finansowych, rozbojach elementów napływowych, korupcji urzędników, destrukcyjnej walce o władzę różnych polityków lub ugrupowań politycznych z wykorzystaniem ulicy, nierówności wobec prawa oraz braku sprawiedliwości społecznej[52].

W Polsce do jednych z wielu zagrożeń o charakterze społecznym należy zaliczyć emigrację zarobkową, emigrację tranzytową, a także emigrację związaną z pobytem stałym. Jedną z podstawowych przyczyn migracji są względy ekonomiczne, gdy ludność przemieszcza się w poszukiwaniu źródeł utrzymania i poprawy warunków bytowych.

w 2007 roku poza granicami Polski przebywało około 2,2 mln emigrantów. […]. Zagraniczna emigracja ekonomiczna po przystąpieniu Polski do Unii Europejskiej przerosła swą skalą migracje wewnętrzne, w tym obserwowaną w Polsce od szeregu lat migrację ze wsi do miasta w poszukiwaniu pracy i lepszych warunków życia. W połączeniu

[50] Z. Narski, *O dyktaturze kapitału globalnego*, Toruń 2004, s. 9–10.

[51] S. Dworecki, op. cit., s. 31.

[52] Ibidem, s. 36.

z procesem starzenia się społeczeństwa zjawisko masowej migracji zagranicznej stanowi zagrożenie dla bezpieczeństwa społecznego, ponieważ z kraju wyjeżdżają najczęściej osoby przedsiębiorcze, zdolne i gotowe do podjęcia zatrudnienia, a więc z punktu widzenia nie tylko gospodarczego rozwoju państwa – najbardziej potrzebne[53].

Jednak prowadzona polityka gospodarcza, która bezpośrednio przekłada się na politykę społeczną, to likwidacja miejsc pracy, która nie zawsze była (jest) uzasadniona. W ten sposób pozbawia się ludzi środków utrzymania. Temu długofalowemu zjawisku towarzyszy nie tylko wspominana migracja zarobkowa, ale postępująca pauperyzacja społeczeństwa.

Do kolejnych przyczyn migracji należy zaliczyć:

- przyczyny polityczne (wojny domowe, represje) i religijne, które zmuszają uchodźców i azylantów do poszukiwania schronienia w innych państwach,
- przyczyny rodzinne, w ramach sprowadzania rodzin do państwa zamieszkania przez członka rodziny (emigranta) lub w ramach repatriacji, czyli powrotu do ojczystego kraju bądź deportacji tzn. przymusowego powrotu do własnego kraju,
- przyczyny związane z katastrofami naturalnymi, gdzie skutki utrudniają lub uniemożliwiają dalsze bytowanie ludności na danym obszarze.

Masowe przemieszczanie się ludności może przyczynić się do pogłębienia różnic etnicznych i kulturowych i tym samym stworzyć poważne wyzwanie dla struktur państwa przyjmującego, ale może też być źródłem siły roboczej, czynnikiem dynamizującym życie gospodarcze i społeczne[54].

Do najważniejszych zagrożeń społecznych w Polsce zaliczyć należy: masową migrację ludności, starzenie się społeczeństwa, bezrobocie, ubóstwo, bezdomność, wykluczenie społeczne (marginalizacja), patologie (alkoholizm, narkomania, przestępczość), korupcję i nepotyzm[55].

„Zgodnie z danymi statystycznymi w Polsce zagrożonych ubóstwem (żyjących na granicy minimum socjalnego) jest około 60% społeczeństwa. Pozbawione właściwych dochodów jednostki i rodziny nie mogą w pełni uczestniczyć w życiu społecznym. Występuje tu zjawisko wykluczenia społecznego, inaczej nazywanego marginalizacją albo ekskluzją społeczną"[56]. W związku z tym występują różnego rodzaju zagrożenia, zwane też niepokojami społecznymi, których powodem są: poziom bezrobocia, stan bezpieczeństwa osobistego obywateli, stan przestrzegania swobód obywatelskich, stan bezpieczeństwa socjalnego, patologiczne zachowania społeczeństwa, pauperyzacja społeczeństwa, różnice statusu materialnego, dostępność do oświaty, nauki, kultury i wypoczynku, podział etniczny i religijny, transformacja ustrojowa, terroryzm polityczny, niestabilność

[53] P.W. Zawadzki, *Bezpieczeństwo społeczne*, [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009, s. 125–126.

[54] Wiatr K., *Migracje na świecie* – http://www.psz.pl/tekst-27340/migracje-na-świecie [pobrano 27.02.2012].

[55] P.W. Zawadzki, op. cit., s. 126.

[56] P.W. Zawadzki, op. cit., s. 129.

prawa, przestępczość, w tym o charakterze międzynarodowym, narkomania, alkoholizm, masowe migracje[57].

Na szczególną uwagę zasługują zagrożenia związane z terroryzmem międzynarodowym, którego skala i skutki społeczne są nieprzewidywalne. Wyznacznikiem terroryzmu są:

- stosowanie siły i przemocy przeciwko osobom lub własności prywatnej albo publicznej jako głównej metody działania,
- bezwzględny i pozbawiony skrupułów sposób działania oparty na zastraszeniu, szantażu i permanentnym poczuciu zagrożenia społecznego,
- dążenie do uzyskania rozgłosu propagandowego, głównie za pomocą środków masowego przekazu poprzez organizowanie lub firmowanie akcji spektakularnych, niejednokrotnie okrutnych i szokujących,
- pozyskiwanie funduszy na działalność terrorystyczną, głównie na drodze przestępstw, poprzez organizacje handlujące bronią, narkotykami czy żywym towarem[58].

Terroryści działają we wszystkich środowiskach i przestrzeniach, posługując się zróżnicowanymi środkami i metodami, jakie uznają za słuszne. Jako cele wybierają dowolne osoby, grupy, obiekty materialne i niematerialne, a scenariusze są zaskakujące, przerażają swoim rozmachem i okrucieństwem. W swojej działalności wykorzystują osiągnięcia naukowo-techniczne i technologiczne, metody i techniki operacyjne właściwe dla służb policyjnych. Posiadają strukturę sieciową, są głęboko zakonspirowani, profesjonalnie szkoleni i przygotowani do akcji.

Współczesny terroryzm jest nieprzewidywalny co do miejsca i czasu ataku, stosowanych form i metod oraz środków. Jego głównym celem jest uzyskanie rozgłosu, maksymalna liczba ofiar (najczęściej ofiary są przypadkowe), permanentny strach i chaos.

Tabela 41. Przykładowe cele ataków terrorystycznych

Środowisko ataków terrorystycznych		
powietrzne	lądowe	morskie
Cele ataków terrorystycznych		
pojedyncze osoby		
grupy społeczne		
skupiska ludności		
państwa		
siły zbrojne		
instytucje publiczne		
obiekty techniczne		
centra gospodarcze		
środki komunikacyjne		
zasoby naturalne		
walory przyrodnicze		
symbole niematerialne		

Źródło: K. Ficoń, *Inżynieria zarządzania systemowego. Podejście systemowe*, Gdynia 2007, s. 101

[57] S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, s. 60–61.

[58] K. Ficoń, op. cit., s. 99.

Do najczęściej stosowanych przez terrorystów metod ataku należą: zamachy na życie konkretnych osób, zamachy bombowe, samochody pułapki, uprowadzenia pojazdów lub samolotów, uprowadzenia osób (kidnaping), wzięcie zakładników, wykorzystanie broni masowego rażenia, sabotaż, żywe bomby, cyberterroryzm[59].

Przestępczość, w tym zorganizowana (o charakterze transgranicznym), obejmuje różne obszary życia społecznego, gospodarczego i politycznego. U progu XXI wieku warunki dla rozwoju przestępczości tworzone są m.in. poprzez likwidację kontroli na granicach wewnętrznych i liberalne prawo, co zapewnia swobodny przepływ ludzi, usług, finansów, towarów, słabość instytucji ścigania i wymiaru sprawiedliwości, korupcja urzędników państwowych, globalizacja i towarzyszące jej procesy, postępująca pauperyzacja społeczeństwa, co stanowi bazę werbunkową dla organizacji przestępczych), migracja (w tym nielegalna).

Tabela 42. Zagrożenia przestępczością zorganizowaną

Zagrożenia	
Zorganizowana przestępczość kryminalna	fałszowanie pieniędzy handel żywym towarem, tkankami i organami ludzkimi przestępczość przeciwko dobrom kultury
Zorganizowana przestępczość ekonomiczna	przestępczość związana z przekształceniami własnościowymi przestępczość podatkowa przestępczość związana z funkcjonowaniem banków przestępstwa paliwowe nielegalny wyrób, przemyt i handel produktami akcyzowymi przestępczość ubezpieczeniowa przestępczość związana z wykorzystywaniem elektronicznych instrumentów płatniczych korupcja jako metoda oddziaływania grup przestępczych pranie brudnych pieniędzy
Zorganizowana przestępczość narkotykowa	produkcja, przemyt i handel narkotykami
Inne obszary działania	handel bronią, amunicją i materiałami wybuchowymi handel technologiami podwójnego zastosowania handel technologiami do produkcji broni masowego rażenia i środkami do jej przenoszenia
Terroryzm	cyberterroryzm terroryzm polityczny, terroryzm z wykorzystaniem broni masowego rażenia terror kryminalny

Źródło: Opracowano na podstawie W. Mądrzejewski, *Przestępczość zorganizowana. System zwalczania,* Warszawa 2008, s. 6

[59] K. Jałoszyński, *O współczesnym terroryzmie i roli państwa w walce z nim*, „Policyjny Biuletyn Szkoleniowy" 1998, nr 1–2, s. 81.

3.5. Zagrożenia militarne

Lata dziewięćdziesiąte XX wieku to początek przemian w sferze politycznej, społecznej, gospodarczej i wojskowej, które wraz z upadkiem dwubiegunowego podziału świata i Związku Radzieckiego zmieniły środowisko bezpieczeństwa poszczególnych państw i środowiska międzynarodowego. W następstwie tych procesów położenie geostrategiczne wielu państw zmieniło się w zasadniczy sposób. Twierdzono wprost, że nastąpił historyczny przełom w stosunkach międzynarodowych, że dotychczasowe zagrożenia zniknęły i świat jest bardziej bezpieczny niż w niedalekiej przeszłości. Tak optymistyczne podejście do zapoczątkowanych zmian w środowisku bezpieczeństwa narodowego okazało się jednak błędne, zaczęły się bowiem pojawiać nowe zagrożenia, a dotychczas tłumione pokazywały swoją faktyczną siłę.

To początek drogi w poszukiwaniu nowej pod względem jakościowym formuły bezpieczeństwa. Nie eliminowała ona istniejących, często ukrytych sprzeczności natury historycznej, narodowościowej, wyznaniowej, społecznej, kulturowej, a tym samym źródeł napięć, sytuacji kryzysowych i konfliktów o charakterze zbrojnym. Obserwując przebieg wydarzeń w różnych rejonach świata należy stwierdzić, że prawdopodobieństwo wybuchów konfliktów o charakterze zbrojnym jest o wiele większe niż zakładano.

Dokonując oceny zagrożeń militarnych, należy brać pod uwagę sytuację geostrategiczną (o czy wspominano) danego państwa, uwzględniając przede wszystkim:

- otoczenie zewnętrzne państwa, a w szczególności obecną i przewidywalną (w określonym horyzoncie czasowym) zdolność sił zbrojnych jego otoczenia w zakresie prowadzenia działań zbrojnych przeciwko niemu,
- dynamikę zmiany woli politycznej w tych państwach co do użycia sił zbrojnych,
- wzajemne relacje państwa z otoczeniem międzynarodowym jako determinantem zewnętrznym obronności,
- przynależność i pozycję państwa w układzie bezpieczeństwa (koalicja, sojusz) jako gwaranta bezpieczeństwa[60].

> W wyniku zmian geopolitycznych utracono kontrolę nad tłumionymi dążeniami i aspiracjami etnicznymi, religijnymi, narodowościowymi, które do tej pory były wewnętrzną sprawą państw hegemonistycznych. Jeżeli nałożymy na to zróżnicowanie poziomu rozwoju: nauki i techniki, technologii produkcji, gospodarczego, społecznego oraz warunków socjalnych itp., to otrzymamy zróżnicowane podłoże, na którym mogą powstać sytuacje konfliktogenne, zagrożenia militarne lub konflikty zbrojne[61].

[60] G. Sobolewski, op. cit., s. 75.

[61] S. Dworecki, op. cit., s. 58.

Zagrożenia militarne państwa to splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa albo naruszenie bądź utrata jego suwerenności i integralności terytorialnej – w wyniku zastosowania wobec niego przemocy zbrojnej (militarnej)[62]. Do podstawowych przyczyn powstawania zagrożeń militarnych należą przyczyny natury ekonomicznej, politycznej, etnicznej, ekologicznej, psychologicznej, społecznej, wyznaniowej, wojskowej[63].

Wskazane obszary w określonych warunkach mogą stać się na tyle konfliktotwórcze, że w skrajnych przypadkach może dojść do wybuchu konfliktu zbrojnego. Pamiętać przy tym należy, że aktualne stosunki międzynarodowe praktycznie na wszystkich płaszczyznach charakteryzują się systemem współzależności i powiązań, zarówno w sferze społecznej, politycznej, gospodarczej (co szczególnie jest widoczne), religijnej, jak wojskowej czy walki z międzynarodowym terroryzmem i zorganizowaną przestępczością transgraniczną.

Tabela 43. Obszary powstawania zagrożeń o charakterze militarnym

Przyczyny	Obszary szczegółowe
polityczne	transformacja ustrojowa rozchwianie sceny politycznej dyskredytowanie władzy szantaż polityczny izolacja polityczna niestabilność prawa terroryzm polityczny tolerancja dla przekonań politycznych
ekonomiczne	recesja gospodarcza restrykcje gospodarcze ograniczenia kredytowo-finansowe status materialny obywateli zadłużenie państwa kryzys ekonomiczny embargo handlowe stan budżetu państwa proces prywatyzacji i reprywatyzacji urynkowienie usług i świadczeń socjalnych
społeczne	stan bezrobocia stan bezpieczeństwa socjalnego stan bezpieczeństwa osobistego obywateli stan przestrzegania swobód obywatelskich podział etniczny i wyznaniowy pauperyzacja społeczeństwa różnice statusu materialnego dostępność oświaty, kultury, nauki i wypoczynku antagonizmy plemienne

62 S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, Warszawa 1994, s. 25.

63 S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, s. 58.

wojskowe	charakter doktryny wojennej wielkość potencjału obronnego państwa stan budżetu MON struktura organizacyjna sił zbrojnych charakter szkolenia wojskowego dyslokacja jednostek wojskowych wyposażenie techniczne wojsk stan produkcji zbrojeniowej wydatki zbrojeniowe sąsiadów
psychologiczne	poczucie zagrożenia praw i swobód obywatelskich patologiczne zachowania społeczeństwa apatia społeczeństwa aktywność ośrodków propagandy
ekologiczne	degradacja środowiska naturalnego próby z bronią nuklearną katastrofy transportów ze środkami toksycznymi wwóz do kraju opadów poprodukcyjnych awarie elektrowni atomowych zanieczyszczenia przemysłowe środowiska stan utylizacji odpadów środków aktywnych

Źródło: S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, s. 59–62

Powyższe przyczyny to szerokie spektrum zagrożeń, które mają duży wpływ na kształtowanie sytuacji w sferze militarnej w regionie, a nawet w skali globalnej. Niekorzystny rozwój we wskazanych obszarach stanowi groźbę realnego zagrożenia o charakterze militarnym, gdzie w skrajnych przypadkach mogą one przybrać postać konfliktu zbrojnego.

Przebieg dotychczasowych konfliktów zbrojnych to przede wszystkim splot wielu złożonych i wzajemnie powiązanych przyczyn o charakterze:

- historyczno-narodowościowym i nacjonalistycznym, należą one do najstarszych przyczyn powstawania konfliktów zbrojnych,
- religijno-kulturowym, które bardzo często jest połączone z aspektem narodowym lub nacjonalistycznym, a nawet terrorystycznym,
- politycznym, które uzasadnia działanie państwa (narodu, grupy etnicznej czy środowiska) zmierzającego do osiągnięcia własnego celu,
- ekonomiczno-ekologicznym, gdy źródłem zagrożeń militarnych i konfliktów zbrojnych mogą być dysproporcje w rozwoju gospodarczym, dostępności do zasobów surowców naturalnych czy postępujący proces degradacji środowiska,
- wojskowym, zwłaszcza militaryzacja niektórych regionów, niekontrolowany handel bronią, dostępność do broni jądrowej oraz terroryzm zbrojny organizacji anarchistycznych i religijnych[64].

Wskazane uwarunkowania powinny być brane pod uwagę przez każde państwo w procesie prognozowania zagrożeń, w tym o charakterze militarnym. Przemawia za tym nie tylko położenie geopolityczne, ale i rozwój sytuacji społeczno-politycznej i wojskowej w otoczeniu zewnętrznym (bliższym i dalszym) państwa.

[64] S. Dworecki, *Od konfliktu…*, op. cit., s. 63.

Zagrożenia militarne mogą przybierać różne formy: przewrotu wojskowego, akcji zbrojnej, blokady militarnej, incydentu granicznego, interwencji zbrojnej, napaści zbrojnej grup nieformalnych, konfliktu lokalnego na terenie sąsiedniego państwa, szantażu militarnego, prowokacji militarnej, ograniczonego użycia środków przemocy zbrojnej, zbrojnego starcia granicznego, militarnego konfliktu w strefie granicznej, konfliktu między państwami bezpośredniego otoczenia[65].

Warto mieć na uwadze, że zagrożenia o charakterze militarnym nie wynikają tylko z posiadanego przez państwo (państwa) sąsiednie potencjału militarnego, ale z woli jego wykorzystania w celu rozwiązania spornych kwestii.

[65] Ibidem, s. 71.

ROZDZIAŁ 4

Podstawy prawne zarządzania kryzysowego

Występujące po upadku bipolarnego podziału świata zagrożenia militarne i niemilitarne przeszły istotną ewolucję, nadal jednak pozostają groźne dla bezpieczeństwa poszczególnych państw i środowiska międzynarodowego. Na szczególną uwagę zasługują zagrożenia o charakterze niemilitarnym, gdzie asymetryczne środowisko międzynarodowe rzutuje na skuteczność zarządzania kryzysowego podejmowanego przez organizacje międzynarodowe i państwa. Ich źródeł należy upatrywać w napięciach politycznych, społecznych, ekonomicznych, nacjonalizmie, antagonizmach etnicznych i religijnych.

> Występujące sprzeczności interesów generują niebezpieczeństwa o wielorakim charakterze: od konfliktów zbrojnych i zamachów terrorystycznych do przestępczości pospolitej i zorganizowanej, ekscesów chuligańskich, infekowania systemów informatycznych czy korupcji. Oprócz niebezpieczeństw wywołanych postawą i działalnością człowieka, niebagatelnego znaczenia dla bezpieczeństwa nabierają też kataklizmy naturalne[1].

Zjawisko globalizacji, rozwój społeczeństwa informacyjnego i nowoczesne techniki zwiększają aktywność społeczności międzynarodowej zarówno w odbiorze pozytywnym, jak negatywnym. Współczesne zagrożenia cywilizacyjne i zagrożenia celowe, których źródłem jest człowiek, gdzie obecny jest terroryzm międzynarodowy (cyberterroryzm) powiązany m.in. z międzynarodową przestępczością zorganizowaną (przestępczością w cyberprzestrzeni) wymagają wielopłaszczyznowego podejścia. Stanowią one przedmiot zainteresowania nie tylko teorii, ale i praktyki.

W walkę z istniejącymi zagrożeniami zaangażowane są organizacje międzynarodowe, m.in. Organizacja Narodów Zjednoczonych, Organizacja Bezpieczeństwa i Współpracy w Europie, Unia Europejska, Sojusz Północnoatlantycki, państwa G8, Wspólnota Niepodległych Państw, Szanghajska Organizacja Współpracy, Stowarzyszenie Narodów Południowo-Wschodniej Azji, Organizacja Państw Amerykańskich, Organizacja Konferencji Islamskiej, Liga Państw Arabskich, Organizacja Jedności Afrykańskiej. Zwalczanie zagrożeń XXI wieku

[1] A. Misiuk, *Administracja porządku i bezpieczeństwa publicznego. Zagadnienia prawno-ustrojowe*, Warszawa 2008, s. 9.

wymaga współpracy społeczności międzynarodowej, a współpraca ta powinna być ścisła i skoordynowana, skupiająca jak największą liczbę organizacji międzynarodowych i państw.

Złożoność otoczenia zewnętrznego i wewnętrznego w powiązaniu z istniejącymi zagrożeniami wymaga odpowiednich instrumentów w ramach prawa międzynarodowego i krajowego. Doświadczenia zebrane w okresie jego obowiązywania i praktycznego stosowania powinny skutkować jego dostosowaniem do zmieniającego się środowiska międzynarodowego.

Z uwagi na wielość regulacji prawnych konieczna jest systematyczna analiza obowiązujących przepisów pod kątem ich praktycznej przydatności. Powinny być one na tyle czytelne, aby można było uruchomić siły i środki na wszystkich poziomach zarządzania kryzysowego.

4.1. Prawo międzynarodowe

W Europie szczególną rolę w zakresie zarządzania kryzysowego odgrywa Unia Europejska, która będąc międzynarodową organizacją regionalną w sposób kompleksowy odnosi się do tej problematyki. Przyjmowane przez Unię Europejską regulacje prawne mają szczególny charakter prawno-międzynarodowy, są bowiem aktami prawnymi przyjmowanymi w ramach organizacji międzynarodowej[2]. Ponadto należy podkreślić, że zmieniający się charakter zagrożeń wymusza na Unii i rządach państw członkowskich podejmowanie aktywnych prac legislacyjnych związanych z bezpieczeństwem ich obywateli.

> Rosnące aspiracje Unii Europejskiej w kwestii (reagowania) zarządzania kryzysowego zostały potwierdzone w dokumencie *Bezpieczna Europa w lepszym świecie. Europejska strategia bezpieczeństwa* w dniach 19–20 czerwca 2003 roku w Salonikach. […] Dokument ten został ostatecznie zatwierdzony przez Radę Europejską na posiedzeniu w Brukseli 12 grudnia 2003 roku. […] w świecie globalnym żaden kraj nie jest w stanie samodzielnie zmierzyć się z obecnymi złożonymi problemami. I mimo że granice zacierają się, to geografia wciąż odgrywa znaczącą rolę[3].

Obok zagrożeń *Europejska strategia bezpieczeństwa* określa sposoby reagowania kryzysowego, gdzie zakłada połączenie wysiłków zarówno wojskowych, jak i pozamilitarnych.

> Zapisy traktatowe dotyczące systemu reagowania (zarządzania) kryzysowego w Unii Europejskiej uzupełniane są wiążącymi państwa członkowskie aktami normatywny-

[2] P. Durys, P. Jasiński, *Walka z terroryzmem międzynarodowym. Wybór dokumentów*, Bielsko-Biała 2005, s. 12.

[3] J. Gryz, *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, Toruń 2009, s. 127–129.

mi, jak rozporządzenia i decyzje wydawane przez najważniejsze instytucje Unii Europejskiej: Radę Unii Europejskiej, Komisję Europejską i Parlament Europejski. Do najważniejszych należą umocowania prawne dla mechanizmów i instrumentów reagowania kryzysowego oraz mechanizmów wczesnego ostrzegania[4].

Unia Europejska nie wypracowała i nie wdrożyła jeszcze systemu, który w sposób kompleksowy regulowałby problematykę reagowania (zarządzania) kryzysowego. Ma to ścisły związek z ewolucją istniejących zagrożeń, a także trudnościami ze wskazaniem tych, które mogą pojawić się w bliżej niekreślonym przedziale czasu. W związku z tym przedstawiony katalog przepisów prawa międzynarodowego jest otwarty na przyjęcie nowych przepisów, które pozwolą na wypracowanie rozwiązań minimalizujących skutki zarówno zagrożeń naturalnych, jak i celowych.

Tabela 44. Przepisy międzynarodowe

Lp.	Przepisy
1.	*Traktat o Unii Europejskiej*, podpisany w Maastricht 7 lutego 1992 roku (Dz. Urz. WE C 191 z 29 lipca 1992 roku)
2.	*Traktat Amsterdamski,* podpisany 2 października 1997 roku (Dz. Urz. WE C 340 z 10 listopada 1997 roku)
3.	*Traktat Nicejski,* podpisany 26 lutego 2001 roku (Dz. Urz. WE C 80 z 10 marca 2001 roku)
4.	*Traktat ustanawiający Konstytucję dla Europy* (Dz. U. UE. C 310, T. 47, z 16 grudnia 2004)
5.	*Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską* sporządzony w Lizbonie w dniu 13 grudnia 2007 roku (Dz. U. UE. C 2007/306/1)
6.	*Konwencja o ochronie praw człowieka i podstawowych wolności,* sporządzona w Rzymie 4 listopada 1950 roku (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.)
7.	*Konwencja o międzynarodowym lotnictwie cywilnym*, przyjęta w 1944 roku w Chicago (Dz. U. z 1959 r. Nr 35, poz. 212)
8.	*Aneks do konwencji o międzynarodowym lotnictwie cywilnym* (Dz. Urz. ULC z 2003 r. Nr 4, poz. 17)
9.	*Europejska Konwencja o ekstradycji,* sporządzona w Paryżu 13 grudnia 1957 roku (Dz. U. z 1994 r. Nr 70, poz. 307)
10.	*Konwencja o morzu otwartym*, przyjęta w 1958 roku w Genewie (Dz. U. z 1963 r. Nr 33, poz. 187)
11.	*Konwencja w sprawie przestępstw i niektórych innych czynów popełnionych na pokładzie statków powietrznych*, przyjęta w 1963 roku w Tokio (Dz. U. z 1971 r. Nr 15, poz. 147)
12.	*Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi,* przyjęta w 1970 roku w Hadze (Dz. U. z 1972 r. Nr 25, poz. 181)
13.	*Konwencja o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego*, przyjęta w 1971 roku w Montrealu (Dz. U. z 1976 r. Nr 8, poz. 37)
14.	*Protokół o zwalczaniu bezprawnych czynów przemocy w portach lotniczych obsługujących międzynarodowe lotnictwo cywilne*, podpisany w 1988 roku w Montrealu (Dz. U. z 2006 r. Nr 48, poz. 348)
15.	*Konwencja o zapobieganiu przestępstwom i karaniu sprawców przestępstw przeciwko osobom korzystającym z ochrony międzynarodowej, w tym przeciwko dyplomatom,* przyjęta 14 grudnia 1973 roku w Nowym Jorku (Dz. U. z 1983 r. Nr 37, poz. 168)
16.	*Konwencja o bezpieczeństwie życia na morzu – SOLAS,* przyjęta w 1974 roku w Londynie i protokół ją uzupełniający sporządzony w 1978 roku w Londynie (Dz. U. z 1984 r. Nr 61, poz. 318 i 319)

[4] Ibidem, s. 139.

17.	*Konwencja przeciwko braniu zakładników*, przyjęta 19 grudnia 1979 roku w Nowym Jorku (Dz. U. z 2000 r. Nr 106, poz. 1123)
18.	*Konwencja o fizycznej ochronie materiałów jądrowych* wraz z załącznikami I i II, otwarta do podpisu w Wiedniu i w Nowym Jorku w dniu 3 marca 1980 r. (Dz. U. z 1989 r. Nr 17, poz. 93)
19.	*Konwencja o prawie morza* sporządzona w 1982 roku w Montego Bay (Dz. U. z 2002 r. Nr 59, poz. 543)
20.	*Konwencja w sprawie przeciwdziałania bezprawnym czynom przeciwko bezpieczeństwu żeglugi morskiej – SUA* wraz z *Protokołem dotyczącym przeciwdziałaniu bezprawnym aktom przemocy przeciwko bezpieczeństwu stałych platform umieszczonych na szelfie kontynentalnym,* przyjętym w 1988 roku w Rzymie (Dz. U. z 1994 r. Nr 129, poz. 635, Dz. U. z 2002 r. Nr 22, poz. 211)
21.	*Konwencja w sprawie znakowania plastycznych materiałów wybuchowych w celu ich wykrywania*, przyjęta w 1991 roku w Montrealu (Dz. U. z 2007 r. Nr 135, poz. 948)
22.	*Konwencja o bezpieczeństwie personelu Organizacji Narodów Zjednoczonych i personelu współdziałającego*, przyjęta 9 grudnia 1994 roku w Nowym Jorku (Dz. U. z 1999 r. Nr 93, poz. 1065)
23.	*Konwencja o zwalczaniu terrorystycznych ataków bombowych*, przyjęta 15 grudnia 1997 r. w Nowym Jorku (Dz. U. z 2007 r. Nr 66, poz. 438)
24.	*Konwencja o zwalczaniu finansowania terroryzmu*, przyjęta 9 grudnia 1999 r. w Nowym Jorku (Dz. U. z 2004 r. Nr 263, poz. 2620)
25.	*Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej,* przyjęta 15 grudnia 2000 roku w Palermo (Dz. U. z 2005 r. Nr 18, poz. 158)
26.	*Międzynarodowa Konwencja o zwalczaniu terroryzmu jądrowego*, przyjęta w dniu 13 kwietnia 2005 roku przez Zgromadzenie Ogólne Narodów Zjednoczonych (UN Doc. A/RES/59/290, 15 kwietnia 2005)
27.	*Konwencja Rady Europy o ekstradycji* sporządzona 13 grudnia 1957 roku w Paryżu wraz z Protokołami zmieniającymi sporządzonymi 15 października 1975 r. i 17 marca 1978 r, w Strasburgu (Dz. U. z 1994 r, Nr 70, poz. 307)
28.	*Konwencja Rady Europy o zwalczaniu terroryzmu* sporządzona 27 stycznia 1977 roku w Strasburgu (Dz. U. z 1996 r. Nr 117, poz. 557)
29.	*Europejska Konwencja o zapobieganiu torturom oraz nieludzkiemu lub poniżającemu traktowaniu albo karaniu*, sporządzona w Strasburgu 26 listopada 1987 roku (Dz. U. z 1995 r. Nr 46, poz. 238)
30.	*Konwencja o utworzeniu Europejskiego Urzędu Policji (Europol)* podpisana 26 lipca 1995 roku wraz z protokołami zmieniającymi (Dz. Urz. We C 316 z 27 listopada 1995 roku)
31.	*Konwencja o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej* podpisana 29 maja 2000 roku wraz z protokołami zmieniającymi (Dz. Urz. WE C 197 z 12 lipca 2000 roku)
32.	Protokół zmieniający *Konwencję o zwalczaniu terroryzmu* z dnia 15 maja 2003 roku (Dz. U. z 2004 r. Nr 172, poz. 1803)
33.	*Konwencja Rady Europy o zapobieganiu terroryzmowi* sporządzona 16 maja 2005 roku w Warszawie (Dz. U. z 2008 r. Nr 161, poz. 998)
34.	*Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu* sporządzona 15 maja 2005 roku w Warszawie (Dz. U. z 2008 r. Nr 165, poz. 1028)
36.	*Konwencja Rady Europy o zapobieganiu terroryzmowi*, sporządzona w Warszawie dnia 16 maja 2005 r. (Dz. U. z 2008 r. Nr 161, poz. 998)
37.	Dyrektywa Rady Europy Nr 96/82/EC z dnia 9 grudnia 1996 r. *o kontroli zagrożeń poważnymi wypadkami (Seveso II)* (Dz. U. UE L 10 z dnia 14 stycznia 1997 roku, 13–33)
38.	Dyrektywa Rady Europy 2003/105/WE z dnia 16 grudnia 2003 roku *w sprawie zarządzania zagrożeniami poważnymi awariami, z udziałem substancji niebezpiecznych* (Dz. U. UE L 345 z dnia 31 grudnia 2003 roku, 97–195)

39.	Dyrektywa 2004/108/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 2004 r. *w sprawie zbliżenia ustawodawstwa Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej oraz uchylająca dyrektywę 89/336/ EWG* (Dz. U. UE L Nr 390, poz. 24)
40.	Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 roku *w sprawie wzmocnienia ochrony portów* (Dz. U. UE L 310/28 z 25 listopada 2005 roku)
41.	Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. *w sprawie oceny ryzyka powodziowego i zarządzania nim* (Dz. U. UE L z 2007 r., Nr 288, poz. 27)
42.	Dyrektywa Rady Europy 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*
43.	Decyzja Rady Europy Nr 91/396/EEC z dnia 29 lipca 1991 r. *w sprawie europejskiego, alarmowego numeru telefonu*
44.	Decyzja Rady z dnia 9 grudnia 1999 r. *ustanawiająca wspólnotowy program działań w dziedzinie ochrony ludności* (Dz. U. WE L 327/53 z 21 grudnia 1999)
45.	Decyzja Rady Europy z dnia 22 styczni 2001 r. *ustanawiająca Komitet Wojskowy Unii Europejskiej* (2001/79/WPZiB) (Dz. U. UE L o2730/01/2001 P. 0004 – 0006)
46.	Decyzja Rady Europy 2002/187/WSiSW z 28 lutego 2002 roku *w sprawie utworzenia Eurojustu w celu wzmocnienia walki z poważną przestępczością* (Dz. Urz. WE L 63 z 6 marca 2002 roku)
47.	Decyzja Rady Europy 2002/956/WSiSW z 28 listopada 2002 roku *w sprawie utworzenia Europejskiej Sieci Ochrony Osób Publicznych* (Dz. Urz. WE L 333 z 10 grudnia 2002 roku)
48.	Decyzja Rady Europy 2008/617/WSiSW z dnia 23 czerwca 2008 r. *w sprawie usprawnienia współpracy pomiędzy specjalnymi jednostkami interwencyjnymi państw członkowskich Unii Europejskiej w sytuacjach kryzysowych* (Dz. Urz. UE L 210 z dnia 23 czerwca 2008 roku)
49.	Decyzja Ramowa Rady Europy 2002/475/WSiSW z dnia 13 czerwca 2002 r. *w sprawie zwalczania terroryzmu* (Dz. Urz. We L 164 z 22 czerwca 2002 roku)
50.	Decyzja Ramowa Rady Europy 2002/584/WSiSW z 13 czerwca 2002 roku *w sprawie Europejskiego Nakazu Aresztowania i procedur przekazywania osób między państwami członkowskimi* (Dz. Urz. WE L 190 z 18 lipca 2002 roku)
51.	Decyzja Ramowa Rady Europy 2002/946/WSiSW z 28 listopada 2002 roku *w sprawie wzmocnienia systemu karnego w celu zapobiegania ułatwieniu nielegalnego wjazdu, tranzytu i pobytu* (Dz. Urz. WE L 328 z 5 grudnia 2002 roku)
52.	Decyzja Rady Europy 2007/162/WE z dnia 5 marca 2007 roku *w sprawie ustanowienia Instrumentu Finansowania Ochrony Ludności dla sytuacji nadzwyczajnych, takich jak klęski żywiołowe i katastrofy spowodowane przez człowieka, akty terroryzmu, w tym terroryzmu chemicznego, biologicznego, radiologicznego i nuklearnego, oraz katastrof technicznych, radiologicznych i ekologicznych, a także usprawnianie środków zapobiegawczych i środków gotowości na wypadek wszelkich sytuacji nadzwyczajnych* (Dz. Urz. L 071 z 10 marca 2007 roku)
53.	Decyzja Komisji Europejskiej z dnia 19 grudnia 2007 roku w *sprawie przystąpienia Europejskiej Wspólnoty Energii Atomowej do Konwencji o ochronie fizycznej materiałów jądrowych i obiektów jądrowych* (Dz. Urz. UE L 034 z dnia 8 lutego 2008 roku)
54.	Rezolucja Nr 2 z dnia 12 grudnia 2002 r. *w sprawie przyjęcia Międzynarodowego Kodeksu dla Ochrony Statku i Obiektu Portowego* (ISPS), (Dz. U. z 2005 r. Nr 120, poz. 1016)
55.	*Europejski konsensus w sprawie pomocy humanitarnej*, Komunikat Komisji do Parlamentu Europejskiego i Rady, Komisja Wspólnot Europejskich, Bruksela, z dnia 13 czerwca 2007, KOM (2007) 317 wersja ostateczna
56.	Konkluzja Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych z dnia 6 grudnia 2007 r. *w sprawie ograniczenia zagrożenia chemicznego, biologicznego, radiologicznego i jądrowego oraz w sprawie gotowości do przeciwdziałania biozagrożeniom*, Rada Unii Europejskiej, Bruksela, dnia 17 grudnia 2007 r. (Dokument 16589/07 z dnia 17 grudnia 2007 roku)
57.	Przepisy Komisji Europejskiej *w sprawie ustanowienia ogólnego systemu szybkiego ostrzegania „ARGUS"* (Dz. U. UE L 19/21 z 24 stycznia 2006 r. PL)

58.	Rozporządzenie (WE) Nr 1717/2006 Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. *ustanawiające instrument na rzecz stabilności* (Dz. U. UE L 327/1 z 24 listopada 2006)
59.	Rozporządzenie Rady (WE) Nr 1257/96 z dnia 20 czerwca 1996 r. *dotyczące pomocy humanitarnej* (Dz. U. L 163, 02/07/1996 P. 0001 – 0006)
60.	Rozporządzenie Rady (WE) Nr 381/2001 z dnia 26 lutego 2001 r. *tworzące mechanizm szybkiego reagowania* (Dz. U. L 057, 27/02/2001 P. 0005 – 0009)
61.	Rozporządzenie Rady (WE) Nr 2580/2001 *w sprawie szczególnych środków restrykcyjnych stosowanych przeciwko niektórym osobom i podmiotom mających na celu zwalczanie terroryzmu* (Dz. Urz. WE L 344 z 28 grudnia 2001 roku)
62.	Rozporządzenie Rady (WE) Nr 881/2002 z dnia 27 maja 2002 roku *wprowadzające niektóre środki ograniczające skierowane przeciwko niektórym osobom i podmiotom związanym z Osamą Bin Ladenem, siecią Al–Kaida i Talibami i* uchylające Rozporządzenie Rady (WE) Nr 467/2001 *zakazujące wywozu niektórych towarów i usług do Afganistanu, wzmacniające zakaz lotów i rozszerzające zamrożenie funduszy i innych środków finansowych w odniesieniu do Talibów w Afganistanie* (Dz. U. WE L 139 z 29 maja 2002 roku, zmienione na mocy Rozporządzenia Rady (WE) Nr 561/2003 z 27 marca 2003 rok – Dz. U. UE L 82 z 29 marca 2003 roku oraz modyfikacji wprowadzonych do załącznika)
63.	Rozporządzenie Komisji (WE) Nr 2320/2002 z dnia 16 grudnia 2002 roku *ustanawiające wspólne zasady w dziedzinie bezpieczeństwa lotnictwa cywilnego* (Dz. Urz. WE L 355 z 30 grudnia 2002 roku)
64.	Rozporządzenie (WE) Nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 roku *w sprawie wzmocnienia ochrony statków i obiektów portowych* (Dz. U. UE L 129 z 9 kwietnia 2001 roku)
65.	Rozporządzenie Rady (WE) Nr 2580/2004 z dnia 26 października 2004 roku *ustanawiające Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej* (Dz. Urz. UE L 349 z 25 listopada 2004 roku)
66.	Rozporządzenie (WE) Nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 roku *ustanawiające kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen),* (Dz. UE L 105/1 z 13 kwietnia 2006 roku)
67.	Rozporządzenie (WE) Nr 1717/2006 Parlamentu Europejskiego i Rady Europy z dnia 15 listopada 2006 roku *ustanawiające Instrument na rzecz Stabilności* (Dz. Urz. UE L 327/1 z 24 listopada 2006 roku PL)
68.	Rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 300/ 2008 z dnia 11 marca 2008 roku *w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego* i uchylające rozporządzenie (WE) Nr 2320/2002 (Dz. U. UE L 97/72 z 9 kwietnia 2008 roku)
69	Rozporządzenie Komisji (WE) Nr 1138/2004 z dnia 21 czerwca 2004 roku *ustanawiające wspólną definicję części krytycznych stref zastrzeżonych w portach lotniczych* (Dz. Urz. UE L 221/6 z 22 czerwca 2004 roku)
70.	Rozporządzenie Komisji (WE) Nr 820/2008 z dnia 8 sierpnia 2008 roku *ustanawiające środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego* (Dz. Urz. UE L 221/8 z 19 sierpnia 2008 roku)
71.	Wspólne oświadczenie Rady Europy i przedstawicieli rządów Państw Członkowskich zebranych w ramach Rady, Parlamentu Europejskiego i Komisji *w sprawie polityki rozwojowej Unii Europejskiej*: *„konsensus Europejski"* (Dz. U. UE 2006/C 46/01 z 24 luty 2006)
72.	*Wzmocnienie zdolności reagowania Unii Europejskiej na klęski żywiołowe i sytuacje kryzysowe w państwach trzecich*, Komunikat Komisji do Rady, Parlamentu Europejskiego i Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, COM/2005/0153
73.	Załącznik do decyzji Rady 2008/298/WPZiB z dnia 7 kwietnia 2008 r. *zmieniające decyzje 2001/80/WPZiB w sprawie ustanowienia Sztabu Wojskowego Unii Europejskiej* (Dz. U. UE L 102/25 z 12 kwietnia 2008)
74.	Zielona Księga *w sprawie europejskiego programu ochrony infrastruktury krytycznej*, Komisja Wspólnot Europejskich, Bruksela, 17 listopad 2005, COM(2005)576 końcowy

75.	*Strategia Unii Europejskiej w zakresie zwalczania terroryzmu* przyjęta w dniu 2 grudnia 2005 roku przez Radę Unii Europejskiej (www.stosunki.pl – pobrano 10.02.2012 roku)
76.	*Strategia Unii Europejskiej w zakresie zwalczania radykalizacji postaw i rekrutacji do ugrupowań terrorystycznych* przyjęta w dniu 16 grudnia 2005 roku przez Radę Europejską Dokument Rady 14781/1/05. Strategia ta została zmieniona w listopadzie 2008 roku. Dokument Rady 15175/08.
77.	*Globalna Strategia Zwalczania Terroryzmu* z załączonym Planem Działania przyjęta w dniu 8 września 2006 roku przez Organizację Narodów Zjednoczonych www.unic.un.org.pl (pobrano 15 marca 2012 roku)

Źródło: Opracowano na podstawie regulacji prawnych

Rada Unii Europejskiej 10 czerwca 2011 roku przyjęła Priorytety Unii Europejskiej na 66 Sesję Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych[5]. W dokumencie tym podkreśla się, że:

1) wejście w życie Traktatu z Lizbony i utworzenie Europejskiej Służby Działań Zewnętrznych (ESDZ) zwiększa zdolności Unii Europejskiej (UE) do działania na arenie międzynarodowej jako podmiotu globalnego. Nasze działania będą zmierzać w kierunku zapewnienia odzwierciedlenia tej zmiany w Organizacji Narodów Zjednoczonych (ONZ). W związku z tym przyjęcie w dniu 3 maja rezolucji nr 65/276 *w sprawie zasad udziału UE w pracach Zgromadzenia Ogólnego* pozwoli UE coraz skuteczniej uczestniczyć w pracach ONZ. UE będzie teraz przywiązywać wagę do pełnego i skutecznego wdrożenia tej rezolucji;

2) Traktat z Lizbony potwierdza zaangażowanie UE na rzecz zasad Karty Narodów Zjednoczonych i wzywa do wypracowywania wielostronnych rozwiązań wspólnych problemów i wyzwań oraz zapewnienia powszechnych dóbr publicznych. By przyczynić się do osiągnięcia tego celu, UE będzie nadal dążyć do stworzenia silniejszego systemu wielostronnego, w szczególności dzięki zwiększeniu reprezentatywności, przejrzystości, odpowiedzialności, skuteczności i efektywności Organizacji Narodów Zjednoczonych. W tym względzie UE będzie aktywnie uczestniczyć w refleksji zainicjowanej na Zgromadzeniu Ogólnym na temat roli ONZ w globalnym zarządzaniu;

3) UE podtrzymuje swoje zobowiązanie do wniesienia wkładu w osiągnięcie celów zarządzania kryzysowego w ramach ONZ; jest także aktywnie zaangażowana w dyskusje dotyczące sposobu zwiększenia wsparcia, którego UE udziela operacjom ONZ w zakresie utrzymywania pokoju. UE będzie nadal wspierać trwający obecnie przegląd działań ONZ w zakresie utrzymywania pokoju, inicjatywy New Horizon, w tym podejścia ukierunkowanego na zdolności, oraz Globalnej Strategii na rzecz Wsparcia Pokojowego;

4) UE przywiązuje wielką wagę do kompleksowego włączania ochrony ludności cywilnej do głównego nurtu polityki. UE traktuje priorytetowo skuteczniejsze wykonanie mandatu w zakresie ochrony ludności cywilnej zapewniające ścisłą koordynację działań wszystkich zainteresowanych podmiotów w tym obszarze, a także skuteczną komunikację ze społecznościami lokalnymi; będzie również popierać, w stosownych przypadkach, podejście ukierunkowane

[5] www.register.consilium.europa.eu (pobrano 19.12.2011).

na zdecydowane działanie w odniesieniu do mandatów misji ONZ w zakresie utrzymywania pokoju. Stosowane przez Unię Europejską podejście będzie obejmować wzmocnienie praworządności przez zwiększenie zgodności z międzynarodowym prawem humanitarnym, międzynarodowym prawem uchodźczym i międzynarodowym prawem dotyczącym praw człowieka, przez zapewnienie odpowiedzialności oraz usprawnienie przekazywania informacji i sprawozdań RB ONZ. W tym kontekście istotne będzie także, aby UE aktywnie uczestniczyła w negocjacjach dotyczących organizacji segmentu wysokiego szczebla w zakresie praworządności na 67 Sesję, który będzie przygotowywany podczas 66 Sesji;

5) Unia Europejska będzie nadal promować koncepcję bezpieczeństwa ludzkiego jako kompleksowego, zintegrowanego i skoncentrowanego na ludziach podejścia w zakresie radzenia sobie z powiązanymi z sobą zagrożeniami dla bezpieczeństwa, środków do życia i godności ludzi oraz słabszych wspólnot. Należy przeprowadzić dalszą analizę w celu określenia obszarów tematycznych, w których wartość dodana uzyskana dzięki zastosowaniu tego podejścia byłaby najlepiej wyeksponowana, a także jego konkretnych zastosowań prowadzących do osiągnięcia tego celu.

4.2. Regulacje krajowe

Członkostwo Polski w Unii Europejskiej jest realizowane na podstawie dokumentów wypracowanych i przyjętych przez państwa członkowskie. Zgodnie z Traktatem o Unii Europejskiej z dnia 7 lutego 1992 roku warunki przyjęcia do Unii nowego państwa i dostosowania do traktatów zawiera traktat (umowa) akcesyjny. Dla Polski warunki te określa traktat podpisany w Atenach 16 kwietnia 2003 roku[6]. Polska została członkiem Unii Europejskiej 1 maja 2004 roku, co skutkowało m.in. koniecznością dokonania harmonizacji polskiego systemu prawa z prawem unijnym, a także uznanie nadrzędności (pierwszeństwa) prawa wspólnotowego nad prawem wewnętrznym i bezpośredniego skutku prawa wspólnotowego[7].

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku[8] jest najważniejszym aktem prawnym obowiązującym w naszym państwie. Określa normy i zasady obowiązujące w państwie we wszystkich dziedzinach życia człowieka. Zawiera także zapisy związane ze sferą bezpieczeństwa wewnętrznego i zewnętrznego państwa, w tym odnosi się do szeroko rozumianej problematyki zarządzania kryzysowego i wymienia trzy rodzaje stanów nadzwyczajnych: klęski żywiołowej, wyjątkowy i wojenny.

6 Dz. U. z 2004 r. Nr 90, poz. 864.

7 S. Pieprzny, *Administracja bezpieczeństwa i porządku publicznego*, Rzeszów 2008, s. 49.

8 Dz. U. z 1997 Nr 78, poz. 483.

Tabela 45. Przepisy Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku dotyczące zarządzania kryzysowego

Lp.	Przepisy Konstytucji RP
1.	Art. 5 stanowi: Rzeczypospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska naturalnego, kierując się zasadą zrównoważonego rozwoju (*Niniejszy artykuł określa funkcje państwa, czyli podstawowe kierunki i cele jego działania. Z tych funkcji wynikają kompetencje i zadania organów państwowych w ogóle, a przede wszystkim tych, które powołuje sama Konstytucja. W aspekcie zarządzania kryzysowego organa te zobowiązane są do zapewnienia obywatelom bezpieczeństwa, a jednocześnie poszanowania ich prawa i wolności*).
2.	Art. 7 stanowi: Organy władzy publicznej działają na podstawie i w granicach prawa (*W odniesieniu do zarządzania kryzysowego każda działalność administracji musi opierać się na przepisach prawnych. Oznacza to, że decyzje podejmowane w sferze zarządzania kryzysowego muszą mieć podstawę prawną*).
3.	Art. 26 ust. stanowi: Siły Zbrojne Rzeczypospolitej Polskiej służą […] zapewnieniu bezpieczeństwa narodowego (*Artykuł ten ma ścisły związek z art. 5 Konstytucji, który określa funkcje Rzeczypospolitej Polskiej m.in. w zakresie bezpieczeństwa narodowego, co ma związek z zarządzaniem kryzysowym. Zgodnie z art. 25 ust. 1 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, o ile inne przepisy nie stanowią inaczej, Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji pododdziały lub oddziały Sił Zbrojnych Rzeczypospolitej Polskiej wraz ze skierowaniem ich do wykonywania zadań z zakresu zarządzania kryzysowego*).
4.	Art. 31 ust. 3 stanowi: Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanowione tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego (*Przepis ten może być zastosowany także w sytuacjach związanych z zarządzaniem kryzysowym*).
5.	Art. 38 stanowi: Rzeczpospolita Polska zapewnia każdemu człowiekowi prawną ochronę życia (*Przepis ten można również odnieść do zarządzania kryzysowego, w ramach którego realizowane są zadania dotyczące ochrony życia m.in. poprzez planowanie i realizowanie działań ratowniczych w miejscach klęsk żywiołowych, awarii technicznych, katastrof oraz innych zdarzeń stanowiących zagrożenie dla życia, zdrowia osób i mienia*).
6.	Art. 95 ust. 1 stanowi: Władzę ustawodawczą w Rzeczypospolitej Polskiej sprawują Sejm i Senat (*W ramach funkcji ustawodawczej Sejm i Senat mają wpływ m.in. na kształt ustawy o zarządzaniu kryzysowym*).
7.	Art. 117 stanowi: Zasady użycia Sił Zbrojnych poza granicami Rzeczypospolitej Polskiej określa ratyfikowana umowa międzynarodowa lub ustawa (*Przepis ten związany jest z aktywną rolą Polski na arenie międzynarodowej, w związku z tym od wielu lat Rzeczpospolita Polska bierze udział w akcjach mających na celu utrzymanie pokoju*).
8.	Art. 126 ust. 2 stanowi: Prezydent Rzeczypospolitej czuwa nad przestrzeganiem Konstytucji, stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium.
9.	Art. 146 ust.1 stanowi: Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną Rzeczypospolitej Polskiej (*W aspekcie zarządzania kryzysowego oznacza to, że domeną Rady Ministrów jest określanie kierunków prowadzonej polityki i kontrola jej bieżącej realizacji*).
10.	Art. 146 ust. 4 stanowi: W zakresie i na zasadach określonych w Konstytucji i ustawach Rada Ministrów w szczególności: zapewnia wykonanie ustaw, wydaje rozporządzenia, koordynuje i kontroluje prace organów administracji rządowej, uchwala projekt budżetu państwa, kieruje wykonaniem budżetu państwa oraz uchwala zamknięcie rachunków państwa i sprawozdanie z wykonania budżetu, zapewnia bezpieczeństwo wewnętrzne państwa i porządek publiczny, […] określa organizację i tryb swojej pracy (*Przepisy tego artykułu dotyczą zarządzania kryzysowego*).

11.	Art. 148 stanowi: Prezes Rady Ministrów kieruje pracami Rady Ministrów, wydaje rozporządzenia, zapewnia wykonanie polityki Rady Ministrów i określa sposoby jej wykonywania, koordynuje i kontroluje pracę członków Rady Ministrów, sprawuje nadzór nad samorządem terytorialnym w granicach i formach określonych w Konstytucji i ustawach, jest zwierzchnikiem służbowym pracowników administracji rządowej (*Przepisy tego artykułu dotyczą zarządzania kryzysowego*).
12.	Art. 149 ust. 1 stanowi: Ministrowie kierują określonymi działami administracji rządowej lub wypełniają zadania wyznaczone im przez Prezesa Rady Ministrów. Zakres działania ministra kierującego działem administracji rządowej określają ustawy. Ust. 2 stanowi: Minister kierujący działem administracji rządowej wydaje rozporządzenia (*Przepisy tego artykułu dotyczą zarządzania kryzysowego*).
13.	Art. 219 ust 1 stanowi: Sejm uchwala budżet państwa na rok budżetowy w formie ustawy budżetowej (*Ustawa budżetowa obejmuje również wydatki związane z zarządzaniem kryzysowym*).
14.	Art. 228 stanowi: W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony: stan wojenny, stan wyjątkowy i stan klęski żywiołowej. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości. Zasady działania władzy publicznej oraz zakres, w jakim mogą zostać ograniczone wolności i prawa człowieka i obywatela w czasie poszczególnych stanów nadzwyczajnych, określa ustawa. Ustawa może określić podstawy, zakres i tryb wyrównania strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela. Działania podjęte w wyniku wprowadzenia stanu nadzwyczajnego muszą odpowiadać stopniowi zagrożenia i powinny zmierzać do jak najszybszego przywrócenia normalnego funkcjonowania państwa (*Przepisy tego artykułu dotyczą zarządzania kryzysowego*).
15.	Art. 230 stanowi: W razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić na czas oznaczony, nie dłużej niż 90 dni, stan wyjątkowy na części albo na całym terytorium państwa. Przedłużenie stanu wyjątkowego może nastąpić tylko raz, za zgodą Sejmu i na czas nie dłuższy niż 60 dni (*Przepisy tego artykułu dotyczą zarządzania kryzysowego*).
16.	Art. 232 stanowi: W celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia Rada Ministrów może wprowadzić na czas oznaczony, nie dłuższy niż 30 dni, stan klęski żywiołowej na części albo na całym terytorium państwa. Przedłużenie tego stanu może nastąpić za zgodą Sejmu (*Przepisy tego artykułu dotyczą zarządzania kryzysowego*).
17.	Art. 233 stanowi: Ustawa określająca zakres ograniczeń wolności i praw człowieka i obywatela w czasie stanu wojennego lub wyjątkowego nie może ograniczać wolności i praw do godności, obywatelstwa, ochrony życia, humanitarnego traktowania, ponoszenia odpowiedzialności karnej, prawa dostępu do sądu, wolności dóbr osobistych, praw rodziny i praw dziecka. (Jednym z podstawowych skutków wprowadzenia stanu nadzwyczajnego jest zawsze ograniczenie sfery wolności i praw jednostki, i tak: ograniczenie wolności działalności gospodarczej, wolności osobistej, nienaruszalności mieszkania, wolności poruszania się i pobytu na terytorium Rzeczypospolitej Polskiej, prawo do strajku, prawo własności, wolności pracy, prawo do bezpiecznych warunków pracy, prawo do wypoczynku) (*Przepisy tego artykułu dotyczą zarządzania kryzysowego*).

Źródło: *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku* (Dz. U. z 1997 r. Nr 78, poz. 483)

Podstawowym aktem prawnym, który reguluje zakres zarządzania kryzysowego, jest ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[9]. Wskazuje ona podmioty odpowiedzialne, zadania organizacyjne, logistyczne i finansowe realizowane w tej sferze, a także struktury. Zakres funkcjonowania

[9] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

państwa w obszarze zarządzania kryzysowego określają również inne przepisy obowiązującego prawa.

Mając na uwadze dynamikę występujących zagrożeń i bezpieczeństwo obywateli, uzasadnione jest systematyczne monitorowanie obowiązujących aktów prawnych i dostosowywanie ich do zmian występujących w otoczeniu wewnętrznym i zewnętrznym państwa.

Tabela 46. Przepisy krajowe

Lp.	Przepisy
	Ustawy
1.	*Konstytucja Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.)
2.	Ustawa z dnia 21 listopada 1967 r. o *powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.)
3.	Ustawa z dnia 4 marca 1985 r. *o Państwowej Inspekcji Sanitarnej* (T. J.: Dz. U. z 2011 r. Nr 212, poz. 1263 z późn. zm.)
4.	Ustawa z dnia 8 marca 1990 r. *o samorządzie gminnym* (T. j.: Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.)
5.	Ustawa z dnia 6 kwietnia 1990 r. *o Policji* (T. j.: Dz. U. z 2011 r. Nr 287, poz. 1687 z późn. zm.)
6.	Ustawa z dnia 5 lipca 1990 r. *Prawo o zgromadzeniach* (Dz. U. z 1990 r. Nr 51, poz. 297 z późn. zm.)
7.	Ustawa z dnia 12 października 1990 r. *o ochronie granicy państwowej* (T. j.: Dz. U. z 2009 r. Nr 12, poz. 67 z późn. zm.)
8.	Ustawa z dnia 12 października 1990 roku *o Straży Granicznej* (T. j.: Dz. U. z 2011 r. Nr 116, poz. 675 z późn. zm.)
9.	Ustawa z dnia 21 marca 1991 r. *o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej* (Dz. U. z 2003 r. Nr 153, poz. 1502 z późn. zm.)
10.	Ustawa z dnia 24 sierpnia 1991 r. *o ochronie przeciwpożarowej* (T. j.: Dz. U. z 2009 r. Nr 178, poz. 1380 z późn. zm.)
11.	Ustawa z dnia 24 sierpnia 1991 r. *o Państwowej Straży Pożarnej* (T. j.: Dz. U. z 2009 r. Nr 12, poz. 68 z późn. zm.)
12.	Ustawa z dnia 4 lutego 1994 r. *Prawo geologiczne i górnicze* (T. j.: Dz. U. z 2005 r. Nr 228, poz. 1947 z późn. zm.)
13.	Ustawa z dnia 7 lipca 1994 r. *Prawo budowlane* (T. j.: Dz. U. z 2010 r. Nr 243, poz. 1623 z późn. zm.)
14.	Ustawa z dnia 29 września 1994 r. *o rachunkowości* (T. j.: Dz. U. z 2009 r. Nr 152, poz. 1223)
15.	Ustawa z dnia 30 maja 1996 r. *o rezerwach państwowych* (T. j.: Dz. U. z 2007 r. Nr 89, poz. 594 z późn. zm.)
16.	Ustawa z dnia 21 czerwca 1996 r. *o urzędzie Ministra Spraw Wewnętrznych i Administracji* (Dz. U. z 1996 r. Nr 106, poz. 491)
17.	Ustawa z dnia 8 sierpnia 1996 r. *o Radzie Ministrów* (Dz. U. z 2003 r. Nr 24, poz. 199 z późn. zm.)
18.	Ustawa z dnia 10 kwietnia 1997 r. *Prawo energetyczne* (T. j.: Dz. U. z 2006 r. Nr 89, poz. 625 z późn. zm.)
19.	Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.)
20.	Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny wykonawczy* (Dz. U. z 1997 r. Nr 90, poz. 557 z późn. zm.)
21.	Ustawa z dnia 20 czerwca 1997 r. *Prawo o ruchu drogowym* (Dz. U. z 2005 r. Nr 108, poz. 908 z późn. zm.)

22.	Ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia* (T. j.: Dz. U. z 2005 r. Nr 145, poz. 1221 z późn. zm.)
23.	Ustawa z dnia 29 sierpnia 1997 r. *o Strażach Gminnych* (Dz. U. z 1997 r. Nr 123, poz. 779 z późn. zm.)
24.	Ustawa z dnia 4 września 1997 r. *o działach administracji rządowej* (T. j.: Dz. U. z 2007 r. Nr 65, poz. 437 z późn. zm.)
25.	Ustawa z dnia 5 czerwca 1998 r. *o samorządzie województwa* (T. j.: Dz. U. z 2001 r. Nr 142, poz. 1590 z późn. zm.)
26.	Ustawa z dnia 5 czerwca 1998 r. *o samorządzie powiatowym* (T. j.: Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.)
27.	Ustawa z dnia 9 listopada 2000 r. *o bezpieczeństwie morskim* (Dz. U. z 2000 r. Nr 109, poz. 1156 z późn. zm.)
28.	Ustawa z dnia 16 listopada 2000 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz. U. z 2010 r. Nr 46, poz. 276)
29.	Ustawa z dnia 29 listopada 2000 r. *Prawo atomowe* (T. j.: Dz. U. z 2008 r. Nr 93, poz. 583 z późn. zm.)
30.	Ustawa z dnia 15 grudnia 2000 r. *o Inspekcji Handlowej* (T. j.: Dz. U. z 2009 r. Nr 151, poz. 25 z późn. zm.)
31.	Ustawa z dnia 21 grudnia 2000 r. *o żegludze śródlądowej* (T. j.: Dz. U. z 2006 r. Nr 123, poz. 1219 z późn. zm.)
32.	Ustawa z dnia 16 marca 2001 r. *o Biurze Ochrony Rządu* (Dz. U. z 2004 r. Nr 163, poz. 1712 z późn. zm.)
33.	Ustawa z dnia 27 kwietnia 2001 r. *Prawo ochrony środowiska* (T. j.: Dz. U. z 2008 r. Nr 25, poz. 150 z późn. zm.)
34.	Ustawa z dnia 6 lipca 2001 r. *o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz o Krajowy Systemie Informatycznym* (Dz. U. z 2006 r. Nr 216, poz. 1585 z późn. zm.)
35.	Ustawa z dnia 18 lipca 2001 r. *Prawo wodne* (T. j.: Dz. U. z 2005 r. Nr 239, poz. 2019 z późn. zm.)
36.	Ustawa z dnia 20 lipca 2001 r. *o Inspekcjo Ochrony Środowiska* (Dz. U. z 2007 r. Nr 44, poz. 287 z późn. zm.)
37.	Ustawa z dnia 11 sierpnia 2001 r. *o szczególnych zasadach odbudowy, remontów i rozbiórek obiektów budowlanych zniszczonych lub uszkodzonych w wyniku działań żywiołu* (Dz. U. z 2001 r. Nr 84, poz. 906 z późn. zm.)
38.	Ustawa z dnia 24 sierpnia 2001 r. *o Żandarmerii Wojskowej i wojskowych organach porządkowych* (Dz. U. z 2001 r. Nr 123, poz. 1353 z późn. zm.)
39.	Ustawa z dnia 6 września 2001 r. *o chorobach zakaźnych i zakażeniach* (Dz. U. z 2001 r. Nr 126, poz. 1384 z późn. zm.)
40.	Ustawa z dnia 6 września 2001 r. *Prawo farmaceutyczne* (T. j.: Dz. U. z 2008 r. Nr 45, poz. 271 z późn. zm.)
41.	Ustawa z dnia 6 września 2001 r. *o transporcie drogowym* (T. j.: Dz. U. z 2007 r. Nr 125, poz. 874 z późn. zm.)
42.	Ustawa z dnia 18 kwietnia 2002 r. *o stanie klęski żywiołowej* (Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.)
43.	Ustawa z dnia 24 maj 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (T. j.: Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.)
44.	Ustawa z dnia 21 czerwca 2002 r. *o stanie wyjątkowym* (Dz. U. z 2002 r. Nr 113, poz. 985 z późn. zm.)
45.	Ustawa z dnia 3 lipca 2002 r. *Prawo lotnicze* (T. j.: Dz. U. z 2006 r. Nr 100, poz. 696 z późn. zm.)
46.	Ustawa z dnia 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2002 r. Nr 156, poz. 1301 z późn. zm.)

47.	Ustawa z dnia 28 października 2002 r. *o przewozie drogowym towarów niebezpiecznych* (Dz. U. z 2002 r. Nr 199, poz. 1671 z późn. zm.)
48.	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 z późn. zm.)
49.	Ustawa z dnia 28 marca 2003 r. *o transporcie kolejowym* (Dz. U. z 2007 r. Nr 16, poz. 94 z późn. zm.)
50.	Ustawa z dnia 24 kwietnia 2003 r. *o działalności pożytku publicznego i o wolontariacie* (T. j.: Dz. U. z 2010 r. Nr 234, poz. 1536 z późn. zm.)
51.	Ustawa z dnia 12 czerwca 2003 r. *Prawo pocztowe* (T. j.: Dz. U. z 2008 r. Nr 189, poz. 1159 z późn. zm.)
52.	Ustawa z dnia 13 czerwca 2003 r. *o cudzoziemcach* (T. j.: Dz. U. z 2011 r. Nr 264, poz. 1573 z późn. zm.)
53.	Ustawa z dnia 13 czerwca 2003 r. *o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej* (Dz. U. z 2009 r. Nr 189, poz. 1472 z późn. zm.)
54.	Ustawa z dnia 12 grudnia 2003 r. *o ogólnym bezpieczeństwie produktów* (Dz. U. z 2003 r. Nr 229, poz. 2275 z późn. zm.)
55.	Ustawa z dnia 18 grudnia 2003 r. *o ochronie roślin* (T. j.: Dz. U. z 2008 r. Nr 133, poz. 849 z późn. zm.)
56.	Ustawa z dnia 29 stycznia 2004 r. *o Inspekcji Weterynaryjnej* (Dz. U. z 2010 r. Nr 112, poz. 744 z późn. zm.)
57.	Ustawa z dnia 11 marca 2004 r. *o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt* (T. j.: Dz. U. z 2004 r. Nr 213, poz. 1342 z późn. zm.)
58.	Ustawa z dnia 12 marca 2004 r. *o pomocy społecznej* (T. j.: Dz. U. z 2009 r. Nr 175, poz. 1362 z późn. zm.)
59.	Ustawa z dnia 31 marca 2004 r. *o przewozie koleją towarów niebezpiecznych* (Dz. U. z 2004 r. Nr 97, poz. 962)
60.	Ustawa z dnia 16 kwietnia 2004 r. *o ochronie przyrody* (T. j.: Dz. U. z 2009 r. Nr 151, poz. 1220 z późn. zm.)
61.	Ustawa z dnia 16 kwietnia 2004 r. *o zmianie ustawy Kodeks karny oraz niektórych innych ustaw* (Dz. U. z 2004 r. Nr 93, poz. 889)
62.	Ustawa z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne* (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.)
63.	Ustawa z dnia 1 lipca 2005 r. *o zmianie ustawy o przewozie drogowym towarów niebezpiecznych oraz o zmianie niektórych innych ustaw* (Dz. U. z 2005 r. Nr 141, poz. 1184)
64.	Ustawa z dnia 5 listopada 2005 r. *o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw* (Dz. U. z 2005 r. Nr 206, poz. 1589 z późn. zm.)
65.	Ustawa z dnia 9 czerwca 2006 r. *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiady Wojskowego* (Dz. U. z 2006 r. Nr 104, poz. 709 z późn. zm.)
66.	Ustawa z dnia 14 lipca 2006 r. *o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin* (Dz. U. z 2006 r. Nr 144, poz. 1043 z późn. zm.)
67.	Ustawa z dnia 8 września 2006 r. *o Państwowym Ratownictwie Medycznym* (Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.)
68.	Ustawa z dnia 9 grudnia 2006 r. *o Polskiej Agencji Żeglugi Powietrznej* (Dz. U. z 2006 r. Nr 249, poz. 1829 z późn. zm.)
69.	Ustawa z dnia 16 lutego 2007 r. *o zapasach ropy naftowej, produktów naftowych, gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym* (Dz. U. z 2007 r. Nr 52, poz. 343 z późn. zm.)
70.	Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.)

71.	Ustawa z dnia 24 maja 2007 r. *o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz o zmianie niektórych innych ustaw* (Dz. U. z 2007 r. Nr 107, poz. 732)
72.	Ustawa z dnia 24 sierpnia 2007 r. *o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej* (Dz. U. z 2007 r. Nr 165, poz. 1170 z późn. zm.)
73.	Ustawa z dnia 4 września 2008 r. *o ochronie żeglugi i portów morskich* (Dz. U. z 2008 r. Nr 171, poz. 1055 z późn. zm.)
74.	Ustawa z dnia 21 listopada 2008 r. *o służbie cywilnej* (Dz. U. z 2008 r. Nr 227, poz. 1505 z późn. zm.)
75.	Ustawa z dnia 5 grudnia 2008 r. *o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi* (Dz. U. z 2008 r. Nr 234, poz. 1570 z późn. zm.)
76.	Ustawa z dnia 23 stycznia 2009 r. *o wojewodzie i administracji rządowej w województwie* (Dz. U. z 2009 r. Nr 31, poz. 206 z późn. zm.)
77.	Ustawa z dnia 20 marca 2009 r. *o bezpieczeństwie imprez masowych* (Dz. U. z 2009 r. Nr 62, poz. 504 z późn. zm.)
78.	Ustawa z dnia 27 sierpnia 2009 r. *o finansach publicznych* (Dz. U. z 2009 r. Nr 157, poz. 1240)
79.	Ustawa z dnia 27 sierpnia 2009 r. *o Służbie Celnej* (Dz. U. z 2009 r. Nr 168, poz. 1323 z późn. zm.)
80.	Ustawa z dnia 9 października 2009 r. *o zmianie ustawy o prokuraturze oraz niektórych innych ustaw* (Dz. U. z 2009 r. Nr 178, poz. 1375 z późn. zm.)
81.	Ustawa z dnia 12 lutego 2010 r. *o zmianie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej i ustawy o ochronie danych osobowych* (dz. U. z 2010 r. Nr 41, poz. 233 z późn. zm.)
82.	Ustawa z dnia 9 kwietnia 2010 r. *o Służbie Więziennej* (Dz. U. z 2010 r. Nr 79 poz. 523 z późn. zm.)
83.	Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182 poz. 1228)
84.	Ustawa z dnia 8 października 2010 r. *o zmianie ustawy o przeciwdziałaniu narkomanii oraz ustawy o Państwowej Inspekcji Sanitarnej* (Dz. U. z 2010 r. Nr 213, poz. 1396)
85.	Ustawa z dnia 29 października 2010 r. *o zmianie ustawy o zarządzaniu kryzysowym* (Dz. U. z 2010 r. Nr 240, poz. 1600)
86.	Ustawa z dnia 26 listopada 2010 r. *o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz ustawy o zasadach użycia lub pobytu Sił Zbrojnych Rzeczypospolitej Polskiej poza granicami państwa* (Dz. U. z 2010 r. Nr 240, poz. 1601)
87.	Ustawa z dnia 25 lutego 2011 roku *o substancjach chemicznych i ich mieszaninach* (Dz. U. z 2011 r. Nr 63, poz. 322)
88.	Ustawa z dnia 30 sierpnia 2011 r. *o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Siła Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (Dz. U. z 2011 r. Nr 222, poz. 1323)
	Rozporządzenia
1.	Rozporządzenie Rady Ministrów z dnia 15 lipca 1992 r. *w sprawie zakresu i trybu korzystania z praw przez kierującego działaniem ratowniczym* (Dz. U. z 1992 r. Nr 54, poz. 259)
2.	Rozporządzenie Rady Ministrów z dnia 31 lipca 1993 r. *w sprawie przyznawania zakwaterowania i bezpłatnego wyżywienia lub równoważnika pieniężnego oraz zwrotu kosztów przejazdu osobom odbywającym służbę w obronie cywilnej* (Dz. U. z 1993 r. Nr 74, poz. 348)
3.	Rozporządzenie Rady Ministrów z dnia 28 września 1993 r. *w sprawie powszechnej samoobrony ludności* (Dz. U. z 1993 r. Nr 91, poz. 421)
4.	Rozporządzenie Rady Ministrów z dnia 15 lipca 1997 r. *zmieniające rozporządzenie w sprawie określenia szczególnych zasad udzielania zamówień publicznych ze względu na ochronę bezpieczeństwa narodowego, ochronę tajemnicy państwowej, stan klęski żywiołowej lub inny ważny interes państwa* (Dz. U. z 1997 r. Nr 81, poz. 515)
5.	Rozporządzenie Rady Ministrów z dnia 22 lipca 1997 r. *w sprawie szczegółowych zasad i trybu udzielania dotacji, pożyczek i kredytów ze środków Krajowego Funduszu Mieszkaniowego na usuwanie skutków powodzi w 1997 r. oraz zasad spłaty pożyczek i kredytów* (Dz. U. z 1997 r. Nr 82, poz. 522)

6.	Rozporządzenie Rady Ministrów z dnia 22 lipca 1997 r. *w sprawie zasad i trybu udzielania odszkodowań za straty spowodowane skierowaniem wód zalewowych w inny obszar w związku z zagrożeniem powodzią* (Dz. U. z 1997 r. Nr 82, poz. 521)
7.	Rozporządzenie Rady Ministrów z dnia 29 lipca 1997 r. *zmieniające rozporządzenie w sprawie określenia wykazu gmin, na obszarze, których stosuje się szczególne zasady odbudowy i remontu obiektów budowlanych zniszczonych lub uszkodzonych wskutek powodzi albo huraganu* (Dz. U. z 1998 r. Nr 113, poz. 719)
8.	Rozporządzenie Rady Ministrów z dnia 26 sierpnia 1997 r. *zmieniające rozporządzenie w sprawie ustanowienia kontyngentu celnego na towary przywożone z zagranicy na potrzeby zapobiegania i likwidacji skutków klęski żywiołowej* (Dz. U. z 1997 r. Nr 103, poz. 654)
9.	Rozporządzenie Rady Ministrów z dnia 25 września 1997 r. *w sprawie szczegółowego trybu oraz warunków uprawniających do ubiegania się o przyznanie bezzwrotnej pomocy w okresie odbudowy gospodarstwa rolnego* (Dz. U. z 1997 r. Nr 124, poz. 785)
10.	Rozporządzenie Rady Ministrów z dnia 30 grudnia 1997 r. *zmieniające rozporządzenie w sprawie ustalenia wykazu gmin, na obszarze, których wystąpiła powódź, oraz zasad udzielania i sposobu rozliczania dotacji celowych dla tych gmin na finansowanie bieżących zadań własnych* (Dz. U. z 1997 r. Nr 162, poz. 1113, Dz. U. z 1997 r. Nr 87, poz. 547, Dz. U. z 1997 r. Nr 97, poz. 594, Dz. U. z 1997 r. Nr 102, poz. 645, Dz. U. z 1997 r. Nr 108, poz. 699, Dz. U. z 1997 r. Nr 135, poz. 915)
11.	Rozporządzenie Rady Ministrów z dnia 30 grudnia 1997 r. *zmieniające rozporządzenie w sprawie ustalenia wykazu gmin szczególnie dotkniętych powodzią* (Dz. U. z 1997 r. Nr 162, poz. 1112), (Dz. U. z 1997r. Nr 108, poz. 698), (Dz. U. z 1997 r. Nr 135, poz. 916)
12.	Rozporządzenie Rady Ministrów z dnia 27 lipca 1998 r. *w sprawie finansowania przedsięwzięć związanych z zakwaterowaniem osób w przypadkach nadzwyczajnych* (Dz. U. z 1998 r. Nr 88, poz. 557)
13.	Rozporządzenie Rady Ministrów z dnia 14 września 1998 r. *w sprawie zakresu, szczegółowych warunków i trybu włączania jednostek ochrony przeciwpożarowej do krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1998 r. Nr 121, poz. 798)
14.	Rozporządzenie Rady Ministrów z dnia 3 listopada 1998 r. *zmieniające rozporządzenie w sprawie ustalenia wykazu gmin, na których obszarze wystąpiła powódź w 1998r.* (Dz. U. z 1998 r. Nr 135, poz. 877)
15.	Rozporządzenie Rady Ministrów z dnia 8 czerwca 1999 r. *w sprawie zasad oraz trybu ustalania i wypłaty odszkodowań za szkody poniesione w związku z akcjami zwalczania klęsk żywiołowych* (Dz. U. z 1999 r. Nr 55, poz. 573)
16.	Rozporządzenie Rady Ministrów z dnia 25 września 2001 r. *w sprawie szczegółowych zasad i sposobu zapewnienia osłony meteorologicznej na potrzeby Morskiej Służby Poszukiwania i Ratownictwa* (Dz. U. z 2001 r. Nr 118, poz. 1252)
17.	Rozporządzenie Rady Ministrów z dnia 25 września 2001 r. *w sprawie prowadzenia nasłuchu radiowego na potrzeby Morskiej Służby Poszukiwania i Ratownictwa* (Dz. U. z 2001 r. Nr 120, poz. 1282)
18.	Rozporządzenie Rady Ministrów z dnia 2 października 2001 r. *w sprawie ustanowienia Pełnomocnika Rządu do Spraw Programu dla Odry-2006* (Dz. U. z 2001 r. Nr 118, poz. 1255)
19.	Rozporządzenie Rady Ministrów z dnia 3 grudnia 2001 r. *zmieniające rozporządzenie w sprawie ustanowienia Pełnomocnika Rządu do Spraw Programu dla Odry-2006* (Dz. U. z 2001 r. Nr 140, poz. 1573)
20.	Rozporządzenie Rady Ministrów z dnia 12 marca 2002 r. *w sprawie ustanowienia Pełnomocnika Rządu do Spraw Programu dla Odry-2006* (Dz. U. z 2002 r. Nr 31, poz. 278)
21.	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)
22.	Rozporządzenie Rady Ministrów z dnia 17 grudnia 2002 r. *w sprawie stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiar skażeń promieniotwórczych* (Dz. U. z 2002 r. Nr 239, poz. 2030)

23.	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)
24.	Rozporządzenie Rady Ministrów z dnia 6 maja 2003 r. *w sprawie szczegółowych zasad użycia oddziałów i pododdziałów Sił Zbrojnych Rzeczypospolitej Polskiej w czasie stanu wyjątkowego* (Dz. U. z 2003 r. Nr 89, poz. 821)
25.	Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. *w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony* (Dz. U. z 2003 r. Nr 116, poz. 1090)
26.	Rozporządzenie Rady Ministrów z dnia 13 stycznia 2004 r. *w sprawie szkolenia obronnego* (Dz. U. z 2004 r. Nr 16 poz. 150)
27.	Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. *w sprawie wartości poziomów interwencyjnych dla poszczególnych rodzajów działań interwencyjnych oraz kryteriów odwoływania tych działań* (Dz. U. z 2004 r. Nr 98, poz. 987)
28.	Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. *w sprawie świadczeń rzeczowych na rzecz obrony w czasie pokoju* (Dz. U. z 2004 r. Nr 181, poz. 1872)
29.	Rozporządzenie Rady Ministrów z dnia 5 października 2004 r. *w sprawie świadczeń osobistych na rzecz obrony w czasie pokoju* (Dz. U. z 2004 r. Nr 229, poz. 2307)
30.	Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. *w sprawie planów postępowania awaryjnego* (Dz. U. z 2005 r. Nr 20, poz. 169)
31.	Rozporządzenie Rady Ministrów z dnia 29 marca 2005 r. *w sprawie zasad zwalniania przez pracodawców z obowiązku świadczenia pracy osób powołanych do służby w obronie cywilnej w związku ze zwalczaniem klęsk żywiołowych, katastrof i zagrożeń środowiska* (Dz. U. z 2005 r. Nr 60, poz. 518)
32.	Rozporządzenie Rady Ministrów z dnia 29 marca 2005 r. *w sprawie stanowisk uznawanych za równorzędne z odbywaniem służby w obronie cywilnej* (Dz. U. z 2005 r. Nr 60, poz. 519)
33.	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)
34.	Rozporządzenie Rady Ministrów z dnia 20 lutego 2007 r. *w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych* (Dz. U. z 2007 r. Nr 131, poz. 912)
35.	Rozporządzenie Rady Ministrów z dnia 9 czerwca 2007 r. *w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego realizującego zasady ochrony lotnictwa* (Dz. U. z 2007 r. Nr 116, poz. 803)
36.	Rozporządzenie Rady Ministrów z dnia 31 października 2007 r. *w sprawie wykonywania funkcji wynikających ze zwierzchnictwa w polskiej przestrzeni powietrznej oraz umacniania obronności na czas pokoju* (Dz. U. z 2007 r. Nr 210, poz. 1523)
37.	Rozporządzenie 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)
38.	Rozporządzenie Rady Ministrów z dnia 13 listopada 2009 r. *w sprawie przydziału broni palnej oraz jej magazynowania, przechowywania i zapewnienia właściwego stanu technicznego* (Dz. U. z 2009 r. Nr 196, poz. 1512)
39.	Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. *w sprawie określenia organów administracji rządowej, które tworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania* (Dz. U. z 2009 r. Nr 226, poz. 1819)
40.	Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. *w sprawi Raportu o zagrożeniach bezpieczeństwa narodowego* (Dz. U. z 2010 r. Nr 83, poz. 540)
41.	Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. *w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej* (Dz. U. z 2010 r. Nr 83, poz. 541)
42.	Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. *w sprawie planów ochrony infrastruktury krytycznej* (Dz. U. z 2010 r. Nr 83, poz. 542)
43.	Rozporządzenie Rady Ministrów z dnia 21 listopada 2011 r. *w sprawie utworzenia Ministerstwa Administracji i Cyfryzacji* (Dz. U. z 2011 r. Nr 250, poz. 1501)

44.	Rozporządzenie Rady Ministrów z dnia 21 listopada 2011 r. *w sprawie utworzenia Ministerstwa Spraw Wewnętrznych* (Dz. U. z 2011 r. Nr 250, poz. 1502)
45.	Rozporządzenie Prezesa Rady Ministrów z dnia 23 września 2002 r. *w sprawie określenia gmin miejscowości, w których stosuje się szczególne zasady odbudowy, remontów i rozbiórek obiektów budowlanych zniszczonych lub uszkodzonych przez żywioły* (Dz. U. z 2002 r. Nr 157, poz. 1311)
46.	Rozporządzenie Prezesa Rady Ministrów z dnia 16 listopada 2007 r. *w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji* (Dz. U. z 2007 r. Nr 216, poz. 1604)
47.	Rozporządzenie Prezesa Rady Ministrów z dnia 28 maja 2008 r. *w sprawie gmin i miejscowości, w których stosuje się szczególne zasady odbudowy, remontów i rozbiórek obiektów budowlanych zniszczonych lub uszkodzonych w wyniku działań żywiołu* (Dz. U. z 2008 r. Nr 99, poz. 642)
48.	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)
49.	Rozporządzenie Ministra Obrony Narodowej z dnia 19 czerwca 1999 r. *w sprawie ochrony przez specjalistyczne uzbrojone formacje ochronne terenów, komórek i jednostek organizacyjnych resortu obrony narodowej* (Dz. U. z 1999 r. Nr 60, poz. 647)
50.	Rozporządzenie Ministra Obrony Narodowej z dnia 16 stycznia 2004 r. *w sprawie wyznaczania żołnierzy zawodowych do służby poza Siłami Zbrojnymi Rzeczypospolitej Polskiej w razie ogłoszenia mobilizacji, ogłoszenia stanu wojennego i w czasie wojny* (Dz. U. z 2004 r. Nr 15, poz. 133)
51.	Rozporządzenie Ministra Obrony Narodowej z dnia 16 stycznia 2004 r. *w sprawie mianowania żołnierzy zawodowych i żołnierzy pełniących służbę kandydacką w razie ogłoszenia mobilizacji, ogłoszenia stanu wojennego i w czasie wojny* (Dz. U. z 2004 r. Nr 15, poz. 134)
52.	Rozporządzenie Ministra Obrony Narodowej z dnia 29 kwietnia 2004r. *w sprawie opiniowania żołnierzy zawodowych i żołnierzy pełniących służbę kandydacką w razie ogłoszenia mobilizacji, ogłoszenia stanu wojennego i w czasie wojny* (Dz. U. z 2004 r. Nr 122, poz. 1275)
53.	Rozporządzenie Ministra Obrony Narodowej dnia 27 kwietnia 2006 r. *w sprawie określenia kategorii żołnierzy rezerwy, których przeznaczenie do służby w obronie cywilnej wymaga zgody wojskowego komendanta uzupełnień* (Dz. U. z 2006 r. Nr 83, poz. 576)
54.	Rozporządzenie Ministra Obrony Narodowej dnia 27 maja 2008 r. *w sprawie przepływu okrętów wojennych obcych państw przez polskie morze terytorialne oraz warunków wejścia okrętów na polskie morskie wody wewnętrzne* (Dz. U. z 2008 r. Nr 131, poz. 834)
55.	Rozporządzenie Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 12 sierpnia 1997 r. *zmieniające rozporządzenie w sprawie określenia rodzajów inwestycji szkodliwych dla środowiska i zdrowia ludzi oraz ocen oddziaływania na środowisko* (Dz. U. z 1997 r. Nr 101, poz. 634)
56.	Rozporządzenie Ministra Środowiska z dnia 6 czerwca 2002 r. *w sprawie dopuszczalnych poziomów niektórych substancji w powietrzu, alarmowych poziomów niektórych substancji w powietrzu oraz marginesów tolerancji dla dopuszczalnych poziomów niektórych substancji* (Dz. U. z 2002 r. Nr 87, poz. 798)
57.	Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 19 września 1997 r. *w sprawie szczegółowych warunków i trybu przyznawania środków Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych w związku z likwidacją skutków powodzi, która miała miejsce w lipcu 1997 r.* (Dz. U. z 1997 r. Nr 120, poz. 762)
58.	Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. *w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy* (Dz. U. z 2003 r. Nr 169, poz. 1650)
59.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 15 listopada 1997 r. *w sprawie wykazu gmin, w których stosowane są szczególne rozwiązania dotyczące zatrudnienia i przeciwdziałania bezrobociu mające na celu likwidację skutków powodzi* (Dz. U. z 1997 r. Nr 153, poz. 1006)
60.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 marca 1998 r. *zmieniające rozporządzenie w sprawie wykazu gmin, w których stosowane są szczególne rozwiązania dotyczące zatrudnienia i przeciwdziałania bezrobociu mające na celu likwidację skutków powodzi* (Dz. U. z 1998 r. Nr 38, poz. 222)

61.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 14 września 1998 r. *w sprawie zakresu, szczegółowych warunków i trybu włączania jednostek ochrony przeciwpożarowej do krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1998 r. Nr 121, poz. 798)
62.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 14 października 1998 r. *w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* (Dz. U. z 1998 r. Nr 129, poz. 858)
63.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 grudnia 1998 r. *w sprawie określenia szczegółowych zasad współpracy specjalistycznych uzbrojonych formacji ochronnych z Policją, jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi (miejskimi)* (Dz. U. z 1998 r. Nr 161, poz. 1108)
64.	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)
65.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 4 września 2001 r. *w sprawie wykazu miejscowości dotkniętych powodzią oraz miejscowości, na których obszarze wystąpiły osuwiska ziemne lub huragany* (Dz. U. z 2001 r. Nr 95, poz. 1046)
66.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 stycznia 2002 r. *zmieniające rozporządzenie w sprawie wykazu miejscowości dotkniętych powodzią oraz miejscowości, na których obszarze wystąpiły osuwiska ziemne lub huragany* (Dz. U. z 2002 r. Nr 6, poz. 57), (Dz. U. z 2002 r. Nr 103, poz. 930)
67.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 maja 2002 r. *w sprawie wzoru odznaki i legitymacji do odznaki wzorowego ratownika obrony cywilnej* (Dz. U. z 2002 r. Nr 119, poz. 1017)
68.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 września 2002 r. *w sprawie odbywania służby w obronie cywilnej* (Dz. U. z 2002 r. Nr 169, poz. 1391)
69.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 marca 2003 r. *w sprawie zakresu, warunków i trybu wykonywania przez funkcjonariuszy Biura Ochrony Rządu zadań ochrony polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych poza granicami Rzeczypospolitej Polskiej* (Dz. U. z 2003 r. Nr 55, poz. 491)
70.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 grudnia 2004 r. *w sprawie szczegółowych zasad współdziałania Straży Granicznej z Siłami Powietrznymi i Marynarką Wojenną Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie ochrony granicy państwowej* (Dz. U. z 2005 r. Nr 6, poz. 50)
71.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 września 2005 r. *w sprawie form kontroli bezpieczeństwa przeprowadzanej w zasięgu terytorialnym przejścia granicznego oraz w środkach komunikacji międzynarodowej przez funkcjonariuszy Straży Granicznej* (Dz. U. z 2005 r. Nr 197, poz. 1642)
72.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 19 grudnia 2005 r. *w sprawie wart ochronnych pełnionych przez funkcjonariuszy Straży Granicznej na pokładzie statku powietrznego* (Dz. U. z 2005 r. Nr 266, poz. 2243)
73.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 15 grudnia 2006 r. *w sprawie kontroli granicznej dokonywanej przez funkcjonariuszy Straży Granicznej* (Dz. U. z 2006 r. Nr 238, poz. 1729)
74.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lipca 2008 r. *w sprawie kontroli ruchu drogowego* (Dz. U. z 2008 r. Nr 132, poz. 841 z późn. zm.)
75.	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* (Dz. U. z 2009 r. Nr 130, poz. 1073)

76.	Rozporządzenie Ministra Gospodarki z dnia 9 kwietnia 2002 r. *w sprawie rodzajów i ilości substancji niebezpiecznych, których znajdowanie się w zakładzie decyduje o zaliczeniu go do zakładu o zwiększonym ryzyku albo zakładu o dużym ryzyku wystąpienia poważnej awarii przemysłowej* (Dz. U. z 2002 r. Nr 58, poz. 535)
77.	Rozporządzenie Ministra Gospodarki z dnia 12 czerwca 2002 r. *w sprawie ratownictwa górniczego* (Dz. U. z 2002 r. Nr 94, poz. 838)
78.	Rozporządzenie Ministra Gospodarki z dnia 8 listopada 2002 r. *w sprawie wymagań, jakim powinien odpowiadać plan postępowania na wypadek zagrożenia życia lub zdrowia ludzkiego, mienia oraz środowiska naturalnego* (Dz. U. z 2002 r. Nr 194, poz. 1632)
79.	Rozporządzenie Ministra Gospodarki z dnia 28 października 2002 r. *w sprawie pomieszczeń magazynowych i obiektów do przechowywania materiałów wybuchowych, broni, amunicji oraz wyrobów o przeznaczeniu wojskowym lub policyjnym* (Dz. U. z 2002 r. Nr 190, poz. 1589)
80.	Rozporządzenie Ministra Zdrowia z dnia 7 maja 2007 r. *w sprawie ramowych procedur przyjmowania wezwań przez dyspozytora medycznego i dysponowania zespołami ratownictwa medycznego* (Dz. U. z 2007 r. Nr 90, poz. 605)
81.	Rozporządzenie Ministra Infrastruktury z dnia 24 grudnia 2001 r. *w sprawie szczegółowej organizacji Morskiej Służby Poszukiwania i Ratownictwa* (Dz. U. z 2001 r. Nr 157, poz. 1845)
82.	Rozporządzenie Ministra Infrastruktury z dnia 12 listopada 2002 r. *w sprawie określenia dokumentów potwierdzających wykonywanie przez przedsiębiorcę przewozów w ramach pomocy humanitarnej, medycznej lub w przypadku klęski żywiołowej* (Dz. U. z 2002 r. Nr 199, poz. 1676)
83.	Rozporządzenie Ministra Infrastruktury z dnia 9 stycznia 2004 r. *w sprawie planu działań operatora w sytuacjach szczególnych zagrożeń* (Dz. U. z 2004 r. Nr 12, poz. 106)
84.	Rozporządzenie Ministra Infrastruktury z dnia 20 kwietnia 2004 r. *w sprawie wykonywania lotów międzynarodowych przez obce cywilne statki powietrzne oraz stałego pobytu polskich cywilnych statków powietrznych za granicą i obcych cywilnych statków powietrznych w Rzeczypospolitej Polskiej* (Dz. U. z 2004 r. Nr 94, poz. 916)
85.	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)
86.	Rozporządzenie Ministra Infrastruktury z dnia 23 listopada 2004 r. *w sprawie przepisów porządkowych obowiązujących na obszarze kolejowym, w pociągach i innych pojazdach kolejowych* (Dz. U. z 2004 r. Nr 264, poz. 2637)
87.	Rozporządzenie Ministra Infrastruktury z dnia 10 stycznia 2005 r. *w sprawie Krajowego Programu Kontroli Jakości w zakresie ochrony lotnictwa cywilnego* (Dz. U. z 2005 r. Nr 25, poz. 208)
88.	Rozporządzenie Ministra Infrastruktury z dnia 7 lipca 2009 r. *w sprawie Krajowego Programu Szkolenia w zakresie ochrony lotnictwa cywilnego* (Dz. U. z 2009 r. Nr 122, poz. 1011)
89.	Rozporządzenie Ministra Transportu z dnia 30 kwietnia 2007 r. *w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego* (Dz. U. z 2007r. Nr 90, poz. 603)
90.	Rozporządzenie Ministra Transportu z dnia 4 czerwca 2007 r. *w sprawie towarów niebezpiecznych, których przewóz drogowy podlega obowiązkowi zgłoszenia* (Dz. U. z 2007 r. Nr 107, poz. 742)
91.	Rozporządzenie Ministra Rolnictwa i Rozwoju Wsi z dnia 26 maja 2004 r. *w sprawie zakresu i warunków współpracy organów administracji rządowej i jednostek samorządu terytorialnego oraz innych podmiotów w tworzeniu planów gotowości zwalczania chorób zakaźnych zwierząt* (Dz. U. z 2004 r. Nr 129, poz. 1372)
92.	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)
93.	Rozporządzenie Ministra Finansów z dnia 28 listopada 2008 r. *w sprawie warunków i kryteriów technicznych, którym muszą odpowiadać kasy rejestrujące oraz warunków ich stosowania* (Dz. U. z 2008 r. Nr 212, poz. 1338)

	Zarządzenia
1.	Zarządzenie Nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. *w sprawie powołania Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*
2.	Zarządzenie Nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 r. *w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego* (M.P. z 2008 r. Nr 61, poz. 538)
3.	Zarządzenie Nr 74 Prezesa Rady Ministrów z dnia 21 września 2009 r. zmieniające zarządzenie *w sprawie powołania Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*
4.	Zarządzenie Nr 29 Ministra Obrony Narodowej z dnia 3 października 2008 r. *w sprawie organizacji, składu oraz miejsca i trybu pracy Zespołu Zarządzania Kryzysowego w Ministerstwie Obrony Narodowej* (Dz. Urz. MON z 2008 r. Nr 19, poz. 250)
5.	Zarządzenie Ministra Finansów z dnia 21 maja 2010 r. *w sprawie strategii działania Służby Celnej na lata 2010–2015*
	Porozumienia
1.	Porozumienie z dnia 6 lipca 2004 r. *o współdziałaniu w zakresie strategii zmierzającej do poprawy stanu bezpieczeństwa na obszarach kolejowych pomiędzy: Komendantem Głównym Policji, Komendantem Głównym Straży Granicznej, Komendantem Głównym Żandarmerii Wojskowej, a Spółką „Polskie Koleje Państwowe Spółka Akcyjna"*
2.	Porozumienie z dnia 20 kwietnia 2005 r. w *sprawie współdziałania Sił Zbrojnych Rzeczypospolitej Polskiej z Policją w zakresie przeciwdziałania sytuacjom kryzysowym* (Dz. Urz. MON z 2005 r. Nr 10, poz. 89)
	Wytyczne
1.	Wytyczne Szefa Obrony Cywilnej Kraju z dnia 20 stycznia 2000 r. *w sprawie zasad zapewnienia ciągłości funkcjonowania urzędów terenowych organów obrony cywilnej w sytuacjach kryzysowych*
	Inne przepisy
1.	*Plan działania w zakresie wdrażania dorobku prawnego Schengen w Polsce*, przyjęty przez Komitet Integracji Europejskiej w dniu 15 sierpnia 2001 roku www.msw.gov.pl (pobrano 15.12.2011)
2.	*Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 roku* www.mon.gov.pl (pobrano 2.03.2012)
3.	*Strategia Obronności Rzeczypospolitej Polskiej z 2009 roku* www.mon.gov.pl (pobrano 2.03.2012)
4.	*Program Zintegrowanego Zarządzania Granicą w latach 2007–2013*, przyjęty przez Radę Ministrów 10 września 2007 roku www.bip.mswio.gov.pl (pobrano 2.03.2012)
5.	*Zintegrowana Koncepcja Bezpieczeństwa EURO 2012*, przyjęta przez Komitet ds. Bezpieczeństwa EURO 201 w dniu 6 września 2010 roku www.msw.gov.pl. (pobrano 20.11.2011)
6.	*Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* www.bip.msw.gov.pl (pobrano 14.04.2012)

ROZDZIAŁ 5

Podsystem informacyjny

5.1. Znaczenie informacji dla zarządzania kryzysowego

> Skuteczne zarządzanie kryzysowe na poziomie państwa, województwa, powiatu i gminy zależy od posiadanych informacji. Ponadto w zarządzaniu kryzysowym potrzebne są koncepcje, metody i motywacja, wiedza specjalistyczna i wyobraźnia, potrzebny jest też czas na przemyślenia, ale informacje są niewątpliwie najważniejsze, gdyż pozwalają poznać zmiany zachodzące w otoczeniu organizacji i odpowiednio wcześniej dostosować do nich jej potencjał i przyszłe możliwości[1].

Oznacza to, że dostęp do wiedzy i zasobów informacyjnych, umożliwiających wczesną weryfikację zagrożeń lub reakcję na już zaistniałe, jest dla systemu zarządzania kryzysowego sprawą priorytetową[2]. Bez znajomości otoczenia wewnętrznego i zewnętrznego państwa, województwa, powiatu i gminy, a także zachodzących tam zmian, które są źródłem szans i zagrożeń, trudno jest sporządzać scenariusze, redukować niepewność działania, podejmować właściwe decyzje, wskazywać możliwe koncepcje rozwoju, a przede wszystkim budować strategie, dla których rozpoznanie zagrożeń i szans w otoczeniu, a także słabych i mocnych stron stanowią bazy danych. Dlatego posiadanie odpowiednich informacji jest dzisiaj dla każdego zarządzającego w sytuacji kryzysowej sprawą o fundamentalnym znaczeniu. Są one również traktowane jako podstawowy czynnik, który decyduje o sukcesie i jakości zarządzania kryzysowego.

Przemiany cywilizacyjne powodują, że informacja współcześnie decyduje o sposobie wykorzystania posiadanych zasobów i możliwości, o zdolności do dostosowania się do nowych warunków i programowania rozwoju w procesie poprzedzającym wystąpienie sytuacji kryzysowej. Każdy podmiot uczestniczący w zarządzaniu kryzysowym powinien znać swoje potrzeby informacyjne i wiedzieć, jakie informacje są potrzebne do tworzenia planów, gromadzenia zasobów

[1] Penc, *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Kraków 1998, s. 106.

[2] R. Kwećka, *Procesy informacyjne w ramach systemu reagowania kryzysowego Unii Europejskiej*, [w:] *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, red. J. Gryz, Toruń 2009, s. 336.

i wykonywania podstawowych funkcji i działań. Powinien także określić, jakie potrzeby informacyjne są zaspokajane w niedostatecznym stopniu, a jakie nie są w ogóle zaspokajane, a także w jakim stopniu przepływ informacji pomaga zarządzającym w procesie podejmowania decyzji i sprawnego kierowania[3].

Informacja jest elementem wiedzy, faktem, wiadomością, komunikatem lub wskazówką gromadzoną, komunikowaną lub przekazywaną komuś za pomocą jakiegoś kodu lub języka[4]. Każda informacja, aby stanowiła wartość dla procesu zarządzania kryzysowego, powinna być pełna i wyczerpująca. Poza treścią powinna zawierać elementy pozwalające na jej identyfikację i ochronę, tzn. czas nadania, czas odbioru, temat, nadawcę, odbiorcę, status (niesklasyfikowana, zastrzeżona, poufna, tajna, ściśle tajna)[5]. Informacja dla podmiotów realizujących ustawowe zadania w sferze zarządzania kryzysowego powinna zapewniać wiedzę konieczną do określenia i realizacji zadań służących do osiągnięcia celów gminy, powiatu, województwa i państwa w sytuacjach kryzysowych. Informacja powinna zmniejszać nieokreśloności lub niepewności co do stanu albo dalszego rozwoju sytuacji, której ta wiadomość dotyczy[6].

Należy zaznaczyć, że każda informacja charakteryzuje się pewnymi cechami, do których zalicza się: aktualność, jakość, istotność, ścisłość, cenność, kompletność, kosztowność, dostępność, spójność, ekonomiczność, powiązanie z zadaniami wykonywanymi na poziomie gminy, powiatu, województwa, państwa. Informacje gromadzone na wszystkich poziomach zarządzania kryzysowego powinna być odpowiedniej jakości, tzn. obiektywne, ważne dla obszaru zarządzania, dostępne, porównywalne, pełne i zwięzłe. Spełnienie tych kryteriów jest bardzo trudne, ponieważ informacje szybko tracą na aktualności. Ponadto w procesie podejmowania decyzji nie uzyskuje się informacji wyczerpujących. Zawsze należy się liczyć z szumem informacyjnym i luką informacyjną z uwagi na wielość kanałów informacyjnych.

Tempo zmian, jakie występują w otoczeniu wewnętrznym i zewnętrznym (bliższym i dalszym) gminy, powiatu, województwa i państwa, a także towarzyszące im zagrożenia naturalne i celowe wymagają dostępu do szerokiego spektrum informacji. Potrzeby informacyjne wynikają z istnienia luki informacyjnej, która jest zawsze odnoszona do konkretnego obserwatora. Ponadto jest wrażliwa na czynnik czasu, który w asymetrycznym środowisku międzynarodowym, skali i dynamice zagrożeń, gdzie występują nieprzewidywalność i chaos, ma kluczowe znaczenie dla skutecznego zarządzania kryzysowego. Na zakres i informacyjną strukturę luki informacyjnej mają wpływ czynniki obiektywne oraz subiektywne[7]. Pierwszy z nich ma ścisły związek z obiektywną wiedzą podmiotów zarządzających i dotyczy celowości prowadzonych obserwacji środowiska podatnego

[3] J. Penc, op. cit., s. 107.

[4] A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych*, Siedlce 2002, s. 22.

[5] Ibidem, s. 22.

[6] D. Kroenke, *Management Information Systems*, McGraw-Hill, New York 1989, s. 14.

[7] W. Flakiewicz, *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje*, Warszawa 2002, s. 31.

na zagrożenia oraz możliwości realizacji takiej obserwacji w ramach zarządzania kryzysowego. Stąd przeprowadzenie obserwacji i stopień jej kompletności, osiągniętej przydatności jest najczęściej kompromisem między oczekiwaniami a możliwościami ich realizacji[8]. Natomiast czynniki subiektywne związane są z faktem, że luka jest zawsze czyjaś, a więc jest adresowana do konkretnego obserwatora (w odniesieniu do zarządzania kryzysowego dotyczy to bezpośrednio podmiotów kierujących)[9], który powinien dążyć do jej zminimalizowania.

W procesie zarządzania kryzysowego informacja spełnia kilka funkcji. Z punktu widzenia jego potrzeb można wyróżnić trzy rodzaje informacji: mające służyć pomocą w podejmowaniu decyzji, mające zapewnić odpowiednią komunikację między przełożonym a pracownikami oraz mające zaspokoić innych użytkowników[10].

Szczególnie istotne są informacje, które warunkują skuteczność zarządzania kryzysowego. Uprawnione podmioty na wszystkich poziomach zarządzania kryzysowego muszą dostosowywać się do zmian zachodzących w ich otoczeniu, muszą rozwiązywać coraz trudniejsze i coraz bardziej złożone problemy związane z pojawiającymi się zagrożeniami i szybko reagować w celu niedopuszczenia do ich wystąpienia lub zminimalizowania negatywnych następstw. Na każdym poziomie zarządzania kryzysowego powinien funkcjonować system wczesnego ostrzegania i sygnalizowania niebezpieczeństw (zagrożeń), który pozwoli na poznanie zagrożenia i podjęcie odpowiednich działań. Pozyskiwanie informacji, sposoby ich zbierania, gromadzenia i przepływu powinny być zorganizowane na zasadzie systemu, obejmującego całe zbiory informacyjne (zasoby informacyjne) oraz elementy umożliwiające zasilanie, nabywanie i dostarczanie użytkownikom tych zasobów[11].

System informacyjny stanowi uporządkowany układ nadawania i odbioru informacji, czyli formalne kanały komunikacji umożliwiające przepływ – przekaz – odbiór wiadomości, poleceń, rozkazów, zadań, obowiązków itd.[12]. Trudno bowiem wyobrazić sobie sprawne i skuteczne zarządzanie kryzysowe bez możliwości wymiany informacji między uprawnionymi podmiotami, w tym wykorzystanie techniki teleinformatycznej. System informacji należy uznać za system nerwowy zarządzania kryzysowego na wszystkich jego poziomach, gdyż za jego pośrednictwem utrzymuje się porządek we wzajemnych relacjach służbowych. System taki, zwany systemem informacji, powinien być rozumiany nowocześnie, tzn. jako komputerowa metoda zbierania, opracowywania, przechowywania, kodowania, dekodowania, aktualizowania, odtwarzania i przetwarzania danych oraz ich dostarczania w najprzydatniejszej formie kadrze kierowniczej do realizacji zadań i celów organizacji (państwa, województwa, powiatu, gminy)[13].

8 Ibidem, s. 31.

9 Ibidem.

10 J. Penc, op. cit., s. 111.

11 J. Kisielnicki, *Informatyczna infrastruktura zarządzania*, Warszawa 1992, s. 15.

12 L. Zbiegień-Maciąg, W. Pawnik, *Zarządzanie organizacją. Aspekt socjologiczny*, Kraków 1998, s. 15.

13 J. Penc, op. cit., s. 115 i 116.

System informacji powinien spełniać następujące warunki:

- być dostosowany do potrzeb zarządzania kryzysowego i obejmować wszystkie jego obszary, poziomy kierowania i poziomy decyzyjne,
- dostarczać informacji kompleksowych i aktualnych, aby gmina, powiat, województwo i państwo reagowało na zmianę warunków wewnętrznych i zewnętrznych,
- dostarczać informacji tym, którzy ich rzeczywiście potrzebują, w formie nadającej się bezpośrednio (bez przetwarzania) do użytku i najdogodniejszej dla podjęcia ostatecznych decyzji,
- zapewnić efektywne wykorzystanie informacji, co jest uwarunkowane szybkością i częstotliwością ich obiegu, oznacza to, że dane powinny być aktualne, kompletne i odpowiednio posegregowane, gdyż to ułatwia ich obieg,
- droga przepływu informacji powinna być możliwie najkrótsza i zgodna ze strukturą organizacyjną państwa, województwa, powiatu i gminy, a poszczególne podsystemy informacji powinny stanowić prosty zbiór, który można szybko przyswoić i wykorzystać w podejmowaniu praktycznych decyzji (sensowne, zwięzłe raporty),
- algorytmy opracowania informacji powinny zapewnić śledzenie przebiegu procesów zarządzania, konstruowanie ocen, prognozowanie przebiegu wydarzeń,
- koszty pozyskiwania i przetwarzania informacji powinny być niewysokie, metody ich zbierania, opracowywania, przechowywania i przepływu uwzględniać możliwości komputeryzacji systemu informacyjnego, a forma ich prezentacji być dostosowana do możliwości odczytywania przez zainteresowanych,
- system powinien być zabezpieczony przed niepożądanym wpływem informacji nieformalnych i stale doskonalony, aby mógł zapewnić właściwy przepływ informacji[14].

System informacyjny powinien być tak skonstruowany, aby wszystkim szczeblom decyzyjnym zapewniał dopływ informacji odpowiednich pod względem treści i w odpowiednim czasie. Powinien on zatem gwarantować ich przepływ przez wszystkie kanały informacyjne wiążące sobą zasoby i informacje o istniejących możliwościach i ograniczeniach[15].

Oznacza to, że:

- informacje muszą być zabezpieczone przed szumem informacyjnym, ponieważ zbyt duża ilość informacji, przekłamania, opóźnienia w odbiorze, mylenie przez człowieka skutków i przyczyn, uprzedzenia ludzkie, naginanie informacji do własnych przewidywań – powodują małą skuteczność i wiarygodność przekazu,
- informacje muszą docierać do każdego uprawnionego uczestnika zarządzania kryzysowego (w uzasadnionych przypadkach również do ludności), a ka-

[14] Opracowano na podstawie J. Penc, op. cit., s. 116.

[15] Ibidem, s. 118.

nały informacyjne muszą być jak najkrótsze, ponieważ długa droga to m.in. przekłamania,
- ogniwa w systemie informacyjnym powinny być obsadzane przez osoby kompetentne,
- należy zapobiegać przerywaniu sieci przekazu informacji,
- w zarządzaniu kryzysowym każdy musi wiedzieć, od kogo otrzymuje informacje i komu przekazuje je dalej (meldunki, sprawozdania itp.)[16].

System informacyjny w zarządzaniu kryzysowym musi być spójny wewnętrznie (państwo, województwo, powiat, gmina – gmina, powiat, województwo, państwo), ponadto kompatybilny z analogicznymi systemami działającymi na poziomie Unii Europejskiej i Sojuszu Północnoatlantyckiego.

System informacyjny musi opierać się na rozbudowanej infrastrukturze informacyjnej uwzględniającej sieć wewnętrzną i zewnętrzną łączącą uprawnione podmioty uczestniczące w zarządzaniu kryzysowym. Sieć wewnętrzna powinna być zorganizowana na zasadzie tzw. mapy informacyjnej zmieniającej się z biegiem czasu pod wpływem zmian otoczenia. Taka mapa musi zawierać węzły informacyjne (składające się z grup pracowników, dokumentów, wyszukiwania danych i komunikowania) oraz linie przepływu między węzłami, ustalane zgodnie z wymaganiami tzw. odwróconej piramidy informacyjnej, która oznacza, że tam, gdzie koncentruje się władza, potrzebne są informacje mniej szczegółowe, a bardziej skondensowane, o szerokim przekroju, dające pogląd na całość działania organizacji (gminy, powiatu, województwa, państwa) i jej powiązania z otoczeniem, ułatwiające zintegrowane zarządzanie kryzysowe[17]. Oznacza to, że system informacyjny zarządzania kryzysowego powinien zawierać informacje uszeregowane według pewnej hierarchii, a mianowicie dla celów strategicznych, operacyjnych i taktycznych.

Systematyczne poznawanie i wykorzystywanie informacji w procesie zarządzania kryzysowego na wszystkich jego poziomach jest obecnie uzasadnioną koniecznością. Podmioty uczestniczące w zarządzaniu kryzysowym powinny być zainteresowane poznawaniem i stosowaniem różnych metod diagnozowania otoczenia (wewnętrznego i zewnętrznego) oraz stałego rozszerzania wiadomości o nim, aby nie zaprzepaścić szans, rozpoznać na czas zbliżające się zagrożenia i dostosować swój potencjał i rodzaje działalności do zmieniających się trendów[18]. Takim rozwiązaniem jest monitorowanie środowiska gminy, powiatu, województwa, państwa, ze szczególnym wskazaniem miejsc o podwyższonym ryzyku. Ważne jest również rozpoznawanie otoczenia zewnętrznego (międzynarodowego) państwa przez uprawnione podmioty pod kątem wykrywania zagrożeń, ich skali, dynamiki i kierunków.

Monitorowanie oznacza systematyczną kontrolę otoczenia bliższego i dalszego, ujawnianie pojawiających się zmian mających wpływ na funkcjonowanie

[16] L. Zbiegień-Maciąg, W. Pawnik, op. cit., s. 15.

[17] J. Ingalls, *Human Energy*, Menlo Park 1976, s. 113.

[18] Opracowano na podstawie J. Penc, op. cit., s. 131.

gminy, powiatu, województwa i państwa oraz przekazywanie o nich informacji uprawnionym podmiotom zarządzającym w celu wykorzystania ich w planowaniu średnio- i długookresowym. Zadaniem tego monitoringu, zwanego często strategicznym, jest dostarczanie podmiotom uczestniczącym w zarządzaniu kryzysowym informacji umożliwiających realizację celów: defensywnych, pasywnych i ofensywnych[19]. „System monitoringu nieustannie śledzi i rozpoznaje sytuacje w aspekcie zagrożeń mogących prowadzić do zakłócenia aktualnego stanu bezpieczeństwa państwa. Procedurę tę realizuje w czasie rzeczywistym, pod kątem natychmiastowego uruchomienia czynności przeciwdziałania kryzysowego"[20]. Jeżeli w procesie prowadzonego monitoringu nie nastąpi wskazanie i rozpoznanie zagrożenia, system zarządzania kryzysowego nie zostanie uruchomiony. Również w sytuacji, gdy zagrożenie nie zostanie rozpoznane w odpowiednim czasie, także system alarmowy nie zostanie uruchomiony, a w konsekwencji nie zostaną wprowadzone siły i środki zarządzania kryzysowego.

Proces identyfikacji i diagnozowania zagrożeń przez system monitoringu można wyrazić za pomocą następującego ciągu czynności:

- cykliczne przeszukiwanie zadanej przestrzeni stanów systemowych, np. za pomocą inteligentnych sensorów, w celu rozpoznania ewentualnego zagrożenia; im krótszy jest okres czasu między poszczególnymi cyklami identyfikacji, tym wyższa jest sprawność danego systemu monitoringu;
- w przypadku zidentyfikowania i zaklasyfikowania danego zdarzenia jako potencjalne zagrożenie, uruchamiany jest program jego szczegółowej oceny celem postawienia hipotetycznej diagnozy co do stopnia i skali stworzonego niebezpieczeństwa;
- stopień generowania niebezpieczeństwa jest dodatkowo weryfikowany w odniesieniu do aktualnej sytuacji i rzeczywistych uwarunkowań; każde zagrożenie musi być odniesione do szerokiego spektrum warunków sytuacyjnych, ograniczeń czasoprzestrzennych i realnych możliwości skutecznego reagowania;
- wszystkie nadchodzące i diagnozowane zagrożenia muszą być relatywizowane względem innych aktualnie zaistniałych i badanych zdarzeń krytycznych, aby jednoznacznie zidentyfikować najbardziej niebezpieczne w danej chwili zagrożenia i nadać im najwyższy priorytet obsługi (reagowania); jednym z lepszych kryteriów diagnozowania zagrożeń jest kryterium oparte na szacowaniu stopnia ryzyka związanego z zaistniałym zagrożeniem;
- końcowym efektem monitoringu jest przygotowanie danych źródłowych do podjęcia decyzji o uruchomieniu kolejnych procedur reagowania (zarządzania) kryzysowego; hierarchicznie uporządkowany zbiór dopuszczalnych decyzji w aktualnej sytuacji kryzysowej powinien być podstawą podjęcia ostatecznej decyzji, najlepiej optymalnej, np. ze względu na poziom ryzyka lub możliwości wykonawcze systemu zarządzania kryzysowego,

[19] Ibidem, s. 131 i 132.

[20] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 251.

- identyfikacja losowo pojawiających się zagrożeń jest procesem ciągłym i dlatego system monitoringu musi działać bardzo sprawnie, szybko i jednoznacznie, identyfikacja musi zakończyć się precyzyjną diagnozą stopnia niebezpieczeństwa albo poziomu stworzonego ryzyka jako następstwo realizacji danego zagrożenia[21].

System monitoringu jest systemem wczesnego ostrzegania i alarmowania przed zagrożeniami. Pozwala na obserwowanie ważnych dla gminy, powiatu, województwa, państwa dziedzin życia, rozpoznanie pojawiających się symptomów zagrożeń oraz dostrzegania zjawisk, dzięki którym możliwe będzie wykorzystanie posiadanych zasobów oraz reakcja na zagrożenia. System wczesnego ostrzegania dostarcza podmiotom uczestniczącym w zarządzaniu kryzysowym użytecznych informacji o zjawiskach i procesach oraz prawdopodobieństwie ich wystąpienia i rozwoju, a dzięki temu umożliwia im w miarę szybkie, elastyczne reagowanie oraz podejmowanie działań zmieniających ich przebieg, a w konsekwencji przystosowanie do nowych wymagań otoczenia[22].

> System monitoringu należy traktować jako system alarmowania, który służy do przekazywania dla określonego zespołu ludzi bądź pojedynczych osób [...] sygnału (znaku umownego) do wykonania ustalonego wcześniej polecenia, zarządzenia, rozkazu nakazującego natychmiastowe przejście do określonego działania, zwykle w wypadku grożącego niebezpieczeństwa napadu (powietrznego, jądrowego, chemicznego) ze strony nieprzyjaciela[23].

W innym ujęciu system monitoringu to system wykrywania i alarmowania, który stanowi zespół ogniw na wszystkich szczeblach kierowania obroną cywilną oraz przygotowanych sił i środków, których celem jest ostrzeganie, alarmowanie oraz uprzedzenie ludności o grożącym niebezpieczeństwie[24]. Z kolei alarmowanie i powiadamianie to przekazywanie odpowiednim organom i ludności cywilnej sygnałów o niebezpieczeństwie[25]. System ten jest bardzo ważny dla poznania niebezpieczeństw, gdzie źródłem jest wciąż zmieniające się i niepewne otoczenie gminy, powiatu, województwa i państwa, w tym i środowisko międzynarodowe. Dlatego uprawnione podmioty na wszystkich poziomach zarządzania kryzysowego w celu niedopuszczenia do zaistnienia zagrożenia lub minimalizowania jego negatywnych następstw potrzebują wyprzedzających informacji pozwalających na skuteczne reagowanie na nadchodzące zmiany.

Proces zdobywania, gromadzenia, przetwarzania i dystrybucji informacji powinien być realizowany i doskonalony w czasie poprzedzającym sytuację kryzysową.

[21] Ibidem, s. 252.

[22] J. Penc, op. cit., s. 135.

[23] *Leksykon wiedzy wojskowej*, t. 1, Warszawa 1973, s. 13.

[24] *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. W. Łepkowski, Warszawa 2009, s. 142.

[25] *Mała encyklopedia wojskowa*, t. 1, Warszawa 1967, s. 15.

W procesie zdobywania informacji o obiektach znajdujących się w sferze zainteresowania podmiotów uczestniczących w zarządzaniu kryzysowym powinny być wykorzystywane na szeroką skalę środki informatyczne, które […] umożliwiają tworzenie komputerowych baz danych. W bazach tych powinny być zawarte zbiory umożliwiające tworzenie danych kompilacji informacyjnych (także w sytuacjach krytycznych), tworzenie prostego dialogu z bazą danych w systemie konwersyjnym (tzn. pytanie – odpowiedź), graficzne zobrazowanie sytuacyjne przeciwnika oraz komputerowe przetwarzanie i dystrybucja w czasie zbliżonym do rzeczywistego[26].

Zmiany, jakie zachodzą w środowisku międzynarodowym, są źródłem nie tylko postępu, ale i zagrożeń. Skala, dynamika i skutki zagrożeń naturalnych i celowych, a także ich umiędzynarodowienie powodują, że pojedyncze państwa nie są w stanie im zapobiegać. Wymaga to zaangażowania całej społeczności międzynarodowej, w tym i organizacji międzynarodowych powszechnych i regionalnych.

Oznacza to konieczność zbudowania jakościowo nowych narzędzi, które pozwolą na skuteczne zarządzanie, w tym i koordynowanie działań w sytuacjach kryzysowych o charakterze wielosektorowym. Tym samym wymaga to stworzenia systemu monitorowania miejsc o podwyższonym ryzyku, co powinno przekładać się na system powiadamiania i alarmowania na poziomie Unii Europejskiej i państw członkowskich. Przyjęcie właściwego systemu monitorowania i wizualizacji w czasie rzeczywistym sytuacji kryzysowych w państwach członkowskich Unii Europejskiej, a także w jej bliższym i dalszym otoczeniu niewątpliwie przyczyni się do zbudowania skutecznego systemu szybkiego reagowania przy uwzględnieniu posiadanych sił i środków.

5.2. Instytucje międzynarodowe

Unia Europejska, uwzględniając zaangażowanie polityczne, ekonomiczne i wojskowe w środowisku międzynarodowym, wzrastające zagrożenia (naturalne i celowe), konieczność zapewnienia bezpieczeństwa państwom członkowskim i ich obywatelom, zbudowała złożony system monitorowania, powiadamiania i alarmowania, obejmujący zróżnicowane obszary swojej działalności. Jest to proces, w ramach którego doskonalone są już istniejące systemy, a także trwają prace nad uruchomieniem nowych, co wynika m.in. ze skali i dynamiki zagrożeń asymetrycznych. Proces zdobywania, gromadzenia, przetwarzania i dystrybucji danych powinien być realizowany i doskonalony w czasie poprzedzającym sytuację kryzysową.

[26] G. Nowacki, *Rozpoznanie satelitarne USA i Federacji Rosyjskiej*, Warszawa 2002, s. 34.

Dla zarządzania kryzysowego ważnym źródłem informacji są służby wywiadowcze państw członkowskich Unii Europejskiej i Sojuszu Północnoatlantyckiego. Organizacje te nie posiadają ponadnarodowych służb wywiadowczych i kontrwywiadowczych z uprawnieniami do wykonywania czynności operacyjno-rozpoznawczych, dlatego tak ważna jest współpraca i koordynacja pracy o tym charakterze narodowych służb państw członkowskich Unii i NATO. Na podstawie informacji otrzymywanych od służb wywiadowczych państw członkowskich opracowywane są informacje o charakterze niejawnym, które są przekazywane dla uprawnionych podmiotów Unii Europejskiej, Sojuszu Północnoatlantyckiego i poszczególnych państw członkowskich. W NATO obowiązuje centralna ocena informacji wywiadowczych i centralne określanie zadań, natomiast wykonanie tych zadań leży w kompetencji wywiadów poszczególnych państw.

Służby wywiadowcze państw członkowskich Unii i NATO posiadają również dostęp do informacji wywiadowczych zdobytych za pośrednictwem wywiadu satelitarnego, który jest uprawiany przez nieliczne państwa członkowskie.

Obok rozpoznania osobowego (HUMINT), które stanowi podstawowe narzędzie pracy służb wywiadowczych każdego państwa, warto zwrócić uwagę na inne kategorie działalności rozpoznawczej:

- rozpoznanie geoprzestrzenne (GEOIT) oznacza wykorzystywanie analizy obrazów oraz informacji geoprzestrzennych w celu opisania, oceny i wizualizacji cech fizycznych i geograficznych, jakie zachodzą na ziemi;
- rozpoznanie obrazowe (IMINT) umożliwia wytwarzanie danych rozpoznawczych na podstawie zobrazowania pochodzącego ze zdjęć fotograficznych (PHOTINT) radiolokatorów, przyrządów elektrooptycznych pracujących w podczerwieni i termowizyjnych oraz innych urządzeń; aby można było wykorzystać określone dane, przekazany obraz musi być czysty, czytelny i jednoznacznie przedstawić obiekt zainteresowania – wtedy również można szukać potwierdzenia w innych źródłach lub przekazać dane do innych elementów wsparcia informacyjnego,
- rozpoznanie pomiarowe i sygnaturowe (MASINT) obejmuje naukowe i techniczne analizy ilościowe oraz jakościowe parametrów technicznych i charakterystycznych cech uzyskiwanych z przyrządów technicznych w celu identyfikacji źródeł, nadajników, urządzeń promieniujących, umożliwiających dalszą identyfikację i porównanie;
- rozpoznanie sygnałów elektromagnetycznych (SIGINT) jest podstawą wytwarzania danych rozpoznawczych pochodzących z przechwytywania sygnałów elektromagnetycznych[27].

Dla skutecznego zarządzania kryzysowego na terytorium państw członkowskich Unii Europejskiej i NATO, a także na obszarach znajdujących się w ich sferach zainteresowania ważnym źródłem informacji jest wspomniane rozpoznanie satelitarne. Dane z rozpoznania satelitarnego pozwalają na zobrazowanie sytuacji w obszarach zainteresowania w czasie niemal rzeczywistym. Rozpoznanie satelitarne może być prowadzone zarówno w czasie pokoju, kryzysu i wojny.

[27] Ibidem, s. 54 i 55.

Według współczesnych koncepcji nie jest możliwe skuteczne zarządzanie kryzysowe bez zastosowania rozpoznania satelitarnego. Satelity w zależności od przeznaczenia dzielą się na: rozpoznawcze, komunikacyjne, naukowo-badawcze, geofizyczne, astronomiczne, meteorologiczne. Dla zabezpieczenia informacyjnego zarządzania kryzysowego obok rozpoznania satelitarnego ważny jest również udział samolotów wczesnego wykrywania i powiadamiania systemu AWACS. Samoloty tego systemu pełnią rolę powietrznych centrów dowodzenia i kierowania działaniami, zabezpieczają kontrolę i wsparcie informacyjne na szerokim obszarze zainteresowania. Wykonują wymienione zadania na korzyść państw członkowskich Unii Europejskiej i Sojuszu Północnoatlantyckiego. Unia Europejska stworzyła i nadal rozbudowuje systemy powiadamiania i alarmowania, których obszary zainteresowania są zróżnicowane. Należą do nich m.in.: Europejska Agencja Kosmiczna (ESA), Globalny Monitoring dla Środowiska i Bezpieczeństwa (GMES), Centrum Satelitarne Unii Europejskiej (EUSC), Instytut Unii Europejskiej Studiów nad Bezpieczeństwem (ISS), System Wczesnego Ostrzegania i Alarmowania (EWRS), System Wczesnego Powiadamiania i Wymiany Informacji o Zagrożeniach Radiologicznych bądź Nuklearnych (ECURIE), System Ochrony Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej (CIWIN), Bezpieczny Ogólny System Szybkiego Ostrzegania (ARGUS), System Wczesnego Ostrzegania Przed Biologiczno-Chemicznymi Atakami i Zagrożeniami (RAS – BICHAT), System Powiadamiania EUROPOLU, System Ostrzegania przed Wadliwymi Produktami (RAPEX), System Szybkiego Ostrzegania o Niebezpiecznych Produktach Żywnościowych (RASFF), Zintegrowany i Skomputeryzowany System Weterynaryjny (TARCES), Europejski System Wczesnego Powiadamiania i Wymiany Informacji o Zdrowiu Roślin (EUROPHYT), System Zgłaszania Chorób Zwierząt (ADNS), Centrum Monitoringu i Informacji (MIC), Europejska Sieć Umacniania Prawodawstwa (LEN).

1. Europejska Agencja Kosmiczna – międzynarodowa organizacja krajów zachodnioeuropejskich, której celem jest eksploracja i wykorzystanie przestrzeni kosmicznej, planowanie, koordynacja i realizacja wspólnych badań kosmicznych oraz wykorzystywanie sztucznych satelitów Ziemi w celach użytkowych (przede wszystkim w telekomunikacji, meteorologii, teledetekcji). Działalność ESA jest ukierunkowana na uzyskiwanie wiedzy o Ziemi, jej środowisku, Układzie Słonecznym i Wszechświecie, rozwój technologii związanych z badaniami przestrzeni kosmicznej, promowanie europejskiego przemysłu kosmicznego. Realizuje programy, które obejmują: badanie przestrzeni kosmicznej, budowę i wykorzystanie sprzętu służącego badaniom, programy naukowe, badania technologiczne, przepływ informacji o programach kosmicznych. Jest organizacją całkowicie niezależną od Unii Europejskiej, z którą ściśle współpracuje. Uczestniczyła w budowie programu Globalnego Monitoringu dla Środowiska i Bezpieczeństwa (GMES).

2. Globalny Monitoring Środowiska i Bezpieczeństwa[28] ma za zadanie monitorowanie stanu środowiska z pułapu satelitarnego, lotniczego i naziemnego. Zgromadzone za pomocą satelitów oraz pomiarów naziemnych dane są przetwarzane w celu świadczenia usług informacyjnych pozwalających na skuteczniejsze zarządzanie środowiskiem oraz poprawę bezpieczeństwa obywateli Unii Europejskiej. Dzięki temu zapewnia się sprawniejsze reagowanie w przypadku katastrof naturalnych, efektywne korzystanie z zasobów naturalnych, lepszy monitoring jakości i czystości wód, powietrza itd.

Program GMES obejmuje:

- komponent usługowy zapewniający dostęp do informacji obejmujących następujące obszary tematyczne: monitoring obszarów lądowych, zarządzanie kryzysowe, bezpieczeństwo, monitoring środowiska morskiego, monitoring atmosfery, dostosowywanie się do zmian klimatu i łagodzenie ich skutków,
- komponent kosmiczny zapewniający trwałe obserwacje z instalacji kosmicznych na potrzeby obszarów tematycznych;
- komponent *in situ* zapewniający obserwacje z instalacji powietrznych, morskich oraz naziemnych na potrzeby obszarów tematycznych.

Początkowe operacje programu GMES obejmują lata 2011–2013 i składają się z działań w następujących dziedzinach: usługi na potrzeby reagowania kryzysowego, monitorowanie obszarów lądowych, środki na rzecz upowszechnienia usług wśród użytkowników, dostęp do danych, w tym wsparcie dla gromadzenia danych *in situ*, komponent kosmiczny GMES.

Cele operacyjne programu Globalnego Monitoringu Środowiska i Bezpieczeństwa to:

- Usługi na potrzeby reagowania kryzysowego, w oparciu o prowadzone już w Europie działania, zapewnią dostępność danych pochodzących z obserwacji Ziemi i produktów pochodnych dla podmiotów zaangażowanych w reagowanie kryzysowe na poziomie międzynarodowym, europejskim, krajowym i regionalnym w kontekście różnych rodzajów katastrof, w tym klęsk wywołanych zjawiskami meteorologicznymi (np. burz, pożarów i powodzi), klęsk wywołanych zjawiskami geofizycznymi (w tym trzęsień ziemi, tsunami, wybuchów wulkanów i osunięć ziemi), zamierzonych lub przypadkowych katastrof spowodowanych przez człowieka i innych katastrof humanitarnych. Ponieważ zmiany klimatu mogą prowadzić do nasilenia się częstotliwości występowania sytuacji kryzysowych, reagowanie kryzysowe z wykorzystaniem GMES będzie miało kluczowe znaczenie dla wspierania środków dotyczących dostosowania się do zmian klimatu w tym obszarze. GMES odgrywa znaczącą rolę w kontekście europejskich działań na rzecz zapobiegania, gotowości, reagowania i naprawiania szkód.

[28] Program GMES opiera się na badaniach zrealizowanych na mocy decyzji Nr 1982/2006/WE oraz w ramach programu Europejskiej Agencji Kosmicznej dotyczącego komponentu kosmicznego GMES – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 911/2010 z dnia 22 września 2010 roku *w sprawie europejskiego programu monitorowania Ziemi (GMES)* i początkowej fazy jego realizacji (lata 2011–2013) – Dz. U. L 276 z 20.10.2010.

- Usługi monitoringu obszarów lądowych zapewnią dostępność danych pochodzących z obserwacji Ziemi oraz produktów pochodnych dla europejskich, krajowych i regionalnych władz odpowiedzialnych za środowiskowy monitoring różnorodności biologicznej, gleb, wód, lasów i zasobów krajowych, jak również przy ogólnym wdrażaniu polityk w zakresie środowiska, gromadzenia informacji geograficznych, rolnictwa, energii, urbanistyki, infrastruktury i transportu. Usługi w zakresie monitoringu obszarów lądowych obejmować będą monitoring zmiennych dotyczących zmian klimatu.
- Środki na rzecz rozpowszechnienia usług wśród użytkowników obejmują wdrożenie technicznych interfejsów dostosowanych do konkretnych użytkowników pod względem środowiska, a także szkolenie, środki informacyjne i rozwój sektora usług pochodnych.
- Dostęp do danych, w tym wsparcie dla gromadzenia danych *in situ* zapewni, że dane pochodzące z obserwacji Ziemi z szerokiej gamy misji europejskich i innych rodzajów infrastruktury, w tym infrastruktury *in situ*, są gromadzone i udostępniane dla osiągnięcia celów GMES i, w szczególności, usług na potrzeby reagowania kryzysowego i usług monitoringu obszarów lądowych.
- Początkowe operacje GMES zapewnią operacje komponentu kosmicznego GMES, na który składa się rozmieszczona w przestrzeni kosmicznej infrastruktura do obserwacji Ziemi i który ma na celu zapewnienie obserwacji podsystemów Ziemi (w tym powierzchni lądowych, atmosfery i oceanów). Będzie się on opierać na istniejącej i planowanej infrastrukturze kosmicznej, zarówno krajowej, jak i europejskiej, oraz na infrastrukturze kosmicznej stworzonej w ramach programu komponentu kosmicznego GMES[29].

3. Centrum Satelitarne Unii Europejskiej jest odpowiedzialne za przetwarzanie i dostarczanie informacji pochodzących m.in. z analizy obrazów satelitarnych. Zadaniem Centrum jest wspieranie procesów decyzyjnych w dziedzinie Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB) Unii Europejskiej. Obszary zainteresowania w działalności EUSC wynikają z kierunków określonych w *Strategii bezpieczeństwa Unii Europejskiej*. Należą do nich zadania związane z monitorowaniem konfliktów regionalnych państw upadłych, grup przestępczości zorganizowanej, ugrupowań terrorystycznych, procesów związanych z proliferacją broni masowego rażenia. Centrum Satelitarne pełni również rolę wczesnego ostrzegania Unii Europejskiej, umożliwiając typizację, a tym samym daje Wspólnocie szansę zapobiegania możliwym konfliktom zbrojnym i kryzysom humanitarnym.

Przy realizacji powyższych zadań EUSC wspiera działania Unii m.in. w obszarach: bezpieczeństwa ogólnego (nadzór nad obszarami zainteresowania), realizacji zadań petersberskich, wykonywania zadań ratowniczych i humanitarnych, zadań realizowanych z udziałem sił zbrojnych w zarządzaniu kryzysowym. Ponadto wsparcie reali-

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 911/2010 z dnia 22 września 2010 roku w *sprawie europejskiego programu monitorowania Ziemi (GMES)* i początkowej fazy jego realizacji (lata 2011–2013) Dz. U. L 276 z 20.10.2010

zowane przez EUSC dotyczy obszarów: planowania wyprzedzającego, kontroli proliferacji uzbrojenia i broni masowego rażenia, wsparcia ćwiczeń oraz innych działań realizowanych przez państwa członkowskie Unii Europejskiej. Działania operacyjne EUSC realizowane są głównie w formie współpracy z Radą DG VIII, Sztabem Wojskowym UE, Wspólnym Centrum Sytuacyjnym[30].

W działalności Centrum można dopatrzyć się początków przyszłego wywiadu satelitarnego Unii Europejskiej.

4. Instytut Unii Europejskiej Studiów nad Bezpieczeństwem prowadzi badania naukowe nad problematyką bezpieczeństwa i obrony w Unii Europejskiej, a jego podstawowym zadaniem jest przyczynianie się do rozwoju Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB).

5. System Wczesnego Ostrzegania i Alarmowania[31] stanowi sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych w Unii Europejskiej. W państwach członkowskich podmiotem odpowiedzialnym za system EWRS jest Ministerstwo Zdrowia, które do 31 marca każdego roku przedstawia Komisji Unii Europejskiej sprawozdanie dotyczące zdarzeń epidemiologicznych. Każde zdarzenie epidemiologiczne występujące w państwie członkowskim Unii musi być odnotowane w Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) oraz informowany jest o nim Komisarz Unii Europejskiej ds. Zdrowia.

W omawianym systemie EWRS występują trzy poziomy alarmów:

- poziom niski (kolor zielony), służby uruchamiają narodowe elementy systemu,
- poziom średni (kolor żółty), służby uruchamiają część proceduralnych mechanizmów,
- poziom trzeci (czerwony), służby uruchamiają pełne zdolności pomocy zdrowotnej Unii Europejskiej (HEOF) oraz struktury alarmowe Dyrekcji Generalnej ds. Zdrowia i Konsumentów (DG SANCO).

W przypadku wystąpienia zdarzenia o wysokim stopniu zagrożenia dla państwa lub grupy państw członkowskich Unii Europejskiej powiadamiane są Centrum ds. Zapobiegania i Kontroli Chorób (ECDC), Komisarz Unii Europejskiej ds. Zdrowia, inne państwa członkowskie Unii i Światowa Organizacja Zdrowia.

6. System Wczesnego Powiadamiania i Wymiany Informacji o Zagrożeniach Radiologicznych bądź Nuklearnych[32] został utworzony w celu powiadamiania

[30] J. Gryz, *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, Toruń 2009, s. 347.

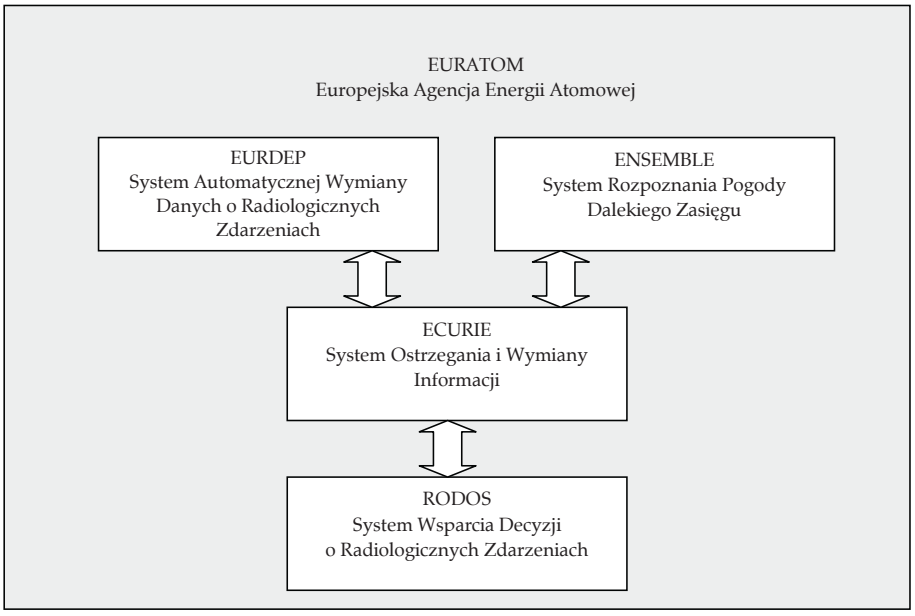
[31] Podstawę prawną sytemu EWRAS stanowi: decyzja Komisji i Parlamentu Europejskiego Nr 2119/98/EC z dnia 24 września 1998 roku o stworzeniu systemu wczesnego ostrzegania i reagowania EWRAS jako sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych we Wspólnocie.

[32] Podstawę prawną funkcjonowania systemu ECURIE stanowią: decyzja Komisji UE Nr 87/600/ EUROATOM *w sprawie utworzenia systemu ECURIE*, decyzja Komisja UE Nr 89/618/ EUROATOM *w sprawie ustalenia narzędzi wykonawczych, członków UE i państw uczestniczących w systemie ECURIE*, umowa między Europejską Wspólnotą Energii Atomowej a państwami nienależącymi do Unii *w sprawie udziału tych ostatnich we wspólnotowych ustaleniach dotyczących wczesnej wymiany informacji w przypadku pogotowia radiologicznego* Nr 2003/C 102.02.

uprawnionych podmiotów państw członkowskich Unii Europejskiej, Chorwacji i Szwajcarii o incydentach w obiektach nuklearnych. System pozwala na uruchomienie przedsięwzięć pozwalających na ochronę ludności. Państwa członkowskie UE i stowarzyszone zobowiązane są do przekazywania informacji o pomiarach promieniowania prowadzonych na własnym terytorium. Europejska Wspólnota Energii Atomowej (EURATOM) pełni rolę organu nadzorczego nad systemem ECURIE. System ten uruchamia się w przypadku zagrożeń radiologicznych, które występują w rejonach obiektów wykorzystujących energię atomową lub w miejscach jej produkcji.

EURATOM jest kluczową jednostką odpowiedzialną za ochronę społeczności Unii Europejskiej przed zagrożeniami radiacyjnymi. W ramach swoich kompetencji zapewnia: wytyczne dla państw członkowskich UE w zakresie ustanowienia standardów bezpieczeństwa radiacyjnego, wczesną i aktualną wymianę informacji w UE i państwach kandydujących, regulacje bezpieczeństwa żywnościowego i jego skażenia radiacyjnego, przekazywanie informacji do wiadomości opinii publicznej państw członkowskich Unii Europejskiej.

Ryc. 1. Miejsce systemu ECURIE w zakresie odpowiedzialności agencji EURATOM



Źródło: Opracowano na podstawie J. Gryz, *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, Toruń 2009, s. 395

Podstawowym celem systemu ECURIE jest ocena zagrożenia społeczeństw państw członkowskich Unii Europejskiej w sytuacji pogotowia radiologicznego:

- z powodu awarii, która nastąpiła na terytorium państwa Unii lub uczestnika programu w wyniku działalności: każdego działającego reaktora jądrowego,

niezależnie od jego lokalizacji, każdego innego obiektu jądrowego, każdego obiektu służącego do zagospodarowania odpadów radioaktywnych, transportu i magazynowania paliw jądrowych i odpadów radioaktywnych, wykorzystania izotopów promieniotwórczych do wytwarzania energii,

- z powodu innych wykrytych awarii, wskutek których wystąpiło znaczne uwolnienie materiału radioaktywnego;
- z wykrycia na terytorium państwa lub poza nim nienormalnych poziomów radioaktywności, które zagrażają bezpieczeństwu publicznemu[33].

Informacje przekazywane w systemie ECURIE dotyczą treści przekazywanych informacji, charakteru i czasu zdarzenia, jego dokładnej lokalizacji oraz związanego z nim obiektu lub rodzaju działalności, zakładanego lub ustalonego powodu i przewidywanego rozwoju awarii, ogólnych właściwości uwalniania materiału radioaktywnego (skład, ilość, typ), warunków meteorologicznych decydujących o dalszym rozwoju sytuacji kryzysowej, wyników monitoringu środowiska, wyników pomiarów radioaktywności w środkach spożywczych, paszach i wodzie, podjętych i planowanych środków ochronnych i środków informowania społecznego, przewidywanych zachowań podczas uwalniania materiału radioaktywnego[34].

Strukturę jednostek specjalistycznych systemu ECURIE stanowią: Krajowe Punkty Kontaktowe, organy centralne państw członkowskich Unii Europejskiej, organy Wspólnoty: Dyrekcja Generalna ds. Energii i Transportu, Dyrekcja Generalna ds. Środowiska, Dyrekcja Generalna ds. Zdrowia i Konsumentów, Dyrekcja Generalna ds. Rolnictwa, Rybołówstwa i Żywności, Wspólne Centrum Badań Naukowych, stałe Centra Awaryjne szczebla krajowego i regionalnego państw członkowskich Unii Europejskiej oraz państw kandydujących i będących użytkownikami systemu ECURIE, platforma informatyczna (sieci, oprogramowania, bazy danych, formy raportów, meldunków), służby reagowania kryzysowego: Stałe Służby Dyżurne, Zespół Reagowania Kryzysowego, Europejskie Biuro Bezpieczeństwa[35].

W ramach systemu ECURIE ważną rolę pełni Komórka Ochrony przed Promieniowaniem i Dyrekcja Generalna ds. Energii i Transportu. Komórka Ochrony przed Promieniowaniem odpowiedzialna jest przed podkomisją Energii Jądrowej za zabezpieczenie techniczne i rozwój wymiany informacji przez komputery wewnętrzne systemu ECURIE. W ramach systemu ECURIE stały dyżur jest pełniony przez: Wspólne Centrum Badawcze, Stałe Służby Dyżurne, Komórkę Ochrony Przed Promieniowaniem, Zespół Reagowania Kryzysowego[36].

Pomiaru skażenia promieniotwórczego w państwach członkowskich Unii Europejskiej dokonują służby meteorologiczne i hydrologiczne, które za pośrednictwem Krajowych Punktów Pomiarowych pobierają próbki ziemi, wody,

[33] J. Gryz, op. cit., s. 391–392.

[34] Ibidem, s. 394.

[35] Ibidem, s. 392–393.

[36] Ibidem, s. 395.

produktów rolnych i żywnościowych. W przypadku stwierdzenia skażenia powiadamiane są (telefonicznie, faksem, pocztą internetową) lokalne i centralne instytucje rozpoznania skażeń oraz służby meteorologiczne i hydrologiczne. Następnie Krajowy Punkt Kontaktowy powiadamia dyżurną służbę ECURIE i Międzynarodową Agencję Energii Atomowej (IAEA).

7. System Ochrony Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej[37] stanowi podstawę wymiany informacji między organami państw członkowskich oraz umożliwia im korzystanie z systemu wczesnego ostrzegania w zakresie ochrony infrastruktury krytycznej. Składa się z trzech zasadniczych poziomów użytkowników: Europejskiego Centrum Ochrony – organu decyzyjnego, Krajowych Punktów Kontaktowych – krajowych punktów wykonawczych, Punktów Kontaktowych sektora prywatnego – prywatnych organów wykonawczych. Użytkownikami systemu CIWIN może być każde państwo członkowskie Unii Europejskiej, państwa graniczące i państwa partnerskie. Przekazywanie informacji w systemie CIWIN obejmuje obszar stałych danych i obszar danych dynamicznych, które służą określonemu celowi. „Zawartość obszaru stałych danych może podlegać zmianom polegającym na nadaniu nowej nazwy lub dodaniu informacji dodatkowej, jednak tych danych nie można usunąć z sieci systemu. Natomiast dane obszaru dynamicznego tworzy się na żądanie i służą określonemu celowi mogą zostać usunięte po wykorzystaniu”[38].

[37] Podstawy prawne systemu CIWIN stanowią: komunikat Komisji UE z dnia 12 grudnia 2006 roku *w spawie Europejskiego Programu Ochrony Infrastruktury Krytycznej* (EPCIP) (COM 2006/786), wniosek Komisji UE z dnia 12 grudnia 2006 roku *w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony* (COM 2006/787), decyzja Rady UE z dnia 8 listopada 2007 roku *w sprawie ustanowienia wspólnotowych mechanizmów ochrony ludności* (2007/779/WE, Euratom), decyzja Rady UE z dnia 14 grudnia 1987 roku *w sprawie wspólnotowych warunków wczesnej wymiany informacji w przypadku zdarzenia radiacyjnego, ustanawiająca wspólnotowy system wczesnego powiadamiania i wymiany informacji w sytuacjach zagrożenia radiacyjnego* (87/600/ Euratom), dyrektywa Rady Nr 82/894/EWG z dnia 21 grudnia 1982 roku *w sprawie zgłaszania chorób zwierząt we Wspólnocie*, dyrektywa Rady z dnia 8 maja 2000 roku *w sprawie środków ochronnych przed wprowadzeniem do Wspólnoty organizmów szkodliwych dla roślin* (2000/29/WE), decyzja Parlamentu Europejskiego i Rady z dnia 24 września 1998 roku *ustanawiająca sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych we Wspólnocie* (2119/98/WE), dyrektywa Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 roku *w sprawie ogólnego bezpieczeństwa produktów* (2001/95/WE), rozporządzenie Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 roku *ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności* (178/2002), decyzja Komisji UE z dnia 19 sierpnia 2003 roku *dotycząca opracowania zintegrowanego skomputeryzowanego systemu weterynaryjnego pod nazwą TRACES* (2003/623/WE), decyzja Komisji z dnia 23 grudnia 2005 roku *zmieniająca regulamin wewnętrzny Komisji* (2006/25/WE, Euratom), Zielona księga *w sprawie rozszerzenia Europejskiego Programu Ochrony Infrastruktury Krytycznej* (EPCIP) przyjęta w dniu 17 listopada 2005 roku *w sprawie konsultacji z państwami członkowskimi Unii Europejskiej oraz przedstawicielami sektora prywatnego.*

[38] J. Gryz, op. cit., s. 409.

Tabela 47. Obszary przekazywania informacji w systemie CIWIN

Obszary przekazywania informacji	
Obszary stałe	Obszary dynamiczne
obszary państw członkowskich umożliwiające uczestniczącym państwom członkowskim stworzenie własnych obszarów w portalu sieci CIWIN	obszar grupy roboczej specjalistów zapewniających wsparcie grupom eksperckim ds. ochrony infrastruktury krytycznej
obszary sektorowe obejmujące 11 oddzielnych sektorów: przemysł chemiczny, energetyka, sektor finansowy, żywność, zdrowie, technologie informacyjne i komunikacyjne, sektor jądrowego cyklu paliwowego, obiekty badawcze, przestrzeń kosmiczna, transport, woda	obszary projektów zawierających informacje na temat projektów finansowanych przez Komisję
obszar organu wykonawczego CIWIN służący jako strategiczna platforma koordynacji i współpracy, mająca na celu propagowanie i usprawnianie działań oraz komunikacji w odniesieniu do ochrony infrastruktury krytycznej	obszary ostrzeżeń, które mogą zostać utworzone jako kanał komunikacyjny podczas działań związanych z ochroną infrastruktury krytycznej
obszar zewnętrznej współpracy Unii Europejskiej ukierunkowany na poprawianie świadomości w zakresie współpracy zewnętrznej dotyczącej ochrony infrastruktury krytycznej i standardów ochrony infrastruktury krytycznej Unii Europejskiej	obszar tematów specjalnych skupiających się na szczególnych zagadnieniach
katalog kontaktów umożliwiających wykorzystywanie danych kontaktowych innych użytkowników CIWIN lub specjalistów z zakresu ochrony infrastruktury krytycznej	

Źródło: Opracowanie własne na podstawie J. Gryz, *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, Toruń 2009, s. 409–410

System Ochrony Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej (CIWIN) funkcjonuje na bazie innych systemów wczesnego ostrzegania, do których zalicza się: Centrum Monitoringu i Informacji (MIC), System Wczesnego Powiadamiania i Wymiany Informacji o Zagrożeniach Radiologicznych bądź Nuklearnych (ECURIE), System Szybkiego Ostrzegania o Niebezpiecznych Produktach Żywnościowych (RASFF), Europejski System Wczesnego Powiadamiania i Wymiany Informacji o Zdrowiu Roślin (EUROPHYT), System Zgłaszania Chorób Zwierząt (ADNS), System Kontroli Obrotu Zwierzętami w Unii Europejskiej (TRACES), System Ostrzegania przed Wadliwymi Produktami (RAPEX), System Powiadamiania EUROPOLU.

8. Bezpieczny Ogólny System Szybkiego Ostrzegania[39] jest systemem wczesnego ostrzegania pozwalającym podjąć niezwłocznie działania przez poszczególne instytucje Unii Europejskiej zgodnie ze specyfiką i rodzajem zagrożenia. System ARGUS składa się z sieci komunikacji wewnętrznej oraz specjalnej proce-

[39] Podstawę funkcjonowania Bezpiecznego Ogólnego Systemu Szybkiego Ostrzegania (ARGUS) stanowi Decyzja Komisji Unii Europejskiej Nr 2006/25/EC z dnia 5 grudnia 2006 roku. Odpowiedzialnymi za system ARGUS są: Zastępca Sekretarza Sekretariatu Generalnego, Główny Oficer Biura Ochrony, Szef Jednostki Programowania i Zabezpieczenia Systemu ARGUS.

dury koordynacyjnej wykonywanej przez Komitet Koordynacji Kryzysowej. Sieć komunikacji wewnętrznej zapewnia dyrekcjom generalnym i służbom Komisji Unii Europejskiej przepływ informacji o występujących sytuacjach kryzysowych o charakterze wielosektorowym, o prawdopodobieństwie ich wystąpienia. Ponadto umożliwia koordynację i dobór odpowiednich środków zaradczych znajdujących się w dyspozycji Komisji UE.

Beneficjenci Bezpiecznego Ogólnego Systemu Szybkiego Ostrzegania to:

Sekretariat Generalny, Dyrekcja Generalna ds. Komunikacji Społecznej, Dyrekcja Generalna ds. Środowiska, Dyrekcja Generalna ds. Zdrowia i Konsumentów, Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa, Dyrekcja Generalna ds. Stosunków Zewnętrznych, Dyrekcja Generalna ds. Pomocy Humanitarnej (obecnie ds. Rozwoju), Dyrekcja Generalna ds. Personelu i Administracji, Dyrekcja Generalna ds. Handlu, Dyrekcja Generalna ds. Informatyki, Dyrekcja Generalna ds. Podatków i Unii Celnej, Wspólne Centrum Badawcze, Służba Prawna. Powyższe Dyrekcje Generalne i Służby mogą zostać uzupełnione innymi dyrekcjami i służbami na ich wniosek po spełnieniu następujących warunków: wyznaczeniu swojego przedstawiciela do Komitetu Koordynacji Kryzysowej systemu, zapewnieniu całodobowych dyżurów pełnionych w systemie przez 7 dni w tygodniu, bezpośredniego kontaktu z podległymi wyspecjalizowanymi sektorowymi służbami, natychmiastowego wykorzystania środków zaradczych w sytuacji kryzysowej[40].

W sytuacji wystąpienia poważnej sytuacji kryzysowej o charakterze wielosektorowym lub groźby jej wystąpienia przewodniczący Komisji Unii Europejskiej podejmuje decyzję o uruchomieniu specjalnej procedury koordynacyjnej. Jednocześnie przewodniczący za pośrednictwem Sekretariatu Generalnego i Komitetu Koordynacji Kryzysowej informuje uprawnione instytucje, a także uruchamia specjalną procedurę operacyjnego zarządzania kryzysowego.

Na uwagę zasługuje Komitet Koordynacji Kryzysowej, Biura Ochrony i Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa, której personel pełni 24-godzinne dyżury przez 7 dni w tygodniu. W sytuacji kryzysowej służby dyżurne za pośrednictwem systemu ARGUS powiadamiają personel poszczególnych zespołów i dyrekcji. O każdej sytuacji kryzysowej informowany jest Sekretarz Generalny Komisji Unii Europejskiej. Ponadto dzięki użyciu systemu informatycznego platformy internetowej ARGUS do poszczególnych Dyrekcji i państw członkowskich Unii Europejskiej trafiają raporty i powiadomienia dotyczące reakcji na zagrożenia. Informowanie jest realizowane w dwóch fazach: wstępnej, określającej charakter zdarzenia i obejmuje informowanie specjalistycznej Dyrekcji (procedura koordynacji i wykorzystania zasobów jednej Dyrekcji), oraz głównej, wykorzystującej system wczesnego ostrzegania podległo Dyrekcjom i środki reagowania kryzysowego (procedura decydowania i zaangażowania kilku Dyrekcji)[41].

[40] J. Gryz, op. cit., s. 360, 361.

[41] Ibidem, s. 363.

Angażowanie środków unijnych reagowania kryzysowego oraz sposób postępowania państw członkowskich Unii w systemie ARGUS zależy od stopnia i skali kryzysu. Jeżeli państwo uczestniczące w systemie nie jest w stanie samodzielnie zareagować na symptomy kryzysu lub zniwelować jego skutków, występuje o pomoc do Unii Europejskiej oraz uruchamia element decyzyjny systemu ARGUS. W tej sytuacji uruchamiana jest faza druga – główna – koordynacji systemu ARGUS[42]. W tych warunkach system pozwala na wykorzystanie narzędzi poszczególnych systemów wczesnego ostrzegania, procedur operacyjnych i instrukcji szczegółowego działania elementów wykonawczych systemu ARGUS zgodnie z decyzjami Przewodniczącego Komisji Europejskiej. Jeżeli państwo członkowskie Unii Europejskiej jest użytkownikiem systemu ARGUS i wystąpi o pomoc unijną, a środki zarządzania kryzysowego znajdują się w dyspozycji tylko jednej Dyrekcji, wówczas uruchamiana jest faza wstępna działania systemu. W przypadku gdy konieczna jest pomoc kilku Dyrekcji, uruchamiana jest faza główna systemu. Przebieg kryzysu jest kontrolowany przez Biuro Ochrony Systemu, które systematycznie przekłada informacje dla użytkowników systemu ARGUS.

Bezpieczny Ogólny System Szybkiego Ostrzegania pozwala przewodniczącemu Komisji Europejskiej na zaangażowanie systemów państw członkowskich Unii Europejskiej oraz współdziałanie z organizacjami o charakterze globalnym, np. ze Światową Organizacją Zdrowia (WHO), co pozwala m.in. na kompleksową wymianę informacji dotyczących zdrowia.

9. System Wczesnego Ostrzegania przed Biologiczno-Chemicznymi Atakami i Zagrożeniami (RAS-BICHAT) jest przeznaczony do ostrzegania przed biologiczno-chemicznymi atakami i zagrożeniami. W ramach systemu określone zostały trzy obszary: pierwszy, dotyczy programu zdrowia publicznego, drugi, obejmuje sieci powiadamiania w zakresie kontroli i prewencji zagrożeń komunikacyjnych, trzeci, obejmuje ochronę zdrowia. Zgodnie z zaleceniami Komisji Unii Europejskiej system RAS – BICHAT musi być zdolny do reagowania na zagrożenia lub ataki środkami biologicznymi lub chemicznymi. W systemie obowiązuje zasada wzajemnego kontaktowania się i wymiany informacji pomiędzy punktami kontaktowymi państw członkowskich Unii Europejskiej i państw stowarzyszonych. W celu uruchomienia systemu w przypadku wystąpienia zagrożenia utworzono: Dyrekcję ds. Zdrowia i Konsumentów, Dyrekcję ds. Zdrowia Publicznego i Oceny Ryzyka, Centrum Komunikacji i Dowodzenia, Biuro Ochrony, Służby Dyżurne, Sztab Reagowania Kryzysowego, Zespół Zarządzania Kryzysowego, Punkty Kontaktowe państw biorących udział w systemie, Punkty Graniczne państw biorących udział w systemie[43].

W sytuacji wystąpienia podwyższonego ryzyka lub próby ataku terrorystycznego państwa uczestniczące w systemie powiadamiają Centrum Komunikacji i Dowodzenia za pośrednictwem Krajowego Punktu Kontaktowego usytuowa-

[42] Ibidem, s. 364.

[43] Ibidem, s. 369.

nego w Ministerstwie Spraw Wewnętrznych. W następstwie tego uruchamiany jest Zespół Zarządzania Kryzysowego, którego zadaniem jest weryfikacja otrzymywanych informacji i przydział w zależności od rodzaju zagrożenia odpowiednich instrumentów. Po zatwierdzeniu środków zaradczych przez Komisję Unii Europejskiej i wyborze neutralizującego systemu, następuje jego aktywacja oraz kontrola działania[44].

W przypadku zagrożenia bezpieczeństwa państwo członkowskie Unii Europejskiej powiadamia nie tylko Centrum Komunikacji i Dowodzenia, ale również Biuro Ochrony w Brukseli lub Dyrekcję ds. Zdrowia i Konsumentów celem powiadomienia Komisji UE. W przypadku poważnego kryzysu uruchamiany jest dodatkowo Sztab Reagowania Kryzysowego, który w sytuacji wybuchu kryzysu w skali globalnej przekazuje informacje do Światowej Inicjatywy Bezpieczeństwa (GHSI), która dysponuje siłami i środkami do walki z terroryzmem stosującym broń biologiczną i/lub broń chemiczną.

10. System powiadamiania EUROPOLU. Europol bezzwłocznie powiadamia jednostki narodowe oraz ich oficerów łącznikowych, o ile jednostki narodowe tego zażądają, o wszelkich informacjach dotyczących ich Państwa Członkowskiego i o ujawnionych powiązaniach między przestępstwami objętymi kompetencją Europolu. Przekazywane mogą być też informacje i dane wywiadowcze dotyczące innych poważnych przestępstw, o których Europol dowiedział się w trakcie wykonywania swych obowiązków.

11. System Ostrzegania przed Wadliwymi Produktami (RAPEX) został utworzony w celu podniesienia bezpieczeństwa produktów oraz poziomu ochrony konsumentów na rynku Unii Europejskiej, a także w celu zapewnienia wysokiego poziomu bezpieczeństwa produktów sprzedawanych na rynkach UE. Wspólnota zobowiązała się do sprawdzania wprowadzanych produktów przez podmioty gospodarcze państw członkowskich Unii Europejskiej i dopuszczania do sprzedaży tylko produktów bezpiecznych. System ostrzegania przed wadliwymi produktami zapewnia możliwość niedopuszczenia do sprzedaży produktów, które mogą doprowadzić do śmierci, utraty zdrowia lub obniżenia bezpieczeństwa klientów Unii Europejskiej. Państwa członkowskie Unii Europejskiej wraz z państwami granicznymi[45] tworzą system ostrzegania ds. bezpieczeństwa produktów współpracy na płaszczyźnie administracyjnej. System ten ma zapewnić: wymianę informacji dotyczących oceny ryzyka, produktów niebezpiecznych, metod badawczych i wyników, odkryć naukowych i czynności kontrolnych Unii Europejskiej, ustanowienie wspólnych projektów nadzoru i badań, wymianę wiedzy specjalistycznej i wiedzy na temat rzetelnych praktyk oraz współpracy w zakresie szkoleń, lepszą współpracę na szczeblu Wspólnoty w aspekcie wykrywania, wycofywania i działania w celu odzyskania niebezpiecznych produktów dla konsumentów[46].

[44] Ibidem.

[45] Państwa graniczne: Islandia, Norwegia, Szwajcaria.

[46] Za J. Gryz, op. cit., s. 371.

Gdy jedno z państw członkowskich Unii Europejskiej podejmie działania prowadzące do ograniczenia lub wycofania niebezpiecznego produktu z rynku zbytu, przekazuje informację o tej decyzji do Komisji i państw członkowskich UE. Informacja powinna zawierać: powody wycofania produktu, wskazanie stosowanych środków zabezpieczających rynek zbytu, wprowadzane wytyczne dla pozostałych państw Unii. Komisja UE po otrzymaniu takiej informacji zobowiązana jest do sprawdzenia jej zgodności z obowiązującymi postanowieniami dyrektywy wprowadzającej system RAPEX. Następnie Komisja przesyła informację o zagrożeniach do pozostałych państw członkowskich Unii Europejskiej[47].

Państwa członkowskie Unii Europejskiej w przekazywanej informacji ostrzegającej muszą podać na stosownym formularzu zgłoszeniowym dane identyfikujące produkt, opis zagrożenia, łącznie z wynikami badań i analiz zagrożenia bezpieczeństwa, charakter i czas trwania środków lub działań zastosowanych w produkcie, informacje o sieciach zaopatrzenia i dystrybucji produktu, w tym kraj przeznaczenia i pochodzenia. Państwo członkowskie UE zgłaszające produkt do wycofania ze sprzedaży musi potwierdzić jego szkodliwość w ciągu 45 dni od daty pierwszego zgłoszenia. W następstwie tego Komisja UE musi w ciągu 3–4 dni rozpatrzyć wniosek państwa zgłaszającego produkt i podjąć właściwe działania neutralizujące.

Komisja Unii Europejskiej od 15 stycznia 2004 roku co trzy lata przedkłada Parlamentowi i Radzie sprawozdanie ze swojej działalności, co wynika z postanowień Dyrektywy Nr 2001/95/EC dotyczącej bezpieczeństwa i ochrony zdrowia.

12. System Szybkiego Ostrzegania o Niebezpiecznych Produktach Żywnościowych (RASFF) został zbudowany w celu informowania państw członkowskich Unii Europejskiej o ryzyku związanym z produktami żywnościowymi i środkami żywienia zwierząt, które nie spełniają wymagań bezpieczeństwa lub poprzez nieprawidłowe oznakowanie stwarzają ryzyko dla konsumentów[48]. Swoim zakresem system obejmuje następujące kategorie produktów: niebezpieczną żywność, niebezpieczną paszę, dozwolone substancje dodatkowe, substancje pomagające w przetwarzaniu żywności, materiały i wyroby przeznaczone do kontaktu z żywnością.

W dniu 28 stycznia 2002 roku rozporządzeniem Parlamentu i Rady Unii Europejskiej Nr 178/2002 powołano do funkcjonowania system powiadamiania o za-

[47] Procedura wycofania produktu przez system i Komisję może trwać od 15 dni do 365 dni. Decyzja o wycofaniu produktu przez Komisję musi być wykonana nie później niż po 20 dniach. Okres przedłożenia opinii producentów i sprzedawców produktów do Komisji może być przedłużony do 1 miesiąca.

[48] System szybkiego ostrzegania obejmujący wymianę informacji istnieje w UE od 1978 roku, kiedy to rozporządzeniem Parlamentu Europejskiego i Rady decyzją Nr 84/133/EEC utworzony został system natychmiastowego powiadamiania o poważnych zagrożeniach życia lub bezpieczeństwa związanego z produktami konsumpcyjnymi. W roku 1992 w związku z rosnącym zagrożeniem bezpieczeństwa żywności decyzją Rady Nr 92/59/EEC określone zostały zasady tworzenia ogólnego poziomu bezpieczeństwa dla wszystkich rodzajów produktów, a także specyfikacja przyszłego systemu ostrzegania obejmującego cały zakres produktów uważanych za pożywienie oraz substancji niebezpiecznych mających kontakt z pożywieniem.

grożeniu żywnościowym, obejmujący aspekty żywienia zwierząt i kontroli towarów i żywności przekraczających granice Unii Europejskiej, określono zadania, strukturę i zasady funkcjonowania systemu, ustanowiono ogólne zasady, procedury i wymagania prawa żywnościowego, powołano Europejski Urząd ds. Bezpieczeństwa Żywności, uczyniono Komisję Unii Europejskiej odpowiedzialną za wymianę informacji między Krajowymi Punktami Kontaktowymi (KPK) państw członkowskich Unii Europejskiej[49].

Każde państwo korzystające z systemu RASFF posiada na swoim terytorium Krajowe Podpunkty Kontaktowe, Graniczne Punkty Kontroli (GPK), które utrzymują łączność z Centralnym Punktem Kontaktowym Unii Europejskiej (CPK). Natomiast Główny Inspektor Sanitarny Europejskiego Urzędu ds. Bezpieczeństwa Żywności posiada łączność z Krajowymi i Granicznymi Punktami Kontroli, które pełnią rolę punktów kontroli na granicach zewnętrznych Unii Europejskiej.

W przypadku pojawienia się produktów zagrażających bezpieczeństwu żywności Krajowy Podpunkt Kontaktowy zobowiązany jest do identyfikacji produktu, oszacowania zagrożenia, uwzględniając przeprowadzone testy i analizy reprezentatywne dla oceny zagrożenia bezpieczeństwa żywności, zebrania danych na temat wyników przeprowadzonych testów, którym został poddany produkt, oraz informacje na temat jego pochodzenia. W takiej sytuacji państwo użytkujące system RASFF przekazuje natychmiast informacje o zagrożeniu do Centralnego Punktu Kontaktowego Unii Europejskiej, które są weryfikowane przez Urząd ds. Bezpieczeństwa Żywności Unii, a następnie sporządzany jest dokument o zagrożeniu w formacie PDF. Na poziomie państw członkowskich Unii siecią systemu RASFF kierują Krajowi Główni Inspektorzy Sanitarni, którzy odpowiedzialni są za funkcjonowanie Krajowego Podpunktu Kontaktowego i przekazywanie informacji w przypadkach stwierdzenia niebezpiecznej żywności lub paszy.

Komisja Unii Europejskiej na podstawie informacji przedłożonych przez państwa członkowskie co roku sporządza raport dotyczący funkcjonowania Systemu Szybkiego Ostrzegania o Niebezpiecznych Produktach Żywnościowych, który m.in. zawiera dane statystyczne (liczbę stwierdzonych incydentów).

Informacje przekazywane w ramach systemu RASFF są sporządzane w postaci formularzy, które zawierają trzy podstawowe rodzaje powiadomień:

- informacyjne – dotyczy produktów, które nie zostały jeszcze wprowadzone na rynek Unii Europejskiej i produktów zakwestionowanych w wyniku obligatoryjnych działań organów urzędowej kontroli żywności szczebla wojewódzkiego, powiatowego lub granicznego, mimo że produkty te nie stanowią bezpośredniego zagrożenia, to jednak istnieje duże prawdopodobieństwo, że mogą zostać ponownie wprowadzone do tego samego lub innego państwa członkowskiego UE; powiadomienie tego rodzaju nie dotyczy produktów zakwestionowanych przez weterynaryjną kontrolę graniczną,

[49] Za J. Gryz, op. cit., s. 374.

- uzupełniające – stanowią dopełnienie uprzednio nadesłanych powiadomień informacyjnych, są konieczne dla podjęcia środków zaradczych,
- o zagrożeniach – dotyczą produktów, które stanowią poważne zagrożenie dla zdrowia, życia obywateli, zwierząt i środowiska UE, wymagają ze strony uprawnionych podmiotów natychmiastowego działania w zakresie kontroli żywności i produktów obecnych na rynku EU[50].

Powiadomienia Systemu Szybkiego Ostrzegania o Niebezpiecznych Produktach Żywnościowych dzielą się według chronologii ich powstania i ze względu na kolejność ich przesłania na: powiadomienia pierwotne, przekazane po raz pierwszy w odniesieniu do konkretnego produktu, powiadomienia dodatkowe, dotyczące przekazanego uprzednio dokumentu, które zawierają ewentualne zmiany wcześniejszych informacji, dodatkowe informacje, niezwiązane bezpośrednio z danym powiadomieniem, ale uzyskane podczas dochodzenia, wycofania lub wprowadzenia produktu na rynek Unii Europejskiej, informacje, które mogą zainteresować właściwe organy[51].

13. Zintegrowany i Skomputeryzowany System Weterynaryjny (TARCES)[52] został utworzony przez Komisję Europejską w celu szybkiego powiadamiania państwa członkowskich o ryzyku dotyczącym transportu zwierząt i produktów zwierzęcych na rynki wewnętrzne Unii i poza nią, a w szczególności transportu: drobiu, żywego bydła i owiec, komórek zwierzęcych, kotów i psów. System udziela pomocy (w tym i certyfikatów) wszystkim władzom weterynaryjnym państw członkowskich i państw graniczących z Unią za pośrednictwem sieci informatycznej w celu poprawy poziomu ochrony sanitarnej w Europie. Do podstawowych zadań systemu TARCES należy:

- stworzenie aktualnej bazy i sieci wymiany informacji o planowanych trasach przewozu zwierząt i produktów od nich pochodzących,
- określenie pozwoleń dla wiarygodnych i sprawdzonych przewoźników Unii Europejskiej,
- wskazanie przydziału pozwoleń jedynie certyfikowanych przez wyspecjalizowane służby fitoweterynaryjne UE dla wspomnianych przewoźników,
- ścisła kontrola jakości przewozów drogą lądową, morską i powietrzną,
- określenie procedur i zasad nadawania pozwoleń transportowych oraz zagrożeń wiążących się z dostarczaniem niebezpiecznych zwierząt i produktów pochodnych,

[50] Za J. Gryz, op. cit., s. 376 i 377.

[51] Ibidem, s. 376 i 377.

[52] System TARCES powstał na mocy Decyzji Komisji Nr 2004/292/WE z dnia 30 marca 2004 roku *w sprawie wprowadzenia systemu TARCES* i zmieniającej Decyzję Komisji Nr 92/486/EWG. Do podstaw prawnych tego systemu zalicza się także decyzję Komisji Europejskiej Nr 92/438/EWG z dnia 13 lipca 1992 roku *o stworzeniu skomputeryzowanego systemu weterynaryjnego i procedurach importu zwierząt do UE*; decyzję Komisji Europejskiej Nr 92/563/EWG z dnia 19 listopada 1992 roku *o stworzeniu baz danych dotyczących przesyłania danych informatycznych i certyfikacji zwierząt i produktów zwierzęcych na wewnętrzne rynki zbytu UE.*

- zapewnienie zdrowia zwierząt państw członkowskich Unii i rynków wewnętrznych Unii poprzez nadawanie certyfikatów jakości zwierząt,
- nadawanie uprawnień zezwalających na wjazd do UE zwierząt i produktów zwierzęcych przez wyspecjalizowane służby fitoweterynaryjne[53].

System wspomaga obrót handlowy żywymi zwierzętami i produktami zwierzęcymi wewnątrz Unii oraz z udziałem państw trzecich. Działa w oparciu o Centralny Punkt Kontaktowy Unii Europejskiej, Krajowe Punkty Kontaktowe i Graniczne Punkty Kontrolne. Wykorzystuje sieć informatyczną CIRCA. Każde państwo użytkujące system TARCES posiada na swoim terytorium Regionalny Organ Władzy (ACR), Lokalny Organ Władzy (ACL) i Graniczne Punkty Kontaktowe, które utrzymują łączność z Właściwym Organem Centralnym Unii Europejskiej (ACC). Państwa trzecie kontaktują się z Regionalnymi Organami Władzy (ACR) i Lokalnymi Organami Władzy (ACL) państw członkowskich w procesie przyznawania certyfikatów na import i eksport zwierząt. Po otrzymaniu zgody na transport zwierząt na rynek wewnętrzny Unii Europejskiej informowane są Punkty Kontroli Granicznej. Kontrola ta pozwala na dokonanie analizy zgodności jakości towaru z przyznanym mu certyfikatem. Gdy jakość towaru nie zostanie potwierdzona, uruchamiany jest system alarmowy do Organów Władzy Centralnej Unii Europejskiej, państw członkowskich UE i państw graniczących z UE. Zaletą Zintegrowanego i Skomputeryzowanego Systemu Weterynaryjnego jest zapobieganie zagrożeniom i wspomaganie zarządzania kryzysowego w Unii.

14. Europejski System Wczesnego Powiadamiania i Wymiany Informacji o Zdrowiu Roślin (EUROPHYT)[54] stanowi system kontroli roślin pochodzących z państw niebędących członkami Unii Europejskiej i niestowarzyszonych. Punkty Kontaktowe systemu EUROPHYT stanowią część narodowych ministerstw rolnictwa, gdzie znajduje się specjalista ds. kontroli roślin. Służby kontroli jakości roślin przez całą dobę sprawdzają produkty w ramach kontroli granicznej. W przypadku zagrożenia uprawniony inspektor badający rośliny w punktach granicznych powiadamia ministerstwo rolnictwa, które alarmuje Komisję i inne państwa członkowskie Unii Europejskiej. W ramach tego systemu wykorzystywane są specjalistyczne jednostki zajmujące się rozpoznaniem bakteriologicznym i wirusowym, a w jego skład wchodzą: Dyrekcja Generalna ds. Zdrowia i Konsumentów, Urząd ds. Bezpieczeństwa Żywności, Urząd Ochrony Odmian Roślin, Dyrekcja ds. Zdrowia i Oceny Ryzyka, Urząd Żywności i Weterynaryjny, Krajowe Punkty Kontaktowe, Specjalistyczne Służby i Inspektoraty odpowiadające za ochronę roślin oraz dystrybucję i przetwarzanie danych[55].

[53] Ibidem, s. 379–380.

[54] Podstawę prawną systemu EUROPHYT stanowi decyzja Komisji Europejskiej Nr 2000/29/EC *w sprawie utworzenia systemu wczesnego ostrzegania o nazwie Europejski System Wczesnego Powiadamiania i Wymiany Informacji o Zdrowiu Roślin.*

[55] J. Gryz, op. cit., s. 390.

15. System Zgłaszania Chorób Zwierząt (ADNS)[56] jest systemem informującym o chorobach zwierząt. Umożliwia państwom członkowskim Unii Europejskiej określenie i przeciwdziałanie zjawisku epidemii zwierząt wewnątrz danego państwa i w Unii, w przypadku wystąpienia epidemii informowanie Komisji UE, która uruchamia procedury alarmowania państw członkowskich, złożenie przez wszystkie państwa członkowskie deklaracji członkowskiej systemu ADNS drogą internetową, wykorzystanie tabel programu Exel jako narzędzia informowania systemu[57]. Ponadto system pozwala na określenie źródła i miejsca epidemii, uaktualnianie i kasowanie informacji o epidemii, odtwarzanie stanu braku epidemii w państwie członkowskim UE, raport biznesowy, tygodniowe powiadomienie, prowadzenie administracji i archiwizacji systemu[58].

Struktura systemu ADNS składa się z następujących podmiotów: Dyrekcji Generalnej ds. Zdrowia i Konsumentów, Dyrekcji Generalnej ds. Zdrowia i Opieki Zwierząt, Krajowych Punktów Kontaktowych Unii Europejskiej, Granicznych Punktów Kontaktowych.

W przypadku wystąpienia epidemii zwierząt na terytorium jednego z państw członkowskich UE, służby weterynaryjne i fitosanitarne tego państwa powiadamiają pozostałe państwa Unii i Unijny Punkt Kontaktowy. Po otrzymaniu potwierdzonej informacji alarmowej państwa członkowskie UE w ciągu 24 godzin wprowadzają właściwe środki ochronne. W każdy piątek o godzinie 15.30 Komisja UE wysyła do państw członkowskich informacje o stanie epidemiologicznym zwierząt na terenie Unii, na podstawie których służby weterynaryjne uruchamiają środki zarządzania kryzysowego. Ponadto w raportach tygodniowych podawane są informacje dotyczące stanu bezpieczeństwa publicznego państw członkowskich UE, zagrożone lub zaatakowane epidemią państwa, charakterystyki hodowli zwierząt, stan sanitarny ubojni zwierząt, stan służb weterynaryjnych, wytyczne polityki Dyrekcji Generalnej ds. Zdrowia i Konsumentów Unii Europejskiej.

16. Centrum Monitoringu i Informacji (MIC)[59] jest strukturą Komisji Europejskiej funkcjonującą w ramach Wspólnotowego Mechanizmu Ochrony Ludności, który może być aktywowany w sytuacjach zagrożeń naturalnych lub spowodowanych przez człowieka. Główne zadania MIC to monitorowanie sytuacji kryzysowych, utrzymywanie stałego kontaktu z punktami kontaktowymi w państwach uczestniczących oraz koordynacja operacji ratowniczych i humanitarnych prowadzonych w ramach Wspólnotowego Mechanizmu Ochrony Ludności.

[56] Podstawę prawną systemu ADNS stanowią decyzja Komisji UE Nr 82/894/EEC z dnia 21 grudnia 1982 roku *w sprawie ustalenia zasad funkcjonowania systemu ADNS* oraz uzupełnienie decyzji Komisji UE nr 2004/216/EC z dnia 1 marca 2004 roku *w sprawie ustalenia zasad i procedur funkcjonowania systemu ADNS*.

[57] J. Gryz, op. cit., s. 399.

[58] Ibidem, s. 400.

[59] Podstawę prawną działania MIC stanowi decyzja Rady z dnia 8 listopada 2007 roku *ustanawiająca wspólnotowy mechanizm ochrony ludności* (2007/779/WE, Euratom).

17. Europejska Sieć Umacniania Prawodawstwa (LEN) została utworzona w celu wzmocnienia nadzoru i przestrzegania prawa w sferze reagowania kryzysowego w Unii Europejskiej i jej państwach członkowskich. Zgodnie z decyzją Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa UE od 2005 roku nadzór nad Europejską Siecią Umacniania Prawodawstwa sprawuje Europol, który sprawuje nadzór nad instytucjami i centrami oraz osobami pełniącymi dyżur w ramach funkcjonujących systemów ostrzegania Unii Europejskiej, a ponadto czuwa nad przestrzeganiem praw w obszarze ostrzegania Unii Europejskiej. Państwa członkowskie zobowiązane są do wskazania punktów, sieci wymiany informacji oraz stron internetowych, które zapewniałyby bezpieczne i zgodne z prawem ich wykorzystywanie w działaniach w zarządzaniu kryzysowym[60].

5.2. Instytucje krajowe

System informacyjny w zarządzaniu kryzysowym powinien zapewniać dopływ informacji dla uprawnionych użytkowników w gminie, powiecie, województwie i państwie z taką częstotliwością i w takich terminach, aby mogły być one wykorzystywane w procesie decyzyjnym na wszystkich poziomach zarządzania kryzysowego.

Tabela 48. Podmioty usytuowane w systemie informacyjnym zarządzania kryzysowego

Podmioty podstawowe	Jednostki nadzorowane
Prezes Rady Ministrów	Rządowe Centrum Bezpieczeństwa Rządowy Zespół Zarządzania Kryzysowego
Wojewoda	Wojewódzkie Centrum Zarządzania Kryzysowego Wojewódzki Zespół Zarządzania Kryzysowego
Starosta/Prezydent Miasta	Powiatowe Centrum Zarządzania Kryzysowego Powiatowy Zespół Zarządzania Kryzysowego
Wójt/Burmistrz	Gminne Centrum Zarządzania Kryzysowego Gminny Zespół Zarządzania Kryzysowego
Ministrowie, Kierownicy urzędów centralnych	Centra i Zespoły Zarządzania Kryzysowego
Kolegium do Spraw Służb Specjalnych	Agencja Bezpieczeństwa Wewnętrznego Agencja Wywiadu Służba Wywiadu Wojskowego Służba Kontrwywiadu Wojskowego Policja Straż Graniczna Żandarmeria Wojskowa Służba Więzienna Biuro Ochrony Rządu Służba Celna Służby rozpoznania Sił Zbrojnych RP

[60] J. Gryz, op. cit., s. 412.

Prezes Rady Ministrów	Agencja Bezpieczeństwa Wewnętrznego Agencja Wywiadu
Minister Spraw Zagranicznych	placówki dyplomatyczne placówki konsularne
Minister Spraw Wewnętrznych	Policja Straż Graniczna Państwowa Straż Pożarna Obrona Cywilna Kraju Biuro Ochrony Rządu
Minister Obrony Narodowej	attaché wojskowy Służba Kontrwywiadu Wojskowego Służba Wywiadu Wojskowego Żandarmeria Wojskowa Służby rozpoznania Sił Zbrojnych RP stacje wczesnego wykrywania skażeń promieniotwórczych Wojskowy Instytut Higieny i Epidemiologii w Warszawie, Zakład Ochrony Radiologicznej i Radiologii Wojskowy Instytut Chemii i Radiometrii w Warszawie, Zakład Pomiarów Dozymetrycznych i Sprzętu Radiometrycznego
Minister Finansów	Służba Celna
Minister Sprawiedliwości	Służba Więzienna
Minister Środowiska	Państwowa Agencja Atomistyki Centralne Laboratorium Ochrony Radiologicznej Centrum Zdarzeń Radiacyjnych Państwowej Agencji Atomistyki stacje wczesnego wykrywania skażeń promieniotwórczych Instytut Meteorologii i Gospodarki Wodnej Centrum Nadzoru Operacyjnego Państwowej Służby Hydrologiczno-Meteorologicznej
Minister Zdrowia	Państwowa Inspekcja Sanitarna Państwowa Inspekcja Farmaceutyczna Państwowy Zakład Higieny
Minister Rolnictwa i Rozwoju Wsi	Główny Inspektor Sanitarny
Minister Gospodarki	Narodowe Centrum Badań Jądrowych Główny Instytut Górnictwa w Katowicach, Laboratorium Radiometrii
Minister Nauki i Szkolnictwa Wyższego	Instytut Fizyki Jądrowej im. H. Niewodniczańskiego w Krakowie Laboratorium Badań Skażeń Radioaktywnych Akademia Górniczo-Hutnicza w Krakowie, Wydział Fizyki i Techniki Jądrowej

Źródło: Opracowanie własne na podstawie obowiązujących regulacji prawnych

Zgodnie z art. 23 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[61] w zależności od skali zagrożenia atakiem o charakterze terrorystycznym lub sabotażowym Prezes Rady Ministrów, ministrowie i kierownicy urzędów centralnych oraz wojewodowie w drodze zarządzenia mogą wprowadzić odpowiedni stopień alarmowy (mogą go również odwołać i zmienić). Rodzaje stopni alarmowych, warunki ich wprowadzenia oraz zadania wykonywane w ramach

[61] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

poszczególnych stopni alarmowych określa się w wykazie, o którym jest mowa w art. 7 ust. 1 ustawy. Wyższy stopień alarmowy może być wprowadzony z pominięciem niższych stopni.

Zadania określone w katalogu stopni alarmowych są realizowane w celu ochrony przed atakiem i przeciwdziałania zagrożeniom atakiem terrorystycznym lub sabotażowym. Stopnie alarmowe mogą być wprowadzane, zmieniane i odwoływane w drodze zarządzenia przez Prezesa Rady Ministrów na obszarze kilku województw lub na całym terytorium Rzeczypospolitej Polskiej, ministra lub kierownika urzędu centralnego w odniesieniu do wszystkich lub wybranych kierowników podległych, podporządkowanych i nadzorowanych jednostek organizacyjnych formacji i urzędów, wojewodę w stosunku do obszarów, obiektów i urządzeń według właściwości miejscowej[62].

Wprowadzanie, zmiany i odwołanie stopnia alarmowego przez wyżej wymienione organy następuje na podstawie pisemnego zalecenia Szefa Agencji Bezpieczeństwa Wewnętrznego. Działające w ramach ABW Centrum Antyterrorystyczne dostarcza informacji o zagrożeniach terrorystycznych lub sabotażowych, co będzie bezpośrednio przekładało się na wprowadzenie odpowiedniego stopnia alarmowego.

W sytuacji zagrożenia atakiem terrorystycznym lub sabotażem wprowadzone zostały cztery stopnie alarmowe.

Pierwszy stopień alarmowy ALFA jest wprowadzany w przypadku uzyskania informacji o możliwości wystąpienia działań terrorystycznych lub sabotażowych, których rodzaj i zakres jest trudny do przewidzenia. Stopień ten ma charakter ogólnego ostrzeżenia, przy czym jego okoliczności nie uzasadniają uruchomienia przedsięwzięć zawartych w wyższych stopniach alarmowych. Organy administracji publicznej i służby właściwe w sferze bezpieczeństwa państwa zobowiązane są do wprowadzenia i utrzymania przedsięwzięć tego stanu na czas nieograniczony.

Drugi stopień alarmowy BRAVO jest wprowadzany w przypadku uzyskania informacji o możliwości wystąpienia działań terrorystycznych lub sabotażowych mogących mieć wpływ na bezpieczeństwo Rzeczypospolitej Polskiej. Stopień ten jest wprowadzany, gdy istnieje zwiększone i bardziej prawdopodobne zagrożenie działalnością terrorystyczną lub aktem sabotażu, jednak cel ataku nie został wskazany. Organy administracji publicznej i służby właściwe w sferze bezpieczeństwa państwa zobowiązane są do utrzymania stopnia alarmowego BRAVO do chwili ustąpienia zagrożenia, co jednak nie powinno zakłócić bieżącej działalności.

Trzeci stopień alarmowy CHARLIE jest wprowadzany, jeżeli miało miejsce konkretne zdarzenie potwierdzające cel ataku terrorystycznego lub w przypadku uzyskania informacji o osobach (grupach) przygotowujących działania terrorystyczne lub sabotażowe stwarzające potencjalne zagrożenie dla Rzeczypo-

[62] W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wrocław 2010, s. 187.

spolitej Polskiej i godzące w bezpieczeństwo innych państw. Stopień alarmowy CHARLIE wymaga ze strony służb właściwych w sferze bezpieczeństwa państwa znacznego wysiłku, to jednak nie powinno mieć wpływu na wykonywanie innych ustawowych zadań.

Czwarty stopień alarmowy DELTA jest wprowadzany w przypadku wystąpienia działań terrorystycznych lub sabotażowych stanowiących zagrożenie dla Rzeczypospolitej Polskiej i godzących w bezpieczeństwo innych państw albo też wysokiego prawdopodobieństwa wystąpienia takich działań na terytorium Polski.

Tabela 49. Stopnie alarmowe

Stopnie alarmowe	Zadania do wykonania
Pierwszy stopień alarmowy ALFA	
Na rzecz ochrony zagrożonej infrastruktury	regularnie informować podległy personel o konieczności zachowania wzmożonej czujności w stosunku do osób zachowujących się w sposób wzbudzający podejrzenia zapewnić dostępność w trybie alarmowym członków personelu niezbędnego do wzmocnienia ochrony obiektu przeprowadzić wzmożone kontrole pojazdów oraz osób wchodzących na teren obiektów ograniczyć w obrębie instytucji ruch pojazdów i osób do niezbędnego minimum regularnie sprawdzać na zewnątrz i od wewnątrz budynki będące w stałym użyciu pod względem osób zachowujących się podejrzanie oraz w poszukiwaniu podejrzanych przedmiotów zamknąć i zabezpieczyć nieużywane regularnie budynki i pomieszczenia sprawdzić działanie środków łączności funkcjonujących w systemie kierowania dokonać przeglądu wszystkich procedur, rozkazów, szczegółowych wymagań osobowych i logistycznych oraz zadań związanych z wprowadzaniem wyższych stanów alarmowych sprawdzić działanie instalacji alarmowych oraz drożność dróg ewakuacji
Na rzecz ochrony ludności	prowadzić wzmożoną kontrolę miejsc dużych skupisk ludzkich, obiektów użyteczności publicznej oraz innych potencjalnych pozamilitarnych obiektów ataku w celu wzmocnienia ochrony informować odpowiednie służby w przypadku zauważenia nieznanych pojazdów na terenie instytucji publicznych lub innych ważnych obiektów, porzuconych paczek i bagaży lub w przypadku zaobserwowania jakichkolwiek innych oznak nietypowej działalności
Drugi stopień alarmowy BRAVO	
Po wprowadzeniu drugiego stopnia alarmowego należy wykonać wszystkie zadania wskazane dla pierwszego stopnia alarmowego, a ponadto:	
Na rzecz ochrony zagrożonej infrastruktury	ostrzec personel o możliwych formach ataku zapewnić dostępność w trybie alarmowym personelu wyznaczonego do wdrażania procedur działania na wypadek aktów terrorystycznych i sabotażowych odsunąć pojazdy oraz wszelkie ruchome obiekty od budynków o szczególnie wrażliwym lub prestiżowym charakterze, rozważyć możliwość wprowadzenia kontroli systemu parkowania

	wzmocnić ochronę ważnych obiektów publicznych oraz sprawdzić systemy ochrony obiektów chronionych przez specjalistyczne, uzbrojone formacje ochronne wzmóc kontrole wszystkich przesyłek pocztowych kierowanych do urzędów (instytucji) dokonać przeglądu stanu posiadanych zapasów materiałowych i sprzętu pod względem sprawności i dostosowania do szacowanych potrzeb poddać kontroli przy wejściu osoby wchodzące na teren obiektu oraz ich bagaże, paczki i inne pojemniki zapewnić ochronę środków transportu służbowego poza terenem obiektu, wprowadzić kontrolę pojazdu przed wejściem do samochodu i jego uruchomieniem
Na rzecz ochrony ludności	wprowadzić nieregularne patrole do kontrolowania pojazdów, ludzi oraz budynków publicznych w rejonach zagrożenia prowadzić akcję informacyjno-instruktażową dla społeczeństwa dotyczącą potencjalnego zagrożenia, jego skutków i sposobu postępowania
Trzeci stopień alarmowy CHARLIE	
Po wprowadzeniu trzeciego stopnia alarmowego należy wykonać wszystkie zadania wymienione dla pierwszego i drugiego stopnia alarmowego, a ponadto:	
Na rzecz ochrony zagrożonej infrastruktury	wprowadzić dyżury dla osób funkcyjnych odpowiedzialnych za wprowadzanie procedur działań na wypadek aktów terroru lub sabotażu ograniczyć do minimum liczbę miejsc ogólnodostępnych w obiekcie (rejonie) w uzasadnionych wypadkach wprowadzić ścisłą kontrolę osób i pojazdów przy wejściu/wjeździe na teren obiektu wprowadzić scentralizowane parkowanie w dużej odległości od najważniejszych obiektów wydać broń i amunicję oraz środki ochrony osobistej uprawnionym osobom wyznaczonym do wykonywania zadań ochronnych wzmocnić służbę ochronną oraz częstotliwość patrolowania obiektów wprowadzić całodobowy nadzór miejsc podlegających ochronie wdrożyć dodatkowe procedury kontrwywiadowczej ochrony i osłony personelu oraz obiektu w placówkach dyplomatycznych poza granicami kraju wdrożyć dodatkowe procedury bezpieczeństwa wynikające z planów ochrony
Na rzecz ochrony ludności	wyznaczyć ochronę organizowanych imprez masowych lub odwołać organizację imprez, jeżeli nie ma możliwości wzmocnienia ochrony lub wzmocnienie nie gwarantuje zapobieżenia atakom terrorystycznym dokonać przeglądu dostępnej bazy i środków medycznych pod kątem możliwości wykorzystania w przypadku ataku terrorystycznego lub sabotażowego zaktualizować bazę danych o alternatywnych możliwościach zaopatrzenia w wodę zweryfikować dane o obiektach wytypowanych dla potrzeb tymczasowego pobytu ludności rozważyć i zdecydować o wdrożeniu dodatkowych przedsięwzięć właściwych dla rodzaju zagrożenia, w zależności od właściwości rzeczowej organu wprowadzającego

Czwarty stopień alarmowy DELTA	
Po wprowadzeniu czwartego stopnia alarmowego należy wykonać wszystkie zadania wymienione dla pierwszego, drugiego i trzeciego stopnia alarmowego, a ponadto:	
Na rzecz ochrony zagrożonej infrastruktury	zabezpieczyć ciągłość pracy zespołów zarządzania kryzysowego (sztabów) przeprowadzić identyfikację wszystkich pojazdów znajdujących się już na terenie obiektu przeszukiwać wszystkie pojazdy wjeżdżające na teren obiektu i ich ładunek, wprowadzić pełną kontrolę obiektu kontrolować wszystkie wnoszone na teren obiektu walizki, torebki i paczki przeprowadzać częste kontrole na zewnątrz budynku i na parkingach ograniczyć liczbę podróży służbowych i wizyt
Na rzecz ochrony ludności	rozważyć i zdecydować o wprowadzeniu ograniczeń komunikacyjnych w rejonach zagrożonych wprowadzić zakaz przeprowadzania imprez masowych zapewnić zaplecze logistyczne oraz medyczno-sanitarne odpowiednio do możliwego zagrożenia

Źródło: Opracowano na podstawie W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy,* Wrocław 2010, s. 190–192

Wprowadzenie powyższych stopni alarmowych ma istotny wpływ na działalność administracji rządowej. Oznacza to konieczność wypracowania i wdrożenia systemu alarmowania włącznie z postępowaniem pracowników co do zachowania po wprowadzeniu jednego z czterech stopni alarmowych.

Ministerstwo Spraw Zagranicznych zobowiązane jest do uczestniczenia w procesie zarządzania kryzysowego, co dotyczy m.in. placówek znajdujących się poza granicami państwa. Według zarządzenia Ministra Spraw Zagranicznych Nr 1 z dnia 3 stycznia 2011 roku *w sprawie systemu bezpieczeństwa placówek zagranicznych*[63] *Rzeczypospolitej Polskiej*[64] stopnie alarmowe stanowią wykaz zaplanowanych czynności do realizacji, których wykonanie ma na celu przeciwdziałanie wszelkim zagrożeniom bezpieczeństwa oraz zapewnienie skuteczności podejmowanych działań w sytuacjach kryzysowych. W sytuacjach kryzysowych wprowadza się odpowiednie do sytuacji stopnie alarmowe:

- Pierwszy stopień alarmowy ALFA wprowadza się po uzyskaniu informacji o możliwości wystąpienia sytuacji kryzysowej w kraju urzędowania lub w kraju trzecim, która ma wpływ na działalność placówki, ale nie na jej obiekty.
- Drugi stopień alarmowy BRAVO wprowadza się w przypadkach zaistnienia:
  a) wysokiego prawdopodobieństwa powstania sytuacji kryzysowej, stanowiącej zagrożenie dla placówki i jej pracowników,

[63] Przez placówki zagraniczne Rzeczypospolitej Polskiej rozumie się przedstawicielstwo dyplomatyczne, stałe przedstawicielstwo przy organizacji międzynarodowej, urząd konsularny, instytut polski lub inną placówkę podległą ministrowi właściwemu do spraw zagranicznych, mającą siedzibę poza granicami Rzeczypospolitej Polskiej w rozumieniu ustawy z dnia 27 lipca 2001 r. *o służbie zagranicznej* (Dz. U. z 2001 r. Nr 128, poz. 1403, z późn. zm.).

[64] Dz. Urz. MSZ 2011 r. Nr 3, poz. 12.

b) bezpośredniego zagrożenia działaniami wojennymi (konfliktem zbrojnym) w państwie przyjmującym,
c) wybuchu konfliktu społecznego w państwie przyjmującym.

- Trzeci stopień alarmowy CHARLIE wprowadza się w przypadkach:
  a) otrzymania informacji o bezpośrednim zagrożeniu dla placówki,
  b) konfliktu zbrojnego na terytorium państwa przyjmującego,
  c) przekształcenia się konfliktów społecznych w państwie przyjmującym w działania o charakterze zbrojnym w skali całego kraju.
- Czwarty stopień alarmowy DELTA w celu przeprowadzenia pełnej planowej ewakuacji placówki oraz jej zamknięcia lub zawieszenia działalności, wprowadza się w przypadkach:
  a) wymuszenia przez państwo przyjmujące zawieszenia wykonywania funkcji placówki,
  b) braku możliwości zażegnania skutków sytuacji kryzysowej za pomocą sił i środków placówki, w wypadku jej długotrwałego charakteru lub eskalacji,
  c) bezpośredniego zagrożenia życia i zdrowia pracowników placówki.

Stopnie alarmowe 1 i 2 wprowadza kierownik placówki po uzgodnieniu z Przewodniczącym Zespołu[65] lub jego Zastępcą, a także dyrektorem komórki organizacyjnej właściwej do spraw bezpieczeństwa dyplomatycznego. Stopnie alarmowe 3 i 4 wprowadza Przewodniczący Zespołu lub jego Zastępca na wniosek kierownika placówki po konsultacji z dyrektorem komórki organizacyjnej właściwej do spraw bezpieczeństwa dyplomatycznego. Stopień alarmowy ogłasza kierownik placówki, powiadamiając wszystkich pracowników, członków ich rodzin oraz inne osoby przebywające w placówce w sposób określony w planie obrony i zarządzania kryzysowego. Stopnie alarmowe mogą być wprowadzane kolejno lub z pominięciem niektórych z nich, z tym że pominięcie niższego stopnia wiąże się z koniecznością realizacji zadań nałożonych na kierownika placówki związanych z wprowadzeniem pominiętych stopni alarmowych.

Odwołania wprowadzonego stopnia alarmowania dokonuje osoba, która go wprowadziła, po ustaniu przyczyny, zgodnie z obowiązującymi procedurami[66].

Wykrywanie skażeń promieniotwórczych zostało uregulowane rozporządzeniem Rady Ministrów z dnia 17 grudnia 2002 roku *w sprawie stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych*[67], które zawiera wykaz stacji wczesnego wykrywania skażeń promieniotwórczych, wykaz placówek prowadzących pomiary skażeń promieniotwórczych, szczegółowe zadania stacji i placówek oraz sposoby wykonywania zadań przez stacje i placówki.

[65] Przewodniczącym Zespołu jest podsekretarz stanu w Ministerstwie Spraw Zagranicznych, do którego zakresu czynności należy zarządzanie kryzysowe (Dz. Urz. MSZ 2011 r. Nr 3, poz. 12).

[66] Zarządzenie Ministra Spraw Zagranicznych Nr 1 z dnia 3 stycznia 2011 roku *w sprawie systemu bezpieczeństwa placówek zagranicznych Rzeczypospolitej Polskiej* (Dz. Urz. MSZ 2011 r. Nr 3, poz. 12).

[67] Dz. U. z 2002 r. Nr 239, poz. 2030.

Wykaz stacji wczesnego wykrywania skażeń promieniotwórczych:

- Stacje podstawowe
  a) działające w Państwowej Agencji Atomistyki oraz w jednostkach ministra właściwego do spraw gospodarki: Białystok (woj. podlaskie), Gdynia (woj. pomorskie), Koszalin (woj. zachodniopomorskie), Kraków (woj. małopolskie), Lublin (woj. lubelskie), Łódź (woj. łódzkie), Olsztyn (woj. mazursko-warmińskie), Sanok (woj. podkarpackie), Szczecin (woj. zachodniopomorskie), Toruń (woj. kujawsko-pomorskie), Warszawa (woj. mazowieckie), Wrocław (woj. dolnośląskie), Zielona góra (woj. lubuskie),
  b) działające w jednostkach ministra właściwego do spraw środowiska: Gdynia (woj. pomorskie), Gorzów Wielkopolski (woj. lubuskie), Legnica (woj. dolnośląskie), Lesko (woj. podkarpackie), Mikołajki (woj. mazursko-warmińskie), Świnoujście (woj. zachodniopomorskie), Warszawa (woj. mazowieckie), Włodawa (woj. Lubelskie), Zakopane (woj. małopolskie).
- Stacje wspomagające
  c) działające w jednostkach Ministra Obrony Narodowej: Bartoszyce (woj. mazursko-warmińskie), Bydgoszcz (woj. mazursko-warmińskie), Gdynia (woj. pomorskie), Kraków (woj. małopolskie), Lublin (woj. lubelskie), Rzeszów (woj. podkarpackie), Śrem (woj. wielkopolskie), Świnoujście (woj. zachodniopomorskie), Szczecin (woj. zachodniopomorskie), Ustka (woj. pomorskie), Warszawa (woj. mazowieckie), Wrocław (woj. dolnośląskie), Żagań (woj. lubelskie).

Wykaz placówek prowadzących pomiar skażeń promieniotwórczych:

- Placówki podstawowe (stacje sanitarno-epidemiologiczne – SSE): Białystok (woj. podlaskie), Łomża (woj. podlaskie), Bydgoszcz (woj. podlaskie), Toruń (woj. podlaskie), Włocławek (woj. podlaskie), Gdańsk (woj. pomorskie), Słupsk (woj. pomorskie), Gorzów Wielkopolski (woj. lubuskie), Zielona Góra (woj. lubuskie), Katowice (woj. śląskie), Bielsko-Biała (woj. śląskie), Częstochowa (woj. śląskie), Kielce (woj. świętokrzyskie), Kraków (woj. małopolskie), Tarnów (woj. małopolskie), Nowy Sącz (woj. małopolskie), Lublin (woj. lubelskie), Zamość (woj. lubelskie), Chełm (woj. lubelskie), Biała Podlaska (woj. lubelskie), Łódź (woj. łódzkie), Piotrków Trybunalski (woj. łódzkie), Skierniewice (woj. łódzkie), Zduńska Wola (woj. łódzkie), Olsztyn (woj. warmińsko-mazurskie), Elbląg (woj. warmińsko-mazurskie), Opole (woj. opolskie), Poznań (woj. wielkopolskie), Kalisz (woj. wielkopolskie), Leszno (woj. wielkopolskie), Piła (woj. wielkopolskie), Konin (woj. wielkopolskie), Rzeszów (woj. podkarpackie), Przemyśl (woj. podkarpackie), Sanok (woj. podkarpackie), Tarnobrzeg (woj. podkarpackie), Szczecin (woj. zachodniopomorskie), Koszalin (woj. zachodniopomorskie), Warszawa (woj. mazowieckie), Ciechanów (woj. mazowieckie), Ostrów Mazowiecka (woj. mazowieckie), Płock (woj. mazowieckie), Radom (woj. mazowieckie), Siedlce (woj. mazowieckie), Wrocław (woj. dolnośląskie), Jelenia Góra (woj. dolnośląskie), Legnica (woj. dolnośląskie), Wałbrzych (woj. dolnośląskie).

- Placówki specjalistyczne: Centralne Laboratorium Ochrony Radiologicznej w Warszawie, Instytut Fizyki Jądrowej im. H. Niewodniczańskiego w Krakowie, Laboratorium Badań Skażeń Radioaktywnych, Państwowy Zakład Higieny w Warszawie, Zakład Ochrony Radiologicznej i Radiobiologii, Akademia Górniczo-Hutnicza w Krakowie, Wydział Fizyki i Techniki Jądrowej, Główny Instytut Górnictwa w Katowicach, Laboratorium Radiometrii, Narodowe Centrum Badań Jądrowych im. Sołtana w Otwocku–Świerku, Służba Ochrony Radiologicznej, Instytut Meteorologii i Gospodarki Wodnej w Warszawie, Wojskowy Instytut Higieny i Epidemiologii w Warszawie, Zakład Ochrony Radiologicznej i Radiologii, Wojskowy Instytut Chemii i Radiometrii w Warszawie, Zakład Pomiarów Dozymetrycznych i Sprzętu Radiometrycznego.

Powoływane rozporządzenie określa również szczegółowe zadania stacji podstawowych i wspomagających (tabela 50), a także zadania placówek podstawowych i placówek specjalistycznych (tabela 51).

Tabela 50. Zadania stacji podstawowych i wspomagających

Zadania
Zadania stacji podstawowych (§ 4)
1) Prowadzenie pomiarów z wykorzystaniem spektrometrii promieniowania gamma, mocy dawki tego promieniowania w celu wykrycia jej wzrostu o wartość 25 nanosiwertów na godzinę (nSv/h) powyżej wartości średniej za okres 24 godzin poprzedzających pomiar, spowodowanego obecnością sztucznych izotopów gamma promieniotwórczych w otoczeniu.
2) Prowadzenie pomiarów z wykorzystaniem spektrometrii promieniowania gamma przez stacje wyposażone w urządzenia służące do zbierania aerozoli atmosferycznych – zawartości sztucznych izotopów w próbkach tych aerozoli, w celu wykrycia: a) po 1 godzinie zbierania aerozoli atmosferycznych – izotopu cezu Cs-137 o stężeniu powyżej 2 bekereli na metr sześcienny (Bq/m^3) i izotopu jodu I-131 o stężeniu powyżej 1 Bq/m^3, b) po 1 tygodniu zbierania aerozoli atmosferycznych – izotopów gamma promieniotwórczych, w szczególności izotopów cezu Cs-137 i jodu I-131, o stężeniu powyżej 5 mikrobekereli na metr sześcienny (Bq/m^3).
3) Prowadzenie pomiarów przez stacje wyposażone w urządzenia służące do zbierania aerozoli atmosferycznych z izotopami alfa i beta promieniotwórczymi – po 1 godzinie zbierania aerozoli całkowitej zawartości sztucznych izotopów alfa i beta promieniotwórczych o stężeniu powyżej 1 Bq/m^3.
4) Systematyczne sprawdzanie prawidłowości działania aparatury pomiarowej służącej do wykonywania pomiarów, o których mowa w pkt 1–3.
5) Prowadzenie rejestru wyników pomiarów, o których mowa w pkt 1–3.
6) Przekazywanie do Centrum do Spraw Zdarzeń Radiacyjnych Państwowej Agencji Atomistyki wyników pomiarów, o których mowa w pkt 1–3, z częstotliwością określoną: dla warunków normalnych – w programach pomiarowych przygotowanych przez jednostki, w których działają te stacje i zatwierdzonych przez Prezesa Państwowej Agencji Atomistyki, dla sytuacji zdarzenia radiacyjnego – przez Prezesa Agencji stosownie do przebiegu tego zdarzenia.
Zadania stacji wspomagających (§ 5)
1) Prowadzenie pomiarów mocy dawki promieniowania gamma co 1 godzinę oraz określanie średniej wartości mocy dawki promieniowania gamma za okres 24 godzin.
2) Systematyczne sprawdzanie prawidłowości działania aparatury pomiarowej służącej do wykonywania pomiarów, o których mowa w pkt 1.
3) Prowadzenie rejestru wyników pomiarów, o których mowa w pkt 1.

4) Przekazywanie do Centrum do Spraw Zdarzeń Radiacyjnych Państwowej Agencji Atomistyki wyników pomiarów, o których mowa w pkt 1, z częstotliwością określoną: a) dla warunków normalnych – w programach pomiarowych przygotowanych przez jednostki, w których działają te stacje i zatwierdzonych przez Prezesa Agencji, b) dla sytuacji zdarzenia radiacyjnego – przez Prezesa Agencji stosownie do przebiegu tego zdarzenia.
Wykonywanie zadania, o którym mowa w § 4 pkt 1, polega na prowadzeniu ciągłego pomiaru mocy dawki na wysokości 1 m nad powierzchnią ziemi, przy wykorzystaniu wyników równoczesnego spektrometrycznego pomiaru promieniowania gamma w powietrzu na tej samej wysokości, z uwzględnieniem temperatury i intensywności opadu atmosferycznego. Wykonywanie zadań, o których mowa w § 4 pkt 2, polega na ciągłym zbieraniu aerozoli atmosferycznych na filtrze, przez który przepływa powietrze atmosferyczne, zasysane na wysokości od 1 m do 1,5 m nad powierzchnią ziemi, prowadzeniu ciągłego pomiaru spektrometrycznego promieniowania gamma emitowanego przez zbierane na filtrze aerozole oraz laboratoryjnym pomiarze spektrometrycznym promieniowania gamma emitowanego przez aerozole osadzone na filtrze po tygodniowym zbieraniu próbki. Wykonywanie zadania, o którym mowa w § 4 pkt 3, polega na ciągłym zbieraniu aerozoli atmosferycznych na filtrze, przez który przepływa powietrze atmosferyczne, zasysane na wysokości od 1 m do 1,5 m nad powierzchnią ziemi oraz prowadzeniu ciągłego pomiaru promieniowania alfa i beta emitowanego przez zebrane w ciągu 1 godziny aerozole atmosferyczne. Wykonywanie zadania, o którym mowa w § 5 pkt 1, polega na prowadzeniu ciągłego pomiaru mocy dawki na wysokości 1 m nad powierzchnią ziemi.

Źródło: Rozporządzenie Rady Ministrów z dnia 17 grudnia 2002 roku *w sprawie stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych* (Dz. U. z 2002 r. Nr 239, poz. 2030)

Tabela 51. Zadania placówek podstawowych i placówek specjalistycznych

Zadania
Zadania placówek podstawowych (§ 7)
1) prowadzenie pomiarów zawartości izotopów promieniotwórczych w próbkach: a) wody powierzchniowej, w szczególności wody z rzek: Wisły, Odry, Bugu, Narwi i Warty, w pobliżu głównych ujęć wody – cezu Cs-137 powyżej 1 bekerela na litr (Bq/l) oraz strontu Sr-90 powyżej 0,6 Bq/l, b) wody do picia z sieci wodociągowej miast polskich stanowiących stolice województw oraz miast o liczbie mieszkańców powyżej 200 000 – cezu Cs-137 powyżej 0,1 Bq/l oraz strontu Sr-90 powyżej 0,06 Bq/l, c) mleka oraz innych produktów żywnościowych, stanowiących podstawowe składniki przeciętnej racji pokarmowej – cezu Cs-137 powyżej 0,5 Bq/l oraz strontu Sr-90 powyżej 0,2 Bq/l, d) pasz surowych – cezu Cs-134 i Cs-137, powyżej 250 Bq/kg.
2) Prowadzenie rejestru pobieranych próbek.
3) Prowadzenie rejestru wyników pomiarów.
4) Uczestniczenie w pomiarach porównawczych organizowanych przez Prezesa Agencji nie rzadziej niż raz w roku.
Próbki, o których mowa w § 7 pkt 1, pobiera się: 1) w warunkach normalnych – w miejscach wskazanych przez Głównego Inspektora Sanitarnego w uzgodnieniu z Głównym Inspektorem Ochrony Środowiska i Prezesem Agencji, nie rzadziej niż: a) dla mleka, produktów żywnościowych i wody do picia – 1 raz na kwartał, b) dla wody rzecznej – 2 razy w roku, w okresie wiosennym i jesiennym; 2) w sytuacji zdarzenia radiacyjnego – w miejscach i z częstotliwością określoną przez Prezesa Agencji stosownie do przebiegu tego zdarzenia.

Zadania placówek specjalistycznych (§ 9 ust. 1)
1) Prowadzenie pomiarów zawartości izotopów promieniotwórczych w próbkach: a) mleka, wody do picia oraz produktów żywnościowych – sztucznych izotopów alfa promieniotwórczych, w szczególności plutonu Pu-239 i ameryku Am-241, powyżej 1 Bq/l lub b) wody powierzchniowej – cezu Cs-137 powyżej 0,1 Bq/l i strontu Sr-90 powyżej 0,06 Bq/l, lub c) wody do picia: – cezu Cs-137 powyżej 0,02 Bq/l i strontu Sr-90 powyżej 0,01 Bq/l lub – wodoru H-3 powyżej 10 Bq/l,lub – naturalnych izotopów alfa promieniotwórczych w przypadku przekroczenia 0,1 Bq/l całkowitej aktywności izotopów alfa promieniotwórczych oraz naturalnych izotopów beta promieniotwórczych w przypadku przekroczenia 1 Bq/l całkowitej aktywności izotopów beta promieniotwórczych lub d) mleka i produktów żywnościowych – sztucznych izotopów gamma promieniotwórczych, w szczególności cezu Cs-137 powyżej 0,1 Bq/kg oraz sztucznych izotopów beta promieniotwórczych, w szczególności strontu Sr-90 powyżej 0,06 Bq/kg lub e) materiałów środowiskowych, w tym: – gleby – cezu Cs-137 powyżej 1 kilobekerela na metr kwadratowy (kBq/m^2) lub – osadów dennych – cezu Cs-137 powyżej 1 Bq/kg oraz izotopów plutonu Pu-238, Pu-239, Pu-240, powyżej 0,1 Bq/kg lub – opadu całkowitego – cezu Cs-137 powyżej 0,05 bekerela na metr kwadratowy razy miesiąc (Bq/m2 x miesiąc) oraz strontu Sr-90 powyżej 0,05 bekerela na metr kwadratowy razy trzy miesiące (Bq/m^2 x 3 miesiące).
2) Prowadzenie rejestru pobieranych próbek.
3) Prowadzenie rejestru wyników pomiarów.
4) Uczestniczenie w pomiarach porównawczych organizowanych przez Prezesa Agencji nie rzadziej niż raz na 2 lata.
5) Opracowywanie projektów technik pomiarowych do oznaczania jakościowego i ilościowego izotopów promieniotwórczych w materiałach środowiskowych i w żywności oraz przedstawianie ich do zatwierdzenia Prezesowi Agencji. Miejsca i częstotliwość pobierania próbek, o których mowa w § 9 ust. 1 pkt 1, oraz zakres pomiarów, określają: 1) dla warunków normalnych – programy pomiarowe przygotowane przez jednostki, w których działają te placówki, i zatwierdzone przez Prezesa Agencji; 2) dla sytuacji zdarzenia radiacyjnego – Prezes Agencji stosownie do przebiegu tego zdarzenia.
1. Wykonywanie zadania, o którym mowa w § 7 pkt 2 i w § 9 ust. 1 pkt 2, polega na prowadzeniu rejestru pobieranych próbek, który zawiera: – określenie rodzaju próbki i sposobu jej przygotowania do pomiaru; – datę oraz godzinę rozpoczęcia i zakończenia pobierania próbki; – informację o miejscu, z którego została pobrana próbka, z podaniem nazwy miejscowości i dokładnego określenia lokalizacji w tej miejscowości. 2. Wykonywanie zadania, o którym mowa w § 4 pkt 5, § 5 pkt 3, § 7 pkt 3 i w § 9 ust. 1 pkt 3, polega na prowadzeniu rejestru wyników pomiarów, który zawiera: – nazwę, adres oraz kod stacji lub placówki wykonującej pomiary, a w przypadku stacji także współrzędne geograficzne jej położenia; – w przypadku stacji wykonujących zadania, o których mowa w § 4 pkt 2 i 3, oraz w przypadku placówek – nazwę i symbol izotopu, którego zawartość jest mierzona; – określenie sposobu prowadzenia pomiaru; – określenie typu aparatury stosowanej do prowadzenia pomiaru oraz rodzaju detektora pomiarowego; – wynik pomiaru z określeniem błędu pomiarowego.
Wykonywanie zadań, o których mowa w § 7 pkt 1 i w § 9 ust. 1 pkt 1, polega w szczególności na zatężaniu pobranych próbek, chemicznym wydzielaniu izotopów oraz pomiarze promieniowania emitowanego przez otrzymane z tych próbek preparaty.

Wyniki pomiaru zawartości izotopów w próbkach, o których mowa w § 7 pkt 1 i w § 9 ust. 1 pkt 1, placówki przekazują do Prezesa Agencji z częstotliwością określoną:
– dla warunków normalnych – w programach pomiarowych przygotowanych przez jednostki, w których działają placówki i zatwierdzonych przez Prezesa Agencji;
– dla sytuacji zdarzenia radiacyjnego – przez Prezesa Agencji stosownie do przebiegu tego zdarzenia.

Źródło: Rozporządzenie Rady Ministrów z dnia 17 grudnia 2002 roku *w sprawie stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych* (Dz. U. z 2002 r. Nr 239, poz. 2030)

Polska infrastruktura informacji geoprzestrzennej. W skład infrastruktury informacji przestrzennej w Polsce wchodzą m.in. Siły Zbrojne Rzeczypospolitej Polskiej, które dysponują Satelitarnym Centrum Operacji Reagowania (SCORA S.A.). Ośrodek ten znajduje się w Komorowie niedaleko Ostrowi Mazowieckiej. Centrum pozwala na przetwarzanie zobrazowań satelitarnych, takich jak mapy, cyfrowe modele terenu czy trójwymiarowe wizualizacje zabudowy miast. Zakłada również prowadzenie specjalistycznych analiz geoprzestrzennych oraz prowadzenie szkoleń z zakresu wykorzystywania zdjęć satelitarnych dla tych jednostek wojska (służby geograficzne, rozpoznanie i wywiad), które są odpowiedzialne za zabezpieczenie sił powietrznych, lądowych i morskich w materiały mapowe, wywiadowcze i operacyjne dla działań w kraju i za granicą.

Satelitarne Centrum Operacji Reagowania ma budować platformy pozwalające na zobrazowanie satelitarne działań związanych z zarządzaniem kryzysowym oraz bezpieczeństwem kraju, jego obywateli i gospodarki. Dzięki tym danym można efektywnie monitorować i rozwiązywać problemy związane z zagrożeniami terrorystycznymi, zaopatrzeniem w surowce energetyczne, udziałem w międzynarodowych programach i członkostwem w międzynarodowych organizacjach.

Centrum zajmuje się dostarczaniem wysokorozdzielczych zobrazowań satelitarnych oraz produktów i usług geoinformatyki klientom w kraju i na świecie. Jest odpowiedzialne za zabezpieczenie Sił Zbrojnych RP w dane teledetekcyjne z obszaru naszego państwa, tzw. bliskiej zagranicy oraz miejsc, gdzie Polska jest lub zamierza być zaangażowana militarnie (Irak, Afganistan, Liban). SCOR S.A. zostało utworzone w 2004 roku przez spółkę giełdową TECHMEX S.A. z udziałem Agencji Mienia Wojskowego.

Wysokorozdzielcze zobrazowania satelitarne są wykorzystywane zarówno dla celów wojskowych jak i cywilnych. Na podstawie danych satelitarnych jest możliwe wykonywanie aktualnych map topograficznych i innych map tematycznych, w tym map zagospodarowania terenu, map leśnych, map pokazujących ukształtowanie powierzchni terenu oraz analiz zmian dokonanych przez człowieka i siły przyrody w zależności od zapotrzebowania konkretnych odbiorców, wykonywanie analiz i studiów morskich terenów przybrzeżnych, w tym wykonywanie map głębokości i torów wodnych oraz wykrywanie płycizn i innych zagrożeń podejść do brzegu oraz charakterystyk dna i stopnia zmętnienia wód, ocenianie i analizowanie współczesnego pola walki w zakresie uzbrojenia, środ-

ków transportu, sprzętu inżynieryjnego czy innego sprzętu wspomagającego, automatycznego wykrywania zmian w rozmieszczeniu sił zbrojnych, wykrywania obiektów zamaskowanych, wykrywanie i analiza morskich i powietrznych środków bojowych, w tym dokładna identyfikacja jednostek morskich i powietrznych, identyfikacja co do kategorii, mniejszych jednostek, identyfikacja i ocena potencjalnych zniszczeń w uzbrojeniu przeciwnika i własnym.

Pozyskane na potrzeby wojska dane geoprzestrzenne są również ważnym źródłem informacji dla procesu zarządzania w administracji cywilnej i gospodarce. Przyjmuje się, że 80% rozstrzygnięć na wszystkich poziomach zarządzania podejmowanych jest na podstawie informacji zawierających komponent przestrzenny związany z informacją o ziemi i jej zagospodarowaniu. Dane geoprzestrzenne są wykorzystywane m.in. w cywilnych procedurach reagowania na akty terroryzmu, zarządzania kryzysowego, ratownictwa medycznego i ekologicznego.

Państwowy Monitoring Środowiska (PMŚ) został utworzony ustawą z dnia 20 lipca 1991 roku *o Inspekcji Ochrony Środowiska*[68] w celu zapewnienia wiarygodnych informacji o stanie środowiska. W ramach niego realizowane są zadania wynikające z odrębnych ustaw, zobowiązań międzynarodowych Rzeczypospolitej Polskiej oraz innych potrzeb wynikających z polityki ekologicznej państwa. Ustawa z dnia 27 kwietnia 2001 roku *Prawo ochrony środowiska* stanowi, że Państwowy Monitoring Środowiska jest systemem pomiarów, ocen i prognoz stanu środowiska oraz gromadzenia, przetwarzania i rozpowszechniania informacji o środowisku[69]. Gromadzone informacje służą wspomaganiu działań na rzecz ochrony środowiska poprzez systematyczne informowanie organów administracji i społeczeństwa o jakości elementów przyrodniczych, dotrzymywaniu standardów jakości środowiska lub innych poziomów określonych przepisami oraz obszarów występowania przekroczeń tych standardów lub innych wymagań, a także o występujących zmianach jakości elementów przyrodniczych, przyczynach tych zmian, w tym powiązaniach przyczynowo-skutkowych występujących pomiędzy emisjami i stanem elementów przyrodniczych.

Ustawowe cele Państwowego Monitoringu Środowiska są realizowane poprzez zadania cząstkowe obejmujące wykonywanie badań wskaźników charakteryzujących poszczególne komponenty środowiska, prowadzenie obserwacji elementów przyrodniczych, gromadzenie i analizę wyników badań i obserwacji, pozyskiwanie informacji o presjach na poszczególne elementy środowiska, ocenę stanu i trendów zmian jakości poszczególnych elementów środowiska w oparciu o ustalone kryteria, identyfikację obszarów przekroczeń standardów jakości środowiska, analizy przyczynowo-skutkowe, opracowywanie zestawień, raportów, komunikatów i ich udostępnianie w formie drukowanej lub zapisu elektronicznego[70].

[68] Dz. U. z 2007 r. Nr 44, poz. 287 z późn. zm.

[69] Ustawa z dnia 27 kwietnia 2001 roku *Prawo ochrony środowiska* (Dz. U. z 2008 r. Nr 25, poz. 150, z późn. zm.), art. 25 ust. 1.

[70] *Program Państwowego Monitoringu Środowiska na lata 2010–2012*, Warszawa 2009, s. 8.

W ramach Państwowego Monitoringu Środowiska podejmowane są działania mające na celu poprawę dostępu do danych PMŚ, stworzenie możliwości wizualizacji gromadzonych informacji, wykorzystanie techniki zobrazowania satelitarnego (GMES) oraz szersze wykorzystanie modelowania matematycznego do wspomagania systemu ocen i prognoz poprzez interpretację danych pomiarowych z zastosowaniem systemu informacji geograficznej (GIS)[71]. Informacje wytwarzane przez Inspekcję Ochrony Środowiska są stopniowo dostosowywane do wymogów dyrektywy Parlamentu Europejskiego i Rady 2007/2/WE z dnia 14 marca 2007 roku *ustanawiającej infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej* (INSPIRE)[72].

PMŚ obejmuje uzyskiwanie na podstawie badań monitoringowych informacji w zakresie jakości powietrza, wód śródlądowych powierzchniowych i podziemnych oraz morskich wód wewnętrznych i wód morza terytorialnego, gleby i ziemi, hałasu, promieniowania jonizującego i pól elektromagnetycznych, stanu zasobów środowiska, w tym lasów, rodzajów i ilości substancji lub energii wprowadzanych do powietrza, wód, gleby i ziemi, wytwarzania i gospodarowania odpadami[73]. Badania monitoringowe są przeprowadzane w sposób cykliczny, stosując ujednolicone metody zbierania, gromadzenia i przetwarzania danych. W systemie monitorowania środowiska są gromadzone i sporządzane dane dotyczące stanu środowiska, do których przekazywania Rzeczypospolita Polska jest obowiązana na mocy zobowiązań międzynarodowych.

Państwowy monitoring środowiska zbiera dane na podstawie:

- pomiarów dokonywanych przez organy administracji, zobowiązane na podstawie ustawy do wykonywania badań monitoringowych,
- danych zbieranych w ramach statystyki publicznej, określanych corocznie w programach badań statystycznych statystyki publicznej,
- informacji udostępnionych przez inne organy administracji,
- pomiarów stanu środowiska, wielkości i rodzajów emisji, a także ewidencji, do których prowadzenia zobowiązane są podmioty z mocy prawa albo na mocy decyzji,
- innych niż wymienione w pkt. 4 informacji, uzyskanych odpłatnie lub nieodpłatnie od podmiotów niebędących organami administracji[74].

Zasady funkcjonowania państwowego monitoringu środowiska oraz zadania organów Inspekcji Ochrony Środowiska w zakresie jego koordynacji określają przepisy ustawy z dnia 20 lipca 1990 roku *o Inspekcji Ochrony Środowiska*.

Podmioty korzystające ze środowiska, zobowiązane z mocy prawa oraz na mocy decyzji do pomiaru poziomu substancji lub energii w środowisku oraz wielkości emisji, gromadzą i przetwarzają dane z zachowaniem zasad określo-

[71] Ibidem, s. 8.

[72] Dz. Urz. UE L 108 z 25.04.2007, s. 1.

[73] Ustawa z dnia 27 kwietnia 2001 roku *Prawo ochrony środowiska* (Dz. U. z 2008 r. Nr 25, poz. 150, z późn. zm.), art. 26 ust. 1.

[74] Ibidem, art. 27 ust. 1.

nych w ustawie i nieodpłatnie udostępniają informacje na potrzeby państwowego monitoringu środowiska[75].

Organy administracji, które zobowiązane są do wykonywania badań monitoringowych, mają obowiązek wzajemnego, nieodpłatnego udostępniania informacji o środowisku, i tak:

- organy Inspekcji Ochrony Środowiska udostępniają nieodpłatnie organom Państwowej Inspekcji Sanitarnej gromadzone w ramach państwowego monitoringu środowiska dane zawierające wyniki pomiarów,
- inne organy administracji dysponujące informacjami, które mogą być wykorzystane na potrzeby państwowego monitoringu środowiska, są obowiązane do ich nieodpłatnego udostępniania uprawnionym organom[76].

Prowadzenie państwowego monitoringu środowiska należy do zadań Inspekcji Ochrony Środowiska[77], którego podstawę prawną stanowi ustawa z dnia 20 lipca 1991 roku *o Inspekcji Ochrony Środowiska*, w zakresie: opracowywania programów państwowego monitoringu środowiska, koordynacji realizacji zadań państwowego monitoringu środowiska, gromadzenia informacji o środowisku w zakresie ujętym w programach państwowego monitoringu środowiska, przetwarzania zgromadzonych informacji o środowisku i dokonywania ocen stanu środowiska, opracowywania raportów o stanie środowiska, udziału w międzynarodowej wymianie informacji o stanie środowiska, w tym koordynacji współpracy z Europejską Agencją Środowiska, o której jest mowa w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 401/2009 z dnia 23 kwietnia 2009 r. w sprawie Europejskiej Agencji Środowiska oraz Europejskiej Sieci Informacji i Obserwacji Środowiska[78].

Państwowy monitoring środowiska realizowany jest na podstawie wieloletnich programów państwowego monitoringu środowiska opracowywanych przez Głównego Inspektora Ochrony Środowiska i zatwierdzanych przez ministra właściwego do spraw środowiska, wojewódzkich programów monitoringu opracowywanych przez wojewódzkiego inspektora ochrony środowiska i zatwierdzanych przez Głównego Inspektora Ochrony Środowiska[79]. Programy państwowego monitoringu środowiska obejmują dla poszczególnych elementów środowiska zadania krajowe, regionalne (wojewódzkie i międzywojewódzkie) oraz lokalne. Działalność państwowego monitoringu środowiska koordynują organy Inspekcji Ochrony Środowiska, w tym: Główny Inspektor Ochrony Środowiska – zadania krajowe i regionalne, Wojewódzki Inspektor Ochrony Środowiska, w uzgodnieniu z Głównym Inspektorem Ochrony Środowiska – zadania

[75] Ibidem, art. 28.

[76] Ibidem, art. 29.

[77] Ustawa z dnia 20 lipca 1991 r. *o Inspekcji Ochrony Środowiska* (T. j.: Dz. U. z 2007 r. Nr 44, poz. 287, z późn. zm.), art. 2 ust. 2.

[78] Dz. Urz. UE L 126 z 21 maja 2009 roku s. 13.

[79] Ustawa z dnia 20 lipca 1991 r. *o Inspekcji Ochrony Środowiska* (T. j.: Dz. U. z 2007 r. Nr 44, poz. 287, z późn. zm.), art. 23.

lokalne[80]. Organy administracji rządowej oraz samorządowej prowadzące rejestry, wykazy, pomiary, analizy i obserwacje stanu środowiska są zobowiązane do nieodpłatnego udostępniania danych o stanie środowiska uzyskanych w trakcie ich działalności dla potrzeb państwowego monitoringu środowiska. Informacje o środowisku i jego ochronie na obszarze województwa objęte państwowym monitoringiem środowiska są gromadzone przez Wojewódzkich Inspektorów Ochrony Środowiska i przekazywane Głównemu Inspektorowi Ochrony Środowiska. Główny Inspektor Ochrony Środowiska ustala sposób gromadzenia i przetwarzania danych oraz zakres i sposób przekazywania informacji[81]. Ponadto opracowuje, nie rzadziej niż raz na 4 lata, raport o stanie środowiska w Polsce, uwzględniając w szczególności dane z państwowego monitoringu środowiska.

Informacje wytworzone w ramach PMŚ wykorzystywane są przez jednostki administracji samorządowej i rządowej dla potrzeb operacyjnego zarządzania środowiskiem za pomocą instrumentów prawnych, takich jak postępowanie w sprawie oceny oddziaływania na środowisko, pozwolenia na wprowadzanie do środowiska substancji lub energii, programy i plany ochrony środowiska jako całości i jego poszczególnych elementów, plany zagospodarowania przestrzennego[82]. Informacje wykorzystywane są także do celów monitorowania skuteczności działań i strategicznego planowania w zakresie ochrony środowiska. Ponadto są podstawą do strategicznych ocen oddziaływania na środowisko oraz służą do planowania zrównoważonego rozwoju na wszystkich poziomach zarządzania. Dodatkowo wykorzystywane są dla potrzeb związanych z rozwojem regionalnym, a także wykorzystaniem funduszy strukturalnych i funduszy spójności[83].

Z punktu widzenia skuteczności zarządzania kryzysowego informacje znajdujące się w systemie państwowego monitoringu środowiska wykorzystywane są w procesie planistycznym, decyzyjnym i wykonawczym, co wpływa na poziom bezpieczeństwa obywateli. Oczywiście należy mieć świadomość tego, że zagrożenia monitorowane przez omawiany system (PMŚ) co do rejonu kraju są zróżnicowane.

System Informacji Przestrzennej (SIP) to system pozyskiwania, przetwarzania i udostępniania danych, zawierających informacje przestrzenne oraz towarzyszące im informacje opisowe o obiektach wyróżnionych w części przestrzeni objętej jego działaniem. Podstawą funkcjonowania jest zgromadzenie odpowiednich danych o obiektach świata rzeczywistego. Dane te, opisujące cechy poszczególnych obiektów, nazywane są atrybutami. Ze względu na rodzaj przechowywanej w atrybutach informacji, dzielimy je na przestrzenne – określające położenie, wielkość i geometryczny kształt obiektów oraz ich przestrzenne (topologiczne) relacje oraz opisowe – określające nieprzestrzenne właściwości i relacje obiektów.

[80] Ibidem, art. 24 .

[81] Ibidem, art. 25a.

[82] *Program Państwowego Monitoringu Środowiska*…, op. cit., s. 7.

[83] Ibidem, s. 7.

W Polsce dostęp do informacji przestrzennej reguluje ustawa z dnia 4 marca 2010 roku *o infrastrukturze informacji przestrzennej*[84]. Ustawa określa zasady tworzenia oraz użytkowania infrastruktury informacji przestrzennej[85] oraz właściwość organów administracji. Zasady tworzenia i użytkowania infrastruktury informacji przestrzennej[86] dotyczą:

- danych przestrzennych[87] i metadanych infrastruktury informacji przestrzennej[88],
- usług danych przestrzennych,
- interoperacyjności zbiorów danych przestrzennych i usług danych przestrzennych,
- wspólnego korzystania z danych przestrzennych,
- współdziałania i koordynacji w zakresie infrastruktury informacji przestrzennej.

Infrastruktura informacji przestrzennej obejmuje zbiory danych przestrzennych odnoszące się do terytorium Rzeczypospolitej Polskiej lub z nim powiązane, występujące w postaci elektronicznej, utrzymywane przez organ administracji lub w jego imieniu, które zgodnie z jego zadaniami publicznymi są tworzone, aktualizowane i udostępniane, lub osobę trzecią, której umożliwiono włączenie się do infrastruktury, należące co najmniej do jednego z tematów danych przestrzennych określonych w załączniku do ustawy z dnia 4 marca 2010 roku *o infrastrukturze informacji przestrzennej*[89].

Organy administracji prowadzące rejestry publiczne, które zawierają zbiory związane z wymienionymi w załączniku do ustawy tematami danych przestrzennych, tworzą i obsługują, w zakresie swojej właściwości, sieć usług dotyczących zbiorów i usług danych przestrzennych, do których zalicza się:

- wyszukiwanie, umożliwiające wyszukiwanie zbiorów oraz usług danych przestrzennych na podstawie zawartości odpowiadających im metadanych oraz umożliwiające wyświetlanie zawartości metadanych,
- przeglądanie, umożliwiające co najmniej: wyświetlanie, nawigowanie, powiększanie i pomniejszanie, przesuwanie lub nakładanie na siebie zobrazo-

[84] Dz. U. z 2010 r. Nr 76, poz. 489.

[85] „Infrastruktura informacji przestrzennej, to opisane metadanymi zbiory danych przestrzennych oraz dotyczące ich usługi, środki techniczne, procesy i procedury, które są stosowane i udostępniane przez współtworzące infrastrukturę informacji przestrzennej organy wiodące, inne organy administracji oraz osoby trzecie" – art. 3 pkt 2 ustawy z dnia 4 marca 2010 roku *o infrastrukturze informacji przestrzennej* (Dz. U. z 2010 r. Nr 76, poz. 489).

[86] Ustawa z dnia 4 marca 2010 roku *o infrastrukturze informacji przestrzennej* (Dz. U. z 2010 r. Nr 76, poz. 489), art. 1 ust. 2.

[87] „Dane przestrzenne, to dane odnoszące się bezpośrednio lub pośrednio do określonego położenia lub obszaru geograficznego" – ibidem, art. 3 pkt 1.

[88] „Metadane infrastruktury informacji przestrzennej, to informacje, które opisują zbiory danych przestrzennych oraz usługi danych przestrzennych i umożliwiają odnalezienie, inwentaryzację i używanie tych danych i usług" – ibidem, art. 3 pkt 4.

[89] Ibidem, art. 4 ust. 1.

wanych zbiorów oraz wyświetlanie objaśnień symboli kartograficznych i zawartości metadanych,
- pobieranie, umożliwiające pobieranie kopii zbiorów lub ich części oraz, gdy jest to wykonalne, bezpośredni dostęp do tych zbiorów,
- przekształcanie, umożliwiające przekształcenie zbiorów w celu osiągnięcia interoperacyjności zbiorów i usług danych,
- uruchamianie usług danych[90].

Powszechny dostęp do zbiorów i usług nie dotyczy danych, które ze względu na wiążące Rzeczpospolitą Polską umowy międzynarodowe, bezpieczeństwo publiczne lub bezpieczeństwo państwa uznane zostały za niejawne lub dostęp do tych danych podlega ograniczeniom na podstawie odrębnych przepisów[91].

Zbiory oraz usługi danych przestrzennych, prowadzone przez organ administracji, podlegają nieodpłatnemu udostępnianiu innym organom administracji w zakresie niezbędnym do realizacji przez nie zadań publicznych. Organy administracji udostępniają zbiory oraz usługi danych przestrzennych również organom administracji z innych państw członkowskich Unii Europejskiej oraz instytucjom i organom Unii Europejskiej na potrzeby zadań publicznych, które mogą oddziaływać na środowisko, z zachowaniem przepisów dotyczących rejestrów publicznych, do których odnoszą się te zbiory i usługi[92]. Czynności te są realizowane na zasadach wzajemności i równości.

Zgodnie z ustawą z dnia 17 maja 1989 r. *Prawo geodezyjne i kartograficzne* dla obszaru całego kraju zakłada się i prowadzi w systemie teleinformatycznym bazy danych, obejmujące zbiory danych przestrzennych infrastruktury informacji przestrzennej, dotyczące:
- państwowego rejestru podstawowych osnów geodezyjnych, grawimetrycznych i magnetycznych,
- ewidencji gruntów i budynków,
- geodezyjnej ewidencji sieci uzbrojenia terenu,
- państwowego rejestru granic i powierzchni jednostek podziałów terytorialnych kraju,
- państwowego rejestru nazw geograficznych,
- ewidencji miejscowości, ulic i adresów,
- rejestru cen i wartości nieruchomości,
- obiektów topograficznych o szczegółowości zapewniającej tworzenie standardowych opracowań kartograficznych w skali 1:10 000–1: 100 000, w tym kartograficznych opracowań numerycznego modelu rzeźby terenu,
- obiektów ogólnogeograficznych o szczegółowości zapewniającej tworzenie standardowych opracowań kartograficznych w skali 1:250 000 i mniejszych, w tym kartograficznych opracowań numerycznego modelu rzeźby terenu,
- szczegółowych osnów geodezyjnych,

[90] Ibidem, art. 9 ust. 1.

[91] Ibidem, art. 11.

[92] Ibidem, art. 15 ust. 1.

– zobrazowań lotniczych i satelitarnych oraz ortofotomapy i numerycznego modelu terenu[93].

Z punktu widzenia zarządzania kryzysowego należy zwrócić uwagę na załącznik do ustawy z dnia 4 marca 2010 roku *o infrastrukturze informacji przestrzennej*, który zawiera tematy danych przestrzennych – zob. tabela 52.

Tabela 52. Tematy danych przestrzennych

Grupy tematyczne	Szczegółowe tematy
Pierwsza	nazwy geograficzne jednostki administracyjne adresy działki ewidencyjne sieci transportowe hydrografia obszary chronione
Druga	ukształtowanie terenu użytkowanie ziemi otoobrazy* geologia
Trzecia	jednostki statystyczne budynki gleba zagospodarowanie przestrzenne zdrowie i bezpieczeństwo ludności usługi użyteczności publicznej i służby państwowe urządzenia do monitorowania środowiska obiekty produkcyjne i przemysłowe obiekty rolnicze i akwakultury rozmieszczenie ludności, demografia gospodarowanie obszarem, strefy ograniczone i regulacyjne oraz jednostki sprawozdawcze strefy zagrożenia naturalnego warunki atmosferyczne, warunki meteorologiczno-geograficzne warunki oceanograficzno-geograficzne obszary morskie regiony biogeograficzne osiedliska i obszary przyrodnicze jednorodne rozmieszczenie gatunków zasoby energetyczne zasoby mineralne

* „Otoobrazy, to dane obrazowe powierzchni ziemi mające odniesienie przestrzenne, pochodzące z rejestracji lotniczej lub satelitarnej" – załącznik do ustawy z dnia 4 marca 2010 roku *o infrastrukturze informacji przestrzennej* (Dz. U. z 2010 r. Nr 76, poz. 489)

Źródło: Załącznik do ustawy z dnia 4 marca 2010 roku *o infrastrukturze informacji przestrzennej* (Dz. U. z 2010 r. Nr 76, poz. 489)

Istotą infrastruktury informacji przestrzennej jest możliwość prowadzenia analiz o charakterze przestrzennym. System ten został stworzony przede wszyst-

[93] Ustawa z dnia 17 maja 1989 r. *Prawo geodezyjne i kartograficzne* (Dz. U. z 2005 r. Nr 240, poz. 2027, z późn. zm.), art. 4 ust. 1a.

kim dla usprawnienia procesu uzyskiwania odpowiedzi m.in. na następujące pytania: gdzie to jest? co znajduje się w tym, a co w tamtym miejscu? co znajduje się w pobliżu tych miejsc? czy występowanie określonych zjawisk jest w jakiś sposób powiązane przestrzennie? jak zmienia się ono w czasie i przestrzeni? czy gdzieś występują warunki, by zaistniało określone zjawisko?[94]

Omawiany system od zwykłych baz danych odróżnia możliwość zadawania zapytań przestrzennych, czyli takich, na które odpowiedź nie jest możliwa bez wykorzystania informacji o położeniu obiektów i relacjach przestrzennych, w jakich obiekty te pozostają (czyli bez topologii).

Analizy w systemach informacji przestrzennej podzielić można na trzy zasadnicze grupy: zapytania do bazy danych, sporządzanie map pochodnych, modelowanie.

Baza danych infrastruktury informacji przestrzennej jest fragmentem realnej rzeczywistości przeniesionym do komputera. Pozwala to na modelowanie w środowisku tej infrastruktury procesów zachodzących w otaczającym nas świecie, czyli daje możliwość dokonywania symulacji i optymalizacji. Składa się ona z kilku grup modułów realizujących odrębne funkcje. Są to procedury: wprowadzania i weryfikacji danych wejściowych, zarządzania i przetwarzania w obrębie bazy danych (system zarządzania bazą danych), przetwarzania i analizy danych geograficznych, wyjściowe: prezentacji graficznej, kartograficznej i tekstowej danych, komunikacji z użytkownikiem.

Dla procesu zarządzania kryzysowego informacje, których źródłem jest infrastruktura informacji przestrzennej, ma istotne znaczenie z uwagi na możliwość ich wykorzystywania m.in. przez Krajowy System Ratowniczo-Gaśniczy, siły zbrojne, inne uprawnione podmioty.

Służby specjalne. Skuteczne zarządzanie kryzysowe wymaga dostępu do informacji o zjawiskach i zdarzeniach występujących zarówno w otoczeniu wewnętrznym, jak i zewnętrznym państwa. Specyfika systemu decyzyjnego związana z zarządzaniem kryzysowym na poziomie państwa, województwa, powiatu i gminy obejmuje wiele elementów, wśród których na uwagę zasługują:

- złożony charakter, jaki można przypisać procesowi decyzyjnemu, który obejmuje etapy inicjatyw, ich analizy i selekcji, przekształcania w projekty, wyjaśnianie i rozstrzyganie sporów, ocenę prawną, rozstrzygnięcia podmiotów decyzyjnych na wszystkich poziomach zarządzania kryzysowego w państwie,
- usytuowanie decydenta w systemie politycznym i prawnym,
- relacje z otoczeniem, gdzie decyzje są podejmowane w warunkach niepewności[95].

[94] J. Górczyński, *Procesy informacyjne zarządzania* – http://www.wszimsochaczew.edu.pl/www/download%5CProcesyInformacyjne%5CArchiwum%5CProcesyInformacyjneZjazd_8.pdf [pobrano 3.03.2012].

[95] G. Rydlewski, *Rządowy system decyzyjny w Polsce,* Warszawa 2002, s. 32–33.

Złożoność procesów decyzyjnych, jakie występują w trakcie zarządzania kryzysowego, określają wprost znaczenie informacji.

> Wszelkie zakłócenia w sferze informacji znajdujące wyraz w niedoinformowaniu lub fałszywym poinformowaniu stanowią dla efektywności rządowego systemu decyzyjnego [zarządzania kryzysowego – przyp. Autora] jedno z najważniejszych zagrożeń. Dotyczy to w równej mierze zakłóceń pojawiających się w obszarach: zasilania systemu w informacje o otoczeniu, wewnątrzsystemowego zarządzania informacjami, zasilania otoczenia informacjami z systemu oraz wiedzy pozyskiwanej przez system na temat percepcji przez otoczenie podjętej decyzji. W ramach rządowego systemu decyzyjnego [zarządzania kryzysowego – przyp. Autora] istnieć w związku z tym muszą gwarancje instytucjonalne i funkcjonalne pozwalające zachować we wszystkich tych płaszczyznach postawę ukierunkowaną na aktywne pozyskiwanie informacji i nimi sprawne zarządzanie[96].

Istotne jest, aby postrzegać zarządzanie kryzysowe będące elementem bezpieczeństwa państwa nie tylko jako stan minimalizacji i/lub wolności od zagrożeń, ale w większym stopniu eksponować ujęcie dynamiczne, obejmujące całokształt wysiłków podejmowanych dla skutecznego zarządzania kryzysowego[97]. Oznacza to, że skuteczne zarządzanie kryzysowe ma ścisły związek z procesem informacyjnym, który jest realizowany w trakcie zdobywania informacji, jej przetwarzania, archiwizacji i udostępniania uprawnionym podmiotom.

W systemie zarządzania kryzysowego służby specjalne (kontrwywiad cywilny i wojskowy oraz wywiad cywilny i wojskowy) realizują funkcję informacyjną, która jest widoczna w ustawowym katalogu wykonywanych zadań związanych z rozpoznawaniem i przeciwdziałaniem zagrożeniom dla bezpieczeństwa wewnętrznego i zewnętrznego państwa. Posiadanie informacji, które przekładają się na wiedzę podmiotów decyzyjnych w procesie zarządzania kryzysowego, a dotyczących zagrożeń dla państwa, wymaga ich gromadzenia, przetwarzania, dystrybucji i ochrony.

W Polsce zadania o charakterze wywiadowczym wykonują Agencja Wywiadu (AW)[98] i Służba Wywiadu Wojskowego (SWW)[99]. Dostarczają one informacji o sytuacji międzynarodowej, postępującej globalizacji, a tym samym o wyzwaniach i zagrożeniach, jakie występują w otoczeniu zewnętrznym bliższym i dalszym państwa oraz ich wpływie na bezpieczeństwo zewnętrzne i wewnętrzne Polski. Do zagrożeń dla bezpieczeństwa państwa w skali międzynarodowej zaliczany jest: terroryzm międzynarodowy, nacjonalizm, totalitaryzm i autorytaryzm, mafie oraz przemyt broni i ludzi, narkobiznes i korupcja, pandemie i epidemie, pro-

[96] Ibidem, s. 200.

[97] Szerzej na ten temat pisze S. Zalewski, *Służby specjalne w państwie demokratycznym,* Warszawa 2005, s. 72.

[98] Ustawa z dnia 24 maja 2002 roku *Agencja Bezpieczeństwa Wewnętrznego oraz Agencja Wywiadu* (T. j.: Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.).

[99] Ustawa z dnia 9 czerwca 2006 roku *Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego* (Dz. U. z 2006 r. Nr 104, poz. 709 z późn. zm.).

liferacja broni masowego rażenia i handel bronią, ludobójstwo, nielegalny handel bronią, spory religijne i ruchy separatystyczne, państwa w stania rozkładu, podmioty pozapaństwowe, kataklizmy (klęski żywiołowe) i katastrofy techniczne, ubóstwo i przeludnienie, konflikty etniczne i terytorialne, masowe migracje (uchodźcy), fundamentalizm religijny, kryzysy energetyczne i żywnościowe, kryzysy ekonomiczne, degradacja środowiska naturalnego, agresja o charakterze terrorystycznym, konflikt przygraniczny, incydent zbrojny, agresja przeciwko państwu, ataki asymetryczne i inne[100].

Zadania o charakterze kontrwywiadowczym realizują Agencja Bezpieczeństwa Wewnętrznego (ABW)[101] i Służba Kontrwywiadu Wojskowego (SKW)[102], które dostarczają informacje o zagrożeniach mających wpływ na bezpieczeństwo wewnętrzne naszego państwa (zob. tabela 53).

Tabela 53. Zagrożenia dla bezpieczeństwa wewnętrznego państwa

Zagrożenia		
Zagrożenia dla bytu ludności	Zagrożenia bezpieczeństwa i porządku publicznego	Zagrożenia dóbr publicznych
degradacja środowiska naturalnego i antropogenicznego	terror polityczny i kryminalny	katastrofy techniczne
kataklizmy i katastrofy	demonstracje i protesty	kataklizmy (klęski żywiołowe)
pandemie i epidemie	zamachy i zabójstwa	skażenia chemiczne i promieniotwórcze
skażenie chemiczne i promieniotwórcze	uprowadzenia	skażenia środkami toksycznymi
skażenie środkami toksycznymi	branie zakładników	degradacja środowiska naturalnego, antropogenicznego i infrastruktury państwa
terror polityczny i kryminalny	korupcja	grabieże majątku i zasobów
bezrobocie i korupcja	grabieże	przestępczość zorganizowana
degradacja miast	mafie i gangi	upadek gospodarki
ubóstwo	przemyt i handel bronią	nielegalne operacje finansowe
narkomania	oszustwa i fałszerstwa	inne
inne	przestępczość zorganizowana	
	inne	

Źródło: Z. Lach, S.A. Łaszczuk, *Geografia bezpieczeństwa*, Warszawa 2004, s. 15

Powyższe zagrożenia dla bezpieczeństwa zewnętrznego i wewnętrznego państwa przekładają się bezpośrednio na realizowane zadania, co wynika z obowiązujących regulacji prawnych stanowiących podstawę prawną działania.

Funkcja informacyjna służb specjalnych sprowadza się do przekazywania informacji i analiz kierownictwu państwa oraz innym uprawnionym podmiotom,

[100] Z. Lach, S.A. Łaszczuk, *Geografia bezpieczeństwa*, Warszawa 2004, s. 15.

[101] Ustawa z dnia 24 maja 2002 roku *Agencja Bezpieczeństwa Wewnętrznego oraz Agencja Wywiadu* (T. j.: Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.).

[102] Ustawa z dnia 9 czerwca 2006 roku *Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego*(Dz. U. z 2006 r. Nr 104, poz. 709 z późn. zm.).

w tym sprawującym funkcje kierownicze w procesie zarządzania kryzysowego na poziomie województwa, powiatu i gminy[103].

Tabela 54. Funkcja informacyjna służb specjalnych w systemie zarządzania kryzysowego

Zadania	Treść	Służba specjalna
rozpoznawanie zapobieganie zwalczanie	zagrożeń dla bezpieczeństwa wewnętrznego i ochrony porządku konstytucyjnego państwa	Agencja Bezpieczeństwa Wewnętrznego
rozpoznawanie zapobieganie wykrywanie	zagrożeń wewnętrznych dla obronności państwa, bezpieczeństwa i zdolności bojowej sił zbrojnych oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej	Służba Kontrwywiadu Wojskowego
rozpoznawanie przeciwdziałanie	zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium RP	Agencja Wywiadu
	zagrożeniom wewnętrznym dla obronności państwa, bezpieczeństwa i zdolności bojowej sił zbrojnych oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej	Służba Wywiadu Wojskowego
uzyskiwanie analizowanie przetwarzanie	informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego	Agencja Bezpieczeństwa Wewnętrznego
	informacji mogących mieć istotne znaczenie dla obronności państwa lub zdolności bojowej sił zbrojnych lub innych jednostek organizacyjnych Ministra Obrony Narodowej	Służba Kontrwywiadu Wojskowego
	informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP oraz jej potencjału ekonomicznego i obronnego	Agencja Wywiadu
	informacji mogących mieć istotne znaczenie dla bezpieczeństwa potencjału obronnego RP, bezpieczeństwa i zdolności bojowej SZ RP, realizacji przez SZ RP zadań poza granicami kraju	Służba Wywiadu Wojskowego
przekazywanie	informacji organom władzy państwowej, w tym uprawnionym podmiotom decyzyjnym uczestniczącym w zarządzaniu kryzysowym	Agencja Bezpieczeństwa Wewnętrznego Służba Kontrwywiadu Wojskowego Agencja Wywiadu Służba Wywiadu Wojskowego

Źródło: Ustawa z dnia 24 maja 2002 roku *Agencja Bezpieczeństwa Wewnętrznego oraz Agencja Wywiadu*, ustawa z dnia 9 czerwca 2006 roku *Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego*

Służby specjalne zasilają

strategiczny system informacyjny, który jest sprzęgnięty ze strukturą organizacyjną państwa na wszystkich poziomach zarządzania jego bezpieczeństwem, w tym zarządzaniem kryzysowym. Jego podstawową cechą jest to, że stanowi uporządkowaną sieć

[103] A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003)*, Kraków 2005, s. 175.

powiązań informacyjnych między służbami specjalnymi, służbami quasispecjalnymi, służbami rozpoznania sił zbrojnych, uprawnionymi organami administracji rządowej i zarządzania kryzysowego. Ponadto służy zaspokajaniu potrzeb informacyjnych Prezesa Rady Ministrów i Rady Ministrów, wynikających przez nich zadań w sferze bezpieczeństwa i obronności, w tym zarządzania kryzysowego[104].

Służby specjalne pełnią rolę systemu wczesnego ostrzegania, a w ściśle określonych warunkach nawet alarmowania. Należy podkreślić, że funkcja informacyjna służb specjalnych powinna być doskonalona już w czasie pokoju. Pozyskiwanie informacji zróżnicowanych co do rodzaju i zakresu zwiększa możliwości wyboru rozwiązań, przez co zmniejsza się ryzyko podejmowania błędnych decyzji[105]. Informacje te warunkują m.in. skuteczność działania państwa, województwa, powiatu i gminy podczas zarządzania kryzysowego. Podmioty decyzyjne uczestniczące w zarządzaniu kryzysowym muszą rozwiązywać coraz trudniejsze i coraz bardziej złożone problemy, a także w sposób właściwy reagować na zmieniające się warunki.

[104] Ibidem, s. 177.

[105] Ibidem, s. 178.

ROZDZIAŁ 6

Podsystem planowania

6.1. Istota planowania w zarządzaniu kryzysowym

Planowanie to proces wyboru celów organizacji, ustalanie polityki i programów potrzebnych do realizacji konkretnych zadań niezbędnych do osiągnięcia tych celów oraz wyboru metod koniecznych do zapewnienia wdrożenia polityki i programów strategicznych[1].

W innym ujęciu:

> planowanie to wyprzedzające przygotowanie właściwego działania. Planowanie stanowi etap preparacji, której znaczenie znajduje się w zmniejszeniu ryzyka strat we właściwym działaniu. Prowadzi do działania celowego, uporządkowanego, zmniejszenia udziału błędnych decyzji. Jest wynikiem racjonalnego przewidywania wszystkich warunków przyszłej działalności. […] jest instrumentem w procesie zarządzania kryzysowego. Racjonalne metody planowania służą dokonywaniu wyboru właściwego wariantu decyzyjnego odnośnie do celów i metod realizacji[2].

Planowanie stanowi szczególny rodzaj podejmowania decyzji, zajmujący się konkretną przyszłością, jakiej pragną uprawnione podmioty dla gminy, powiatu, województwa i państwa. Planowanie nie jest przedsięwzięciem jednorazowym o wyraźnym początku i końcu. Jest procesem ciągłym, stanowiącym odzwierciedlenie zmian, jakie zachodzą w otoczeniu wewnętrznym i zewnętrznym gminy, powiatu, województwa i państwa w związku z uruchomieniem zarządzania kryzysowego. Planowanie jest procesem ustalania celów i wybierania środków do ich osiągania. Bez planów trudno jest skutecznie organizować zasoby informacyjne, osobowe, materiałowe czy finansowe, a także wykorzystywać je w procesie zarządzania kryzysowego.

> Planowanie jest więc procesem decydowania o tym, co dla przyszłości organizacji jest najwłaściwsze, czym się powinna zajmować, w jaki sposób zapewnić sobie lepsze funkcjonowanie i większą skuteczność. Podstawą tego planowania jest zespolenie na

[1] J. Penc, *Leksykon biznesu*, Warszawa 1997, s. 314.

[2] *Słownik ekonomiczny dla przedsiębiorcy w warunkach rynku,* red. Z. Dowgiałło, Szczecin 1994, s. 142 i 143.

każdym poziomie zarządzania, myślenia strategicznego z operacyjnym podejmowaniem decyzji i włączenie w te procesy wszystkich obszarów funkcjonowania organizacji[3].

Według ustawy z dnia 27 kwietnia 2007 roku *o zarządzaniu kryzysowym* przez planowanie cywilne należy rozumieć:

- całokształt przedsięwzięć organizacyjnych mających na celu przygotowanie administracji publicznej do zarządzania kryzysowego,
- planowanie w zakresie wspierania Sił Zbrojnych Rzeczypospolitej Polskiej w razie ich użycia oraz planowanie wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego[4].

Planowanie cywilne w ramach zarządzania kryzysowego ma przede wszystkim na celu: wskazanie zagrożeń, jakie w danej społeczności mogą wystąpić, ma udzielić odpowiedzi na pytania: jakimi siłami i środkami dysponujemy? jakie siły i środki są niezbędne w celu niedopuszczenia do sytuacji kryzysowej lub zminimalizowania jej skutków? Planowanie ma również za zadanie określić: struktury, siły i środki niezbędne do realizacji m.in. przedsięwzięć ratowniczych. Planowanie powinno uwzględnić procedury współpracy w pionie i w poziomie, w tym z innymi państwami w ramach umów bilateralnych. Kolejna kwestia to uwzględnienie wsparcia sił zbrojnych w ramach zarządzania kryzysowego, wprowadzenia wyższych stanów gotowości obronnej państwa[5].

W procesie planowania należy również uwzględnić procedury dotyczące współpracy i współdziałania z przełożonymi (Rada Ministrów, województwo, starostwo), z sąsiadami (województwami, starostwami, gminami), a także państwami graniczącymi (umowy sojusznicze, umowy bilateralne).

Pod pojęciem planowania ustawodawca rozumie nie tylko sam proces opracowywania dokumentów planistycznych, ale również przygotowanie zasobów i wszystkie inne działania natury organizacyjnej zmierzające do właściwego przygotowania administracji na sytuacje kryzysowe, w tym związane z wykorzystywaniem sił zbrojnych[6].

Administracja publiczna o charakterze samorządowym (województwo, powiat, gmina), jak i rządowa (rząd, województwo) jest zobowiązana do opracowywania dokumentacji planistycznej. Celem tej działalności jest przygotowanie personelu kierowniczego i pracowników administracji do rozwiązywania m.in. problemów związanych z zarządzaniem kryzysowym.

Do zadań z zakresu planowania cywilnego należy: przygotowanie planów zarządzania kryzysowego, przygotowanie struktur uruchamianych w sytuacjach

[3] J. Penc, op. cit., s. 314.

[4] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

[5] K. Sienkiewicz-Małyjurek, F.R. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej*, Warszawa 2010, s. 104.

[6] W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wrocław 2010, s. 29.

kryzysowych, przygotowanie i utrzymywanie zasobów niezbędnych do wykonywania zadań ujętych w planie zarządzania kryzysowego, utrzymywanie baz danych niezbędnych w procesie zarządzania kryzysowego, przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej, zapewnienie spójności między planami zarządzania kryzysowego a innymi planami sporządzanymi w tym zakresie przez właściwe organy administracji publicznej, których obowiązek wykonania wynika z odrębnych przepisów.

Zadania powinny uwzględniać: zapewnienie funkcjonowania administracji publicznej w sytuacji kryzysowej, zapewnienie funkcjonowania i możliwości odtwarzania infrastruktury krytycznej, zapewnienie ciągłego monitorowania zagrożeń, racjonalne gospodarowanie siłami i środkami w sytuacjach kryzysowych, pomoc udzielaną ludności w zapewnieniu jej warunków przetrwania w sytuacjach kryzysowych[7].

W celu realizacji powyższych zadań zgodnie z literą ustaw z dnia 26 kwietnia 2007 roku o *zarządzaniu kryzysowym* tworzone są następujące plany[8]:

- Krajowy Plan Zarządzania Kryzysowego oraz wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego (art. 5),
- na potrzeby Krajowego Planu Zarządzania Kryzysowego ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają Raport o zagrożeniach bezpieczeństwa narodowego (art. 5a ust. 1),
- Narodowy Program Ochrony Infrastruktury Krytycznej (art. 5b ust. 1),
- plany ochrony infrastruktury krytycznej (art. 6 ust. 5).

Planowanie na wszystkich poziomach zarządzania kryzysowego powinno być:

- kompleksowe, tj. uwzględniać konieczność jego realizacji z perspektywy: gminy, powiatu, województwa, państwa,
- spójne, z planami wytworzonymi przez poszczególne organy, inspekcje, służby i straże na bazie własnych przepisów branżowych,
- kreatywne, tj. poszukujące najlepszych rozwiązań w systemie zarządzania kryzysowego, które obejmuje gminę, powiat, województwo, państwo ich otoczenie oraz wzajemne relacje,
- antycypacyjne, tj. wyprzedzające rozpoznanie warunków działania, problemów, zagrożeń, skutków.

Planowanie umożliwia konsekwentne ukierunkowanie działalności gminy, powiatu, województwa i państwa w procesie zarządzania kryzysowego. Ponadto ułatwia zarządzającym przewidywanie problemów, zanim powstaną, i rozwiązywanie ich, zanim staną się trudne, a także dostrzeżenie okazji ryzykownych i pewnych oraz dokonanie wyboru między nimi[9]. Dokładna analiza związana

[7] Ustawa z dnia 27 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 4 ust. 1 i 2.

[8] Dz. U. z 2007 r. Nr 89, poz. 580 z późn. zm.

[9] J. Penc, op. cit., s. 314.

z opracowaniem planu dostarcza zarządzającym większej ilości informacji, co ma wpływ na podejmowanie decyzji.

Mając na uwadze czas realizacji zadań, można wyróżnić następujące rodzaje planów[10], co odnosi się również do planowania związanego z zarządzaniem kryzysowym, i tak:

- strategiczne, plan przyszłości, wizja gminy, miasta realizowana w skali jednej kadencji dzięki odpowiedniemu postępowaniu i realizowaniu zadań ku temu zmierzających (powyżej 5 lat),
- długoterminowe, konkretne czynności związane z realizacją celu głównego (od 2 do 5 lat),
- średnioterminowe, to część składowa realizacji planu długoterminowego (od kilku miesięcy do roku),
- krótkoterminowe, konkretne zadania do wykonania będące częścią składową planu średnioterminowego (do trzech miesięcy),
- bieżące, szczegółowe czynności realizowane codziennie lub w skali tygodnia.

6.2. Raport o zagrożeniach bezpieczeństwa narodowego

Jednym z warunków, pozwalającym uprawnionym podmiotom skutecznie realizować zadania związane z zarządzaniem kryzysowym, jest posiadanie informacji i wiedzy o zagrożeniach, ich rodzaju i skali, a także prawdopodobieństwie wystąpienia. Informacje na ten temat znajdują się w posiadaniu różnych służb, inspekcji, straży, a także administracji działającej na wszystkich poziomach zarządzania bezpieczeństwem państwa. W związku z tym *Raport o zagrożeniach bezpieczeństwa narodowego*, a raczej jego części składowe (raporty cząstkowe), sporządzane są hierarchicznie i resortowo na kolejnych szczeblach administracji, począwszy od poziomu województwa[11]. *Raport o zagrożeniach bezpieczeństwa narodowego* sporządzany jest na potrzeby Krajowego Planu Zarządzania Kryzysowego przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów[12]. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie *Raportu o zagrożeniach bezpieczeństwa narodowego* w § 3 ust. 1 stanowi, że raporty cząstkowe mają być wykonane zgodnie z właściwością rzeczową poszczególnych organów[13]. Oznacza to, że w trakcie tworzenia raportu ma miejsce proces analizy zagrożeń na poszczególnych po-

[10] K. Sienkiewicz-Małyjurek, F.R. Krynojewski, op. cit., s. 104.

[11] W. Skomra, op. cit., s. 64.

[12] Ustawa z dnia 27 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 5a ust. 1.

[13] Dz. U. z 2010 r. Nr 83, poz. 540.

ziomach administracji, którego efekty powinny być wykorzystane nie tylko przy sporządzaniu raportu całościowego, ale i poszczególnych planów zarządzania kryzysowego. Jednocześnie możliwe jest porównanie wiedzy zarówno w układzie pionowym (czy postrzegane zagrożenie na szczeblu wojewódzkim koreluje z zagrożeniami wymienionymi w raportach cząstkowych sporządzanych przez ministrów kierowników urzędów centralnych), jak i w układzie resortowym[14].

Za koordynację przygotowania Raportu odpowiedzialny jest dyrektor Rządowego Centrum Bezpieczeństwa (RCB), a w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego[15]. Dyrektor RCB posiada decydujący wpływ na całościowy charakter i kształt Raportu także w części koordynowanej przez Szefa Agencji Bezpieczeństwa Wewnętrznego. Ponadto dokonuje systematycznej aktualizacji Raportu, zobowiązany jest również do jego przedkładania Radzie Ministrów raz na dwa lata wraz z informacjami o wprowadzonych zmianach.

Raport o zagrożeniach bezpieczeństwa narodowego zawiera następujące elementy: wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka, określenie celów strategicznych, określenie priorytetów w reagowaniu na konkretne zagrożenia, wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych, programowanie zadań w zakresie poprawy bezpieczeństwa przez uwzględnienie regionalnych i lokalnych inicjatyw, wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych[16].

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego* określa sposób wykonania poszczególnych jego części i wyznacza cztery grupy tematyczne obejmujące ocenę możliwości powstania zagrożeń, działania, jakie należy podjąć w celu zminimalizowania zagrożeń, działania, jakie należy podjąć, gdy zagrożenie wystąpi, inne informacje, które zdaniem wykonawcy mogą być przydatne przy tworzeniu Krajowego Planu Zarządzania Kryzysowego.

Tabela 55. Elementy cząstkowe *Raportu o zagrożeniach bezpieczeństwa narodowego*

Ogólne	Szczegółowe
Wskazanie najważniejszych zagrożeń i skutków ich wystąpienia przez stworzenie mapy ryzyka, o której mowa w art. 3 pkt 10 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*, obejmującej wyszczególnienie rodzajów i charakterystyki zagrożeń	a) o istotnym wpływie na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego b) których skutki mogą: – godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, a w szczególności w suwerenność, niepodległość i nienaruszalność terytorium

[14] W. Skomra, op. cit., s. 67.

[15] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 5a ust. 2.

[16] Ibidem, art. 5a ust. 3.

	– zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach – oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa – dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie c) występujących w innych rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych d) o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej
Określenie celów strategicznych, w szczególności:	a) wskazanie celów, jakie należy osiągnąć, aby zminimalizować możliwości wystąpienia zagrożenia lub jego skutków b) hierarchizację celów według kryteriów ważności lub wskazanie celów priorytetowych
Wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych, a szczególnie tych, których realizacja wymaga działań wykraczających poza posiadane kompetencje.	
Wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych,	
Programowanie zadań w zakresie poprawy bezpieczeństwa państwa przez wskazanie określonych regionalnych i lokalnych inicjatyw, w szczególności:	a) wyszczególnienie programów krajowych, wojewódzkich, powiatowych i gminnych b) wskazanie realizatorów programów: – rządowych – samorządowych – pozarządowych c) sposoby finansowania programów d) okresy trwania programów
Wyznaczenie priorytetów w reagowaniu na określone zagrożenia, w tym ich wpływ na:	a) zasady reagowania w przypadku wystąpienia zagrożenia b) hierarchizację działań
Inne informacje, które zdaniem wykonawcy mogą być przydatne przy tworzeniu Krajowego Planu Zarządzania Kryzysowego.	

Źródło: § 4 rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego* (Dz. U. z 2010 r. Nr 83, poz. 540)

Mapę ryzyka, o której jest mowa w § 4 pkt 1 rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego,* przedstawia się w formie:

- mapy topograficznej, a w postaci elektronicznej – mapy wektorowej lub rastrowej, przedstawiającej zasięg geograficzny zagrożeń z przypisanym prawdopodobieństwem wystąpienia i oceny skutków wystąpienia dla ludności, gospodarki i środowiska,
- tabeli opisującej parametry zagrożeń oraz ich prognozowane skutki,
- opisowej, jeżeli charakter zagrożenia uniemożliwia przedstawienie informacji w sposób określony w pkt. 1 i 2.

Pozostałe dokumenty wchodzące w skład Raportu opracowuje się w formie tabelarycznej, a w przypadku gdy nie jest to możliwe, w formie opisowej. Jest

to niezwykle istotne dla procesu planowania elementów Raportu, gdyż pozwala, szczególnie przy zazwyczaj występującym deficycie sił i środków, skupić się na przygotowaniu reagowania na najpoważniejsze zagrożenia według gradacji prawdopodobieństwa wystąpienia jak i dotkliwości dla ludności i infrastruktury[17].

Wykonawcy *Raportu* zobowiązani są do jego systematycznej aktualizacji. Zaktualizowany *Raport* cząstkowy wykonawca, nie rzadziej niż raz na dwa lata, przedkłada dyrektorowi Rządowego Centrum Bezpieczeństwa oraz w przypadku zagrożenia terrorystycznego Szefowi Agencji Bezpieczeństwa Wewnętrznego.

Cząstkowy *Raport o zagrożeniach bezpieczeństwa narodowego* jest wykonywany i przekazywany z zachowaniem przepisów ustawy z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*[18].

6.3. Narodowy Program Ochrony Infrastruktury Krytycznej

Narodowy Program Ochrony Infrastruktury Krytycznej stanowi podstawowy dokument dotyczący infrastruktury krytycznej państwa, a także wyznacza główny cel, jaki sobie stawia Rada Ministrów w przedmiotowej sprawie. Tym celem jest szeroko rozumiane bezpieczeństwo infrastruktury krytycznej państwa, które należy postrzegać w kategoriach jego bezpieczeństwa strategicznego. Przyjęcie właściwych celów odpowiadających aktualnym i przyszłym zagrożeniom dla infrastruktury krytycznej, wyodrębnienie obiektów, instalacji, urządzeń i usług zaliczanych do systemu infrastruktury krytycznej, wskazanie zadań i uprawnionych podmiotów, określenie zasad współpracy, a także zabezpieczenie finansowe realizacji *Narodowego Program Ochrony Infrastruktury Krytycznej* pozwoli na ochronę ludności przed negatywnymi skutkami. Jakość i skuteczność przyjętego do realizacji Programu w dużej mierze zależy od przyjętych kryteriów. Z uwagi na niejawny charakter tej problematyki możemy odnieść się do niej w dużym uogólnieniu. Generalnie kryteria zostały podzielone na dwa rodzaje:

- systemowe, które określają ilościowo i podmiotowo parametry obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do infrastruktury krytycznej, kryteria te opracowywane są odrębnie dla każdego z systemów infrastruktury krytycznej,
- przekrojowe, które opisują parametry odnoszące się do skutków zniszczenia lub zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi[19].

[17] W. Skomra, op. cit., s. 69.

[18] Dz. U. z 2010 r. Nr 182, poz. 1228.

[19] W. Skomra, op. cit., s. 100.

Obiekt, urządzenie, instalacja lub usługa są zaliczane do infrastruktury krytycznej po spełnieniu następujących warunków:

- dany obiekt, instalacja, urządzenie lub usługa musi spełniać kryteria sektorowe, właściwe dla odpowiedniego systemu infrastruktury krytycznej; kryterium sektorowe charakteryzuje ilościowo lub podmiotowo parametry i funkcje danego obiektu, instalacji, urządzenia lub usługi,
- następnie należy sprawdzić, czy potencjalna infrastruktura krytyczna wyłoniona w pierwszym kroku wypełnia przesłanki infrastruktury krytycznej określonej w ustawie *o zarządzaniu kryzysowym*,
- potencjalna infrastruktura krytyczna może zostać zakwalifikowana do wykazu, jeżeli spełnia co najmniej dwa kryteria przekrojowe, które określają skutki zniszczenia lub zaprzestania prawidłowego działania danej infrastruktury; z kryteriów przekrojowych należy wybrać te, które najlepiej odzwierciedlają charakterystykę systemu, w ramach którego przeprowadzany jest proces wyznaczania infrastruktury krytycznej.

Wymaga to zaangażowania wielu podmiotów będących właścicielami czy też użytkownikami infrastruktury krytycznej[20].

Wychodząc naprzeciw zagrożeniem i potrzebom dotyczącym zabezpieczenia poszczególnych elementów infrastruktury krytycznej, Rada Ministrów wydała przepisy wykonawcze, które uszczegółowiają zagadnienia dotyczące ochrony infrastruktury krytycznej państwa. Są to rozporządzenia z dnia 30 kwietnia 2010 roku *w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*[21] oraz z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury krytycznej*[22].

Zgodnie ustawą z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* Rada Ministrów przyjmuje w drodze uchwały Narodowy Program 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[23].

Program ten określa:

- narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej,
- ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy, o których mowa w art. 3 pkt 2,

[20] Ibidem.

[21] Dz. U. z 2010 r. Nr 83, poz. 541.

[22] Dz. U. z 2010 r. Nr 83, poz. 542.

[23] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 5b ust. 1.

- 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[24].

Program przygotowuje dyrektor Rządowego Centrum Bezpieczeństwa (RCB) we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za funkcjonowanie infrastruktury krytycznej[25] oraz właściwymi w sprawach bezpieczeństwa narodowego[26]. Program jest aktualizowany nie rzadziej niż raz na dwa lata. Do programu stosuje się przepisy o ochronie informacji niejawnych.

Dyrektor Rządowego Centrum Bezpieczeństwa[27]:

- sporządza na podstawie szczegółowych kryteriów[28] we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy; w wykazie wyróżnia się także europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską (wykaz ma charakter niejawny);
- opracowuje wyciągi z wykazu infrastruktury krytycznej, o którym mowa w pkt. 1, znajdującej się w danym systemie oraz przekazuje je ministrom i kierownikom urzędów centralnych odpowiedzialnym za dany system;
- opracowuje wyciągi z wykazu infrastruktury krytycznej, o którym mowa w pkt. 1, znajdującej się na terenie województw oraz przekazuje je właściwym wojewodom;
- informuje o ujęciu w wykazie, o którym mowa w pkt 1, obiektów, instalacji lub urządzeń – ich właścicieli, posiadaczy samoistnych i zależnych.

Dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za funkcjonowanie infrastruktury krytycznej na bieżąco rozpoznaje potencjalną europejską infrastrukturę krytyczną, badając, czy infrastruktura ta spełnia kolejno następujące wymogi:

- kryteria sektorowe – przybliżone progi liczbowe ustalone przez Komisję Europejską i państwa członkowskie Unii Europejskiej, charakteryzujące parametry wchodzących w skład systemów infrastruktury krytycznej obiektów, urządzeń oraz instalacji lub funkcje realizowane przez te obiekty, urządzenia oraz instalacje, warunkujące identyfikację infrastruktury krytycznej,

[24] Ibidem, art. 5b ust. 2.

[25] Ibidem, art. 3 pkt 2.

[26] Ibidem, art. 5b ust. 3.

[27] Ibidem, art. 5b ust. 7.

[28] Ibidem, art. 5b ust. 2 pkt 3.

- stanowi składnik, system lub część infrastruktury, 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 Rzeczpospolitą Polską w wyniku utraty tych funkcji,
- jej zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie Unii Europejskiej,
- kryteria przekrojowe – w zakresie przybliżonych progów ustalonych przez Komisję Europejską i państwa członkowskie Unii Europejskiej – obejmujące:
  a) kryterium ofiar w ludziach – oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych,
  b) kryterium skutków ekonomicznych – oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia jakości towarów lub usług, w tym potencjalnych skutków ekologicznych,
  c) kryterium skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych osób i zakłócenia codziennego życia, w tym utraty podstawowych usług[29].

Infrastruktura krytyczna jest uznawana za potencjalną europejską infrastrukturę krytyczną po spełnieniu wymienionych wyżej wymogów[30].

O potencjalnej europejskiej infrastrukturze krytycznej dyrektor Rządowego Centrum Bezpieczeństwa informuje właściwe organy państw członkowskich Unii Europejskiej na które ta infrastruktura może mieć istotny wpływ. Dyrektor RCB podaje nazwę i lokalizację potencjalnej europejskiej infrastruktury krytycznej i przyczyny jej wyznaczenia[31].

W celu wyznaczenia europejskiej infrastruktury krytycznej oraz dokładnych progów kryteriów dyrektor Rządowego Centrum Bezpieczeństwa prowadzi rozmowy z właściwymi organami państw członkowskich Unii Europejskiej, na które potencjalna europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej może mieć istotny wpływ, a także na terytorium których jest zlokalizowana potencjalna europejska infrastruktura krytyczna mogąca mieć istotny wpływ na Rzeczpospolitą Polską[32]. Dyrektor w powyższych rozmowach przedstawia stanowisko uzgodnione z ministrami i kierownikami urzędów centralnych odpowiedzialnych za systemy, których przedstawiciele mogą brać udział w rozmowach.

W przypadku gdy infrastruktura zlokalizowana na terytorium innego państwa członkowskiego Unii Europejskiej, która nie została rozpoznana jako europejska infrastruktura krytyczna, może mieć istotny wpływ na Rzeczpospolitą Polską, dyrektor RCB informuje Komisję Europejską o zamiarze przeprowadze-

[29] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

[30] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 6a ust. 1 pkt 1–4.

[31] Ibidem, art. 6b ust. 1.

[32] Ibidem, art. 6b ust. 2.

nia rozmów na ten temat. Na podstawie ustaleń będących wynikiem rozmów Rada Ministrów wyznacza, w drodze uchwały, z zakresu potencjalnej europejskiej infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej europejską infrastrukturę krytyczną. Właściwym organom państw członkowskich Unii Europejskiej, na które ma wpływ europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej, dyrektor RCB przekazuje dane identyfikujące europejską infrastrukturę krytyczną, w tym jej nazwę i lokalizację.

Ponadto Dyrektor Rządowego Centrum Bezpieczeństwa przekazuje Komisji Europejskiej:

- co roku informacje o liczbie infrastruktur krytycznych:
  a) w odniesieniu do których prowadzono z właściwymi organami państw członkowskich Unii Europejskiej rozmowy na temat progów kryteriów przekrojowych, umożliwiających wyznaczenie europejskiej infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej,
  b) zlokalizowanych na terytorium Rzeczypospolitej Polskiej wchodzących w skład europejskiej infrastruktury krytycznej w poszczególnych systemach, o których mowa w art. 3 pkt. 2a, oraz o liczbie państw członkowskich Unii Europejskiej, na które ma ona wpływ;
- co 2 lata sprawozdanie zawierające ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów stwierdzonych w każdym z systemów, w których została wyznaczona europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej[33].

Dane dotyczące infrastruktury krytycznej oraz uchwała mają charakter niejawny.

Właściwi wojewodowie, jeżeli istnieje potrzeba wynikająca z wojewódzkiego planu zarządzania kryzysowego, są upoważnieni do przekazywania niezbędnej informacji o infrastrukturze krytycznej na terenie województwa właściwemu organowi administracji publicznej działającemu na tym terenie, z zachowaniem przepisów o ochronie informacji niejawnych.

Rada Ministrów na podstawie delegacji ustawowej określonej w art. 5b ust. 9 ustawy *o zarządzaniu kryzysowym* 30 kwietnia 2010 roku wydała rozporządzenie *w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*[34]. Rozporządzenie określa sposób realizacji obowiązków i współpracy w zakresie *Narodowego Programu Ochrony Infrastruktury Krytycznej* przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej oraz innymi organami i służbami publicznymi[35]. Uczestnikami Programu są organy administracji publicznej i służby odpowiedzialne za

[33] Ibidem, art. 6c ust.

[34] Dz. U. z 2010 r. Nr 83, poz. 541.

[35] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej* (Dz. U. z 2010 r. Nr 83, poz. 541), § 1.

bezpieczeństwo państwa, operatorzy infrastruktury krytycznej oraz inne organy i służby publiczne, które realizują obowiązki określone w ustawie z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* i współpracują w zakresie *Narodowego Programu Ochrony Infrastruktury Krytycznej*[36].

W celu sporządzenia *Narodowego Programu Ochrony Infrastruktury Krytycznej* dyrektor Rządowego Centrum Bezpieczeństwa opracowuje kryteria pozwalające wyodrębnić infrastrukturę krytyczną i przekazuje je do uzgodnienia ministrom odpowiedzialnym za systemy, o których jest mowa w tej ustawie kierownikom urzędów centralnych odpowiedzialnym za systemy, o których jest mowa w ustawie, kierownikom urzędów centralnych właściwymi w sprawach bezpieczeństwa. W terminie 6 tygodni od daty otrzymania 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 wchodzących w skład infrastruktury krytycznej z podziałem na systemy[37]. Dyrektor RCB po dokonaniu weryfikacji przedłożonych propozycji w aspekcie zgodności z kryteriami sporządza wykaz w postaci tabeli obejmującej:

- nazwę i lokalizację infrastruktury krytycznej,
- podległość organizacyjną, w tym w stosunku do ministrów i kierowników urzędów centralnych, jeśli taka występuje,
- dane operatora infrastruktury krytycznej,
- dane zarządzającego w imieniu operatora infrastruktury krytycznej, jeśli taki występuje.

Ministrowie i kierownicy urzędów centralnych przygotowują w zakresie ich właściwości i przedkładają dyrektorowi Rządowego Centrum Bezpieczeństwa informacje zawierające[38]:

- charakterystykę obszaru zadaniowego pozostającego w ich właściwości, obejmującą identyfikację jego 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 będących skutkiem zakłócenia funkcjonowania infrastruktury krytycznej,

[36] Ibidem, § 2.

[37] Ibidem, § 4 ust. 2.

[38] Ibidem, § 5 ust. 1.

- propozycje programów badawczych i rozwojowych mogących przyczynić się do zwiększenia bezpieczeństwa infrastruktury krytycznej[39].

Mając na względzie zapewnienie spójności i kompletności *Narodowego Programu Ochrony Infrastruktury Krytycznej*, dyrektor Rządowego Centrum Bezpieczeństwa może wystąpić o przekazanie także innych informacji, jeżeli uzna je za niezbędne do umieszczenia w Programie.

Na podstawie przedłożonych informacji dyrektor Centrum opracowuje projekt Programu, który podlega uzgodnieniu z uczestnikami Programu[40]. Uczestnicy mogą wnosić do projektu uwagi i zastrzeżenia wraz z uzasadnieniem swojego stanowiska. Dyrektor RCB, po rozpatrzeniu uwag i zastrzeżeń, przedstawia projekt Programu Radzie Ministrów wraz z protokołem rozbieżności w terminie jednego miesiąca od daty dokonania ostatniego uzgodnienia.

Stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej następuje przez:

- realizację wyznaczonych priorytetów oraz celów Programu,
- zapewnienie warunków do doskonalenia ochrony i ciągłości funkcjonowania infrastruktury krytycznej,
- przygotowanie na sytuacje kryzysowe mogące być skutkiem zakłócenia funkcjonowania infrastruktury krytycznej lub niekorzystnie wpłynąć na tę infrastrukturę,
- przygotowanie do reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- zapewnienie warunków do odtwarzania infrastruktury krytycznej,
- przestrzeganie standardów oraz wymagań zawartych w Programie,
- współpracę w realizacji Programu[41].

Współpraca w realizacji Programu polega na utrzymywaniu kontaktów pomiędzy jego uczestnikami przez konferencje, seminaria, forum dyskusyjne, przygotowanie i udział w ćwiczeniach i szkoleniach oraz wymianę informacji dotyczących:

- identyfikacji obszarów działań niezbędnych w celu podniesienia poziomu ochrony infrastruktury krytycznej,
- zidentyfikowanych zagrożeń dla infrastruktury krytycznej,
- spodziewanego lub zaobserwowanego zwiększenia zapotrzebowania na usługi lub produkty dostarczane przez operatorów infrastruktury krytycznej,
- spodziewanych przerw lub zakłóceń w dostawach usług lub produktów dostarczanych przez operatorów infrastruktury krytycznej,
- wsparcia działań podejmowanych przez operatorów infrastruktury krytycznej w przypadku zniszczenia lub zakłócenia funkcjonowania tej infrastruktury,

[39] Ibidem, § 5 ust. 2.

[40] Ibidem, § 6 ust. 1.

[41] Ibidem, § 7 ust. 1.

- ochrony infrastruktury krytycznej, funkcjonowania wewnętrznych mechanizmów tej ochrony i zarządzania kryzysowego,
- przygotowania i aktualizacji Programu[42].

Ministrowie i kierownicy urzędów centralnych koordynują współpracę pomiędzy operatorami infrastruktury krytycznej w danym systemie oraz zapewniają wymianę informacji pomiędzy administracją publiczną a tymi operatorami.

Aktualizacja Programu jest dokonywana w zależności od potrzeb z własnej inicjatywy dyrektora Rządowego Centrum Bezpieczeństwa lub na uzasadniony wniosek uczestnika *Narodowego Programu Ochrony Infrastruktury Krytycznej*. Dyrektor Rządowego Centrum Bezpieczeństwa w terminie 6 tygodni od dnia zatwierdzenia Programu opracowuje wyciągi z wykazu dla ministrów i kierowników urzędów centralnych odpowiedzialnych za systemy oraz dla wojewodów w zakresie infrastruktury krytycznej znajdującej się na terenie województw, a także informuje na piśmie operatorów infrastruktury krytycznej o ujęciu w wykazie obiektów, instalacji, urządzeń i usług wchodzących w jej skład. Wykaz podlega aktualizacji, która jest przeprowadzana przez dyrektora Rządowego Centrum Bezpieczeństwa z własnej inicjatywy albo na wniosek właściwego ministra lub kierownika urzędu centralnego odpowiedzialnego za dany system, wojewody lub operatora infrastruktury krytycznej[43].

6.4. Plany ochrony infrastruktury krytycznej

W celu właściwego sporządzenia *Narodowego Programu Ochrony Infrastruktury Krytycznej* przez dyrektora Rządowego Centrum Bezpieczeństwa Rada Ministrów zobowiązała w drodze rozporządzenia uprawnione podmioty do sporządzania planów ochrony infrastruktury krytycznej, każdy w zakresie swojej właściwości, i przedkładania ich w określonym przedziale czasu dyrektorowi Centrum. W związku z tym na podstawie art. 6 ust. 7 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[44] Rada Ministrów rozporządzeniem z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury krytycznej*[45] określiła:

- sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej opracowywanych przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej,
- warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

[42] Ibidem, § 7 ust. 2.

[43] Ibidem, § 11.

[44] Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.

[45] Dz. U. z 2010 r. Nr 83, poz. 542.

Tabela 56. Elementy struktury planu ochrony infrastruktury krytycznej

Elementy struktury	Szczegóły
Dane ogólne	nazwa i lokalizacja infrastruktury krytycznej
	pozwalające zidentyfikować operatora infrastruktury krytycznej: nazwa, adres i siedziba, numery REGON, NIP i KRS
	pozwalające zidentyfikować zarządzającego przedsiębiorstwem w imieniu operatora infrastruktury krytycznej: nazwa, adres i siedziba, numery REGON, NIP i KRS
	obejmujące w zakresie niezbędnym do realizacji zadań wynikających z ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* dane służbowe osoby, o której mowa w art. 6 ust. 5a ustawy, odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej
	imię i nazwisko osoby sporządzającej plan
Dane infrastruktury krytycznej	charakterystyka i podstawowe parametry techniczne
	plan (mapa) z naniesieniem lokalizacji obiektów, instalacji lub systemu
	funkcjonalne połączenia z innymi obiektami, instalacjami, urządzeniami lub usługami
Charakterystyka	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
	zapewnienie ciągłości funkcjonowania infrastruktury krytycznej
	odtwarzanie infrastruktury krytycznej
Zasady współpracy z właściwymi miejscowo	centrami zarządzania kryzysowego
	organami administracji publicznej

Źródło: Rozporządzenie z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury krytycznej* (Dz. U. z 2010 r. Nr 83, poz. 542), § 2 ust. 3

Plan podpisuje operator infrastruktury krytycznej, który może w nim uwzględnić inne elementy niż wymienione w rozporządzeniu, biorąc pod uwagę specyfikę infrastruktury krytycznej lub charakterystykę zagrożeń. W trakcie jego sporządzania operator zobowiązany jest do przestrzegania przepisów o ochronie informacji niejawnych lub o ochronie tajemnicy przedsiębiorstwa. Operator infrastruktury krytycznej sporządza plan w terminie 9 miesięcy od daty otrzymania od dyrektora Rządowego Centrum Bezpieczeństwa informacji o ujęciu w wy-

kazie obiektów, instalacji lub urządzeń, ich właścicieli, posiadaczy samoistnych i zależnych.

Zgodnie z § 4 ust. 1 rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury krytycznej* treść tego planu wymaga uzgodnienia[46] w zakresie ich dotyczącym 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, dyrektorem Urzędu Morskiego, z ministrem lub kierownikiem urzędu centralnego, we właściwości którego znajduje się system, do którego została zaliczona dana infrastruktura krytyczna. Uzgodnienie następuje przez podpisanie arkusza uzgodnień przez podmioty wymienione wyżej w terminie 14 dni od daty otrzymania przez nie planu, ministra lub kierownika urzędu centralnego w terminie 45 dni od daty przedłożenia planu.

W określonych przypadkach może mieć miejsce odmowa uzgodnienia planu, co wymaga pisemnego uzasadnienia oraz wskazania elementów wymagających poprawy lub uzupełnienia i nowego terminu przedłożenia planu. Odmowa uzgodnienia planu w całości lub części może nastąpić w przypadku:

- niespełnienia wymogów określonym w rozporządzeniu,
- przedstawienia rozwiązań niegwarantujących bezpieczeństwa infrastruktury krytycznej,
- braku spójności z *Narodowym Programem Ochrony Infrastruktury Krytycznej* w zakresie:
  a) zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej,
  b) przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,
  c) reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
  d) odtwarzania infrastruktury krytycznej.

Operator infrastruktury krytycznej przedkłada plan wraz z arkuszem uzgodnień do zatwierdzenia dyrektorowi Centrum w terminie 14 dni od daty dokonania ostatniego uzgodnienia[47]. W przypadku braku uzgodnienia ze względu na rozbieżność stanowisk operator infrastruktury krytycznej przedkłada plan wraz z protokołem rozbieżności do zatwierdzenia dyrektorowi Centrum w terminie 14 dni od daty zakończenia uzgodnień ze wszystkimi podmiotami wskazanymi w rozporządzeniu Rady Ministrów *w sprawie planów ochrony infrastruktury krytycznej*. Dyrektor RCB, po rozpatrzeniu ewentualnych rozbieżności, zatwierdza plan w terminie 90 dni od daty przedłożenia. Aktualizacja planów odbywa się w zależności od potrzeb, nie rzadziej jednak niż raz na dwa lata.

[46] Ibidem.

[47] Dz. U. z 2010 r. Nr 83, poz. 542.

Operator infrastruktury krytycznej, który jest w posiadaniu innego planu, opracowanego na podstawie przepisów odrębnych i odpowiadającego wymogom określonym przez rozporządzenie, może przedłożyć ten plan dyrektorowi Centrum w celu uznania spełnienia obowiązku posiadania wymaganego planu.

Dyrektor Rządowego Centrum Bezpieczeństwa, kierując się potrzebą zapewnienia ciągłości funkcjonowania infrastruktury krytycznej oraz *Narodowym Programem Ochrony Infrastruktury Krytycznej* uznaje spełnienie obowiązku posiadania planu odpowiadającego wymogom planu w trybie określonym w rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury krytycznej.*

6.5. Krajowy Plan Zarządzania Kryzysowego

Na potrzeby zarządzania kryzysowego zgodnie z art. 5 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[48] tworzy się *Krajowy Plan Zarządzania Kryzysowego oraz wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego*. Art. 12 ust. 2 niniejszej ustawy stanowi, że ministrowie kierujący działaniami administracji rządowej oraz kierownicy urzędów centralnych zgodnie z zakresem swojej właściwości opracowują plany zarządzania kryzysowego, w których w szczególności uwzględnia się:

- analizę i ocenę możliwości wystąpienia zagrożeń, w tym dla infrastruktury krytycznej uwzględnionej w wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy,
- szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczenia i likwidacji ich skutków,
- organizację monitoringu zagrożeń i realizację zadań stałego dyżuru w ramach podwyższenia gotowości obronnej państwa,
- organizację realizacji zadań z zakresu ochrony infrastruktury krytycznej.

Sporządzenie Krajowego Planu Zarządzania Kryzysowego jest poprzedzone wykonaniem innych dokumentów planistycznych, które są uwzględniane w procesie jego tworzenia.

Na potrzeby Krajowego Planu Zarządzania Kryzysowego ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają Raport o zagrożeniach bezpieczeństwa narodowego (art. 5a ust. 1). Kierunki działania wynikające z wniosków z Raportu stanowią element Krajowego Planu Zarządzania Kryzysowego oraz są uwzględniane w planach zarządzania kryzysowego.

[48] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

Tabela 57. Plany uwzględniane w procesie tworzenia Krajowego Planu Zarządzania Kryzysowego

Plany	Elementy składowe
Raport o zagrożeniach bezpieczeństwa narodowego	
Narodowy Program Ochrony Infrastruktury Krytycznej	
Plany ochrony infrastruktury krytycznej	
Siatki bezpieczeństwa	
Mapy zagrożeń	
Mapy ryzyka	mapa topograficzna, a w postaci elektronicznej mapa wektorowa lub rastrowa przedstawiająca zasięg geograficzny zagrożeń z przypisanym prawdopodobieństwem wystąpienia i oceną skutków wystąpienia dla ludności, gospodarki lub środowiska
	tabela opisująca parametry zagrożeń oraz ich prognozowane skutki
	forma opisowa, jeżeli charakter zagrożenia uniemożliwia przedstawienie informacji w sposób określony wyżej
Inne plany w zarządzaniu kryzysowym	operacyjne plany przeciwpowodziowe dla gmin, powiatów, województw, zakładów pracy uczestniczących w tym procesie
	plany ochrony zabytków na wypadek konfliktu zbrojnego i sytuacji kryzysowych – dla zabytku, gminy, powiatu, województwa, które stanowią uzupełnienie planów OC
	dokumentacje planowych działań zapewnienia funkcjonowania publicznych urządzeń zaopatrzenia w wodę w warunkach specjalnych – dla gmin – również forma uzupełnienia planu OC
Plany Obrony Cywilnej sporządzane w formie opisowej, składające się z następujących rozdziałów:	ocena zagrożeń i zamiarów realizacji zadań Obrony Cywilnej
	plan ewakuacji
	plan zabezpieczenia logistycznego działań Obrony Cywilnej
	plan działania Obrony Cywilnej w procesie osiągania Wyższych Stanów Gotowości Obronnej (WSGO)
Załączniki do planów Obrony Cywilnej	instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w obiekcie użyteczności publicznej
	wskazówki do prowadzenia rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego
	wzór protokołu z przeprowadzonego rozpoznania minersko-pirotechnicznego
	wykaz skrótów stosowanych w tekście
	rodzaj alarmów, sygnały alarmowe potwierdzenie zapoznania się z dokumentem osób funkcyjnych
	wnioski, uwagi i zalecenia osób kontrolujących plan obrony cywilnej
	arkusz kalkulacyjny planu obrony cywilnej
	część graficzna planu

Źródło: Obowiązujące przepisy prawa

Minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii dyrektora Rządowego Centrum Bezpieczeństwa, wydaje w drodze zarządzenia wojewo-

dom wytyczne do wojewódzkich planów zarządzania kryzysowego[49]. Do zadań wojewody w sprawach zarządzania kryzysowego należy realizacja zadań z zakresu planowania cywilnego, w tym wydawanie starostom zaleceń do powiatowych planów zarządzania kryzysowego[50]. Do zadań starosty w sprawach zarządzania kryzysowego należy realizacja zadań z zakresu planowania cywilnego, w tym wydawanie organom gminy zaleceń do gminnych planów zarządzania kryzysowego[51]. Plany działania na poszczególnych poziomach zarządzania kryzysowego powinny być spójne, cele działania ujęte w planie niższego szczebla nie mogą być sprzeczne z planami wyższego szczebla.

W celu zapewnienia spójności poszczególnych planów zarządzania kryzysowego w ustawie z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* przyjęto, że muszą one być oparte na wspólnych dokumentach wyjściowych, i tak: wnioski z Raportu o zagrożeniach bezpieczeństwa narodowego (dla planów sporządzanych na poziomie centralnym), wytyczne ministra właściwego do spraw wewnętrznych (dla planów wojewódzkich), zalecenia wojewody (dla planów powiatowych), zalecenia starosty (dla planów gminnych).

W każdym działaniu zorganizowanym, a takim jest zarządzanie kryzysowe, działania planistyczne pozwalają:

- ukierunkować zarządzanie kryzysowe,
- dokonać przeglądu sił i środków przeznaczonych do wykorzystania w zarządzaniu kryzysowym,
- stworzyć stanowisko kierowania wraz z niezbędnym wyposażeniem,
- wypracować i przyjąć odpowiednie procedury postępowania w zarządzaniu kryzysowym.

Na poziomie krajowym, wojewódzkim, powiatowym i gminnym sporządzane są plany zarządzania kryzysowego, które składają się z planu głównego, zespołu przedsięwzięć na wypadek sytuacji kryzysowych oraz załączników funkcjonalnych planu głównego.

Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* określa również skład planów zarządzania kryzysowego – zob. tabela 58.

Tabela 58. Skład planów zarządzania kryzysowego

Skład plan	Elementy planu
Plan główny	charakterystyka zagrożeń oraz ocena ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej oraz mapy ryzyka i mapy zagrożeń
	zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa
	zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych

[49] Ibidem, art. 13 ust. 3.

[50] Ibidem, art. 14 ust. 2 pkt 2.

[51] Ibidem, art. 17 ust. 2 lit. c.

Zespół przedsięwzięć na wypadek sytuacji kryzysowych	zadania w zakresie monitorowania zagrożeń
	tryb uruchamiania niezbędnych sił i środków uczestniczących w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowej
	procedury reagowania kryzysowego, określające sposób postępowania w sytuacjach kryzysowych współdziałanie między siłami o których mowa w trybie uruchomienia niezbędnych sił i środków
Załączniki funkcjonalne	procedury realizacji zdań z zakresu zarządzania kryzysowego, w tym związane z ochroną infrastruktury krytycznej
	organizacja łączności
	organizacja systemu monitorowania zagrożeń, ostrzegania i alarmowania
	zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń
	organizacja ewakuacji z obszarów zagrożonych
	organizacja ratownictwa, opieki medycznej, pomocy społecznej oraz pomocy psychologicznej
	organizacja ochrony przed zagrożeniami charakterystycznymi dla danego obszaru
	wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie zarządzania kryzysowego
	zasady oraz tryb oceniania i dokumentowania szkód
	procedury uruchamiania rezerw państwowych
	wykaz infrastruktury krytycznej znajdującej się odpowiednio na terenie województwa, powiatu lub gminy objętej planem zarządzania kryzysowego
	priorytety w zakresie ochrony oraz odtworzenia infrastruktury krytycznej

Źródło: Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 5 ust. 2

Plany zarządzania kryzysowego podlegają systematycznej aktualizacji, a cykl planowania nie może być dłuższy niż dwa lata. Cykl planowania jest realizowany przez właściwe organy administracji publicznej oraz podmioty przewidywane do realizacji przedsięwzięć określonych w planie zarządzania kryzysowego w zakresie ich dotyczącym. Plany zarządzania kryzysowego są uzgadniane z kierownikami jednostek organizacyjnych w zakresie ich właściwości.

Na podstawie art. 14 ust. 3 ustawy z dnia 2007 roku *o zarządzaniu kryzysowym*, minister właściwy do spraw wewnętrznych po zasięgnięciu opinii dyrektora Rządowego Centrum Bezpieczeństwa wydaje w drodze zarządzenia wojewodom wytyczne do wojewódzkich planów zarządzania kryzysowego.

Przykład wytycznych do wojewódzkich planów zarządzania kryzysowego[52]

I. Podstawy prawne opracowania Planu Zarządzania Kryzysowego

II. Zasady ogólne

1. Celem opracowania Planów Zarządzania Kryzysowego jest zapewnienie systemowego, skoordynowanego i efektywnego reagowania na zdarzenia, które

[52] K. Sienkiewicz-Małyjurek, F.R. Krynojewski, op. cit., s. 113–117.

powodują lub mogą spowodować stan kryzysu, poprzez kierowanie działaniem wszystkich jednostek organizacyjnych administracji rządowej i samorządowej oraz innych osób prawnych i fizycznych w zakresie:
a) zapobiegania zagrożeniu życia, zdrowia i mienia,
b) zagrożenia środowiska i bezpieczeństwa państwa oraz
c) utrzymania porządku publicznego.

2. Plany Zarządzania Kryzysowego powinny:
   a) określać sposób kierowania działaniami zarządzania kryzysowego,
   b) przydzielać organizacjom i osobom zadania, które powinny być wykonywane w przypadku podjęcia decyzji o uruchomieniu planu zarządzania kryzysowego,
   c) określać możliwe do użycia siły i środki,
   d) opisywać procedury uruchomienia działań ujętych w planie oraz procedury zwracania się do przełożonych o pomoc.
3. Podstawą opracowania Planów Zarządzania Kryzysowego są analizy zagrożeń, potrzeby w zakresie ochrony ludzi i zwierząt, a także:
   a) obowiązujące przepisy dotyczące realizacji zadań ochrony ludzi i zwierząt,
   b) decyzje organów administracji rządowej oraz wytyczne władz samorządowych wyższego szczebla,
   c) zarządzenia organów resortowych,
   d) porozumienia z organizacjami pozarządowymi,
   e) uzgodnienia z organami i instytucjami w zakresie realizacji zadań ochrony ludzi i zwierząt.
4. Plany Zarządzania Kryzysowego powinny zawierać następujące części:
   a) plan główny:
      – charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej oraz mapy ryzyka i mapy zagrożeń,
      – zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa,
      – zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych,
   b) zespół przedsięwzięć na wypadek sytuacji kryzysowych, a w nim:
      – zadania w zakresie monitorowania zagrożeń,
      – tryb uruchamiania niezbędnych sił i środków, uczestniczących w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowej,
      – procedury reagowania kryzysowego określające sposoby postępowania w sytuacjach kryzysowych,
      – współdziałanie między siłami (uczestnikami zarządzania kryzysowego),
   c) załączniki funkcjonalne planu głównego określające:
      – procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną infrastruktury krytycznej,

- organizację łączności,
- organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania,
- zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,
- organizację ewakuacji z obszarów zagrożonych,
- organizację ratownictwa, opieki medycznej, pomocy społecznej oraz pomocy psychologicznej,
- organizację ochrony przed zagrożeniami charakterystycznymi dla danego obszaru,
- wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie zarządzania kryzysowego,
- zasady oraz tryb oceniania i dokumentowania szkód,
- procedury uruchamiania rezerw państwowych,
- wykaz infrastruktury krytycznej znajdującej się odpowiednio na terenie województwa, powiatu lub gminy objętej planem zarządzania kryzysowego,
- priorytety w zakresie ochrony oraz odtworzenia infrastruktury krytycznej.

5. Dokumenty graficzne planu należy opracować na mapach:
   a) województwo – skala 1:100 000,
   b) powiat – skala 1:50 000,
   c) gmina – skala 1:10 000.
6. Do współdziałania w ramach systemu zarządzania kryzysowego należy stosować sieć meldunkową UTM.
7. Instytucje i osoby, którym w planie powierzono zadania, zobowiązane są do opracowania swoich planów operacyjnych (procedur postępowania). Plany operacyjne powinny zawierać harmonogramy realizacji otrzymanych zadań oraz inne ważne informacje.
8. Koordynatorami prac planistycznych są Naczelnicy Wydziałów Zarządzania Kryzysowego starostw i gmin.
9. Plany Zarządzania Kryzysowego przeznaczone są dla właściwych Zespołów Zarządzania Kryzysowego.
10. Zarządzającymi planami są koordynatorzy programów kryzysowych, którzy w imieniu starostów, prezydentów, burmistrzów i wójtów prowadzą uzgodnienia, ustalenia oraz zapewniają ich aktualizację i doskonalenie.
11. Plany Zarządzania Kryzysowego podpisują starostowie, prezydenci, burmistrzowie, wójtowie.
12. Plany podlegają uzgodnieniu:
    a) w Wydziale Zarządzania Kryzysowego Urzędu Wojewódzkiego – plany powiatowe,
    b) w powiatowych wydziałach zarządzania kryzysowego – plany gminne.

13. Plany są zatwierdzane przez:
    a) wojewodów – plany powiatowe,
    b) starostów – plany gminne.
13. Plany Zarządzania Kryzysowego są dokumentami jawnymi, o ile odrębne przepisy nie stanowią inaczej.
14. Wzorcem Planów Zarządzania Kryzysowego gmin i powiatów jest Plan Zarządzania Kryzysowego Województwa stanowiący załącznik do niniejszych wytycznych.
15. Opierając się o rozwiązania przyjęte w planach wojewódzkich, przy opracowaniu powiatowych i gminnych planów należy stosować następujące zasady:
    a) plan powinien być realny do wykonania, a w szczególności:
        – dostosowany do występujących zagrożeń,
        – dostosowany do możliwości organizacyjnych i personalnych podmiotów wchodzących w skład systemu zarządzania kryzysowego powiatu/gminy,
    b) dopuszczalne jest stosowanie wcześniej przyjętych rozwiązań, takich jak:
        – zasady współdziałania,
        – szczegółowe rozwiązania organizacyjne,
        – organizacja i numeracja elementów planu,
    c) plan powinien zapewnić wypełnienie następujących funkcji:
        – plan wojewódzki:
            ▫ koordynacja działań,
            ▫ dysponowanie siłami odwodowymi,
            ▫ zapewnienie wsparcia szczebla centralnego,
            ▫ współdziałanie z Siłami Zbrojnymi RP,
            ▫ współdziałanie z sąsiadami,
            ▫ pomoc międzynarodowa,
            ▫ ocena strat,
        – plan powiatowy:
            ▫ koordynacja działań,
            ▫ dysponowanie siłami powiatowymi,
            ▫ zapewnienie wsparcia szczebla wojewódzkiego,
            ▫ współdziałanie z sąsiadami,
            ▫ ocena strat,
        – plan gminny:
            ▫ bezpośrednia likwidacja skutków zdarzenia,
            ▫ organizacja pomocy dla poszkodowanej ludności,
            ▫ zapewnienie wsparcia szczebla powiatowego,
            ▫ współdziałanie z sąsiadami,
            ▫ szacowanie i wycena strat.
17. Tracą moc obowiązujące wytyczne wojewody z dnia.../.../ r. w sprawie zasad opracowania powiatowego planu zarządzania kryzysowego.
18. Wytyczne wchodzą w życie z dniem podpisania.

Przykład gminnego/powiatowego planu zarządzania kryzysowego[53]

I. Opis miasta i gminy/powiatu
1. Położenie miasta i gminy/powiatu.
2. Podział administracyjny.
3. Ludność.
4. Klimat, zasoby wodne, zasoby leśne.
5. Ukształtowanie terenu.
6. Charakterystyka zabudowy.
7. Charakterystyka obiektów kultury.
8. Gospodarka, rolnictwo.
9. Charakterystyka ochrony zdrowia i opieki społecznej.

II. Charakterystyka zagrożeń miasta i gminy/powiatu i ocena ryzyka ich występowania

1. Analiza ilościowa zagrożeń miasta i gminy/powiatu
   - zagrożenia naturalne,
   - zagrożenia techniczne,
   - zagrożenia ekologiczne,
   - zagrożenia biologiczne,
   - pożary,
   - katastrofy,
   - terroryzm,
   - przestępczość zorganizowana,
   - niepokoje społeczne,
   - prognoza zmian zachodzących w środowisku.
3. Analiza przyczyn i skutków zagrożeń.
4. Ocena ryzyka wystąpienia zagrożeń.
5. Wnioski i oceny zagrożeń.

III. Organizacja reagowania, planowanie przedsięwzięcia oraz podział obowiązków

1. Organizacja systemu monitorowania zagrożeń, ostrzegania i alarmowania.
2. Obieg informacji pomiędzy podmiotami zarządzania kryzysowego:
   - informowanie,
   - ostrzeganie,
   - alarmowanie.
3. Informowanie, ostrzeganie, alarmowanie ludności.
4. Organizacja łączności.
5. Zadania i odpowiedzialność wydziałów oraz jednostek organizacyjnych urzędu.
6. Procedura uruchamiania działań Gminnego/Powiatowego Zespołu Zarządzania Kryzysowego:
   - ogólna koncepcja ratownictwa,

[53] J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego*, Kraków 2010, s. 172–174.

- przewidywane warianty działań w sytuacjach kryzysowych,
- procedura działań Gminnego/Powiatowego Zespołu Zarządzania Kryzysowego w fazie reagowania,
- zadania Gminnego/Powiatowego Zespołu Zarządzania Kryzysowego i osób funkcyjnych Zespołu,
- wsparcie organów niższego szczebla administracji publicznej,
- zasady współdziałania podmiotów lokalnych w sytuacjach kryzysowych,
- organizacja ewakuacji ludności z obszarów zagrożonych,
- organizacja pomocy społecznej i medycznej,
- organizacja ochrony przed zagrożeniami radiologicznymi, chemicznymi i biologicznymi,
- działania w fazie odbudowy, zasady oraz tryb oceniania i dokumentowania szkód.

7. Zasady współdziałania z sąsiednimi powiatami.
8. Przyjmowanie pomocy humanitarnej.

IV. Charakterystyka zasobów sił i środków zarządzania kryzysowego oraz ocena możliwości ich wykorzystania.

1. Udział administracji publicznej w zarządzaniu kryzysowym:
   - wykaz jednostek administracji publicznej działających na terenie miasta i gminy/powiatu,
   - jednostki organizacyjne podporządkowane wójtowi/burmistrzowi,
   - analiza funkcjonowania administracji publicznej i możliwości wykorzystania w sytuacji kryzysowej.
2. Struktura zarządzania kryzysowego w miesicie i gminie/powiecie – baza danych sił i środków reagowania.
3. Zasady pozyskiwania zasobów finansowych.
4. Sposoby wykorzystania sił i środków spoza miasta i gminy/powiatu:
   - pomoc wojewody,
   - możliwości wykorzystania organizacji pozarządowych,
   - możliwości przyjęcia międzynarodowej pomocy humanitarnej i ratowniczej.
5. Zasoby specjalistycznych sił i środków.
6. Udział formacji obrony cywilnej szczebla gminnego w sytuacjach kryzysowych.
7. Wykorzystanie regionalnych środków masowego przekazu w stanach klęsk żywiołowych:
   - podstawy prawne,
   - procedura przekazania mediom informacji w sytuacji będącej/ niebędącej stanem klęski żywiołowej.

Załączniki do planu:

Załącznik nr 1. Zadania grup stałych i czasowych.

Załącznik nr 2. Wykaz organizacji pozarządowych.

Załącznik nr 3. Obowiązujące akty prawne zarządzania kryzysowego.

Załącznik nr 4. Wykaz specjalistycznych sił i środków.

Załącznik nr 5. Materiały pomocnicze z zakresu zagrożeń epidemiologicznych, chemicznych i radiacji.

Załącznik nr 6. Wykaz regionalnych środków masowego przekazu.

Załącznik nr 7. Porozumienia i uzgodnienia z zakresu realizacji zadań w sytuacjach kryzysowych.

Załącznik nr 8. Procedury postępowania w sytuacji kryzysowej na szczeblu powiatu.

Załącznik nr 9. Wykaz telefonów stacjonarnych i komórkowych osób funkcyjnych oraz podmiotów, które mogą być zaangażowane do likwidacji powstałych zagrożeń.

Załącznik nr 10. Objaśnienia skrótów użytych w Powiatowym Planie Zarządzania Kryzysowego.

Załącznik nr 11. Wykaz podmiotów zapoznanych z planem.

Załącznik nr 12. Zasady i tabela aktualizacji planu.

Istotą planu zarządzania kryzysowego jest integracja różnych podmiotów w celu skutecznego wykonawstwa zadań określonych w ustawie z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* i innych ustawach. W tym celu każdy plan musi zawierać siatkę bezpieczeństwa, przez którą należy rozumieć zestawienie potencjalnych zagrożeń ze wskazaniem podmiotów wiodących przy ich usuwaniu oraz podmiotów współpracujących[54]. Jest ona sporządzana na każdym poziomie zarządzania kryzysowego przy uwzględnieniu specyfiki danego terenu. Przykładową siatkę bezpieczeństwa przedstawia tabela 59.

Tabela 59. Siatka bezpieczeństwa

Nr algorytmu działania	Zdarzenie kryzysowe lub sytuacje mogące prowadzić do zdarzeń kryzysowych	MSW	MZ	MŚ	MI	MRiRW	MON	ABW	AW	MSZ	MPiPS	MG	MF
1.	Pożary	PWi	PWs	PWs			PWs						PWs
2.	Huragany	PWi	PWs	PWs			PWs						PWs
3.	Powodzie	PWi	PWs	PWs			PWs						PWs
4.	Mrozy	PWi	PWs	PWs			PWs						PWs
5.	Susze	PWi	PWS	PWs			PWs						PWs
6.	Lawiny błotne, osuwiska	PWi	PWs	PWs			PWs						PWs
7.	Smog	PWi	PWs	PWs			PWs						PWs
8.	Trzęsienie ziemi	PWi	PWs	PWs									PWs

[54] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 3 pkt 8.

9.	Skażenia chemiczne/ ekologiczne	PWi	PWs	PWs	PWs		PWs	PWs					PWs
10.	Skażenia radiacyjne	PWi	PWs	PWs			PWs	PWs					PWs
11.	Zakłócenia w systemie energetycznym	PWs					PWs	PWs				PWi	PWs
12.	Zakłócenia w systemie gazowym	PWs					PWs	PWs				PWi	PWs
13.	Zakłócenia w systemie paliwowym	PWs					PWs	PWs				PWi	PWs
14.	Terroryzm	Zaangażowanie poszczególnych instytucji zgodnie z siatką bezpieczeństwa dla zdarzeń terrorystycznych											
15.	Zagrożenia dla obywateli RP poza granicami państwa	PWs					PWs	PWs	PWs	PWi			
16.	Protesty	PWi									PWs		PWs
17.	Choroby zwierząt		PWs			PWi							PWs
18.	Choroby ludzi (epidemie)		PWi							PWs			PWs
19.	Choroby roślin					PWi							PWs
20.	Awarie sieci telekomunikacyjnej				PWi			PWs	PWs	PWs			PWs
21.	Zagrożenia o charakterze polityczno-militarnym	PWs					PWs		PWs	PWi			PWs

Legenda: PWi – podmioty wiodące, PWs – podmioty współpracujące

Ponadto siatka bezpieczeństwa jest sporządzana na poziomie centralnym dla zagrożeń terrorystycznych.

Zgodnie z art. 5 ust. 3 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* Krajowy Plan Zarządzania Kryzysowego oraz wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego podlegają systematycznej aktualizacji, a cykl planowania nie może być dłuższy niż dwa lata. Plany zarządzania kryzysowego uzgadnia się z kierownikami jednostek organizacyjnych w zakresie dotyczącym planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planie.

Przy Radzie Ministrów tworzy się Rządowy Zespół Zarządzania Kryzysowego (RZZK) jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania

i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego[55]. Do zadań Rządowego Zespołu Zarządzania Kryzysowego należy opiniowanie i przedkładanie Radzie Ministrów Krajowego Planu Zarządzania Kryzysowego[56]. Plany zarządzania kryzysowego są uzgadniane z dyrektorem Rządowego Centrum Bezpieczeństwa i stanowią załącznik do Krajowego Planu Zarządzania Kryzysowego[57]. Organem właściwym w sprawach zarządzania kryzysowego na terenie województwa jest wojewoda[58]. Do zadań wojewody w sprawach zarządzania kryzysowego należy realizacja zadań z zakresu planowania cywilnego, w tym zatwierdzanie powiatowych planów zarządzania kryzysowego. Minister właściwy do spraw wewnętrznych zatwierdza wojewódzkie plany zarządzania kryzysowego i ich aktualizację, po zasięgnięciu opinii dyrektora Rządowego Centrum Bezpieczeństwa[59]. Organem właściwym w sprawach zarządzania kryzysowego na obszarze powiatu jest starosta jako przewodniczący zarządu powiatu[60]. Do zadań starosty w sprawach zarządzania kryzysowego należy realizacja zadań z zakresu planowania cywilnego, w tym zatwierdzanie planu zarządzania kryzysowego.

Podstawowe elementy składowe powiatowych i wojewódzkich planów ratowniczych

System ratowniczy na obszarze województwa i powiatu działa na podstawie planów ratowniczych, które, poprzedzone analizą wystąpienia na danym obszarze możliwych zagrożeń, a także analizą zabezpieczenia operacyjnego terenu, powinny zawierać:

- zadania i zakres czynności realizowanych przez podmioty systemu ratowniczego,
- zbiór procedur ratowniczych wynikających z zadań systemu ratowniczego,
- wykaz sił i środków podmiotów systemu ratowniczego,
- dokumentację graficzną,
- arkusze uzgodnień i aktualizacji planów ratowniczych.

Plany ratownicze działań w czasie katastrof, klęsk żywiołowych i zdarzeń nadzwyczajnych muszą być spójne z planami zarządzania kryzysowego, o czym stanowi ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*. Problematyka planowania ratowniczego na poziomie województwa i powiatu została uregulowana rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 grudnia 1999 roku *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego*[61].

[55] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 8.

[56] Ibidem, art. 9.

[57] Ibidem, art. 12 ust. 2a.

[58] Ibidem, art. 14 ust. 1.

[59] Ibidem, art. 14 ust. 4.

[60] Ibidem, art. 17 ust. 1.

[61] Dz. U. z 1999 r. Nr 111, poz. 1311.

Tabela 60. Elementy składowe powiatowych i wojewódzkich planów ratowniczych

Elementy podstawowe	Elementy szczegółowe
Zadania dla podmiotów ratowniczych oraz podmiotów współpracujących z systemem w zakresie alarmowania o zagrożeniu, prognozowania jego rozwoju, prowadzenia działań ratowniczych oraz usuwania skutków zdarzenia	
Rozmieszczenie (sieć) podmiotów systemu według podziału	Państwowa Straż Pożarna
	ochotnicze straże pożarne
	specjalistyczne grupy ratownicze
	krajowa baza sprzętu specjalistycznego, w tym miejsca składowania środków gaśniczych, sorbentów, neutralizatorów oraz sprzętu logistycznego na potrzeby zabezpieczenia działań ratowniczych
	pozostałe siły i środki systemu
Rozmieszczenie podmiotów współdziałających z systemem	
Wykaz powiatowych, wojewódzkich i krajowych specjalistów do spraw ratownictwa	
Zbiorczy wykaz sił i środków przeznaczonych do prowadzenia działań ratowniczych w zakresie:	ratownictwa medycznego
	ratownictwa chemicznego i ekologicznego
	ratownictwa technicznego
	gaszenia pożarów
	walki z klęskami żywiołowymi
Zbiorczy wykaz sił i środków przeznaczonych do wsparcia kwatermistrzowskiego i logistycznego działań ratowniczych	
Wykaz szpitali posiadających możliwość przyjęcia poszkodowanych w wyniku zdarzeń jednostkowych i masowych	
Wykaz podmiotów odpowiedzialnych za przyjęcie ewakuowanej ludności do kwater zastępczych lub tymczasowych	
Wykaz podmiotów realizujących działania z zakresu ładu i porządku, usuwania skutków zdarzenia, w tym oczyszczania i usuwania odpadów poakcyjnych oraz zabezpieczenia sanitarno-epidemiologicznego	
Zbiorcze zestawienie procedur	przyjmowania informacji o zdarzeniu oraz alarmowania i dysponowania sił i środków systemu w zależności od rodzaju i wielkości zdarzenia oraz sił współdziałających z systemem
	powiadamiania podmiotów odpowiedzialnych za ostrzeganie ludności przy prognozowanym lub istniejącym zagrożeniu
	powiadamiania przez powiatowe stanowiska kierowania: starosty prezydenta (burmistrza, wójta) członków powiatowego zespołu do spraw ochrony przeciwpożarowej i ratownictwa członków sztabu komendanta powiatowego Państwowej Straży Pożarnej kierownictw podmiotów tworzących i wspomagających system na poziomie powiatowym
	powiadamiania przez wojewódzkie stanowisko koordynacji ratownictwa: Krajowego Centrum Koordynacji Ratownictwa wojewody starostów

	członków wojewódzkiego zespołu ds. ochrony przeciwpożarowej i ratownictwa członków sztabu komendanta wojewódzkiego Państwowej Straży Pożarnej dowódców odwodów operacyjnych kierownictw podmiotów tworzących i wspomagających system na poziomie wojewódzkim
	alarmowania: podmiotów odpowiedzialnych za transport i przyjęcie poszkodowanych podmiotów odpowiedzialnych za przyjęcie i zabezpieczenie potrzeb socjalnych ewakuowanej ludności podmiotów wspomagających działania ratownicze oraz zaplecze kwatermistrzowsko-logistyczne sił systemu podmiotów wspierających psychicznie i humanitarnie ewakuowaną ludność podmiotów współdziałających z systemem
	funkcjonowania stanowisk kierowania oraz sił systemu podczas katastrof, klęsk żywiołowych i sytuacji nadzwyczajnych zagrożeń życia, zdrowia lub środowiska
	postępowania podmiotów systemu przy zdarzeniach uwzględniających specyfikę zagrożeń na danym obszarze operacyjnym
Zasady współdziałania	sztabu lub kierującego działaniem ratowniczym z podmiotami systemu i wspomagającymi system
	kierującego działaniem ratowniczym, sztabu lub stanowisk kierowania ze środkami masowego przekazu
	kierującego działaniem ratowniczym, sztabu lub stanowisk kierowania z zagranicznymi podmiotami ratowniczymi
Załączniki do powiatowych planów ratowniczych	
plan alarmowania i prowadzenia działań ratowniczych poszczególnych podmiotów systemu	
sposoby postępowania na wypadek powstania pożaru, klęski żywiołowej lub innego miejscowego zagrożenia dla zakładów (zakładowe plany ratownicze)	
plany działań ratowniczych na autostradach i drogach szybkiego ruchu	
plany działań ratowniczych na obszarach leśnych	
gminne plany ratownicze (dotyczy gmin posiadających plany ratownicze)	
plany działań ratowniczych według potrzeb poszczególnych powiatów	
plan działania powiatowego zespołu do spraw ochrony przeciwpożarowej i ratownictwa	
Załączniki do wojewódzkich planów ratowniczych	
plany alarmowania i uruchamiania wojewódzkich odwodów operacyjnych oraz Krajowych Baz Sprzętu Specjalistycznego	
plany ewakuacji ludzi, zwierząt i mienia z miast, gmin i powiatów na czas klęsk żywiołowych lub sytuacji nadzwyczajnych zagrożeń życia, zdrowia lub środowiska	
powiatowe plany ratownicze	
plany działań ratowniczych według potrzeb poszczególnych województw	
plan działania wojewódzkiego zespołu do spraw ochrony przeciwpożarowej i ratownictwa	

Źródło: Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 grudnia 1999 roku *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311)

6.6. Planowanie logistyczne w zarządzaniu kryzysowym

Uczestnictwo grup logistycznych (grup zabezpieczenia logistycznego, grup opieki zdrowotnej i pomocy socjalno-bytowej) w fazie decyzyjnej planowania ma na celu dostarczenie danych logistycznych niezbędnych całemu Zespołowi Zarządzania Kryzysowego (ZZK), w tym szczególnie jego szefowi (przewodniczącemu, kierownikowi), co do oceny sytuacji kryzysowej, podjęcia decyzji i sprecyzowania zamiaru prowadzenia operacji kryzysowej, zarządzeń i decyzji administracyjnych dla podległych i podporządkowanych podmiotów wykonawczych[62].

Istotnym przedsięwzięciem jest opracowanie planu pracy grup logistycznych, który jest swoistą kalkulacją czasu, prowadzoną w celu wskazania terminów wykonania podstawowych zadań logistycznych. W planie tym w uzasadnionych przypadkach należy uwzględnić czas na:

- przeprowadzenie rekonesansu logistycznego rejonu działania, w którym wystąpiła sytuacja kryzysowa,
- udzielenie pomocy logistycznym grupom roboczym ZZK na niższym szczeblu administracji publicznej,
- udzielenie instruktażu kierownikom podmiotów wykonujących zadania logistyczne na rzecz ludności poszkodowanej, a także czas na kontrolę[63].

Załączniki do planu zarządzania kryzysowego opracowywane przez grupy logistyczne ZZK to przede wszystkim[64]:

- przygotowane przez grupę zabezpieczenia logistycznego:
  - plan dostaw zaopatrzenia dla ludności poszkodowanej,
  - plan świadczenia usług gospodarczo-bytowych,
  - plan organizacji tymczasowych miejsc zakwaterowania,
  - inne plany w zależności od potrzeb.
- przygotowane przez grupę opieki zdrowotnej i pomocy socjalno-bytowej:
  - plan organizacji ewakuacji medycznej,
  - plan organizacji przedsięwzięć sanitarno-higienicznych,
  - plan organizacji przedsięwzięć przeciwepidemicznych,
  - plan zaopatrzenia w sprzęt i materiały medyczne,
  - plan organizacji pomocy socjalno-bytowej,
  - inne plany w zależności od potrzeb.

62 E. Nowak, *Zarządzanie logistyczne w sytuacjach kryzysowych*, Warszawa 2008, s. 56.

63 Szerzej na ten temat ibidem, s. 57.

64 Ibidem, s. 60–61.

Przykładowe dokumenty logistyczne opracowywane przez grupy logistyczne Zespołów Zarządzania Kryzysowego[65]

1. Plan gromadzenia i dostaw zaopatrzenia dla ludności poszkodowanej

Tabela 61. Stan zapasów zaopatrzenia

Rodzaj zaopatrzenia	Miejsce składowania	Wielkość zapasów			Uwagi
		norma	faktyczna	niedobór	
Woda butelkowana	m. m. m. m.	5000 litrów 2000 litrów 1800 litrów 3000 litrów	4500 litrów 2000 litrów 1500 litrów 3000 litrów	500 litrów – 300 litrów –	przydatność do spożycia 12 miesięcy
Należność żywnościowa „PS-L" „S"	m. m. m. m.	4000 rdz 5000 rdz 1600 rdz 1900 rdz	5000 rdz 7000 rdz 1600 rdz 1900 rdz	1000 rdz 2000 rdz – –	przydatność do spożycia 24 miesiące przydatność do spożycia 36 miesięcy
Zestawy medyczne, pomoc przedlekarska	m. m. m. m	10 kpl 20 kpl 15 kpl 10 kpl	8 kpl 18 kpl 15 kpl 10 kpl	2 kpl 2 kpl – –	
Torba ratownika	m. m. m. m	5 kpl 6 kpl 4 kpl 2 kpl	3 kpl 4 kpl 4 kpl 2 kpl	2 kpl 2 kpl – –	
Itd.					

Tabela 62. Plan dostaw zaopatrzenia

Rodzaj zaopatrzenia	Norma dzienna	Kalkulacja dostaw w dniu…				Uwagi
		limit	miejsce dostawy	potrzeby	wielkość	
Woda butelkowana	1 litr 1 litr 1 litr 1 litr	0,5 litra 0,5 litra 0,5 litra 0,5 litra	m. m. m. m.	800 osób 400 osób 300 osób 200 osób	400 litrów 200 litrów 150 litrów 100 litrów	Dostawy samochodem
Należność żywnościowa „PS-L" „S"	1 rdz 1 rdz	2/3 rdz 1/2 rdz	m. m. m. m.	800 osób 250 osób 300 osób 200 osób	534 rdz 167 rdz 150 rdz 100 rdz	8.30 10.00 12.00 16.00
Zupa regeneracyjna	1 porcja	1 porcja	m.	800 osób	800 porcji	Restauracja „Miła"
Obiad	1 zestaw	1 zestaw	m.	400 osób	400 zestawów	Z kuchni polowej
Itd.						

[65] Plany wykonano na podstawie: ibidem, s. 100–106.

2. Plan świadczenia usług gospodarczo-bytowych dla ludności poszkodowanej

Tabela 63. Plan świadczenia usług gospodarczo-bytowych dla ludności poszkodowanej

Rodzaj usługi	Sposób realizacji usługi				Uwagi
	Miejscowość	Czas realizacji	Sposób świadczenia	Odpowiedzialny	
Zaopatrywanie w produkty powszechnego użytku	m. m. m. m	8.00–12.00 17.07.12 16.00–19.00 18.07.12	magazyn pomocy społecznej	Wójt Sołtys Sołtys Sołtys	wydawanie wg rozdzielnika
Usługi handlowe	m. m. m. m	8.00–12.00 17.07.12 16.00–19.00 18.07.12	system obwoźny system obwoźny	Referat handlu i usług Gminy…	samochód z przyczepą
Itd.					

3. Plan ewakuacji m… i gminy… dotkniętych powodzią

Tabela 64. Plan ewakuacji m… i gminy… dotkniętych powodzią

Rodzaj zadania	Wielkość zadania (osoby)	Docelowy rejon ewakuacji	Specyfika zadania transportowego					Uwagi
			Odległość w km	Rodzaj transportu	Liczba środków transportu	Liczba kursów	Czas rozpoczęcia ewakuacji	
Ewakuacja mieszkańców gminy… Sektor I Sektor II Sektor III	4320 1500 1620 1200	Zgrupowanie tymczasowe	… … … …	Kolumna MZK Kolumna MZK Kolumna MZK	liczba autobusów liczba osób	... … … …	04.12 10.00 04.12 11.00 04.12 12.00 04.12	ul. ul. ul. ul.
Ewakuacja mieszkańców pozostałych m… Gminy… Sektor I Sektor II Sektor III		Zgrupowanie tymczasowe	… … … …	Kolumna MZK Kolumna MZK Kolumna MZK	liczba autobusów liczba osób	… … … …	04.12 10.00 04.12 11.00 04.12 12.00 04.12	ul. ul. ul. ul.
Itd.								

4. Plan organizacji tymczasowych miejsc zakwaterowania w akcji przeciwpowodziowej w gminie…

Tabela 65. Plan organizacji tymczasowych miejsc zakwaterowania w akcji przeciwpowodziowej w gminie…

Nazwa tymczasowego miejsca zakwaterowania, miejscowość, wielkość zadania	Rodzaj zakwaterowania i pojemność		Warunki gospodarczo-bytowe			Opieka medyczna	Uwagi
	budynki stałe	namioty	źródło wody pitnej	sposób żywienia	odbiór ścieków		
Zgrupowanie nr 1 Zakwaterowanie osób… m. m. m. m.	 -miejsc -miejsc -miejsc -miejsc	 -miejsc -miejsc -miejsc -miejsc	 wodociągi wodociągi cysterny cysterny	 stołówka kuchnia polowa	 kanalizacja kanalizacja TOI TOI kanalizacja	 NZOZ „OME-GA” w m…	
Razem	-miejsc	-miejsc					
Zgrupowanie nr 2 Zakwaterowanie osób… m. m. m. m.	 -miejsc -miejsc -miejsc -miejsc	 -miejsc -miejsc -miejsc -miejsc	 wodociągi wodociągi cysterny cysterny	 stołówka kuchnia polowa	 kanalizacja kanalizacja TOI TOI kanalizacja	 NZOZ „S-MED” w m…	
Razem	-miejsc	-miejsc					
Zgrupowanie nr 3 Zakwaterowanie osób… m. m. m. m	 -miejsc -miejsc -miejsc -miejsc	 -miejsc -miejsc -miejsc -miejsc	 wodociągi wodociągi cysterny cysterny	 stołówka kuchnia polowa	 kanalizacja kanalizacja TOI TOI kanalizacja	 NZOZ „E-MED” w m…	
Razem	-miejsc	-miejsc					
Zgrupowanie nr 3 Zakwaterowanie osób… m. m. m. m	 -miejsc -miejsc -miejsc -miejsc	 -miejsc -miejsc -miejsc -miejsc	 wodociągi wodociągi cysterny cysterny	 stołówka kuchnia polowa	 kanalizacja kanalizacja TOI TOI kanalizacja	 NZOZ „ALFA” w m…	
Razem	-miejsc	-miejsc					
Ogółem	-miejsc	-miejsc					

5. Plan ewakuacji i opieki socjalno-bytowej

Tabela 66. Ewakuacja medyczna

Rodzaj zadania	Wielkość zadania	Miejsce		Kalkulacja ewakuacji				Uwagi
		Załad.	Wyład.	Rodzaj transportu	Liczba środków ewakuacji	Odległość ewakuacji	Liczba rejsów	
Ewakuacja ciężko rannych i chorych	60 osób	m…	m…	samochód ciężarowy	3	30	5	Droga ewakuacji
Ewakuacja lekko rannych	180 osób	m…	m…	samochód ciężarowy	5	40	2	Droga ewakuacji

Tabela 67. Opieka socjalno-bytowa

Rodzaj zadania	Liczba potrzebujących	Miejsce realizacji	Wielkość		Uwagi
			jednostkowa	ogółem	
Wypłata zasiłku pieniężnego	600 rodzin	m…	300 zł	18 000 zł	Urząd Pocztowy
Wypłata zasiłku pieniężnego	400 rodzin	m…	300 zł	12 000 zł	Bank Spółdzielczy
Gorący posiłek	1000 osób	m…	Zupa regeneracyjna	1000 porcji	Restauracja „MIŁA”
Gorący posiłek	900 osób	m…	Zupa regeneracyjna	900 porcji	Bar „Turysta”
Zaopatrzenie w buty gumowe	500 osób	m…	Par butów	500	Punkt pomocy społecznej

6.7. Plany obrony cywilnej

Plan zarządzania kryzysowego nie jest jedynym dokumentem, opracowywanym przez uprawnione podmioty na wszystkich poziomach zarządzania kryzysowego w państwie. Jego uzupełnienie w formie załącznika stanowi m.in. plan obrony cywilnej. W zależności od oceny zagrożeń na danym terenie opracowuje się również:

- operacyjne plany przeciwpowodziowe dla gmin, powiatów, województw, zakładów pracy, które uczestniczą w tym procesie,
- plany ochrony zabytków na wypadek sytuacji kryzysowych i konfliktu zbrojnego, dla zabytków gminy, powiatu, województwa, które z założenia stanowią uzupełnienie planów obrony cywilnej,

- dokumentację planowych działań zapewnienia funkcjonowania publicznych urządzeń zaopatrzenia w wodę w warunkach specjalnych – dla gmin – również forma uzupełnienia planu obrony cywilnej[66].

Podstawę tworzenia Planu obrony cywilnej stanowią Wytyczne Szefa Obrony Cywilnej Kraju z dnia 27 grudnia 2011 roku *w sprawie zasad opracowania planu obrony cywilnej województw, powiatów, gmin i zakładów pracy*. Wytyczne do opracowania planów obrony cywilnej są bardzo szczegółowe i obowiązują na wszystkich poziomach administracyjnych. Występujące różnice mają związek nie tylko z realizowanymi zadaniami, ale i specyfiką danego województwa, powiatu czy gminy.

Plan obrony cywilnej opracowuje się w celu ustalenia i przygotowania sposobu realizacji zadań obrony cywilnej na czas zewnętrznego zagrożenia bezpieczeństwa państwa i wojny. Plan obrony cywilnej podlega bieżącej aktualizacji, nie rzadziej jednak niż co dwa lata. O nadaniu klauzuli niejawności planu obrony cywilnej decyduje organ sporządzający plan, stosownie do zawartych w nim informacji.

Szef obrony cywilnej województwa określa szczegółowe zasady opracowania planu obrony cywilnej powiatów, analogiczne zasady określa szef obrony cywilnej dla planów obrony cywilnej gmin.

Plan obrony cywilnej podpisany przez kierownika komórki organizacyjnej koordynującej jego opracowanie zatwierdza odpowiednio[67]:

- plan obrony cywilnej województwa – szef obrony cywilnej województwa,
- plan obrony cywilnej powiatu – szef obrony cywilnej powiatu,
- plan obrony cywilnej gminy – szef obrony cywilnej gminy,
- kartę realizacji zadania obrony cywilnej jednostki organizacyjnej – kierownik tej jednostki.

Plan obrony cywilnej składa się z planu głównego, procedur postępowania oraz kart realizacji zadań obrony cywilnej, załączników funkcjonalnych, informacji uzupełniających, innych dokumentów, według decyzji organu sporządzającego plan[68]. Plan powinien odwoływać się do informacji zawartych w planie zarządzania kryzysowego, o którym mowa w ustawie z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[69], dokonując korelacji danych rzeczowo-materiałowych i osobowych oraz informacji wynikających z planu operacyjnego funkcjonowania województwa, powiatu i gminy w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.

Plan obrony cywilnej opracowywany jest w formie dokumentów opisowych i aplikacji komputerowych pozwalających na zbieranie i przetwarzanie danych niezbędnych do planów obrony cywilnej oraz dokumentów graficznych – map,

[66] K. Sienkiewicz-Małyjurek, F.R. Krynojewski, op. cit., s. 113–117.

[67] Wytyczne Szefa Obrony Cywilnej Kraju z dnia 27 grudnia 2011 roku *w sprawie zasad opracowania planu obrony cywilnej województw, powiatów, gmin i zakładów pracy*, § 13. – www.uw.olsztyn.pl/zkso/prawo/wytyczneplan oc (pobrano 15.04.2012).

[68] Ibidem, § 17.

[69] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

planów, szkiców i aplikacji komputerowych pozwalających zbierać, przetwarzać i wizualizować dane graficzne.

Tabela 68. Elementy planu obrony cywilnej

Elementy planu obrony cywilnej	Szczegóły elementów planu obrony cywilnej
Plan główny	zarządzenie wprowadzające plan obrony cywilnej do zastosowania
	arkusz uzgodnień
	rejestr zmian
	wnioski z oceny zagrożenia czasu pokoju oraz charakterystyka zagrożeń na wypadek zagrożenia zewnętrznego państwa i w czasie wojny
	zadania i obowiązki osób i podmiotów, którym powierzono realizację zadań obrony cywilnej, a także zestawienie zadań obrony cywilnej realizowanych przez jednostki organizacyjne na administrowanym terenie
	charakterystyka struktur organizacyjnych i zasobów oraz możliwości ich wykorzystania
	ogólna koncepcja działania w okresie zagrożenia zewnętrznego państwa i w czasie wojny
	terminy i tryb realizacji
	inne
Procedury postępowania	związane z podnoszeniem gotowości obronnej i odnoszące się głównie do czasu zewnętrznego zagrożenia bezpieczeństwa państwa i wojny
	inne według decyzji organu sporządzającego plan
Załączniki funkcjonalne	monitorowanie zagrożeń, ostrzeganie i alarmowanie, w tym informowanie ludności o zagrożeniach i sposobach postępowania,
	kierowanie i łączność,
	ewakuacja ludności, zwierząt i mienia na wypadek zagrożenia bezpieczeństwa państwa i wojny,
	opieka medyczna, pomoc społeczna i pomoc psychologiczna i religijna,
	odkażanie i inne podobne działania ochronne,
	przygotowanie i organizowanie budowli ochronnych,
	obsługa środków zaciemnienia,
	ratownictwo,
	walka z pożarami,
	wykrywanie i oznaczenie stref niebezpiecznych,
	dostarczanie doraźnych pomieszczeń i zaopatrzenia,
	doraźne przywrócenie działania niezbędnych służb użyteczności publicznej
	doraźne grzebanie zmarłych
	pomoc w ratowaniu dóbr niezbędnych do przetrwania,
	doraźna pomoc dla przywrócenia i utrzymania porządku w strefach dotkniętych klęskami
	dodatkowe rodzaje działalności, niezbędne dla wypełnienia któregoś z zadań wyżej wymienionych, w tym planowanie i prace organizacyjne
Informacje uzupełniające stanowią niezbędny zbiór danych potrzebnych do planowania i podejmowania decyzji oraz kierowania działaniami takimi, jak mapy, schematy, dane informatyczne, zestawienia itp.	

Wykazy dokumentów planistycznych na szczeblu jednostki organizacyjnej opracowującej plany obrony cywilnej, określonych wymogami innych przepisów (według uznania organu sporządzającego plan)	plany operacyjne plany ochrony plany ratownicze itp.

Źródło: Wytyczne Szefa Obrony Cywilnej Kraju z dnia 27 grudnia 2011 roku *w sprawie zasad opracowania planu obrony cywilnej województw, powiatów, gmin i zakładów pracy*

Tabela 69. Struktura planu obrony cywilnej*

Nazwa dokumentu	Województwo	Powiat	Gmina	Zakład pracy	Uwagi
Ocena zagrożenia i zamiar działania	X	X			
Plan ewakuacji/przyjęcia ludności	X	X			
Plan zabezpieczenia logistycznego OC	X	X	X	X	
Plan działania OC w procesie osiągania wyższych stanów gotowości bojowej	X	X	X	X	
Dokumenty specjalistyczne zespołu kierowania	-	–	–	–	

* X oznacza, że wykonuje się jako jeden dokument: na szczeblu powiatowym dopuszcza się łączenie dokumentów nr 1 i 2; na szczeblu gminy dopuszcza się łączenie dokumentów nr 1 i 3 lub opracowanie dokumentu nr 1, 2 i 3 oddzielnie.

Źródło: K. Sienkiewicz-Małyjurek, F.R. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej,* Warszawa 2010, s. 152

ROZDZIAŁ 7

Podsystem kierowania

7.1. Istota podsystemu kierowania

Kierowanie jest procesem planowania, organizowania, przewodzenia i kontrolowania działalności członków organizacji oraz wykorzystywania wszelkich zasobów organizacji do osiągnięcia jej celów[1]. Kierowanie możemy również rozpatrywać jako zbiór funkcji kierowniczych bądź jako fazy kierowania. Do funkcji kierowniczych zalicza się wspomniane planowanie, organizowanie, przewodzenie i kontrolowanie. Natomiast na fazy kierowania składają się:

– wybór zadania,
– przekazanie podwładnym ogólnie sformułowanego zadania,
– przekazanie ewentualnych instrukcji w sprawie sposobu wykonania zadań,
– stworzenie sytuacji motywacyjnych,
– stworzenie warunków wykonania zadań,
– nadzór, kontrola kierownicza i dopilnowanie wykonania zadań[2].

Oznacza to, że kierowanie jest procesem, gdzie wszyscy kierownicy, bez względu na osobiste uzdolnienia i umiejętności, podejmują pewne wzajemnie powiązane działania prowadzące do osiągania pożądanych celów[3].

Kierowanie to także jeden ciąg decydowania, czyli nielosowego wyboru w działaniu[4]. Wyboru tego dokonuje się według pewnych kryteriów i mierników, np. prakseologicznych, spośród wariantów opracowanych przez decydenta, w odniesieniu do zarządzania kryzysowego: Radę Ministrów, Prezesa Rady Ministrów, ministra, kierownika urzędu centralnego, wojewodę, starostę, wójta/burmistrza/, prezydenta miasta, kierownika, komendanta, dowódcę, podległy mu zespół bądź otrzymanych z otoczenia[5].

1 J.A.F. Stoner, R.E. Freeman, D.R. Gilbert, *Kierowanie*, Warszawa 1999, s. 20.

2 *Leksykon zarządzania*, Warszawa 2004, s. 197.

3 J.A.F. Stoner, R.E. Freeman, D.R. Gilbert, op. cit., s. 25.

4 *Teoria organizacji i zarządzania*, red. J. Kurnal, Warszawa 1979, s. 189.

5 M. Lisiecki, *Zarządzanie bezpieczeństwem publicznym*, Warszawa 2011, s. 145.

Wynikiem decydowania jest decyzja. W istocie jest to poczucie decydenta, czyli osoby podejmującej decyzję, że proces decydowania został zakończony i że wskutek tego on wie, jak ma działać, a więc nie tylko, czego chce w danej sytuacji, ale również, jak zamierza to osiągnąć [...].

Problem decyzyjny może powstać z kilku powodów. Najczęstszym jest wystąpienie odstępstw od normalnego stanu rzeczy, tj. stanu uznanego za pożądany w danej sytuacji. Jeżeli występują różnice między takim stanem a stanem faktycznym, konieczne staje się przywrócenie normalnego stanu rzeczy. Innym powodem powstania problemu decyzyjnego jest potrzeba udoskonalenia stanu obecnego, mimo że jest on oceniany jako normalny[6].

Ta kwestia w pełni odnosi się do zarządzania kryzysowego na poziomach państwa, województwa, powiatu i gminy (miasta).

Kierowanie w systemie zarządzania kryzysowego to przede wszystkim kierowanie zespołami ludzkimi i wykorzystaniem znajdujących się w ich dyspozycji środkami. Na kierowanie zespołem składa się regulowanie splotu działań zespołu (kierowanie zespołem jako całością) i regulowanie poszczególnych pasm działania członków zespołu ze względu na splatanie w całość (organizowanie i koordynowanie wewnętrznych stosunków w zespole)[7].

Kierowanie w systemie zarządzania kryzysowego jest integralną częścią podsystemu kierowania bezpieczeństwem państwa i jest realizowane przez te same organy władzy i administracji publicznej. Natomiast różny jest zakres udziału tych podmiotów w realizacji funkcji kierowniczych.

Podsystem kierowania w systemie zarządzania kryzysowego tworzą organy władzy i administracji publicznej (rządowej i samorządowej) wraz z obsługującymi te organy urzędami i strukturami pomocniczymi (o charakterze opiniodawczo-doradczym i koordynacyjno-wykonawczym) wraz z niezbędną infrastrukturą[8]. Jego rola polega na sprzężeniu wszystkich elementów i ogniw systemu zarządzania kryzysowego na poziomie państwa, województwa, powiatu i gminy (miasta) w jednolitą sprawnie funkcjonującą całość, umożliwiającą realizację wszystkich zadań związanych z zarządzaniem kryzysowym[9].

W literaturze przedmiotu znajdują się terminy podkreślające charakter i cele administracji:

- rządowej – w skład której wchodzą następujące organy: Rada Ministrów, Prezes Rady Ministrów, ministrowie kierujący określonym działami administracji publicznej, kierownicy urzędów centralnych; wojewódzkie (zespolone) – wo-

[6] Ibidem, s. 145, 146.

[7] J. Zieleniewski, *Organizacja zespołów ludzkich. Wstęp do teorii organizacji i kierowania*, Warszawa 1976, s. 381.

[8] B. Szlachcic, *Bezpieczeństwo wewnętrzne państwa. Administracja rządowa i samorządowa w zarządzaniu reagowaniem kryzysowym*, [w:] *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, red. K. Liedel, J. Prońko, B. Wiśniewski, Bielsko-Biała–Warszawa 2007, s. 24.

[9] J. Wojnarowski, *System obronności państwa*, Warszawa 2005, s. 13.

jewodowie i podlegli kierownicy zespolonych służb, inspekcji i straży; powiatowe (zespolone) – starostowie i podlegli kierownicy zespolonych służb, inspekcji i straży; niezespolone,

- samorządowej – które stanowią organy terytorialne (gmina, powiat, województwo); wykonawcze (wybierane przez rady i sejmiki; zarządy oraz prezydenci, burmistrzowie, wójtowie, starostowie i marszałkowie); zawodowe i gospodarcze,
- specjalnej (zwanej również administracją niezespoloną), która nie podlega wojewodzie, a bezpośrednio właściwym ministrom[10].

Organy te podejmują decyzje w sprawach związanych z zarządzaniem kryzysowym w zakresach określonych w Konstytucji Rzeczypospolitej Polskiej, ustawach zwykłych oraz aktach wykonawczych.

> W sytuacjach kryzysowych stwarzających zagrożenia dla bezpieczeństwa Polski nie będą wprowadzane nadzwyczajne zmiany w ogólnych zasadach kierowania w systemie zarządzania kryzysowego, a jedynie zostaną uruchomione dodatkowe procedury i środki. Zachowane zostaną dotychczasowe struktury i kompetencje organów kierowania czasu pokojowego, z ewentualnym rozwinięciem systemu kierowania w procesie zarządzania kryzysowego, a nawet niektórych elementów wojennego systemu kierowania państwem oraz niezbędnych elementów wojennego systemu dowodzenia siłami zbrojnymi wydzielonymi do zapobieżenia skutkom zagrożenia lub jego likwidacji[11].

Podsystem kierowania w zarządzaniu kryzysowym przygotowuje się w celu zapewnienia ciągłości podejmowania decyzji i działań dla utrzymania bezpieczeństwa państwa i ma zapewnić on monitorowanie źródeł, rodzajów, kierunków i skali zagrożeń, zapobieganie powstawaniu zagrożeń na terytorium Polski, skutkom zagrożeń bezpieczeństwa państwa, a także ich usuwanie[12].

> Systemowo zorganizowane zarządzanie kryzysowe podporządkowuje administrację publiczną jednoosobowemu kierownictwu zarówno na poziomie całego kraju, jak i na poziomie poszczególnych jednostek samorządu terytorialnego. Odgrywa to istotną rolę szczególnie w procesie koordynacji działań wielu instytucji, służb i inspekcji podczas realizacji przedsięwzięć zapobiegających zagrożeniom kryzysowym, jak i prowadzenia działań w celu usunięcia ich skutków[13].

Rada Ministrów rozporządzeniem z dnia 27 kwietnia 2004 roku *w sprawie przystosowania systemu kierowania bezpieczeństwem narodowym*[14] określiła organizację i tryb przygotowania systemu kierowania bezpieczeństwem narodowym, warunki funkcjonowania organów władzy publicznej na stanowiskach kierowania.

[10] B. Szlachcic, op. cit., s. 26.

[11] J. Wojnarowski, op. cit., s. 14.

[12] Ibidem, s. 15.

[13] B. Szlachcic, op. cit., s. 35.

[14] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 roku *w sprawie przystosowania systemu kierowania bezpieczeństwem narodowym* (Dz. U. z 2004 r. Nr 98, poz. 978), § 1.

Tabela 70. System kierowania w zarządzaniu kryzysowym

Podmioty	Zadania
Rada Ministrów	analiza i zadania oraz propozycje rozwiązań, rekomendacje
Prezes Rady Ministrów	
Rządowy Zespół Zarządzania Kryzysowego	propozycje decyzji (rozwiązań) i działań, oraz uchwał, zarządzeń i wniosków wymagających konsultacji i uzgodnień
Rządowe Centrum Bezpieczeństwa	koordynacja działań na szczeblu centralnym w zakresie: a) monitorowania i analizy zagrożeń bezpieczeństwa państwa b) realizacji decyzji Rady Ministrów i Prezesa Rady Ministrów c) rozwiązywania sytuacji kryzysowych oraz usuwania ich skutków
Ministrowie kierujący określonym działam administracji publicznej, kierownicy urzędów centralnych	kierowanie zapobieganiem i rozwiązywaniem sytuacji kryzysowej oraz likwidacją skutków kryzysu, jeżeli kryzys obejmuje obszar więcej niż jednego województwa (każdy w zakresie swojej właściwości)
Wojewodowie Wojewódzkie Zespoły Zarządzania Kryzysowego	kierowanie, jeżeli kryzys obejmuje obszar więcej niż jednego powiatu
Starostowie Powiatowe Zespoły Zarządzania Kryzysowego	kierowanie, jeżeli kryzys obejmuje obszar więcej niż jednej gminy
Wójtowie Gminne Zespoły Zarządzania Kryzysowego	kierowanie, jeżeli kryzys obejmuje obszar gminy

Źródło: Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.)

Przygotowanie podsystemu systemu kierowania obejmuje planowanie, organizowanie i realizowanie przedsięwzięć zapewniających organom wykonywanie zadań związanych z zarządzaniem kryzysowym w razie wewnętrznego lub zewnętrznego zagrożenia bezpieczeństwa państwa, w tym wystąpienia działań terrorystycznych lub innych szczególnych zdarzeń[15]. Przedsięwzięcia te obejmują przygotowanie organów i obsługujących je urzędów do funkcjonowania w podsystemie kierowania, wykonywanie planów, przygotowanie infrastruktury umożliwiającej kierowanie.

Organy podsystemu kierowania w zarządzaniu kryzysowym w zależności od skali zagrożenia wykorzystują główne i zapasowe stanowiska[16]. Główne stanowiska przygotowuje się w dotychczasowych siedzibach tych organów dla następujących podmiotów: Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, ministrów, centralnych organów administracji oraz wojewodów, kierowników urzędów centralnych niewchodzących w skład administracji rządowej, kierowników zespolonych służb, inspekcji i straży działających pod zwierzchnictwem wojewody oraz organów administracji niezespolonej, ustalonych przez

[15] Ibidem, § 4 ust. 1.

[16] Ibidem, § 2 ust. 1.

ministrów i wojewodów stosownie do kompetencji, organów wykonawczych samorządu terytorialnego[17]. Natomiast zapasowe stanowiska kierowania przygotowuje się dla: Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, ministrów centralnych organów administracji wskazanych przez Prezesa Rady Ministrów, wojewodów[18]. Usytuowanie zapasowych stanowisk kierowania wojewodowie uzgadniają z Ministrem Spraw Wewnętrznych i Ministrem Obrony Narodowej. Wojewodowie, w ramach zapasowych stanowisk kierowania, zapewniają miejsca pracy marszałkowi województwa i komisarzowi rządowemu powołanemu na podstawie odrębnych przepisów, a także innym organom.

Zakres przygotowania stanowiska:

- opracowanie dokumentacji związanej z przemieszczaniem i zapewnieniem warunków funkcjonowania organu na stanowisku kierowania,
- utrzymywanie stanu technicznego oraz modernizacja infrastruktury przez jej użytkowników w czasie pokoju,
- ustalenie zasad i trybu informacji dotyczącej gotowości organu do podjęcia zadań ich realizacji oraz zorganizowanie specjalnych, w tym utajnionych, systemów informatycznych,
- wyposażenie w urządzenia łączności zapewniającej możliwość niezakłóconej pracy organu,
- wyposażenie w urządzenia filtrowentylacyjne, źródła energii elektrycznej i cieplnej oraz ujęcia wody, których działanie jest niezależne od ogólnodostępnej infrastruktury techniczno-użytkowej,
- wyposażenie w urządzenia techniczne i sanitarne oraz sprzęt biurowy i kwaterunkowy niezbędny do pracy i odpoczynku,
- uodpornienie na oddziaływanie środków rozpoznania i rażenia przeciwnika, głównie przez maskowanie oraz budowę i modernizację ukryć i schronów,
- zorganizowanie żywienia i zaopatrywania w artykuły codziennego użytku, zabezpieczenia medycznego, transportu oraz obsługi pojazdów i urządzeń technicznych, zaopatrywania w paliwa i materiały eksploatacyjne, osłony kontrwywiadowczej, punktów zabiegów specjalnych,
- zorganizowanie systemu powiadamiania i alarmowania o zagrożeniu z powietrza oraz skażeniach i zakażeniach,
- przygotowanie środków do rozwinięcia i odtworzenia systemu łączności oraz utrzymania bezpieczeństwa teleinformatycznego, ochrony i obrony stanowisk kierowania, w tym przed rozpoznaniem i obezwładnianiem radioelektronicznym, prowadzenia akcji ratowniczych, przemieszczania na zapasowe miejsca pracy i zapasowe stanowiska kierowania,
- szkolenie pracowników zapewniających utrzymanie obiektów specjalnych stanowisk kierowania w gotowości do ich wykorzystania,
- weryfikacja przydziału obiektów budowlanych oraz monitorowanie należytego ich utrzymania przez kolejnych użytkowników[19].

[17] Ibidem, § 11 ust. 1.

[18] Ibidem, § 12 ust. 1.

[19] Ibidem, § 16.

Podsystem kierowania w zarządzaniu kryzysowym zmierza do skoordynowanego wykorzystania będących w dyspozycji organów władzy i administracji państwa zasobów ludzkich i materiałowych do osiągnięcia założonych celów. W tym celu niezbędna jest: diagnoza zaistniałej sytuacji kryzysowej, ostrzeganie podmiotów i obywateli o rozwoju zagrożeń w sytuacji kryzysowej, monitorowanie i ocena zagrożeń w sytuacji kryzysowej oraz weryfikowanie planów działania, wzmożenie ochrony granic i terytorium Rzeczypospolitej Polskiej, podejmowanie decyzji wykorzystania (użycia) sił i środków, prowadzenie operacji antykryzysowych, prowadzenie operacji ratowniczych, odtwarzanie (odbudowa) i przywracanie stanu pierwotnego, nadzór (kontrola) nad przebiegiem sytuacji kryzysowej i działaniem sił ludzkich[20].

7.2. Rada Ministrów

Rada Ministrów w świetle Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku jest naczelnym organem władzy wykonawczej, prowadzącym politykę wewnętrzną i zagraniczną państwa, spełniającym złożone zadania o charakterze politycznym, kierującym, koordynującym i kontrolującym działania całej administracji rządowej, funkcjonującym pod kontrolą Sejmu i przed Sejmem ponoszącym odpowiedzialność[21].

> Na szczególną uwagę zasługuje pozycja i rola ustrojowa Prezesa Rady Ministrów, którego pozycję prawną określa art. 148 Konstytucji. Stwierdza on, że Prezes Rady Ministrów kieruje pracami rządu, jak również koordynuje i kontroluje pracę członków rządu. Kierowanie pracami Rady Ministrów obejmuje zwoływanie posiedzeń rządu, przewodniczenie jego obradom, dzięki czemu premier może skutecznie oddziaływać na tok jego prac i na treść podejmowanych uchwał. […] Prezes Rady Ministrów ma prawo wydawania rozporządzeń, a więc aktów wykonawczych w stosunku do ustaw[22].

Akty te wydaje na podstawie ustaw i w celu ich wykonywania. Ponadto zgodnie z Konstytucją premier jest zwierzchnikiem wszystkich pracowników administracji rządowej. Z punktu widzenia zarządzania kryzysowego na poziomie państwa istotna jest treść pkt. 6 art. 148 Konstytucji RP, który stanowi, że Prezes Rady Ministrów sprawuje nadzór nad samorządem terytorialnym w granicach i formach określonych w Konstytucji i ustawach[23].

[20] J. Wojnarowski, *System obronności państwa*, Warszawa 2005, s. 59.

[21] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Kraków 2002, s. 192.

[22] Ibidem, s. 199–200.

[23] Dz. U. z 1997 r. Nr 78, poz. 483.

Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* w art. 7 ust. 1 stanowi, że Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium Rzeczypospolitej Polskiej[24]. W sytuacjach nagłych zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów[25]. Decyzje podjęte przez ministra właściwego do spraw wewnętrznych podlegają rozpatrzeniu na najbliższym posiedzeniu 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.

W celu zapewnienia realizacji ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* Rada Ministrów wydała akty wykonawcze, które uszczegółowiają realizację zadań, i tak:

- rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego*[26],
- rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Narodowego programu Ochrony Infrastruktury Krytycznej*[27],
- rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury krytycznej*[28],
- rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 roku w sprawie określenia organów administracji rządowej, które tworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania[29],
- rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 roku w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa[30],
- zarządzenie Nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 roku w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego[31].

Ponadto na podstawie delegacji ustawowej Rada Ministrów przyjmuje w drodze uchwały Raport o zagrożeniach bezpieczeństwa narodowego[32], Narodowy Program Ochrony Infrastruktury Krytycznej, którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej[33].

[24] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

[25] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 7 ust. 2.

[26] Dz. U. z 2010 r. Nr 83, poz. 540.

[27] Dz. U. z 2010 r. Nr 83, poz. 541.

[28] Dz. U. z 2010 r. Nr 83, poz. 542.

[29] Dz. U. z 2009 r. Nr 226, poz. 1810.

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

[31] M.P. z 2008 r. Nr 61, poz. 538.

[32] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 5a ust. 4.

[33] Ibidem, art. 5b ust. 1.

Na poziomie krajowym przy Radzie Ministrów tworzy się Rządowy Zespół Zarządzania Kryzysowego (RZZK), który jest organem o charakterze opiniodawczo-doradczym, właściwym w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego państwem[34]. W jego skład wchodzą:

– Prezes Rady Ministrów – przewodniczący,
– Minister Obrony Narodowej – zastępca przewodniczącego,
– minister właściwy do spraw wewnętrznych – zastępca przewodniczącego,
– Minister Spraw Zagranicznych,
– Minister Koordynator Służb Specjalnych – jeżeli został powołany;
– członkowie: ministrowie kierujący działami administracji rządowej: administracja publiczna, budownictwo, gospodarka przestrzenna i mieszkaniowa, finanse publiczne, gospodarka, gospodarka morska, gospodarka wodna, instytucje finansowe, informatyzacja, kultura i ochrona dziedzictwa narodowego, łączność, oświata i wychowanie, rolnictwo, sprawiedliwość, środowisko, transport, zdrowie, praca, zabezpieczenie społeczne, Skarb Państwa, 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.

Prezydent Rzeczypospolitej Polskiej może skierować do prac Zespołu, na prawach członka, Szefa Biura Bezpieczeństwa Narodowego lub innego przedstawiciela. W przypadku nieobecności przewodniczącego, pracami Zespołu kieruje wyznaczony przez niego zastępca albo członek Zespołu, w którego właściwości – wynikającej z kierowania danym działem administracji rządowej – pozostaje rodzaj zaistniałej sytuacji kryzysowej. Członkowie Zespołu mogą wyznaczać do udziału w jego pracach swoich przedstawicieli: Prezes Rady Ministrów – wiceprezesa Rady Ministrów, minister – sekretarza lub podsekretarza stanu, pozostałe organy – swojego zastępcę[35].

Do zadań Rządowego Zespołu Zarządzania Kryzysowego 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,

[34] Ibidem, art. 8 ust. 1.

[35] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 8 ust. 2 i 3.

- opiniowanie potrzeb w zakresie odtwarzania infrastruktury lub przywrócenia jej pierwotnego charakteru,
- opiniowanie i przedkładanie Radzie Ministrów *Krajowego Planu Zarządzania Kryzysowego*,
- opiniowanie projektu zarządzenia Prezesa Rady Ministrów, z zachowaniem przepisów o ochronie informacji niejawnych, określanie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego oraz organy odpowiedzialne za ich uruchamianie[36].

Prezes Rady Ministrów Zarządzeniem Nr 86 z dnia 14 sierpnia 2008 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego[37] określi organizację i tryb pracy Zespołu, z uwzględnieniem rozwiązań pozwalających na niezwłoczne zebranie się Zespołu i zapewnienie uzyskania pełnej informacji o zdarzeniach będących przedmiotem posiedzenia. Posiedzenia Rządowego Zespołu Zarządzania Kryzysowego odbywają się raz na kwartał – posiedzenia zwyczajne lub w razie potrzeby – posiedzenia nadzwyczajne, które zwołuje przewodniczący, a w przypadku jego nieobecności jeden z wyznaczonych przez niego zastępców albo członek Zespołu, w którego właściwości, wynikającej z kierowania danym działem administracji rządowej, pozostaje rodzaj zaistniałej sytuacji kryzysowej. Ustalenia RZZK są podejmowane w drodze przyjmowanych jednomyślnie uzgodnień. W przypadku nieosiągnięcia jednomyślnego uzgodnienia przewodniczący, a w razie jego nieobecności wyznaczony przez niego zastępca lub członek Zespołu, nakazuje sporządzenie protokołu rozbieżności, w którym zamieszcza się wszystkie stanowiska uczestników posiedzenia Zespołu oraz przyczyny uniemożliwiające podjęcie ustalenia. Ustalenia Zespołu albo protokół rozbieżności jest niezwłocznie przedstawiany Radzie Ministrów. Obsługę RZZK i całodobowy obieg informacji na potrzeby Zespołu zapewnia Rządowe Centrum Bezpieczeństwa (RZB)[38].

W pracach Rządowego Zespołu Zarządzania Kryzysowego uczestniczy również sekretarz Zespołu, do zadań którego należy: organizowanie posiedzeń, zapewnienie przygotowania opinii, ekspertyz i projektów dokumentów, niezbędnych do realizacji zadań Zespołu, zapewnienie wymiany informacji związanych z realizacją zadań, współpraca z Rzecznikiem Prasowym Rządu dotycząca przygotowywania projektów komunikatów prasowych z posiedzeń, w zakresie treści uzgodnionej z przewodniczącym Zespołu[39]. Sekretarz Zespołu sporządza ponadto protokół z posiedzenia, zatwierdzany przez przewodniczącego, a w razie jego nieobecności przez wyznaczonego przez niego zastępcę lub członka Zespołu. Sporządza on w uzgodnieniu z przewodniczącym sprawozdanie z prac Zespołu

[36] Ibidem, art. 9 ust. 1.

[37] M. P. z 2008 r. Nr 61, poz. 538.

[38] Zarządzenie Nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 r. *w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego* (M. P. z 2008 r. Nr 61, poz. 538), § 4.

[39] Ibidem, § 5 ust. 1.

za rok ubiegły w terminie do dnia 31 marca roku kalendarzowego następującego po roku, którego sprawozdanie dotyczy. Prezes Rady Ministrów przedkłada sprawozdanie do zatwierdzenia Radzie Ministrów najpóźniej w terminie do dnia 30 kwietnia roku kalendarzowego następującego po roku, którego sprawozdanie dotyczy[40].

Informacje o przebiegu posiedzenia, zawarte w ustaleniach, protokole rozbieżności lub informacje o opiniach i stanowiskach wyrażanych na tym posiedzeniu przez jego uczestników mogą być ujawniane wyłącznie w trybie i na zasadach przewidzianych w ustawie z dnia 6 września 2001 roku *o dostępie do informacji publicznej*[41]. Prawo do informacji podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych[42]. Przewodniczący, a w razie jego nieobecności wyznaczony przez niego zastępca przewodniczącego lub członek RZZK, może z własnej inicjatywy lub na wniosek każdego członka Zespołu zarządzić niejawny charakter posiedzenia Zespołu. Z posiedzenia RZZK jest sporządzany komunikat prasowy, informujący w szczególności o przedmiocie posiedzenia oraz o podjętych ustaleniach. W przypadku zarządzenia niejawnego charakteru posiedzenia Zespołu nie sporządza się komunikatu prasowego. Komunikat przygotowuje i przekazuje Rzecznikowi Prasowemu Rządu sekretarz Zespołu.

Rządowe Centrum Bezpieczeństwa

Na poziomie krajowym (centralnym), zgodnie z ustawą z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[43] i rozporządzeniem Prezesa Rady Ministrów z dnia 10 lipca 2008 roku *w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*[44], utworzono Rządowe Centrum Bezpieczeństwa (RCB), ponadresortową strukturę, której misją i zadaniem jest pełna analiza zagrożeń w oparciu o informacje uzyskiwane ze wszystkich centrów zarządzania kryzysowego, organów administracji publicznej oraz instytucji międzynarodowych[45].

RCB funkcjonuje przy Radzie Ministrów jako organ opiniodawczo-doradczy odpowiedzialny za inicjowanie i koordynowanie działań w zakresie zarządzania kryzysowego[46]. Jest państwową jednostką budżetową podlegającą Prezesowi

[40] Ibidem, § 5 ust. 5.

[41] Dz. U. z 2001 r. Nr 112, poz. 1198, z późn. zm. § 6 ust. 1 Zarządzenia Nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 r. *w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego* (M. P. z 2008 r. Nr 61, poz. 538).

[42] Ibidem, § 6 ust. 2.

[43] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 10 ust. 1.

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

[45] *Organizacja i funkcjonowanie centrum zarządzania kryzysowego*, red. G. Sobolewski, Warszawa 2011, s. 43.

[46] S. Karleszko, *Zarządzanie kryzysowe i logistyka humanitarna jako rola i zadania rządowe i samorządu terytorialnego – wybrane zagadnienia,* [w:] *Logistyka humanitarna i zarządzanie kryzysowe – wybrane problemy*, red. T. Pokusa, M. Dumezal, Opole 2009, s. 273.

Rady Ministrów, która rozpoczęła działalność 2 sierpnia 2008 roku. Pracami RCB kieruje dyrektor powoływany i odwoływany przez Prezesa Rady Ministrów, który pełni jednocześnie funkcję sekretarza Rządowego Zespołu Zarządzania Kryzysowego, zastępców dyrektora RCB powołuje i odwołuje Prezes Rady Ministrów na wniosek dyrektora Centrum.

Rządowe Centrum Bezpieczeństwa zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, Rządowego Zespołu Zarządzania Kryzysowego i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełni funkcję Krajowego Centrum Zarządzania Kryzysowego (KCZK)[47]. Koszty związane z funkcjonowaniem Centrum są pokrywane z budżetu państwa z części, której dysponentem jest minister właściwy do spraw wewnętrznych.

Rolą Rządowego Centrum Bezpieczeństwa w systemie Zarządzania Kryzysowego Rzeczypospolitej Polskiej jest realizacja następujących funkcji: dyplomatycznej, administracyjnej, społecznej, prognostyczno-planistycznej, koordynacyjnej, kontrolnej, informacyjnej, monitorowania[48].

Do zadań Rządowego Centrum Bezpieczeństwa należy:

- planowanie cywilne, w tym:
  a) przedstawianie szczegółowych sposobów i środków reagowania na zagrożenia oraz ograniczania ich skutków,
  b) opracowywanie i aktualizowanie Krajowego Planu Zarządzania Kryzysowego we współpracy z właściwymi komórkami organizacyjnymi urzędów obsługujących ministrów oraz kierowników urzędów centralnych,
  c) analiza i ocena możliwości wystąpienia zagrożeń lub ich rozwoju,
  d) gromadzenie informacji o zagrożeniach i analiza zebranych materiałów,
  e) wypracowywanie wniosków i propozycji zapobiegania i przeciwdziałania zagrożeniom,
  f) planowanie wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań, o których mowa w art. 25 ust. 3,
  g) planowanie wsparcia przez organy administracji publicznej realizacji zadań Sił Zbrojnych Rzeczypospolitej Polskiej;
- monitorowanie potencjalnych zagrożeń;
- uzgadnianie planów zarządzania kryzysowego sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych;
- przygotowanie uruchamiania, w przypadku zaistnienia zagrożeń, procedur związanych z zarządzaniem kryzysowym;
- przygotowywanie projektów opinii i stanowisk RZZK;
- przygotowywanie i obsługa techniczno-organizacyjna prac RZZK;
- zapewnienie koordynacji polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej;

[47] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 11 ust. 1.

[48] *Organizacja i funkcjonowanie…*, op. cit., s. 43.

- współdziałanie z podmiotami, komórkami i jednostkami organizacyjnymi Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej oraz innych organizacji międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej;
- organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych;
- zapewnienie obiegu informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego;
- realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa;
- realizacja zadań z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym;
- współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym;
- realizacja zadań planistycznych i programowych z zakresu ochrony infrastruktury krytycznej oraz europejskiej infrastruktury krytycznej, w tym opracowywanie i aktualizacja załącznika funkcjonalnego do Krajowego Planu Zarządzania Kryzysowego dotyczącego ochrony infrastruktury krytycznej, a także współpraca, jako krajowy punkt kontaktowy, z instytucjami Unii Europejskiej i organizacji Paktu Północnoatlantyckiego oraz ich krajami członkowskimi w zakresie ochrony infrastruktury krytycznej;
- przygotowanie projektu zarządzenia Prezesa Rady Ministrów z zachowaniem przepisów o ochronie informacji niejawnych, w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w NATO oraz organy odpowiedzialne za ich uruchomienie;
- informowanie, zgodnie z właściwością podmiotów (przewodniczącego, zastępców, Ministra Spraw Zagranicznych, Ministra Koordynatora Służb Specjalnych – jeżeli został powołany, członków RZZK) o potencjalnych zagrożeniach oraz działaniach podjętych przez właściwe organy;
- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej.

Rada Ministrów lub Prezes Rady Ministrów mogą zlecić Rządowemu Centrum Bezpieczeństwa dodatkowe zadania związane z zarządzaniem kryzysowym w razie wystąpienia klęski żywiołowej, katastrofy naturalnej, awarii technicznej bądź też zagrożeń terrorystycznych. Przedsięwzięcia RCB będą koncentrować się na następujących kwestiach:

- realizowaniu polityki informacyjnej organów administracji publicznej o zaistniałej sytuacji kryzysowej,
- monitorowaniu i prognozowaniu bieżącego rozwoju sytuacji kryzysowej,
- informowaniu o potencjalnych zagrożeniach i działaniach, które zostały podjęte przez właściwe organy,

- współpracy i koordynowaniu przedsięwzięć ratowniczych z centrami zarządzania kryzysowego, jak również współdziałaniu z ratowniczymi organizacjami społecznymi oraz innymi podmiotami działającymi w swoich obszarach zainteresowania, w tym przy ewakuacji ludności z terenu, na którym wystąpiło bezpośrednie zagrożenie dla życia i zdrowia obywateli, również obywateli znajdujących się poza terytorium Rzeczypospolitej Polskiej[49].

Rządowe Centrum Bezpieczeństwa w procesie realizowania ustawowych zadań informuje Komisję Europejską i państwa członkowskie Unii Europejskiej o środkach zastosowanych w sytuacji kryzysowej w celu zabezpieczenia prawidłowego działania publicznej sieci telekomunikacyjnej oraz stacji nadawczych i odbiorczych używanych do zapewnienia bezpieczeństwa, w zakresie dotyczącym systemu łączności i sieci teleinformatycznych[50]. Ma to na celu utrzymanie oraz wzmocnienie zdolności sojuszniczych w zakresie zarządzania kryzysowego, a także zapewnienie obiegu informacji między krajowymi i zagranicznymi podmiotami odpowiedzialnymi za zarządzanie kryzysowe.

Prezes Rady Ministrów w drodze rozporządzenia z dnia 11 kwietnia 2011 roku *w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*[51] określił organizację i tryb jego działania, uwzględniając potrzebę ciągłości jego funkcjonowania.

W skład Rządowego Centrum Bezpieczeństwa wchodzą:

1) kierownictwo: dyrektor, zastępcy dyrektora,
2) doradcy,
3) Wydział Operacyjny,
4) Wydział Polityki Informacyjnej,
5) Wydział Planowania,
6) Wydział Szkoleń i Ćwiczeń,
7) Wydział Analiz,
8) Wydział Ochrony Infrastruktury Krytycznej,
9) Wydział Ochrony Informacji Niejawnych i Kontroli,
10) Wydział Administracyjno-Finansowy[52].

Centrum kieruje dyrektor przy pomocy zastępców i kierowników komórek organizacyjnych.

Do zadań dyrektora Rządowego Centrum Bezpieczeństwa należy:

- powoływanie i odwoływanie kierowników komórek organizacyjnych oraz doradców,
- udzielanie pełnomocnictw osobom fizycznym i prawnym do dokonywania określonych czynności cywilnoprawnych i faktycznych,

[49] Ibidem, s. 36 i 37.

[50] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 11a.

[51] Dz. U. z 2011 r. Nr 86, poz. 471.

[52] Rozporządzenie Prezes Rady Ministrów z dnia 11 kwietnia 2011 roku *w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa* (Dz. U. z 2011 r. Nr 86, poz. 471), § 1 ust. 1.

- reprezentowanie Centrum na zewnątrz w sprawach dotyczących zakresu jego działania, a także na podstawie upoważnień i pełnomocnictw udzielonych przez Prezesa Rady Ministrów,
- planowanie, organizowanie, koordynowanie i sprawowanie kontroli wewnętrznej wykonywania zadań przez komórki organizacyjne Centrum,
- ustalanie zakresu obowiązków pracowników Centrum na poszczególnych stanowiskach,
- prowadzenie polityki kadrowej Centrum oraz nadzór nad przestrzeganiem przez podległych pracowników dyscypliny pracy,
- podejmowanie działań na rzecz rozwoju Centrum, podnoszenia kwalifikacji pracowników, zapewnienia wyposażenia technicznego oraz bezpieczeństwa i higieny pracy.

Ponadto dyrektor Rządowego Centrum Bezpieczeństwa może: tworzyć zespoły doradcze i opiniodawcze niezbędne do realizacji poszczególnych zadań Centrum, w zakresie niezbędnym do realizacji zadań Centrum zlecać przeprowadzanie ekspertyz, analiz oraz innych opracowań, zlecać podległym pracownikom wykonywanie innych zadań niż określone w zakresie czynności na zajmowanym stanowisku, wydawać decyzje i wytyczne w sprawach związanych z zakresem działania Centrum. Dyrektor Centrum może wprowadzić tryb pracy ciągłej w sytuacji prowadzenia lub udziału w ćwiczeniach z zakresu zarządzania kryzysowego, a także w innych szczególnie uzasadnionych przypadkach[53].

Funkcja Krajowego Centrum Zarządzania Kryzysowego jest realizowana przez pełnienie całodobowego dyżuru w Centrum[54]. Rządowe Centrum Bezpieczeństwa pracuje w trybie ciągłym, z zapewnieniem zmianowej pracy osób w nim zatrudnionych w czasie obowiązywania stanu nadzwyczajnego oraz występowania sytuacji kryzysowej, w których działania podejmuje właściwy organ zarządzania kryzysowego obsługiwany przez RCB.

Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* daje upoważnienie dla Prezesa Rady Ministrów, z własnej inicjatywy, na wniosek właściwego ministra, kierownika urzędu centralnego lub wojewody, do wprowadzenia na całym terytorium Rzeczypospolitej Polskiej albo jego części, w drodze zarządzenia, następujących stopni alarmowych w zależności od skali zagrożenia atakiem o charakterze terrorystycznym lub sabotażowym:

- pierwszy stopień alarmowy – w przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym lub innego zdarzenia, których rodzaj i zakres jest trudny do przewidzenia;
- drugi stopień alarmowy – w przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym lub innego zdarzenia, powodujących zagrożenie bezpieczeństwa Rzeczypospolitej Polskiej;
- trzeci stopień alarmowy – w przypadku uzyskania informacji o osobach lub organizacjach przygotowujących działania terrorystyczne godzące w bezpie-

[53] Ibidem, § 2 ust. 4 i 5.

[54] Ibidem, § 3 ust. 1.

czeństwo Rzeczypospolitej Polskiej lub wystąpienia aktów terroru godzących w bezpieczeństwo innych państw albo w przypadku uzyskania informacji o możliwości wystąpienia innego zdarzenia godzącego w bezpieczeństwo Rzeczypospolitej Polskiej lub innych państw;

- czwarty stopień alarmowy – w przypadku wystąpienia zdarzenia o charakterze terrorystycznym lub innego zdarzenia, powodujących zagrożenie bezpieczeństwa Rzeczypospolitej Polskiej lub innych państw[55].

Wyższy stopień alarmowy może być wprowadzony z pominięciem niższych stopni. Zadania realizowane w poszczególnych stopniach alarmowych ujmuje się w Planie Reagowania Obronnego Rzeczypospolitej Polskiej. Prezes Rady Ministrów, w drodze zarządzenia, odwołuje albo zmienia stopień alarmowy.

Stan klęski żywiołowej

Stan klęski żywiołowej może być wprowadzony dla zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia[56]. Ustawa z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej*[57] określa tryb wprowadzenia i zniesienia stanu klęski żywiołowej oraz zakres ograniczeń wolności i praw człowieka i obywatela w czasie stanu klęski żywiołowej. Stan klęski żywiołowej może być wprowadzony na obszarze, na którym wystąpiła klęska żywiołowa, a także na obszarze, na którym wystąpiły lub mogą wystąpić skutki tej klęski[58]. Stan klęski żywiołowej wprowadza się na czas niezbędny dla zapobieżenia skutkom klęski żywiołowej lub ich usunięcia, nie dłuższy niż 30 dni[59].

Rada Ministrów w drodze rozporządzenia może wprowadzić stan klęski żywiołowej z własnej inicjatywy lub na wniosek właściwego wojewody[60]. W niniejszym rozporządzeniu określa się przyczyny, datę wprowadzenia oraz obszar i czas trwania stanu klęski żywiołowej, a także w zakresie dopuszczonym przez ustawę z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej* rodzaje niezbędnych ograniczeń wolności i praw człowieka i obywatela. Rozporządzenie ogłasza się w Dzienniku Ustawa Rzeczypospolitej Polskiej, ponadto podaje się do publicznej wiadomości w drodze obwieszczenia właściwego wojewody przez rozplakatowanie w miejscach publicznych, a także w sposób zwyczajowo przyjęty na danym obszarze. Redaktorzy naczelni dzienników oraz nadawcy programów radiowych i telewizyjnych są obowiązani do niezwłocznego, nieodpłatnego podania do publicznej wiadomości rozporządzenia Rady Ministrów o wprowadze-

[55] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 23.

[56] Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.

[57] Ibidem.

[58] Ustawa z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej* (Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.), art. 4 ust. 1.

[59] Ibidem, art. 4 ust. 2.

[60] Ibidem, art. 5 ust. 1.

niu stanu klęski żywiołowej, przekazanego im przez wojewodę właściwego ze względu na siedzibę redakcji lub nadawcy.

Stan klęski żywiołowej może zostać przedłużony na czas oznaczony, w drodze rozporządzenia Rady Ministrów po wyrażeniu przez Sejm zgody na to przedłużenie[61]. Rada Ministrów w drodze rozporządzenia znosi stan klęski żywiołowej na całym obszarze jego obowiązywania lub na części tego obszaru przed upływem czasu, na który został wprowadzony, jeżeli ustaną przyczyny jego wprowadzenia[62].

Zgodnie z ustawą z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej* organy władzy publicznej działają w dotychczasowych strukturach organizacyjnych państwa i w ramach przysługujących im kompetencji, z zastrzeżeniem przepisów niniejszego aktu prawnego[63].

W czasie stanu klęski żywiołowej działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia kierują:

- wójt (burmistrz, prezydent miasta), jeżeli stan klęski żywiołowej wprowadzono tylko na obszarze gminy,
- starosta, jeżeli stan klęski żywiołowej wprowadzono na obszarze więcej niż jednej gminy wchodzącej w skład powiatu,
- wojewoda, jeżeli stan klęski żywiołowej wprowadzono na obszarze więcej niż jednego powiatu wchodzącego w skład województwa,
- minister właściwy do spraw wewnętrznych lub inny minister, do zakresu działania którego należy zapobieganie skutkom danej klęski żywiołowej lub ich usuwanie, a w przypadku wątpliwości co do właściwości ministra lub w przypadku gdy właściwych jest kilku ministrów – minister wyznaczony przez Prezesa Rady Ministrów – jeżeli stan klęski żywiołowej wprowadzono na obszarze więcej niż jednego województwa[64].

W czasie stanu klęski żywiołowej, jeżeli użycie innych sił i środków jest niemożliwe lub niewystarczające, Minister Obrony Narodowej może przekazać do dyspozycji wojewody, na którego obszarze działania występuje klęska żywiołowa, pododdziały lub oddziały Sił Zbrojnych Rzeczypospolitej Polskiej, wraz ze skierowaniem ich do wykonywania zadań związanych z zapobieżeniem skutkom klęski żywiołowej lub ich usunięciem[65].

Rada Ministrów w drodze rozporządzenia określa szczegółowe zasady udziału pododdziałów i oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu, uwzględniając rodzaje działań ratowniczych lub prewencyjnych, w których pododdziały i oddziały Sił Zbrojnych Rzeczypospolitej Polskiej mogą brać udział, sposób koordynowania

[61] Ibidem, art. 6 ust. 1.

[62] Ibidem, art. 6 ust. 2.

[63] Ibidem, art. 7.

[64] Ibidem, art. 8.

[65] Ibidem, art. 18 ust. 1.

i dowodzenia ich działaniami oraz sposób zapewnienia im zabezpieczenia logistycznego[66].

Stan wyjątkowy

Zgodnie z ustawą z dnia 21 czerwca 2002 roku *o stanie wyjątkowym*[67] w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami terrorystycznymi, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego. We wniosku, o którym mowa, Rada Ministrów określa przyczyny wprowadzenia i niezbędny czas trwania stanu wyjątkowego oraz obszar, na jakim stan wyjątkowy powinien być wprowadzony, a także odpowiednie do stopnia i charakteru zagrożenia, w zakresie dopuszczonym niniejszą ustawą, rodzaje ograniczeń wolności i praw człowieka i obywatela.

Prezydent Rzeczypospolitej Polskiej na wniosek Rady Ministrów w drodze rozporządzenia znosi stan wyjątkowy przed upływem czasu, na jaki został wprowadzony, jeżeli ustaną przyczyny wprowadzenia tego stanu oraz zostanie przywrócone normalne funkcjonowanie państwa[68]. Prezes Rady Ministrów w przypadku wprowadzenia stanu wyjątkowego na obszarze większym niż obszar jednego województwa, koordynuje i kontroluje funkcjonowanie administracji rządowej i samorządowej w zakresie przywracania konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego[69]. Prezes Rady Ministrów jest obowiązany do informowania na bieżąco Prezydenta Rzeczypospolitej Polskiej o skutkach wprowadzenia stanu wyjątkowego oraz o rodzaju i rezultatach działań podejmowanych w celu przywrócenia normalnego funkcjonowania państwa[70]. W czasie stanu wyjątkowego Prezydent Rzeczypospolitej Polskiej, na wniosek Prezesa Rady Ministrów może postanowić o użyciu oddziałów i pododdziałów Sił Zbrojnych Rzeczypospolitej Polskiej do przywrócenia normalnego funkcjonowania państwa, jeżeli dotychczas zastosowane siły i środki zostały wyczerpane[71]. Rada Ministrów w drodze rozporządzenia, określa szczegółowe zasady użycia oddziałów i pododdziałów Sił Zbrojnych Rzeczypospolitej Polskiej w czasie stanu wyjątkowego, uwzględniając stopień i rodzaj zagrożeń stanowiących przyczyny wprowadzenia i trwania stanu wyjątkowego[72].

66 Ibidem, art. 18 ust. 3.

67 Ustawa z dnia 21 czerwca 2002 roku *o stanie wyjątkowym* (Dz. U. z 2002 r. Nr 113, poz. 985), art. 2 ust. 1.

68 Ibidem, art. 5 ust. 1.

69 Ibidem, art. 9 pkt 1.

70 Ibidem, art. 10.

71 Ibidem, art. 11 ust. 1.

72 Ibidem, art. 11 ust. 4.

Prezes Rady Ministrów, na wniosek właściwego wojewody, może zawiesić te organy do czasu zniesienia stanu wyjątkowego lub na czas określony i ustanowić w ich miejsce zarząd komisaryczny sprawowany przez komisarza rządowego, jeżeli organy gminy, powiatu lub samorządu województwa nie wykazują dostatecznej skuteczności w wykonywaniu zadań publicznych lub w realizacji działań wynikających z przepisów o wprowadzeniu stanu wyjątkowego[73]. Komisarza rządowego powołuje i odwołuje Prezes Rady Ministrów na wniosek wojewody, który z dniem powołania przejmuje wykonywanie zadań i kompetencji zawieszonych organów gminy, powiatu lub samorządu województwa. Stan zawieszenia organów gminy, powiatu lub samorządu województwa ustaje z upływem czasu określonego przez Prezesa Rady Ministrów oraz z mocy prawa z dniem zniesienia stanu wyjątkowego.

Rada Ministrów określa w drodze rozporządzeń szczegółowy tryb i sposoby oraz obszarowy, podmiotowy i przedmiotowy zakres wprowadzenia oraz stosowania ograniczeń wolności i praw człowieka i obywatela ustalonych przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniach, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń[74]. Jeżeli stan wyjątkowy został wprowadzony na obszarze jednego województwa lub jego części, kompetencje Rady Ministrów przejmuje właściwy wojewoda.

Stan wojenny

Ustawa z dnia 29 sierpnia 2002 roku *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*[75] stanowi, w razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami terrorystycznymi, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, że Prezydent Rzeczypospolitej Polskiej może na wniosek Rady Ministrów wprowadzić stan wojenny na części albo na całym terytorium państwa[76]. W niniejszym wniosku Rada Ministrów określa przyczyny i obszar, na którym ma być wprowadzony stan wojenny, a także odpowiednie do stopnia i charakteru zagrożenia, w zakresie dopuszczonym niniejszą ustawą, rodzaje ograniczeń wolności oraz praw człowieka i obywatela.

Prezydent Rzeczypospolitej Polskiej na wniosek Rady Ministrów w drodze rozporządzenia znosi stan wojenny, jeżeli ustaną przyczyny, dla których stan wojenny został wprowadzony oraz zostanie przywrócone normalne funkcjonowanie państwa[77]. Jeżeli w czasie stanu wojennego wystąpi konieczność obrony

[73] Ibidem, art. 12 ust. 1.

[74] Ibidem, art. 22 ust. 1.

[75] Dz. U. z 2002 r. Nr 156, poz. 1301 z późn. zm.

[76] Ustawa z dnia 29 sierpnia 2002 roku *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2002 r. Nr 156, poz. 1301 z późn. zm.), art. 2 ust. 1.

[77] Ibidem, art. 8 ust. 1.

państwa, obroną tą kieruje Prezydent Rzeczypospolitej Polskiej we współdziałaniu z Radą Ministrów[78].

W aspekcie kompetencji Rady Ministrów Prezydent Rzeczypospolitej Polskiej w czasie stanu wojennego w szczególności:

- postanawia, na wniosek Rady Ministrów, o przejściu organów władzy publicznej na określone stanowiska kierowania,
- postanawia, na wniosek Rady Ministrów, o stanach gotowości bojowej Sił Zbrojnych Rzeczypospolitej Polskiej,
- określa, na wniosek Rady Ministrów, zadania Sił Zbrojnych w czasie stanu wojennego,
- może mianować, na wniosek Prezesa Rady Ministrów, Naczelnego Dowódcę Sił Zbrojnych.

Rada Ministrów w czasie stanu wojennego w szczególności:

- zarządza uruchomienie systemu kierowania obroną państwa,
- zarządza przejście na wojenne, określone w odrębnych przepisach, zasady działania organów władzy publicznej,
- określa, na wniosek Naczelnego Dowódcy Sił Zbrojnych, zasady działania organów władzy publicznej w strefie bezpośrednich działań wojennych,
- może zawiesić funkcjonowanie organów władzy publicznej w strefie bezpośrednich działań wojennych,
- może przekazać organom wojskowym określone kompetencje organów władzy publicznej w strefie bezpośrednich działań wojennych[79].

W przypadku gdy Rada Ministrów nie może zebrać się w czasie stanu wojennego na posiedzenie, konstytucyjne kompetencje Rady Ministrów wykonuje Prezes Rady Ministrów.

Jeżeli organy gminy, powiatu lub samorządu województwa nie wykazują dostatecznej skuteczności w wykonywaniu zadań publicznych lub w realizacji działań wynikających z przepisów o wprowadzeniu stanu wojennego, Prezes Rady Ministrów na wniosek właściwego wojewody może zawiesić te organy do czasu zniesienia stanu wojennego lub na czas określony i ustanowić w ich miejsce zarząd komisaryczny sprawowany przez komisarza rządowego[80]. Komisarza rządowego powołuje i odwołuje Prezes Rady Ministrów na wniosek wojewody, który z dniem powołania przejmuje wykonywanie zadań i kompetencji zawieszonych organów gminy, powiatu lub samorządu województwa. Stan zawieszenia organów gminy, powiatu lub samorządu województwa ustaje z upływem czasu określonego przez Prezesa Rady Ministrów oraz z mocy prawa z dniem zniesienia stanu wojennego.

78 Ibidem, art. 10 ust. 1.

79 Ibidem, art. 11 ust. 1.

80 Ustawy z dnia 29 sierpnia 2002 roku *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2002 r. Nr 156, poz. 1301 z późn. zm.), art. 14 ust. 1.

Rada Ministrów na podstawie rozporządzenia Prezydenta Rzeczypospolitej Polskiej w sprawie wprowadzenia stanu wojennego w drodze rozporządzenia określa przyczyny wprowadzenia ograniczenia wolności i praw człowieka i obywatela w zakresie:

- dostępu do towarów konsumpcyjnych, poprzez całkowitą lub częściową reglamentację zaopatrzenia ludności,
- wolności działalności gospodarczej, poprzez nakazanie okresowego zaniechania prowadzenia działalności gospodarczej określonego rodzaju albo ustanowienie obowiązku uzyskania zezwolenia na rozpoczęcie działalności gospodarczej określonego rodzaju,
- dostępu do informacji publicznej[81].

Ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniu w sprawie wprowadzeniu stanu wojennego wprowadza i stosuje w drodze rozporządzeń Rady Ministrów – w przypadku ograniczeń określonych dotyczących:

- nałożenia na osoby fizyczne i osoby prawne prowadzące gospodarstwa rolne obowiązku wykonywania świadczeń polegających na dostawach na rzecz określonych podmiotów produktów rolno-spożywczych oraz na uprawie określonych gatunków roślin i hodowli zwierząt,
- wprowadzenia najmu lokali i budynków na podstawie decyzji administracyjnej o przydziale w stosunku do wszystkich lokali i budynków, a w uzasadnionych przypadkach także dokwaterowywanie osób do lokalu mieszkalnego lub budynku,
- wprowadzenia zajęcia nieruchomości niezbędnych dla Sił Zbrojnych lub obrony państwa[82].

Obronność państwa

Ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[83] stanowi, iż ogólne kierownictwo w dziedzinie obronności państwa należy do Rady Ministrów. Określa również zakres zadań Rady Ministrów wykonywanych w ramach zapewniania zewnętrznego bezpieczeństwa państwa i sprawowania ogólnego kierownictwa w dziedzinie obronności kraju:

- opracowywanie projektów strategii bezpieczeństwa narodowego,
- planowanie i realizacja przygotowań obronnych państwa zapewniających jego funkcjonowanie w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny, w tym planowanie przedsięwzięć gospodarczo-obronnych oraz zadań wykonywanych na rzecz Sił Zbrojnych Rzeczypospolitej Polskiej i wojsk sojuszniczych,

[81] Ibidem, art. 24 ust. 2 pkt 1.

[82] Ibidem, art. 25 ust. 2 pkt 1.

[83] Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

- przygotowywanie systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, i organów władzy publicznej do funkcjonowania na stanowiskach kierowania,
- utrzymywanie stałej gotowości obronnej państwa, wnioskowanie do Prezydenta Rzeczypospolitej Polskiej o jej podwyższanie w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny oraz o jej obniżanie stosownie do zmniejszania stopnia zagrożenia,
- określanie obiektów szczególnie ważnych dla bezpieczeństwa państwa, w tym obronności oraz przygotowywanie ich szczególnej ochrony,
- przygotowanie na potrzeby obronne państwa i utrzymywanie w stałej gotowości jednolitych systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania,
- przygotowanie systemu stałych dyżurów na czas zewnętrznego zagrożenia bezpieczeństwa państwa i wojny,
- określanie zasad wykorzystania służby zdrowia i infrastruktury technicznej państwa na potrzeby obronne, w tym sposobu zabezpieczania przestrzeni powietrznej i wód terytorialnych w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny,
- zapewnianie funkcjonowania systemu szkolenia obronnego w państwie,
- prowadzenie kontroli stanu przygotowań obronnych w państwie[84].

Rada Ministrów określa w drodze rozporządzenia tryb realizacji powyższych zadań:

- warunki i tryb planowania i finansowania zadań wykonywanych w ramach przygotowań obronnych państwa realizowanych przez organy administracji rządowej i organy samorządu terytorialnego, sposób ich nakładania oraz właściwość organów w tych sprawach, w tym ujętych w planowaniu operacyjnym i programach obronnych,
- organizację i tryb przygotowania systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa oraz warunki funkcjonowania organów władzy publicznej na stanowiskach kierowania,
- stany gotowości obronnej państwa, ich rodzaje, warunki wprowadzania, zadania związane z podwyższaniem gotowości obronnej państwa i tryb ich realizacji, organizację i zadania w zakresie tworzenia systemu stałych dyżurów na potrzeby podwyższania gotowości obronnej państwa oraz właściwość organów w tych sprawach,
- obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa, ich kategorie, a także zadania w zakresie ich szczególnej ochrony oraz właściwość organów w tych sprawach,
- organizację i warunki przygotowania oraz funkcjonowania systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania o skażeniach pro-

[84] Ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.), art. 6 ust. 1.

mieniotwórczych na terytorium Rzeczypospolitej Polskiej oraz właściwość organów w tych sprawach,

- warunki i sposób przygotowania i wykorzystania:
  - transportu morskiego, samochodowego, lotniczego, żeglugi śródlądowej oraz drogownictwa na potrzeby obronne państwa, a także ich ochrony w czasie wojny oraz właściwość organów w tych sprawach,
  - systemów łączności na potrzeby obronne państwa oraz właściwość organów w tych sprawach,
  - publicznej i niepublicznej służby zdrowia na potrzeby obronne państwa oraz właściwość organów w tych sprawach,
- organizacja szkolenia obronnego w państwie, podmioty objęte tym szkoleniem, zadania w zakresie planowania i realizacji szkolenia obronnego oraz właściwość organów w tych sprawach,
- zakres i sposób prowadzenia przez organy administracji rządowej i samorządu terytorialnego kontroli realizacji zadań obronnych wykonywanych przez jednostki organizacyjne i przedsiębiorców[85].

Inne kompetencje Rady Ministrów określone w ustawie:

- art. 14 ust. 5. Rada Ministrów w drodze rozporządzenia tworzy, przekształca i znosi okręgi wojskowe, określa szczegółowe zadania ich dowódców, jako organów rządowej administracji niezespolonej, oraz określa siedziby i terytorialny zasięg działania okręgów wojskowych, uwzględniając w szczególności podział terytorialny państwa;
- art. 17 ust. 8. Rada Ministrów określa w drodze rozporządzenia szczegółowy zakres działania Szefa Obrony Cywilnej Kraju oraz szefów obrony cywilnej województw, powiatów i gmin, jak również zasady i tryb kierowania oraz koordynowania przez nich przygotowań i realizacji przedsięwzięć obrony cywilnej;
- art. 18 ust. 2. Rada Ministrów określa w drodze rozporządzenia ogólne zasady wykonywania zadań w ramach powszechnego obowiązku obrony przez ministrów, wojewodów, marszałków województw, starostów i wójtów lub burmistrzów (prezydentów miast) oraz przedsiębiorców i inne jednostki organizacyjne, a także organizacje społeczne;
- art. 174 ust. 1. w razie ogłoszenia mobilizacji i w czasie wojny Rada Ministrów może objąć militaryzacją jednostki organizacyjne, które wykonują zadania szczególnie ważne dla obronności lub bezpieczeństwa Państwa, a także jednostki organizacyjne specjalnie tworzone do wykonywania takich zadań;
- art. 174 ust. 2. Rada Ministrów, na wniosek ministrów i wojewodów, po uprzednim zaopiniowaniu przez Ministra Obrony Narodowej, ustala istniejące i specjalnie tworzone jednostki organizacyjne, które przewiduje się objąć militaryzacją (jednostki przewidziane do militaryzacji) oraz jednostki organizacyjne stanowiące bazę formowania specjalnie tworzonych jednostek zmi-

[85] Ibidem, art. 6 ust. 2.

litaryzowanych, a także limity osób, które przewiduje się powołać do służby w jednostkach zmilitaryzowanych;

- art. 174 ust. 3. Rada Ministrów określi w drodze rozporządzenia kategorie zadań uzasadniających militaryzację oraz tryb ustalania jednostek organizacyjnych i limitów osób, o których mowa w ust. 2, a także wzór wniosku o objęcie poszczególnych jednostek organizacyjnych przygotowaniami do militaryzacji. Rozporządzenie uwzględni w szczególności potrzeby związane z rozwinięciem systemu obronności i funkcjonowaniem jego elementów w warunkach zewnętrznego zagrożenia państwa i w czasie wojny, w tym mobilizacyjne i wojenne potrzeby Sił Zbrojnych Rzeczypospolitej Polskiej oraz zapewnienia wsparcia wojskom sojuszniczym na terytorium Rzeczypospolitej Polskiej, z wyszczególnieniem we wzorze wniosku przeznaczenia tych jednostek, ich siedzib, organów oraz organów, według których ustaleń będą przygotowywane poszczególne jednostki, jak również specyfikacji przewidywanych wydatków z tym związanych;
- art. 174 ust. 4. Jednostki organizacyjne, o których mowa w ust. 1 i 2 niniejszego artykułu, Rada Ministrów może objąć militaryzacją również w razie wprowadzenia stanu wyjątkowego na całym terytorium Rzeczypospolitej Polskiej;
- art. 176 ust. 2. Rada Ministrów określa w drodze rozporządzenia jednostki przewidziane do militaryzacji, do których osoby posiadające przydziały organizacyjno-mobilizacyjne mogą być powoływane do odbywania ćwiczeń;
- art. 176 ust. 3. Rada Ministrów określi corocznie w drodze rozporządzenia liczbę osób powoływanych w roku kalendarzowym do odbycia ćwiczeń w jednostkach przewidzianych do militaryzacji, z uwzględnieniem potrzeby zapewnienia realizacji zadań przewidzianych dla tych jednostek na czas mobilizacji oraz wojny;
- art. 176 ust. 4. Przeprowadzenie ćwiczeń w jednostkach przewidzianych do militaryzacji zarządza Prezes Rady Ministrów;
- art. 176 ust. 6. Rada Ministrów określi w drodze rozporządzenia tryb postępowania związanego z powoływaniem do odbycia ćwiczeń w jednostkach przewidzianych do militaryzacji oraz wzór wezwania, uwzględniając w szczególności sposób wzywania osób, które przewiduje się powołać do odbycia ćwiczeń w jednostkach przewidzianych do militaryzacji organizowanych w związku ze zwalczaniem klęsk żywiołowych lub usuwaniem ich skutków, a także ćwiczeń przeprowadzanych w trybie natychmiastowego stawiennictwa. Wzór wezwania powinien uwzględniać dane osobowe, przewidywany czas trwania ćwiczeń oraz termin i miejsce stawienia się, a także poświadczenie przyjęcia do wiadomości faktu powołania na ćwiczenia;
- art. 178. Rada Ministrów określi w drodze rozporządzenia:
  a) zadania związane z przygotowaniem jednostek organizacyjnych przewidzianych do objęcia ich militaryzacją oraz organy zobowiązane do realizacji tych zadań, z uwzględnieniem zakresu przedsięwzięć, trybu ich wykonania, terminów gotowości do działania, zabezpieczenia potrzeb, zapewnienia środków finansowych,

b) zasady wyposażania jednostek przewidzianych do militaryzacji i jednostek zmilitaryzowanych w środki transportowe, maszyny i urządzenia oraz w sprzęt wojskowy, z uwzględnieniem źródeł ich pochodzenia,
c) zasady i tryb przeprowadzania kontroli stanu przygotowania jednostek organizacyjnych przewidzianych do objęcia ich militaryzacją oraz organy właściwe w tych sprawach, z uwzględnieniem przedmiotu kontroli i podmiotów objętych kontrolą;

- art. 188 ust. 1. Rada Ministrów może przydzielić jednostki zmilitaryzowane ministrom (wojewodom) albo organom obrony cywilnej;
- art. 188 ust. 2. Rada Ministrów może przydzielić jednostki zmilitaryzowane do Sił Zbrojnych Rzeczypospolitej Polskiej;
- art. 188 ust. 3. W wypadkach, o których mowa w ust. 2 niniejszego artykułu jednostka zmilitaryzowana podlega organowi wojskowemu określonemu przez Ministra Obrony Narodowej;
- art. 188 ust. 4. Rada Ministrów określi, w drodze rozporządzenia, szczegółowe zasady i tryb postępowania w sprawach, o których mowa w ust. 1–3, z uwzględnieniem w szczególności potrzeb organizacyjnych Sił Zbrojnych Rzeczypospolitej Polskiej oraz struktury dowodzenia tymi Siłami Zbrojnymi w czasie pokoju i na wypadek wojny;
- art. 207 ust. 1. Rada Ministrów określi, w drodze rozporządzenia:
  a) tryb i zakres planowania i nakładania obowiązku świadczeń osobistych, przeznaczania do tych świadczeń i zwalniania z nich oraz ich wykonywania,
  b) wzory planów i wykazów świadczeń osobistych prowadzonych przez wojewodę, terenowe organy administracji wojskowej, organy samorządu terytorialnego i jednostki organizacyjne, na rzecz których może być wykonywane świadczenie osobiste,
  c) wzory decyzji administracyjnych, wniosków, wezwań i obwieszczeń oraz zaświadczeń wydawanych w sprawach świadczeń osobistych,
  d) tryb wypłacania ryczałtu i należności pieniężnych za wykonanie świadczeń osobistych oraz dokumenty składane w celu ich wypłacenia.
- art. 207 ust. 2. W rozporządzeniu, o którym mowa w ust. 1 niniejszego artykułu, należy uwzględnić w szczególności priorytet zadań realizowanych przez Siły Zbrojne lub zadań realizowanych na ich rzecz, obowiązek informowania się tych organów oraz ich powiadamiania przez osoby przeznaczone lub zobowiązane do wykonania świadczeń osobistych o sytuacjach i okolicznościach mających wpływ na ich wykonanie, sposób i miejsce przechowywania dokumentów oraz zakres udostępniania lub doręczania planów i wykazów świadczeń osobistych bądź ich wyciągów lub innych dokumentów sporządzanych w tych sprawach, możliwość wypłacania ryczałtu i należności pieniężnych nie wcześniej niż po wykonaniu świadczenia osobistego oraz obowiązek ich zwrotu w przypadku nienależnej wypłaty;
- art. 208 ust. 5. Rada Ministrów określi w drodze rozporządzenia dla wykonania niezbędnych świadczeń rzeczowych:

a) rodzaj i liczbę nieruchomości, które mogą być w tym celu w użytkowaniu w danym roku kalendarzowym,
b) rodzaj i liczbę rzeczy ruchomych, które w danym roku kalendarzowym mogą być w tym celu pobrane,
c) uwzględniając w szczególności potrzeby związane z prowadzeniem kwalifikacji wojskowej, przeprowadzaniem ćwiczeń wojskowych, w tym organizowanych z zastosowaniem natychmiastowego stawiennictwa żołnierzy rezerwy i sprawdzaniem gotowości mobilizacyjnej Sił Zbrojnych;

- art. 215 ust. 1. Rada Ministrów określi w drodze rozporządzenia:
  a) tryb i zakres planowania i nakładania obowiązku świadczeń rzeczowych, przeznaczania do tych świadczeń i zwalniania z nich oraz ich wykonywania,
  b) rodzaje planów, zestawień i wykazów świadczeń rzeczowych prowadzonych przez wojewodę, terenowe organy administracji wojskowej, organy samorządu terytorialnego i jednostki organizacyjne, na rzecz których może być wykonywane świadczenie rzeczowe,
  c) wzory decyzji administracyjnych, wniosków, wezwań w sprawach świadczeń rzeczowych,
  d) tryb i zakres żądania oraz przekazywania informacji,
  e) tryb oddania, przyjęcia i zwrotu przedmiotu świadczeń rzeczowych oraz tryb dochodzenia roszczeń,
  f) wykaz dobowych stawek ryczałtu za używanie poszczególnych przedmiotów świadczeń rzeczowych.
- art. 215 ust. 2. W rozporządzeniu, o którym mowa w ust. 1 niniejszego artykułu, należy uwzględnić w szczególności priorytet zadań realizowanych przez Siły Zbrojne lub zadań realizowanych na ich rzecz; obowiązek informowania się organów i jednostek organizacyjnych właściwych w sprawach świadczeń rzeczowych oraz ich powiadamiania przez osoby zobowiązane do wykonywania tych świadczeń o sytuacjach i okolicznościach mających wpływ na ich wykonanie; sposób i miejsce przechowywania dokumentów oraz zakres udostępniania lub doręczania planów, zestawień i wykazów świadczeń rzeczowych bądź ich wyciągów lub innych dokumentów sporządzanych w tych sprawach; możliwość przechowywania i doręczania wezwań w sprawach świadczeń rzeczowych przez organy lub jednostki organizacyjne, na rzecz których będzie wykonywane świadczenie rzeczowe; możliwość dokonywania oględzin nieruchomości i rzeczy ruchomych, które mogą być lub są przedmiotem świadczeń rzeczowych; dopuszczenie drogi postępowania sądowego w dochodzeniu roszczeń, o których mowa w art. 213, a także fakt, że ryczałt za używanie poszczególnych przedmiotów świadczeń rzeczowych podlega corocznej waloryzacji;
- art. 219 ust. 8. Rada Ministrów określi w drodze rozporządzenia:
  a) tryb i zakres nakładania obowiązku świadczeń osobistych i rzeczowych,

b) wzory decyzji administracyjnych, wniosków i obwieszczeń oraz zaświadczeń wydawanych w sprawach świadczeń osobistych i rzeczowych,
b) szczegółowe zasady i tryb odpłatności za używanie przedmiotów świadczeń rzeczowych,
c) tryb i sposób ustalania i wypłacania odszkodowań za szkody w nich powstałe,
d) tryb wypłacania ryczałtu i należności pieniężnych za wykonanie świadczeń osobistych, a także dokumenty składane w celu ich wypłacania;

- art. 219 ust. 9. W rozporządzeniu, o którym mowa w ust. 8 niniejszego artykułu, należy uwzględnić w szczególności priorytet zadań realizowanych przez Siły Zbrojne lub zadań realizowanych na ich rzecz; obowiązek informowania się tych organów oraz ich powiadamiania przez osoby zobowiązane do wykonywania świadczeń o sytuacjach i okolicznościach mających wpływ na ich wykonanie; możliwość dokonania odpłatności za używanie przedmiotu świadczenia rzeczowego lub wypłacenia ryczałtu i należności pieniężnych za wykonanie świadczenia osobistego nie wcześniej niż po wykonaniu tego świadczenia oraz obowiązek ich zwrotu w przypadku nienależnej wypłaty.

7.3. Minister właściwy do spraw wewnętrznych

Podstawowe zadania z zakresu bezpieczeństwa i porządku publicznego ustawodawca powierzył ministrowi właściwemu do spraw wewnętrznych, który kieruje działem sprawy wewnętrzne[86]. Zgodnie z art. 29 ust. 1 ustawy z dnia 4 września 1997 *roku o działach administracji rządowej*[87] do działu tego należą: ochrona bezpieczeństwa i porządku publicznego, ochrona granicy państwa, kontrola ruchu granicznego i cudzoziemców oraz koordynacja działań związanych z polityką migracyjną państwa, zarządzanie kryzysowe, obrona cywilna, ochrona przeciwpożarowa, przeciwdziałanie skutkom klęsk żywiołowych i innych podobnych zdarzeń zagrażających bezpieczeństwu powszechnemu, usuwanie skutków klęsk żywiołowych i innych podobnych zdarzeń zagrażających bezpieczeństwu powszechnemu, nadzór nad ratownictwem górskim i wodnym, sprawy obywatelstwa, ewidencja ludności, dowodów osobistych i paszportów, rejestracja stanu cywilnego oraz zmiany imion i nazwisk.

W następstwie zniesienia z dniem 21 listopada 2011 roku Ministerstwa Spraw Wewnętrznych i Administracji utworzone zostało Ministerstwo Spraw Wewnętrznych i Ministerstwo Administracji i Cyfryzacji. W związku z tym Prezes Rady Ministrów na podstawie delegacji ustawowej zawartej w art. 33 ust. 1

[86] T. j.: Dz. U. z 2007 r. Nr 65, poz. 437 z późn. zm.

[87] Ibidem.

i 1a ustawy z dnia 8 sierpnia 1996 roku *o Radzie Ministrów*[88] w rozporządzeniu z dnia 18 listopada 2011 roku określił szczegółowy zakresu działania Ministra Spraw Wewnętrznych, który kieruje działem administracji rządowej – sprawy wewnętrzne[89]. Zgodnie z tym rozporządzeniem minister właściwy do spraw wewnętrznych sprawuje nadzór nad działalnością Policji, Straży Granicznej, Państwowej Straży Pożarnej, Obrony Cywilnej Kraju, Szefa Urzędu do Spraw Cudzoziemców, Krajowego Centrum Informacji Kryminalnej oraz Biura Ochrony Rządu[90]. Wykonuje także określone w ustawie i w odrębnych przepisach zadania dotyczące obronności i ochrony bezpieczeństwa państwa oraz uprawnienia w stosunku do terenowych organów rządowej administracji ogólnej oraz organów samorządu terytorialnego.

Minister Spraw Wewnętrznych na podstawie art. 39 ust. 6 ustawy z dnia 8 sierpnia 1996 roku *o Radzie Ministrów*[91] zarządzeniem nr 4 z dnia 9 grudnia 2011 roku nadał regulamin organizacyjny Ministerstwa Spraw Wewnętrznych[92]. Regulamin określa zakres zadań i tryb pracy komórek organizacyjnych Ministerstwa Spraw Wewnętrznych oraz jednostek organizacyjnych podległych Ministrowi Spraw Wewnętrznych lub przez niego nadzorowanych, w tym realizujących zadania w sferze zarządzania kryzysowego.

Art. 12 ust. 1 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[93] stanowi, że ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują zgodnie z zakresem swojej właściwości zadania dotyczące zarządzania kryzysowego, zapis ten dotyczy także Ministra Spraw Wewnętrznych. Z kolei z treści w art. 7 ust. 1 ustawy wynika, że w przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, który niezwłocznie zawiadamia o swoich działaniach Prezesa Rady Ministrów. Decyzje podjęte przez ministra właściwego do spraw wewnętrznych podlegają rozpatrzeniu na najbliższym posiedzeniu Rady Ministrów[94].

88 T. j.: Dz. U. z 2003 r. Nr 24, poz. 199 z późn. zm.

89 Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2011 roku *w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych* (Dz. U. z 2011 r. Nr 248, poz. 1491).

90 Załącznik do Rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 roku *w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych* (Dz. U. z 2011 r. Nr 248, poz. 1491).

91 T. j.: Dz. U. z 2003 r. Nr 24, poz. 199 z późn. zm.

92 Zarządzenie Nr 4 z dnia 9 grudnia 2011 roku *w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Spraw Wewnętrznych*. Niniejsze zarządzenie poprzedzało zarządzenie Nr 8 Ministra Spraw Wewnętrznych i Administracji z dnia 9 marca 2011 roku *w sprawie regulaminu organizacyjnego Ministerstwa Spraw Wewnętrznych i Administracji* (Dz. Urz. Min. Spraw Wew. i Adm. Nr 4, poz. 21 i Nr 7, poz. 35) zmienione zarządzeniem Nr 28 Ministra Spraw Wewnętrznych i Administracji z dnia 25 października 2011 roku, które utraciło moc obowiązującą w związku z wejściem w życie rozporządzenia Rady Ministrów z dnia 21 listopada 2011 roku *w sprawie zniesienia Ministerstwa Spraw Wewnętrznych i Administracji oraz Ministerstwa Infrastruktury* (Dz. U. z 2011 r. Nr 250, poz. 1500).

93 Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

94 Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 7 ust. 3.

Minister Spraw Wewnętrznych opracowuje plan zarządzania kryzysowego, który uzgadnia z dyrektorem Rządowego Centrum Bezpieczeństwa. Plan ten stanowi załącznik funkcjonalny do Krajowego Plany Zarządzania Kryzysowego. Ponadto w drodze zarządzenia wydaje wojewodom wytyczne do opracowania wojewódzkich planów zarządzania kryzysowego, a także je zatwierdza i aktualizuje po zasięgnięciu opinii dyrektora RCB[95].

Na potrzeby realizacji zadań z zakresu zarządzania kryzysowego Minister Spraw Wewnętrznych tworzy Zespół Zarządzania Kryzysowego, w skład którego wchodzą kierujący właściwymi komórkami organizacyjnymi obsługującego ministra, a także inne osoby przez niego wskazane.

Skład Zespołu Zarządzania Kryzysowego MSW: przewodniczący – Minister Spraw Wewnętrznych, członkowie: zastępca przewodniczącego – Podsekretarz Stanu w Ministerstwie Spraw Wewnętrznych, do którego zakresu czynności należy zarządzanie kryzysowe, Sekretarze i Podsekretarze Stanu w Ministerstwie Spraw Wewnętrznych, Komendant Główny Państwowej Straży Pożarnej, Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef Biura Ochrony Rządu, Szef Obrony Cywilnej Kraju, Dyrektor Biura do Spraw Usuwania Skutków Klęsk Żywiołowych MSW, Dyrektor Generalny MSW, Dyrektor Departamentu Ewidencji Państwowych i Teleinformatyki MSW, Dyrektor Departamentu Zdrowia MSW, sekretarz Zespołu – Dyrektor Departamentu Ratownictwa i Ochrony Ludności MSW.

Pracami Zespołu kieruje przewodniczący, a w razie jego nieobecności zastępca przewodniczącego. Przewodniczący Zespołu, z własnej inicjatywy lub na wniosek członka Zespołu, może zapraszać do udziału w jego pracach na prawach członka innych przedstawicieli Ministerstwa Spraw Wewnętrznych oraz jednostek organizacyjnych podległych Ministrowi Spraw Wewnętrznych lub przez niego nadzorowanych oraz inne osoby zaproszone do udziału w pracach Zespołu niewymienione w zarządzeniu. Ponadto przewodniczący Zespołu może powierzać poszczególnym członkom Zespołu wykonanie określonych czynności, niezbędnych do realizacji jego zadań.

Do zadań Zespołu Zarządzania Kryzysowego MSW należy:

- dokonywanie okresowej oceny zagrożeń na potrzeby Raportu o zagrożeniach bezpieczeństwa narodowego,
- opiniowanie projektów planów zarządzania kryzysowego,
- opiniowanie wykazu obiektów, instalacji i urządzeń wchodzących w skład infrastruktury krytycznej w ramach swojej właściwości,
- wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom[96].

Minister Spraw Wewnętrznych odpowiedzialny za dział administracji rządowej – sprawy wewnętrzne tworzy Centrum Zarządzania Kryzysowego.

[95] Ibidem, art. 14 ust. 3 i 4.

[96] Ibidem, art. 12 ust. 2c.

Do zadań Centrum Zarządzania Kryzysowego MSW należy:

- pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego,
- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej.
- nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,
- współpraca z podmiotami realizującymi monitoring środowiska,
- współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne,
- dokumentowanie działań podejmowanych przez centrum,
- realizacja zadań stałego dyżuru na potrzeby podwyższenia gotowości obronnej państwa,
- współdziałanie na wszystkich szczeblach administracji rządowej w zakresie informowania i przekazywania poleceń do wykonania w systemie całodobowym dla jednostek ochrony zdrowia w przypadkach awaryjnych, losowych, jak również zaburzeń funkcjonowania systemu[97].

Zadania w sferze zarządzania kryzysowego w Ministerstwie Spraw Wewnętrznych wykonują również inne jednostki organizacyjne, i tak w Departamencie Analiz i Nadzoru Wydział Przeciwdziałania Zagrożeniom Terrorystycznym i Przestępczości Zorganizowanej, w Departamencie Ratownictwa i Ochrony Ludności: Wydział Ochrony Ludności, Wydział Nadzoru nad Ratownictwem Górskim i Wodnym, Wydział Zarządzania Kryzysowego, Wydział Spraw Obronnych, ponadto Biuro do Spraw Usuwania Skutków Klęsk Żywiołowych[98].

W aspekcie zarządzania kryzysowego istotną pozycję w Ministerstwie Spraw Wewnętrznych zajmuje Departament Analiz i Nadzoru, do zadań którego należy m.in.:

- prowadzenie spraw związanych z nadzorem ministra nad wykonywaniem zadań z zakresu ochrony i bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa i porządku publicznego, ochrony osób, obiektów i urządzeń realizowanych przez BOR, przygotowania i wdrożenia programów profilaktycznych na rzecz bezpieczeństwa obywateli,
- prowadzenie spraw związanych z nadzorem ministra nad prawidłowością działania Krajowego Systemu Informatycznego (KSI) oraz zadań, o których mowa w art. 18–20 ustawy z dnia 24 sierpnia 2007 roku *o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym*,
- przygotowywanie analiz, opinii, wniosków oraz propozycji rozwiązań systemowych w sprawach:

[97] Ibidem, art. 13 ust. 1 i 2.

[98] www.bip.msw.gov.pl [pobrano 29.04.2012].

- gromadzenia informacji, analizowania i prognozowania zagrożeń dla bezpieczeństwa i porządku publicznego, w tym zagrożeń terroryzmem, ekstremizmem i przestępczością zorganizowaną,
- opracowywania koncepcji i programów w zakresie przeciwdziałania i zwalczania zagrożeń terrorystycznych, ekstremizmu i przestępczości zorganizowanej,
- inicjowania, opracowywania i wdrażania koncepcji ogólnokrajowych działań profilaktycznych służb odpowiedzialnych za bezpieczeństwo i porządek publiczny,
- przygotowywania programów, inicjatyw i rozwiązań z zakresu przeciwdziałania przestępczości i patologiom społecznym generującym przestępczość,
- koordynacji prac w obszarze badań naukowych i prac rozwojowych prowadzonych na rzecz bezpieczeństwa państwa w zakresie właściwości Departamentu,

▫ obsługa zespołów, których zakres kompetencji pozostaje we właściwości Departamentu, a w szczególności Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, Rady Bezpieczeństwa Imprez Sportowych, Wspólnej Polsko-Amerykańskiej Grupy Roboczej do Spraw Zwalczania Terroryzmu,

▫ prowadzenie spraw związanych ze zleceniem – jednostkom niezaliczanym do sektora finansów publicznych, prowadzącym działalność pożytku publicznego – zadań publicznych z zakresu bezpieczeństwa i porządku publicznego oraz przeciwdziałania patologiom społecznym, zgodnie z ustawą z dnia 24 kwietnia 2003 roku *o działalności pożytku publicznego i o wolontariacie*,

▫ prowadzenie postępowań administracyjnych pozostających we właściwości ministra dotyczących:
  - odwołań od decyzji i postanowień wojewodów wynikających z ustawy z dnia 20 marca o bezpieczeństwie imprez masowych,
  - realizacji zadań wynikających z art. 10 ust. 3 ustawy z dnia 12 czerwca 2003 roku – *Prawo pocztowe*,
  - odwołań od decyzji wojewodów w sprawach umieszczania w ewidencji obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie przez specjalistyczne formacje ochronne lub odpowiednie zabezpieczenie techniczne, wydanych na podstawie art. 5 ust. 6 ustawy z dnia 22 sierpnia 1997 roku *o ochronie osób i mienia*,

▫ współpraca z samorządem terytorialnym, strażami gminnymi (miejskimi) organizacjami pozarządowymi i pożytku publicznego oraz innymi podmiotami działającymi na rzecz bezpieczeństwa i porządku publicznego,

▫ koordynowanie działań związanych z udziałem w Europejskiej Sieci Zapobiegania Przestępczości (EUCPN),

- przygotowanie i udział w ćwiczeniach w zakresie przeciwdziałania i zwalczania zagrożeń terrorystycznych oraz usuwania skutków ewentualnych zamachów[99].

Do zadań Wydziału Przeciwdziałania Zagrożeniom Terrorystycznym i Przestępczości Zorganizowanej Departamentu Analiz i Nadzoru MSW należy:

- sporządzanie raportów dotyczących przygotowania służb podległych i nadzorowanych przez ministra w zakresie przeciwdziałania zagrożeniom terrorystycznym i przestępczości zorganizowanej,
- przygotowywanie bieżących analiz, opinii, wniosków i propozycji rozwiązań systemowych na potrzeby ministra w zakresie zagrożeń terrorystycznych, ekstremizmu i przestępczości zorganizowanej,
- przygotowywanie opracowań dotyczących krajowych i międzynarodowych rozwiązań w zakresie przeciwdziałania, zapobiegania i reagowania na zagrożenia terrorystyczne oraz przestępczość zorganizowaną,
- obsługa merytoryczna, biurowa i techniczna posiedzeń:
  - Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, Sekretarza tego Zespołu oraz Zespołu Zadaniowego – Stałej Grupy Eksperckiej działającej przy Zespole,
  - Wspólnej Polsko-Amerykańskiej Grupy Roboczej do Spraw Zwalczania Terroryzmu,
- prowadzenie spraw związanych z udziałem przedstawiciela ministra w pracach Międzyresortowego Zespołu do spraw zapobiegania nielegalnemu rozprzestrzenianiu broni masowego rażenia i Inicjatywy Krakowskiej,
- prowadzenie spraw związanych z tworzeniem i implementacją systemu przeciwdziałania rozprzestrzenianiu środków chemicznych, biologicznych, radiologicznych i nuklearnych (CBRN) w zakresie Inicjatywy Krakowskiej oraz innych analogicznych inicjatyw w zakresie dotyczącym Ministerstwa oraz służb podległych i nadzorowanych przez ministra,
- udział w ćwiczeniach z zakresu zwalczania terroryzmu dotyczących Ministerstwa oraz służb podległych i nadzorowanych przez ministra[100].

Kolejna struktura Ministerstwa Spraw Wewnętrznych, która wykonuje zadania w sferze zarządzania kryzysowego na poziomie państwa, to Departament Ratownictwa i Ochrony Ludności z wydziałami: Ochrony Ludności, Nadzoru nad Ratownictwem Górskim i Wodnym, Zarządzania Kryzysowego, Spraw Obronnych. Do zadań Departamentu Ratownictwa i Ochrony Ludności należy:

- prowadzenie spraw związanych z nadzorem ministra nad:
  - działalnością Państwowej Straży Pożarnej w zakresie niezastrzeżonym dla innych komórek organizacyjnych Ministerstwa,

[99] Zarządzenie Nr 13 Ministra Spraw Wewnętrznych z dnia 20 marca 2012 roku *w sprawie regulaminu organizacyjnego Ministerstwa Spraw Wewnętrznych,* § 14a, www.bip.msw.gov.pl [pobrano 29.04. 2012].

[100] Ibidem.

- działalnością szefa Obrony Cywilnej Kraju w zakresie przygotowania założeń i zasad działania obrony cywilnej, ustalania ogólnych zasad realizacji obrony cywilnej oraz opracowywania planu obrony cywilnej państwa,
- funkcjonowaniem systemu powiadamiania ratunkowego w zakresie koncepcji systemowych i strategii finansowania tego systemu, z wyłączeniem zadań związanych z administrowaniem, zarządzaniem i finansowaniem systemów teleinformatycznych,
- ratownictwem górskim i wodnym,
- działalnością Polskiego Czerwonego Krzyża dotyczącą prowadzenia Krajowego Biura Informacji,

▫ prowadzenie spraw związanych z realizacją zadań w zakresie właściwości ministra dotyczących:
- ochrony przeciwpożarowej,
- obrony cywilnej,
- przeciwdziałania skutkom klęsk żywiołowych i innych podobnych zdarzeń zagrażających bezpieczeństwu powszechnemu,
- koordynacji zadań wynikających ze zobowiązań sojuszniczych, ratyfikowanych umów i konwencji międzynarodowych w zakresie ochrony ludności, obrony cywilnej, zarządzania kryzysowego oraz ratownictwa,
- koordynacji planowania, przeprowadzania i udziału w ćwiczeniach w zakresie ochrony ludności, obrony cywilnej i ratownictwa oraz udziału i nadzoru nad ćwiczeniami w zakresie zarządzania kryzysowego w odniesieniu do Ministerstwa oraz służb podległych i nadzorowanych przez ministra,

▫ prowadzenie spraw związanych z realizacją – w zakresie właściwości ministra – zadań wynikających z ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* dotyczących:
- wojewódzkich planów zarządzania kryzysowego, Krajowego Planu Zarządzania Kryzysowego, Raportu o Zagrożeniach Bezpieczeństwa Narodowego, Narodowego Planu Ochrony Infrastruktury Krytycznej oraz wykazu przedsięwzięć i procedur zarządzania kryzysowego,
- wykazu obiektów, instalacji i urządzeń wchodzących w skład infrastruktury krytycznej,
- opracowywania planów zarządzania kryzysowego resortu spraw wewnętrznych,
- przygotowania analiz, opinii, wniosków oraz innych niezbędnych dokumentów na potrzeby Zespołu Zarządzania Kryzysowego Ministerstwa oraz jego obsługa organizacyjna,
- prowadzenie spraw związanych ze zlecaniem – jednostkom niezaliczanym do sektora finansów publicznych, prowadzącym działalność pożytku publicznego – zadań publicznych z zakresu bezpieczeństwa i porządku publicznego oraz przeciwdziałania patologiom społecznym, zgodnie z ustawą z dnia 24 kwietnia 2003 roku o działalności pożytku publicznego i o wolontariacie,

– koordynowanie i nadzór nad realizacją zadań Ministerstwa oraz organów i jednostek organizacyjnych podległych ministrowi lub przez niego nadzorowanych związanych z:
- osiąganiem gotowości obronnej państwa,
- planowaniem obronnym, szkoleniem obronnym, przygotowaniami obronnymi w zakresie spraw organizacyjno-mobilizacyjnych i militaryzacji,
- realizacji zadań ministra wynikających z zobowiązań międzynarodowych Rzeczypospolitej Polskiej w zakresie kontroli uzbrojenia, rozbrojenia i broni chemicznej, udziału resortu spraw wewnętrznych w realizacji wsparcia państwa gospodarza (HNS), Celów Sił Zbrojnych NATO i Wymagań Długoterminowych oraz pobytu wojsk obcych na terytorium kraju,
- przygotowaniem i zabezpieczeniem funkcjonowania stanowisk kierowania dla kierowniczych organów państwa na czas zewnętrznego zagrożenia bezpieczeństwa państwa i wojny,
- prowadzeniem spraw związanych z nadzorem nad Służbą Dyżurną Ministra[101].

Do zadań Wydziału Ochrony Ludności Departamentu Ratownictwa i Ochrony Ludności MSW należy:
- prowadzenie spraw związanych z nadzorem Ministra Spraw Wewnętrznych nad:
  – działalnością Państwowej Straży Pożarnej,
  – funkcjonowaniem krajowego systemu ratowniczo-gaśniczego,
  – działalnością Szefa Obrony Cywilnej Kraju,
  – funkcjonowaniem systemu powiadamiania ratunkowego,
  – działalnością Polskiego Czerwonego Krzyża,
- opiniowanie programów, informacji i sprawozdań przedkładanych ministrowi przez Komendanta Głównego Państwowej Straży Pożarnej,
- prowadzenie spraw dotyczących zlecenia organizacjom społecznym zadań publicznych z zakresu ochrony przeciwpożarowej,
- prowadzenie spraw związanych z:
  – realizacją zadań w zakresie właściwości ministra dotyczących ochrony przeciwpożarowej,
  – funkcjonowaniem zakładowych straży pożarnych oraz zakładowych służb ratowniczych, w szczególności przygotowywanie decyzji ministra dotyczących powoływania, przekształcania oraz likwidacji zakładowych straży pożarnych i zakładowych służb ratowniczych oraz przedkładania opinii i analiz w tym zakresie, zgodnie z art. 17 ustawy z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej*,
- prowadzenie spraw pozostających w zakresie właściwości ministra związanych z:
  – nadzorem i koordynacją planowania, przeprowadzania i udziału w ćwiczeniach z zakresu obrony cywilnej, ratownictwa i ochrony ludności oraz służb podległych ministrowi lub przez niego nadzorowanych,

[101] Ibidem, § 17.

- koordynacji realizacji zadań wynikających ze zobowiązań sojuszniczych, ratyfikowanych umów i konwencji międzynarodowych w zakresie ratownictwa, obrony cywilnej i ochrony ludności,

- realizacja zadań w zakresie właściwości ministra związanych z funkcjonowaniem Krajowego Systemu Wykrywania Skażeń i Alarmowania,
- przygotowanie i aktualizacja Programu Doskonalenia Obrony Cywilnej Ministerstwa Spraw Wewnętrznych zgodnie z przepisami rozporządzenia Rady Ministrów z dnia 3 października 2007 roku w sprawie warunków i trybu planowania i finansowania zadań wykonywanych w ramach przygotowań obronnych państwa przez organy administracji rządowej i organy samorządu terytorialnego,
- przygotowywanie dla ministra opinii służbowych o Komendancie Głównym Państwowej Straży Pożarnej,
- opiniowanie projektów budżetów, realizacji dochodów i wydatków oraz wniosków Państwowej Straży Pożarnej,
- prowadzenie spraw związanych z realizacją zadań w zakresie właściwości ministra dotyczących programów operacyjnych w obszarze ochrony ludności, z zastrzeżeniem spraw realizowanych przez Departament Budżetu,
- przygotowanie analiz, ocen i innych informacji dotyczących ochrony ludności, obrony cywilnej oraz funkcjonowania podmiotów uczestniczących w krajowym systemie ratowniczo-gaśniczym.

Do zadań Wydziału Nadzoru nad Ratownictwem Górskim i Wodnym należy:

- prowadzenie spraw związanych z nadzorem ministra nad ratownictwem górskim i wodnym,
- prowadzenie spraw dotyczących:
  - zlecania społecznym organizacjom ratowniczym uprawnionym do wykonywania ratownictwa górskiego zadań z zakresu ratownictwa górskiego,
  - zlecania społecznym organizacjom ratowniczym uprawnionym do wykonywania ratownictwa wodnego zadań z zakresu ratownictwa wodnego,
  - przygotowywania umów dotacyjnych na finansowanie zadań z zakresu ratownictwa górskiego i wodnego ze środków przeznaczonych w budżecie państwa na ten cel oraz ich rozliczanie,
  - nadzoru merytorycznego oraz finansowego nad sposobem realizacji umów dotacyjnych,
  - współpracy z komórkami organizacyjnymi Ministerstwa właściwymi w sprawach prawnych, finansowych i kontroli w zakresie zlecenia społecznym organizacjom ratowniczym zadań publicznych – w trybie ustawy z dnia 24 kwietnia 2003 roku *o działalności pożytku publicznego i o wolontariacie*,
- prowadzenie postępowań administracyjnych w trybie art. 5 ust. 2 ustawy z dnia 18 sierpnia 2011 roku *o bezpieczeństwie i ratownictwie w górach i na zorganizowanych terenach narciarskich* oraz w trybie art. 12 ust. 2 ustawy z dnia 18 sierpnia 2011 roku *o bezpieczeństwie osób przebywających na obszarach wodnych*,

- przygotowywanie analiz i opracowań dotyczących funkcjonowania ratownictwa górskiego i wodnego w Polsce oraz perspektywy ich rozwoju,
- współpraca z wojewodami oraz jednostkami samorządu terytorialnego w sprawach związanych z ratownictwem górskim i wodnym,
- przedstawianie ministrowi opinii dotyczących przepisów prawnych odnoszących się bezpieczeństwa na wodach i w górach,
- prowadzenie spraw związanych z realizacją zadań w zakresie właściwości ministra dotyczących służb ratowniczych oraz społecznych organizacji ratowniczych, w szczególności współpraca z właściwymi podmiotami administracji publicznej w tym zakresie,
- obsługa merytoryczna, biurowa i techniczna posiedzeń organu pomocniczego ministra powołanego w sprawach z zakresu nadzoru nad ratownictwem górskim i wodnym,
- koordynacja spraw związanych z planowaniem, wykonaniem i sprawozdawczością budżetową Departamentu w skaldzie finansowym i zadaniowym.

Do zadań Wydziału Zarządzania Kryzysowego należy:

- prowadzenie spraw związanych z realizacją – w zakresie właściwości ministra – zadań wynikających z ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, a w szczególności współpraca z właściwymi instytucjami krajowymi i zagranicznymi w tym zakresie,
- przygotowywanie analiz, opinii, wniosków i propozycji rozwiązań systemowych w zakresie bezpieczeństwa powszechnego i zarządzania kryzysowego na potrzeby ministra oraz Zespołu Zarządzania Kryzysowego Ministerstwa Spraw Wewnętrznych,
- obsługa organizacyjna i merytoryczna Zespołu Zarządzania Kryzysowego Ministerstwa Spraw Wewnętrznych,
- przygotowanie i aktualizacja planu zarządzania kryzysowego resortu spraw wewnętrznych,
- przygotowanie i aktualizacja wykazów obiektów, instalacji i urządzeń wchodzących w skład infrastruktury krytycznej w zakresie właściwości ministra,
- nadzór nad przygotowaniem planów ochrony obiektów, instalacji oraz urządzeń infrastruktury krytycznej w zakresie właściwości ministra,
- opracowywanie i aktualizacja Narodowego Planu Ochrony Infrastruktury Krytycznej w części dotyczącej resortu spraw wewnętrznych,
- opracowywanie i aktualizacja Krajowego Planu Zarządzania Kryzysowego w części dotyczącej resortu spraw wewnętrznych,
- opracowywanie i aktualizacja wkładu resortu spraw wewnętrznych do Raportu o zagrożeniach bezpieczeństwa narodowego,
- prowadzenie spraw związanych z przygotowaniem, aktualizacją i uruchamianiem procedur z wykazu przedsięwzięć i procedur zarządzania kryzysowego w zakresie właściwości ministra,
- realizacja zadań związanych z wydawaniem wytycznych ministra do wojewódzkich planów zarządzania kryzysowego,

- analiza wojewódzkich planów zarządzania kryzysowego i ich aktualizacja w celu przygotowania do zatwierdzenia przez ministra,
- nadzór i udział w ćwiczeniach z zakresu zarządzania kryzysowego dotyczących Ministerstwa oraz służb podległych i nadzorowanych przez ministra,
- prowadzenie spraw w zakresie właściwości ministra związanych z koordynacją realizacji zadań wynikających ze zobowiązań sojuszniczych, ratyfikowanych umów i konwencji międzynarodowych w zakresie zarządzania kryzysowego,
- prowadzenie spraw związanych z realizacja zadań właściwości ministra dotyczących przeciwdziałania skutkom klęsk żywiołowych i innych podobnych zdarzeń zagrażających bezpieczeństwu powszechnemu,
- prowadzenie spraw związanych z nadzorem nad funkcjonowaniem Służby Dyżurnej Ministra.

Istotną pozycję w procesie zarządzania kryzysowego w Ministerstwie Spraw Wewnętrznych zajmuje Biuro do Spraw Usuwania Skutków Klęsk Żywiołowych. W skład tego biura wchodzą następujące jednostki organizacyjne: Wydział Pomocy Jednostkom Samorządu Terytorialnego, Wydział Koordynacji i Realizacji Programów, Wydział Organizacyjno-Prawny.

Zadania Biura do Spraw Usuwania Skutków Klęsk Żywiołowych MSW to:

- prowadzenie spraw związanych z inicjowaniem, programowaniem i koordynowaniem działań administracji rządowej w zakresie usuwania skutków powodzi, osuwisk ziemnych i innych klęsk żywiołowych,
- opracowywanie projektów programów dotyczących usuwania skutków klęsk żywiołowych oraz oszacowywania kosztów z tym związanych,
- prowadzenie spraw w zakresie pomocy finansowej udzielanej dla jednostek samorządu terytorialnego z rezerwy celowej budżetu państwa przeznaczonej na przeciwdziałanie i usuwanie skutków klęsk żywiołowych,
- prowadzenie spraw w zakresie udzielania pomocy finansowej z budżetu państwa osobom i rodzinom poszkodowanym w wyniku zdarzeń o charakterze klęsk żywiołowych,
- przygotowywanie opinii ministra w zakresie dofinansowania z rezerwy celowej budżetu państwa na przeciwdziałanie i usuwanie skutków klęsk żywiołowych kosztów związanych z realizacją obiektów liniowych oraz wywłaszczeń gruntów objętych miejscowym planem odbudowy,
- obsługa finansowa działań administracji rządowej związanych z usuwaniem skutków klęsk żywiołowych, w tym prowadzenie dokumentacji ponoszonych wydatków,
- koordynowanie wydatkowania i rozliczenia środków przeznaczonych na usuwanie skutków klęsk żywiołowych, pochodzących z innych źródeł niż rezerwa celowa budżetu państwa na przeciwdziałanie i usuwanie skutków klęsk żywiołowych, w szczególności środków pochodzących z Funduszu Solidarności Unii Europejskiej,

- prowadzenie spraw dotyczących Projektu ochrony przeciwpowodziowej w dorzeczu rzeki Odry i Programu ochrony przed powodzią w dorzeczu górnej Wisły,
- planowanie środków finansowych na przeciwdziałanie i usuwanie skutków klęsk żywiołowych,
- współpraca z organami administracji rządowej, organami administracji samorządowej i ich jednostkami organizacyjnymi oraz organizacjami pozarządowymi w zakresie realizacji zadań Biura.

7.4. Ministrowie i kierownicy urzędów centralnych

Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują zgodnie z zakresem swojej właściwości zadania dotyczące zarządzania kryzysowego. Podstawę prawną stanowi ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* wraz z aktami wykonawczymi[102].

Ministrowie i kierownicy opracowują plany zarządzania kryzysowego, w których uwzględnia się:

- analizę i ocenę możliwości wystąpienia zagrożeń, w tym dla infrastruktury krytycznej uwzględnionej w wykazie,
- szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczania i likwidacji ich skutków,
- organizację monitoringu zagrożeń i realizację zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa,
- organizację realizacji zadań z zakresu ochrony infrastruktury krytycznej[103].

Plany, o których jest mowa w ustawie, są uzgadniane z dyrektorem Rządowego Centrum Bezpieczeństwa i stanowią załączniki funkcjonalne do Krajowego Planu Zarządzania Kryzysowego[104].

Ministrowie i kierownicy na potrzeby realizacji zadań z zakresu zarządzania kryzysowego tworzą zespoły zarządzania kryzysowego, w skład których wchodzą kierujący właściwymi komórkami organizacyjnymi urzędu obsługującego ministra lub kierownika, a także inne osoby przez nich wskazane. Określają oni w drodze zarządzenia organizację, skład oraz miejsce i tryb pracy tych zespołów[105].

Do zadań zespołów zarządzania kryzysowego należy:

- dokonywanie okresowej oceny zagrożeń na potrzeby Raportu o zagrożeniach bezpieczeństwa narodowego,

[102] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 12 ust. 1.

[103] Ibidem, art. 12 ust. 2.

[104] Ibidem, art. 12 ust. 2a.

[105] Ibidem, art. 12 ust. 4.

- opiniowanie projektów planów zarządzania kryzysowego,
- opiniowanie wykazu obiektów, instalacji i urządzeń wchodzących w skład infrastruktury krytycznej w ramach swoich właściwości,
- wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.

Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, starostowie i wójtowie, burmistrzowie, prezydenci miast mogą powoływać ekspertów do udziału w pracach właściwych zespołów zarządzania kryzysowego[106]. Ponadto ministrowie i centralne organy administracji rządowej, do których zakresu działania należą sprawy związane z zapewnieniem bezpieczeństwa narodowego, w tym ochrony ludności lub gospodarczych podstaw bezpieczeństwa państwa, tworzą centra zarządzania kryzysowego[107].

Do zadań centrów zarządzania kryzysowego ministerstw i centralnych organów administracji rządowej należy:

- pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego,
- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej,
- nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,
- współpraca z podmiotami realizującymi monitoring środowiska,
- współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne,
- dokumentowanie działań podejmowanych przez centrum,
- realizacja zadań stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa,
- współdziałanie na wszystkich szczeblach administracji rządowej w zakresie informowania i przekazywania poleceń do wykonania w systemie całodobowym dla jednostek ochrony zdrowia w przypadkach awaryjnych, losowych, jak również zaburzeń funkcjonowania systemu[108].

Obowiązek utworzenia centrum zarządzania kryzysowego uznaje się za spełniony, jeżeli organ utworzył komórkę organizacyjną w urzędzie go obsługującym lub jednostkę organizacyjną jemu podległą lub nadzorowaną, odpowiedzialną za pełnienie całodobowych dyżurów i stwarzającą gwarancję realizacji ustawowych zadań w sferze zarządzania kryzysowego.

Rada Ministrów w drodze rozporządzenia z dnia 15 grudnia 2009 roku *w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania*[109] określiła organy administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposób ich funkcjonowania,

[106] Ibidem, art. 22.

[107] Ibidem, art. 13 ust. 1.

[108] Ibidem, art. 13 ust. 2.

[109] Dz. U. z 2009 r. Nr 226, poz. 1810.

uwzględniając w szczególności warunki techniczne i standardy ich wyposażenia oraz procedury współpracy z Rządowym Centrum Bezpieczeństwa i innymi organami administracji publicznej.

Organy tworzące centrum zarządzania kryzysowego to: Minister Obrony Narodowej, Minister Sprawiedliwości, Minister właściwy do spraw rolnictwa, Minister właściwy do spraw środowiska, Minister właściwy do spraw zagranicznych, Minister właściwy do spraw zdrowia, Komendant Główny Państwowej Straży Pożarnej, Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Wywiadu Wojskowego. Minister kierujący więcej niż jednym działem administracji rządowej tworzy jedno centrum zarządzania kryzysowego. Minister może utworzyć wspólne centrum zarządzania kryzysowego z organami mu podległymi lub przez niego nadzorowanymi[110].

Centrum zarządzania kryzysowego umieszcza się w kompleksie wyodrębnionych pomieszczeń, dostępnych wyłącznie dla osób upoważnionych, w tym pomieszczeń operatorsko-dyspozytorskich, których wyposażenie umożliwia gromadzenie, przetwarzanie i wymianę niezbędnych informacji w zakresie zarządzania kryzysowego, prowadzenie analiz i ocen sytuacji kryzysowych oraz przekazywanie decyzji właściwych organów zarządzania kryzysowego. Centrum realizuje zadania określone w ustawie z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*, w ustawie z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[111], w oparciu o standardy określone w przepisach niniejszej ustawy, w ustawie z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*[112] z zachowaniem wymogów bezpieczeństwa systemów i sieci teleinformatycznych.

W procesie realizacji zadań przez centra zarządzania kryzysowego muszą być zachowane ciągłości działania i wymiany informacji oraz możliwości pracy w przypadku braku zasilania zewnętrznego, uszkodzenia systemów łączności czy wystąpienia innych awarii.

Centrum zarządzania kryzysowego współpracuje z Rządowym Centrum Bezpieczeństwa i innymi organami administracji publicznej w zakresie:

- wzajemnego informowania się o potencjalnych zagrożeniach i możliwościach wystąpienia sytuacji kryzysowej, stratach i środkach, w tym finansowych, niezbędnych do odtworzenia zasobów i infrastruktury krytycznej, pomocy krajowej i międzynarodowej,
- analizowania i oceny sytuacji kryzysowej, w tym prognozowania jej rozwoju,

[110] Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 roku *w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania* (Dz. U. z 2009 r. Nr 226, poz. 1810), § 2 ust.

[111] Dz. U. z 2004 r. Nr 241, poz. 2416, z późn. zm.

[112] Dz. U. z 2010 r. Nr 182, poz. 1228.

- zrealizowanych i planowanych działań podejmowanych przez właściwe organy w sprawie zarządzania kryzysowego w związku z wystąpieniem sytuacji kryzysowej[113].

Współpraca uprawnionych podmiotów jest realizowana przez bieżące przekazywanie informacji i analiz oraz sporządzanie raportów doraźnych i sytuacyjnych przekazywanych przez techniczne środki łączności, z zachowaniem przepisów o ochronie informacji niejawnych.

Centrum zarządzania kryzysowego utworzone przez organy administracji rządowej przekazuje raporty sytuacyjne do Rządowego Centrum Bezpieczeństwa w przypadku wprowadzenia jednego ze stanów nadzwyczajnych lub wystąpienia sytuacji kryzysowej – zgodnie z zapotrzebowaniem, w pozostałych przypadkach – jeden raz dziennie. W sytuacjach kryzysowych wiodącą rolę w zakresie pozyskiwania informacji, ich analizy i dystrybucji pełni centrum zarządzania kryzysowego obsługujące organ, we właściwości którego pozostaje rodzaj zaistniałej sytuacji kryzysowej. Jeżeli wystąpi sytuacja kryzysowa, która wykracza poza właściwość jednego organu lub w przypadku wprowadzenia jednego ze stanów nadzwyczajnych obejmujących obszar dwóch lub więcej województw, wiodącą rolę w zakresie pozyskiwania informacji, ich analizy i dystrybucji przejmuje Rządowe Centrum Bezpieczeństwa, o ile przepisy odrębne nie stanowią inaczej[114].

7.5. Wojewoda

Wśród terenowych organów administracji rządowej szczególne miejsce zajmuje wojewoda, który zgodnie z art. 152 ust. 1 *Konstytucji Rzeczypospolitej Polskiej*[115] jest przedstawicielem Rady Ministrów na obszarze województwa. Jest powoływany i odwoływany przez Prezesa Rady Ministrów. Szczegółowe zadania wojewody są określone w ustawie z dnia 23 stycznia 2009 roku *o wojewodzie i administracji rządowej w województwie*[116].

Zgodnie z art. 3 ust. 1 niniejszego aktu prawnego wojewoda jest:

- przedstawicielem Rady Ministrów w województwie,
- zwierzchnikiem rządowej administracji zespolonej w województwie,
- organem rządowej administracji zespolonej w województwie,

[113] Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 roku *w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania* (Dz. U. z 2009 r. Nr 226, poz. 1810), § 6 ust. 1.

[114] Ibidem, § 7 ust. 3.

[115] Dz. U. z 1997 r. Nr 78, poz. 483.

[116] Dz. U. z 2009 r. Nr 31, poz. 206 z późn. zm.

- organem nadzoru nad działalnością jednostek samorządu terytorialnego i ich związków pod względem legalności,
- organem administracji rządowej w województwie, do którego właściwości należą wszystkie sprawy z zakresu administracji rządowej w województwie niezastrzeżone w odrębnych ustawach do właściwości innych organów tej administracji,
- reprezentantem Skarbu Państwa w zakresie i na zasadach określonych w odrębnych ustawach,
- organem wyższego stopnia w rozumieniu ustawy z dnia 14 czerwca 1960 roku – *Kodeks postępowania administracyjnego*[117].

Zadania i kompetencje wojewody w stanach nadzwyczajnych określają odrębne ustawy[118].

Obok wojewody zadania administracji rządowej w województwie wykonują:

- organy rządowej administracji zespolonej w województwie, w tym kierownicy zespolonych służb, inspekcji i straży,
- organy niezespolonej administracji rządowej,
- jednostki samorządu terytorialnego i ich związki, jeżeli wykonywanie przez nie zadań administracji rządowej wynika z odrębnych ustaw lub zawartego porozumienia,
- starosta, jeżeli wykonywanie przez niego zadań administracji rządowej wynika z odrębnych ustaw,
- inne podmioty, jeżeli wykonywanie przez nie zadań administracji rządowej wynika z odrębnych ustaw[119].

Wojewoda kontroluje pod względem legalności, gospodarności i rzetelności wykonywanie przez organy samorządu terytorialnego zadań z zakresu administracji rządowej, realizowanych przez nie na podstawie ustawy lub porozumienia z organami administracji rządowej. Ponadto jako zwierzchnik rządowej administracji zespolonej w województwie kieruje nią, koordynuje i kontroluje jej działalność, zapewnia warunki skutecznego jej działania, ponosi odpowiedzialność za rezultaty jej działania[120]. Oznacza to, że wojewoda, będąc organem administracji rządowej, kieruje pracą oraz zapewnia warunki działania rządowej administracji zespolonej, która realizuje również zadania związane z zarządzaniem kryzysowym, co wynika z postanowień ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*.

W województwie obok rządowej administracji zespolonej funkcjonują także organy niezespolonej administracji rządowej, którymi są terenowe organy administracji rządowej podporządkowane właściwemu ministrowi lub centralnemu organowi administracji rządowej oraz kierownicy państwowych osób prawnych

[117] Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.

[118] Ustawa z dnia 23 stycznia 2009 roku *o wojewodzie i administracji rządowej w województwie* (Dz. U. z 2009 r. Nr 31, poz. 206 z późn. zm.), art. 3 ust. 3.

[119] Ibidem, art. 2.

[120] Ibidem, art. 51.

i kierownicy innych państwowych jednostek organizacyjnych wykonujących zadania z zakresu administracji rządowej[121]. Organy niezespolonej administracji rządowej na terenie województwa uczestniczą w realizacji zadań związanych z zarządzaniem kryzysowym, których podstawę prawną stanowi ustawa *o zarządzaniu kryzysowym*, a także inne akty prawne.

Tabela 71. Rządowa administracja zespolona w województwie

Rządowa administracja zespolona	
Wojewódzkie zespolone służby, inspekcje i straże	Powiatowe zespolone służby, inspekcje i straże
Komenda Wojewódzka Policji	Komenda Powiatowa Policji
Komenda Wojewódzka Państwowej Straży Pożarnej	Komenda Miejska Policji
Kuratorium Oświaty	Komenda Powiatowa Państwowej Straży Pożarnej
Wojewódzki Inspektorat Farmaceutyczny	Komenda Miejska Państwowej Straży Pożarnej
Wojewódzki Inspektorat Inspekcji Handlowej	Powiatowy Inspektorat Nadzoru Budowlanego
Wojewódzki Inspektorat Jakości Handlowej Artykułów Rolno-Spożywczych	Powiatowa Stacja Sanitarno-Epidemiologiczna
Wojewódzki Inspektorat Nadzoru Budowlanego	Powiatowy Inspektorat Weterynarii
Wojewódzki Inspektorat Ochrony Roślin i Nasiennictwa	Graniczna Stacja Sanitarno-Epidemiologiczna
Wojewódzki Inspektorat Ochrony Środowiska	Wojewódzki Inspektorat Ochrony Środowiska
Wojewódzki Inspektorat Transportu Drogowego	Państwowa Inspekcja Ochrony Roślin i Nasiennictwa. Wojewódzki Inspektorat – Oddział w…
Wojewódzki Urząd Ochrony Zabytków	Urząd Ochrony Zabytków
Wojewódzka Stacja Sanitarno-Epidemiologiczna	Inspektorat Inspekcji Handlowej
Wojewódzki Inspektorat Weterynarii	Inspektorat Farmaceutyczny
	Delegatura Kuratorium Oświaty
	Wojewódzki Inspektorat Transportu Drogowego – Zespół Terenowy

Źródło: Opracowano na podstawie rządowej administracji zespolonej Województwa Małopolskiego

Organy niezespolonej administracji rządowej w województwie stanowią: dowódcy okręgów wojskowych, szefowie wojewódzkich sztabów wojskowych, wojskowi komendanci uzupełnień, dyrektorzy izb celnych i naczelnicy urzędów celnych, dyrektorzy izb skarbowych, naczelnicy urzędów skarbowych, dyrektorzy urzędów kontroli skarbowej, dyrektorzy okręgowych urzędów górniczych i specjalistycznych urzędów górniczych, okręgowych urzędów miar i naczelnicy obwodowych urzędów miar, okręgowych urzędów probierczych i naczelnicy obwodowych urzędów probierczych, dyrektorzy regionalnych zarządów gospodarki wodnej, urzędów morskich, urzędów statystycznych, urzędów żeglugi śródlądowej, graniczni i powiatowi lekarze weterynarii, komendanci oddziałów Straży Granicznej, placówek i dywizjonów Straży Granicznej, okręgowi inspek-

[121] Ibidem, art. 56 ust. 1.

torzy rybołówstwa morskiego, państwowi graniczni inspektorzy sanitarni, regionalni dyrektorzy ochrony środowiska[122].

Organy niezespolonej administracji rządowej działające w województwie są obowiązane do składania wojewodzie rocznych informacji o swojej działalności w województwie do końca każdego roku[123]. W przypadku gdy obszar działalności organu przekracza obszar jednego województwa, informację przekłada się wszystkim właściwym wojewodom.

Wojewoda zgodnie z art. 22 ustawy z dnia 23 stycznia 2009 roku *o wojewodzie i administracji rządowej w województwie* odpowiada za realizację polityki Rady Ministrów w województwie, a w szczególności:

- dostosowuje do miejscowych warunków cele polityki Rady Ministrów oraz w zakresie i na zasadach określonych w odrębnych ustawach koordynuje i kontroluje wykonanie wynikających stąd zadań,
- zapewnia współdziałanie wszystkich organów administracji rządowej i samorządowej działających w województwie i kieruje ich działalnością w zakresie zapobiegania zagrożeniu życia, zdrowia lub mienia oraz zagrożeniom środowiska, bezpieczeństwa państwa i utrzymania porządku publicznego, ochrony praw obywatelskich, a także zapobiegania klęskom żywiołowym i innym nadzwyczajnym zagrożeniom oraz zwalczania i usuwania ich skutków na zasadach określonych w odrębnych ustawach,
- dokonuje oceny stanu zabezpieczenia przeciwpowodziowego województwa, opracowuje plan operacyjny ochrony przed powodzią oraz ogłasza i odwołuje pogotowie i alarm przeciwpowodziowy,
- wykonuje i koordynuje zadania w zakresie obronności i bezpieczeństwa państwa oraz zarządzania kryzysowego, wynikające z odrębnych ustaw,
- przedstawia Radzie Ministrów za pośrednictwem ministra właściwego do spraw administracji publicznej projekty dokumentów rządowych w sprawach dotyczących województwa,
- wykonuje inne zadania określone w odrębnych ustawach oraz ustalone przez Radę Ministrów i Prezesa.

W realizacji ustawowych zadań wojewoda współdziała z właściwymi organami innych państw oraz międzynarodowych organizacji rządowych i pozarządowych na zasadach określonych przez ministra właściwego do spraw zagranicznych[124]. Ma to istotne znaczenie dla województw graniczących z innymi państwami podczas wykonywania zadań związanych z zarządzaniem kryzysowym.

Dla procesu zarządzania kryzysowego na poziomie województwa ma również istotne znaczenie treść art. 26 ust. 1 ustawy *o wojewodzie i administracji rządowej w województwie,* zgodnie z którym wojewoda w zakresie zadań administracji rządowej realizowanych w województwie ma prawo żądać od organów admini-

[122] Ustawa z dnia 23 stycznia 2009 roku *o wojewodzie i administracji rządowej w województwie* (Dz. U. z 2009 r. Nr 31, poz. 206 z późn. zm.), art. 56 ust. 1.

[123] Ibidem, art. 58 ust. 1.

[124] Ibidem, art. 23 ust. ust. 1 pkt 2.

stracji rządowej działających w województwie bieżących informacji i wyjaśnień o ich działalności. Ponadto z uwzględnieniem przepisów o ochronie informacji niejawnych lub innych tajemnic prawnie chronionych wojewoda ma prawo wglądu w tok każdej sprawy prowadzonej w województwie przez organy administracji rządowej, a także przez organy samorządu terytorialnego w zakresie zadań przejętych na podstawie porozumienia lub zadań zleconych[125].

Wojewoda może wydawać polecenia obowiązujące wszystkie organy administracji rządowej działające w województwie, a w sytuacjach nadzwyczajnych obowiązujące również organy samorządu terytorialnego[126]. O wydanych poleceniach wojewoda niezwłocznie informuje właściwego ministra. Sytuacjami nadzwyczajnymi, o których mowa w art. 22 pkt 2 ustawy *o wojewodzie i administracji rządowej w województwie*, są również sytuacje kryzysowe w rozumieniu ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[127].

Na terenie województwa organem właściwym w sprawach zarządzania kryzysowego jest wojewoda[128]. W procesie zarządzania kryzysowego na poziomie województwa uczestniczy również Zarząd województwa, który w ramach swoich kompetencji realizuje zadania m.in. związane z planowaniem cywilnym[129].

Zadania wojewody w sprawach zarządzania kryzysowego:

- kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa,
- realizacja zadań z zakresu planowania cywilnego, w tym: wydawanie starostom zaleceń do powiatowych planów zarządzania kryzysowego, zatwierdzanie powiatowych planów zarządzania kryzysowego, przygotowywanie i przedkładanie do zatwierdzenia ministrowi właściwemu do spraw wewnętrznych wojewódzkiego planu zarządzania kryzysowego, realizacja wytycznych do wojewódzkich planów zarządzania kryzysowego,
- 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, o których mowa w art. 25 ust. 3,
- wykonywanie przedsięwzięć wynikających z dokumentów planistycznych przygotowanych w ramach planowania operacyjnego realizowanego w województwie,
- zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym,

[125] Ibidem, art. 26 ust. 2.

[126] Ibidem, art. 25 ust. 1.

[127] Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.

[128] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.), art. 14 ust. 1.

[129] Ibidem, art. 15.

- 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[130].

Wojewoda zadania w sprawach zarządzania kryzysowego wykonuje we współpracy z właściwymi organami administracji publicznej. Zadania w sprawach zarządzania kryzysowego w urzędzie wojewódzkim realizuje komórka organizacyjna właściwa w przedmiotowej sprawie.

Zadania komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim to: gromadzenie i przetwarzanie danych oraz ocena zagrożeń występujących na obszarze województwa, monitorowanie, analizowanie i prognozowanie rozwoju zagrożeń na obszarze województwa, dostarczanie niezbędnych informacji dotyczących aktualnego stanu bezpieczeństwa dla wojewódzkiego zespołu zarządzania kryzysowego, zespołu zarządzania kryzysowego działającego w urzędzie obsługującym ministra właściwego do spraw wewnętrznych oraz Centrum, współpraca z powiatowymi zespołami zarządzania kryzysowego, zapewnienie funkcjonowania wojewódzkiego zespołu zarządzania kryzysowego, w tym dokumentowanie jego prac, realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa, opracowywanie i aktualizacja wojewódzkiego planu zarządzania kryzysowego, przygotowywanie na podstawie analizy zagrożeń w poszczególnych powiatach zaleceń wojewody do powiatowych planów zarządzania kryzysowego, opiniowanie oraz przedkładanie do zatwierdzenia wojewodzie powiatowych planów zarządzania kryzysowego, opracowywanie i aktualizacja wojewódzkiego planu ochrony infrastruktury krytycznej, planowanie wsparcia innych organów właściwych w sprawach zarządzania kryzysowego, planowanie użycia pododdziałów lub oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań, o których mowa w ustawie o zarządzaniu kryzysowym, planowanie wsparcia przez organy administracji publicznej realizacji zadań Sił Zbrojnych Rzeczypospolitej Polskiej[131].

Organem pomocniczym wojewody w zapewnieniu wykonywania zadań zarządzania kryzysowego jest Wojewódzki Zespół Zarządzania Kryzysowego (WZZK), powoływany przez wojewodę, który określa jego skład, organizację, siedzibę oraz tryb pracy[132].

Do zadań Wojewódzkiego Zespół Zarządzania Kryzysowego należy w szczególności:

- ocena występujących i potencjalnych zagrożeń mogących mieć wpływ na bezpieczeństwo publiczne i prognozowanie tych zagrożeń,
- przygotowywanie propozycji działań i przedstawianie wojewodzie wniosków dotyczących wykonania, zmiany lub zaniechania działań ujętych w wojewódzkim planie zarządzania kryzysowego,

[130] Ibidem, art. 14 ust 2.

[131] Ibidem, art. 14 ust. 6.

[132] Ibidem, art. 14 ust. 7.

- przekazywanie do wiadomości publicznej informacji związanych z zagrożeniami,
- opiniowanie wojewódzkiego planu zarządzania kryzysowego[133].

W skład WZZK wchodzą wojewoda jako przewodniczący, kierownik komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim jako zastępca przewodniczącego, a także inne osoby wskazane przez przewodniczącego w zależności od potrzeb spośród kierowników zespolonych służb, inspekcji i straży wojewódzkich, osób zatrudnionych w urzędzie wojewódzkim lub w jednostkach organizacyjnych służb, inspekcji i straży wojewódzkich, w regionalnych zarządach gospodarki wodnej, wojewódzkich zarządach melioracji i urządzeń wodnych oraz Instytucie Meteorologii i Gospodarki Wodnej. Przewodniczący WZZK może postanowić o włączeniu w skład zespołu Szefa Wojewódzkiego Sztabu Wojskowego lub jego przedstawiciela, a także przedstawiciela samorządu województwa, wyznaczonego przez marszałka województwa oraz inne osoby zaproszone przez przewodniczącego.

Wojewódzki Zespół Zarządzania Kryzysowego składa się z szefa, zastępców oraz grup roboczych o charakterze stałym i czasowym (zob. tabela 72).

Tabela 72. Skład Wojewódzkiego Zespołu Zarządzania Kryzysowego

Wojewódzki Zespół Zarządzania Kryzysowego	
Szef Wojewódzkiego Zespołu Zarządzania Kryzysowego	
Grupy robocze o charakterze stałym	Grupy robocze o charakterze czasowym
Grupa bezpieczeństwa powszechnego i porządku publicznego	Grupa operacji i organizacji działań
Grupa planowania cywilnego	Grupa zabezpieczenia logistycznego
Grupa monitorowania, prognoz i analiz	Grupa opieki zdrowotnej i pomocy socjalno-bytowej

Źródło: J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego*, Kraków 2010, s. 151

WZZK działa na podstawie zatwierdzonych przez wojewodę rocznych planów pracy, planów zarządzania kryzysowego, planów ćwiczeń, protokołów posiedzeń grup roboczych o charakterze stałym i czasowym, raportów bieżących i okresowych, kart zdarzeń w przypadku uruchomienia roboczych grup o charakterze czasowym, raportów odbudowy[134].

Zgodnie z art. 16 ust. 1 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[135] tworzy się Wojewódzkie Centra Zarządzania Kryzysowego (WCZK), których obsługę zapewniają komórki organizacyjne właściwe w sprawach zarządzania kryzysowego w urzędach wojewódzkich. Kolejnym dokumentem, który reguluje funkcjonowanie centrum zarządzania kryzysowego, w tym WCZK, jest rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 roku *w sprawie określenia*

[133] Ibidem, art. 14 ust. 8.

[134] Ziarko J., Walas-Trębacz J., op. cit., s. 150.

[135] Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.

organów administracji rządowej, które tworzą centra zarządzania kryzysowego oraz sposób ich funkcjonowania[136]. Do innych dokumentów należy zaliczyć: zarządzenie wojewody *w sprawie składu i sposobu funkcjonowania Wojewódzkiego Zespołu Zarządzania Kryzysowego* wraz z *Regulaminem Wojewódzkiego Zespołu Zarządzania Kryzysowego*, który stanowi załącznik do zarządzenia oraz zarządzenie wojewody *w sprawie zasad przygotowania i zapewnienia działania Wojewódzkiego Systemu Wczesnego Ostrzegania o zagrożeniach oraz Wojewódzkiego Systemu Wykrywania i Alarmowania*. Zasady organizacji i zadania WCZK wynikają także z zakresów kompetencji poszczególnych osób funkcyjnych, odpowiedzialnych za organizacje zarządzania kryzysowego, w tym głównie wojewody, dyrektora Wydziału Bezpieczeństwa i Zarządzani Kryzysowego i kierownika Centrum Zarządzania Kryzysowego[137].

Wojewódzkie Centrum Zarządzania Kryzysowego pełni rolę:

- punktu systemu wczesnego ostrzegania,
- ośrodka zarządzania kryzysowego koordynującego działania podejmowane w sytuacjach kryzysowych,
- zaplecza koordynacyjno-operacyjnego dla organu, instytucji lub organizacji odpowiedzialnej za podejmowanie działań wspierających, w sytuacji gdy własne zasoby są niewystarczające,
- ośrodka przekazywania informacji oraz pracy zespołów doradczych wspomagających podejmowanie decyzji w sytuacjach zagrożenia, katastrof bądź kryzysów,
- punktu kontaktowego do współpracy międzyresortowej i międzynarodowej, w tym również do koordynacji udzielania i przyjmowania pomocy humanitarnej, technicznej i eksperckiej,
- ośrodka zbierania informacji z systemów monitorowania[138].

Do zadań Wojewódzkiego Centrum Zarządzania Kryzysowego należy:

- pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego,
- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej,
- nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,
- współpraca z podmiotami realizującymi monitoring środowiska,
- współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne,
- dokumentowanie działań podejmowanych przez centrum,
- realizacja zadań stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa,

136 Dz. U. z 2009 r. Nr 226, poz. 1810.

137 G. Sobolewski, *Organizacja i funkcjonowanie Centrum Zarządzania Kryzysowego*, Warszawa 2011, s. 49–50.

138 J. Ziarko, J. Walas-Trębacz, op. cit., s. 152.

- pełnienie całodobowego dyżuru lekarza koordynatora ratownictwa medycznego, o którym mowa w art. 25 ust. 1 pkt 2 i art. 29 ustawy z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym* (Dz. U. z 2006 r. Nr 191, poz. 1410)[139].

Najważniejszym i zarazem najbardziej szczegółowym dokumentem określającym zakres działania dla Centrum Zarządzania Kryzysowego województwa jest Szczegółowy Zakres Działania Wojewódzkiego Centrum Zarządzania Kryzysowego. Niniejszy dokument opracowywany jest przez dyrektora Wydziału Bezpieczeństwa i Zarządzania Kryzysowego w konsultacji specjalistycznej z pozostałymi kierownikami tego wydziału[140].

Szczegółowy zakres działania Wojewódzkiego Centrum Zarządzania Kryzysowego na przykładzie województwa lubuskiego przedstawiono poniżej:

- zapewnianie całodobowych dyżurów dyżurnej służby wojewody:
  - utrzymywanie kontaktu i współdziałanie z instytucjami realizującymi ciągły monitoring środowiska,
  - wymiana informacji ze służbami dyżurnymi administracji zespolonej i niezespolonej oraz innymi służbami i inspekcjami województwa,
  - pozyskiwanie informacji i opracowywanie dobowych meldunków o sytuacji w województwie,
  - przygotowywanie i przekazywanie ostrzeżeń, komunikatów, informacji o ekstremalnych warunkach meteorologicznych i hydrometeorologicznych, w tym syntetycznych informacji dla lokalnych środków masowego przekazu,
  - dostarczanie niezbędnych dla WZZK informacji dotyczących aktualnego stanu bezpieczeństwa,
  - monitorowanie zagrożeń związanych z rozwojem cywilizacyjnym i siłami przyrody oraz alarmowanie ludności w wypadku ich wystąpienia,
  - prowadzenie monitoringu w zakresie występujących zagrożeń i bieżących sytuacji w placówkach służby zdrowia,
  - utrzymywanie stałego kontaktu z dyżurną służbą operacyjną MSW oraz powiatowymi centrami zarządzania kryzysowego,
  - realizacja zadań w ramach stałych dyżurów na potrzeby podwyższania gotowości obronnej państwa,
- programowanie procesu zapobiegania zagrożeniom i ustalanie procedur zarządzania kryzysowego,
- prowadzenie spraw związanych z funkcjonowaniem WZZK, w tym: opracowywanie wniosków dotyczących ustalenia (zmiany) składu WZZK, dokumentów działań i prac zespołu, organizowanie i prowadzenie ćwiczeń i treningów WZZK,

[139] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.), art. 16 ust. 2.

[140] G. Sobolewski, op. cit., s. 56.

- koordynowanie realizacji zadań zarządzania kryzysowego przez organy terenowej administracji rządowej, instytucje, przedsiębiorstwa i organizacje społeczne na terenie województwa,
- koordynowanie przedsięwzięć w zakresie organizacyjnego przygotowania do prowadzenia likwidacji skażeń,
- koordynowanie współdziałania jednostek organizacyjnych administracji rządowej, samorządowej, zespolonej, niezespolonej w przypadku działania podczas klęsk żywiołowych i w czasie innych nadzwyczajnych zagrożeń, w tym: zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu reagowania na potencjalne zagrożenia, w tym opracowywanie i realizowanie treningów z zakresu łączności, ćwiczeń z zakresu zdarzeń radiacyjnych, a także ćwiczeń z zakresu ochrony przeciwpowodziowej,
- koordynowanie współdziałania jednostek organizacyjnych administracji rządowej, samorządowej, zespolonej i niezespolonej w przypadku działania podczas klęsk żywiołowych i w czasie innych nadzwyczajnych zagrożeń,
- realizowanie zadań z zakresu ochrony infrastruktury krytycznej, w tym: gromadzenie i przetwarzanie informacji dotyczących infrastruktury krytycznej, opracowywanie i wdrażanie procedur na wypadek zagrożeń infrastruktury krytycznej, współpraca z właścicielami (posiadaczami) w zakresie ochrony obiektów,
- organizowanie i zapewnienie działania wojewódzkiego systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania, w tym: organizacja i przygotowanie do działania wojewódzkiego ośrodka analizy danych i alarmowania (WOADA), nadzór nad tworzeniem i przygotowaniem do działania wojewódzkich i powiatowych elementów systemu, organizowanie i prowadzenie ćwiczeń i treningów ze szczególnym uwzględnieniem zasad formowania meldunków,
- planowanie, organizowanie i utrzymywanie systemu łączności w sieci zarządzania wojewody, sieci koordynacji ratownictwa i dla potrzeb obrony cywilnej, w tym: planowanie środków finansowych na zakup urządzeń łączności, ich utrzymanie i konserwację, prowadzenie treningów z zakresu powszechnego ostrzegania ludności o zagrożeniach, prowadzenie treningów w odbiorze sygnałów o zagrożeniach w sieci radiowej korpusu obrony powietrznej,
- zbieranie i dokumentowanie dla potrzeb wojewody informacji w zakresie zapobiegania zagrożeniom życia, zdrowia, mienia, środowiska, bezpieczeństwa państwa i utrzymania porządku, a także zapobiegania klęskom żywiołowym,
- prowadzenie spraw związanych z ochroną przeciwpowodziową w województwie i współpraca z regionalnymi zarządami gospodarki wodnej, instytutem meteorologii i gospodarki wodnej oraz wojewódzkim zarządem melioracji i urządzeń wodnych, w tym: monitoring hydrometeorologiczny i zjawisk lodowych, udział w przeglądach stanu technicznego urządzeń melioracyjnych i wałów przeciwpowodziowych,

- współdziałanie w prowadzeniu spraw związanych z usuwaniem skutków powodzi,
- koordynowanie szacowania strat w sytuacjach występowania kryzysów,
- opracowywanie raportów nt. strat, programów odbudowy i nadzorowanie ich wykonania,
- ewidencja i nadzór nad przewozem drogowych i kolejowych ładunków i towarów niebezpiecznych,
- prowadzenie katalogu charakterystyki zasadniczych, szkodliwych substancji chemicznych,
- wykonywanie zadań w zakresie zapewnienia bezpieczeństwa imprez masowych, wynikających z ustawy o bezpieczeństwie imprez masowych[141].

Wojewoda na obszarze województwa na podstawie art. 14 ust. 3 ustawy z dnia 24 sierpnia 2001 roku *o ochronie przeciwpożarowej*[142] określa zadania krajowego systemu ratowniczo-gaśniczego, koordynuje jego działanie i kontroluje wykonywanie wynikających stąd zadań, a w sytuacjach nadzwyczajnych zagrożenia życia, zdrowia lub środowiska kieruje tym systemem. Wojewoda, przy pomocy komendanta wojewódzkiego Państwowej Straży Pożarnej oraz komendantów powiatowych (miejskich) Państwowej Straży Pożarnej na obszarze województwa organizuje oraz koordynuje funkcjonowanie systemu powiadamiania ratunkowego[143]. Wojewoda może w drodze porozumienia powierzyć organizowanie centrów powiadamiania ratunkowego starostom lub prezydentom miast na prawach powiatów. Porozumienie określa prawa i obowiązki stron oraz zasady współfinansowania centrów powiadamiania ratunkowego[144]. Wojewoda może żądać informacji związanych z wykonywaniem zadań w zakresie ochrony przeciwpożarowej na terenie danego województwa, od związku ochotniczych straży pożarnych, ochotniczej straży pożarnej pozostającej poza strukturami związku ochotniczych straży pożarnych, organów wykonawczych gmin i powiatów, instytucji, organizacji, osób prawnych i fizycznych, które utworzyły jednostki ochrony przeciwpożarowej[145].

Stan klęski żywiołowej

Wojewoda posiada również szerokie uprawnienia w przypadku wprowadzenia stanu klęski żywiołowej na obszarze większym niż jeden powiat. Zgodnie z art. 11 ust. 1 ustawy z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej*[146] wojewoda kieruje działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia na obszarze województwa. W takiej sytuacji woje-

141 G. Sobolewski, *Organizacja i funkcjonowanie centrum zarządzania kryzysowego*, Warszawa 2011, s. 56–58.

142 Dz. U. z 2001 r. Nr 147, poz. 1229 z późn. zm.

143 Ustawa z dnia 24 sierpnia 2001 roku *o ochronie przeciwpożarowej* (Dz. U. z 2001 r. Nr 147, poz. 1229 z późn. zm.), art. 14a ust. 8.

144 Ibidem, art. 14c ust. 3.

145 Ibidem, art. 21.

146 Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.

wodzie są podporządkowane organy i jednostki organizacyjne administracji rządowej i samorządu województwa działające na obszarze województwa oraz inne siły i środki wydzielone do jego dyspozycji i skierowane do wykonywania tych działań na obszarze województwa, w tym pododdziały i oddziały Sił Zbrojnych Rzeczypospolitej Polskiej[147].

W czasie stanu klęski żywiołowej, jeżeli użycie innych sił i środków jest niemożliwe lub niewystarczające, Minister Obrony Narodowej może przekazać do dyspozycji wojewody, na którego obszarze działania występuje klęska żywiołowa, pododdziały lub oddziały Sił Zbrojnych Rzeczypospolitej Polskiej, wraz ze skierowaniem ich do wykonywania zadań związanych z zapobieżeniem skutkom klęski żywiołowej lub ich usunięciem[148]. W tym przypadku pododdziały i oddziały Sił Zbrojnych Rzeczypospolitej Polskiej pozostają pod dowództwem przełożonych służbowych i wykonują zadania określone przez wojewodę[149].

Stan wyjątkowy

Ustawa z dnia 21 czerwca 2002 roku *o stanie wyjątkowym* w art. 9 stanowi, że wojewoda w przypadku wprowadzenia stanu wyjątkowego na obszarze lub części obszaru jednego województwa koordynuje i kontroluje funkcjonowanie administracji rządowej i samorządowej w zakresie działań związanych z przywracaniem konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego[150]. Jeżeli organy gminy, powiatu lub samorządu województwa nie wykazują dostatecznej skuteczności w wykonywaniu zadań publicznych lub w realizacji działań wynikających z przepisów o wprowadzeniu stanu wyjątkowego, Prezes Rady Ministrów na wniosek właściwego wojewody może zawiesić te organy do czasu zniesienia stanu wyjątkowego lub na czas określony i ustanowić w ich miejsce zarząd komisaryczny sprawowany przez komisarza rządowego[151]. Komisarza rządowego powołuje i odwołuje Prezes Rady Ministrów na wniosek wojewody, który z dniem powołania przejmuje wykonywanie zadań i kompetencji zawieszonych organów gminy, powiatu lub samorządu województwa. Stan zawieszenia organów gminy, powiatu lub samorządu województwa ustaje z upływem czasu określonego przez Prezesa Rady Ministrów oraz z mocy prawa z dniem zniesienia stanu wyjątkowego.

W czasie stanu wyjątkowego może być odosobniona osoba mająca ukończone 18 lat, w stosunku do której zachodzi uzasadnione podejrzenie, że pozostając na wolności będzie prowadziła działalność zagrażającą konstytucyjnemu ustrojowi państwa, bezpieczeństwu obywateli lub porządkowi publicznemu albo gdy odosobnienie jest niezbędne dla zapobieżenia popełnienia czynu karalnego lub

147 Ustawa z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej* (Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.), art. 11 ust. 2.

148 Ibidem, art. 18 ust. 1.

149 Ibidem, art. 18 ust. 2.

150 Dz. U. 2002 nr 113 poz. 985.

151 Ustawa z dnia 21 czerwca 2002 roku *o stanie wyjątkowym* (Dz. U. 2002 nr 113 poz. 985), art. 12 ust. 1.

uniemożliwienia ucieczki po jego popełnieniu. Nie narusza to immunitetów wynikających z odrębnych przepisów[152]. Odosobniona może być również osoba, która ukończyła 17 lat, jeżeli przeprowadzona uprzednio z nią rozmowa ostrzegawcza okazała się nieskuteczna. Należy podkreślić, że odosobnienie następuje na podstawie decyzji wojewody właściwego ze względu na miejsce pobytu stałego lub czasowego osoby odosobnionej i jest wykonywane przez właściwego komendanta wojewódzkiego Policji, w drodze zatrzymania tej osoby i przymusowego doprowadzenia do ośrodka odosobnienia podległego Ministrowi Sprawiedliwości[153]. Wojewoda, o którym mowa w ust. 3 art. 17 ustawy *o stanie wyjątkowym*, wszczyna postępowanie w sprawach odosobnienia na wniosek właściwych organów prokuratury, Policji, Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej, Żandarmerii Wojskowej lub Służby Kontrwywiadu Wojskowego[154].

Określone w art. 21 ustawy z dnia 21 czerwca 2002 roku *o stanie wyjątkowym*, ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniach, wprowadza się i stosuje w drodze rozporządzeń wydawanych przez właściwego wojewodę w przypadku stosowania ograniczenia wolności i praw człowieka i obywatela w zakresie działalności edukacyjnej, poprzez okresowe zawieszenie zajęć dydaktycznych w szkołach, z wyjątkiem szkół duchownych i seminariów duchownych, z wyłączeniem szkół wyższych, oraz stosowania ograniczeń w zakresie dostępu do towarów konsumpcyjnych, poprzez całkowitą lub częściową reglamentację zaopatrzenia ludności, wolności działalności gospodarczej, poprzez nakazanie okresowego zaniechania prowadzenia działalności gospodarczej określonego rodzaju albo ustanowienie obowiązku uzyskania zezwolenia na rozpoczęcie działalności gospodarczej określonego rodzaju, transportu drogowego, kolejowego i lotniczego oraz w ruchu jednostek pływających, na morskich wodach wewnętrznych i na morzu terytorialnym, a także na śródlądowych drogach wodnych[155].

Stan wojenny

W czasie stanu wojennego wojewoda kieruje realizacją zadań obronnych i obroną cywilną na terenie województwa, co wynika z art. 13 ust. 1 ustawy z dnia 29 sierpnia 2002 roku *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*[156]. Do zadań wojewody w czasie stanu wojennego w szczególności należy:

- ocena zagrożeń,
- wprowadzanie, w zakresie nienależącym do właściwości innych organów, ograniczenia wolności i praw człowieka i obywatela oraz łagodzenie i uchylanie tych ograniczeń,

[152] Ibidem, art. 17 ust. 1.

[153] Ibidem, art. 17 ust. 3.

[154] Ibidem, art. 17 ust. 4.

[155] Ibidem, art. 22 ust. 3 pkt 6.

[156] Dz. U. z 2002 r. Nr 156, poz. 1301.

- występowanie z wnioskami do właściwych organów o wprowadzenie ograniczeń wolności i praw człowieka i obywatela, jak również o ich złagodzenie lub uchylenie,
- określanie zadań wynikających z przepisów stanu wojennego,
- koordynowanie i kontrolowanie działalności organów władzy publicznej, przedsiębiorców oraz innych jednostek organizacyjnych działających na obszarze województwa,
- wyznaczanie zadań i nakazywanie jednostkom samorządu terytorialnego dokonywania określonych wydatków, na zasadach określonych w odrębnych przepisach.

W zakresie powyższych działań wojewodzie są podporządkowane wszystkie jednostki organizacyjne administracji rządowej i samorządowej działające na obszarze województwa oraz inne siły i środki wydzielone do jego dyspozycji i skierowane do wykonywania zadań związanych z obroną państwa i województwa, a także związanych z obroną cywilną.

Jeżeli organy gminy, powiatu lub samorządu województwa nie wykazują dostatecznej skuteczności w wykonywaniu zadań publicznych lub w realizacji działań wynikających z przepisów o wprowadzeniu stanu wojennego, Prezes Rady Ministrów, na wniosek właściwego wojewody, może zawiesić te organy do czasu zniesienia stanu wojennego lub na czas określony i ustanowić w ich miejsce zarząd komisaryczny sprawowany przez komisarza rządowego[157]. Komisarza rządowego powołuje i odwołuje Prezes Rady Ministrów na wniosek wojewody, który z dniem powołania przejmuje wykonywanie zadań i kompetencji zawieszonych organów gminy, powiatu lub samorządu województwa. Stan zawieszenia organów gminy, powiatu lub samorządu województwa ustaje z upływem czasu określonego przez Prezesa Rady Ministrów oraz z mocy prawa z dniem zniesienia stanu wojennego.

Obronność państwa

Ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[158] określa zadania wojewody dotyczące obronności państwa na obszarze województwa. Art. 20 ust. 1 ustawy stanowi, że kierowanie sprawami obronności w województwie należy do wojewody. Do zadań wojewody związanych z kierowaniem w sferze obronności należy:

- określenie szczegółowych kierunków działania dla kierowników zespolonych służb, inspekcji i straży, organów administracji niezespolonej oraz jednostek samorządu terytorialnego w zakresie realizacji zadań obronnych,
- realizacja przedsięwzięć związanych z podwyższaniem gotowości obronnej państwa wykonywanych przez starostów, wójtów lub burmistrzów (prezy-

[157] Ustawa z dnia 29 sierpnia 2002 roku *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2002 r. Nr 156, poz. 1301), art. 14 ust. 1.

[158] T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

dentów miast), przedsiębiorców oraz innych jednostek organizacyjnych i organizacyjnych społecznych mających swoją siedzibę na terenie województwa,
- koordynacja przedsięwzięć niezbędnych dla zabezpieczenia mobilizacji jednostek wojskowych i wykonywania świadczeń na rzecz obrony,
- kierowanie realizacją przedsięwzięć związanych z przygotowaniem stanowisk kierowania dla organów terenowych,
- organizowanie wykorzystania miejscowych sił i środków na potrzeby obronności państwa i obszaru województwa, w tym ochrony ludności oraz dóbr materialnych i kultury przed środkami rażenia, jak również niesienia pomocy poszkodowanym,
- kontrola i ocena wykonania zadań obronnych przez organy, podmioty, jednostki organizacyjne i organizacje, o których mowa w pkt 1 i 2,
- organizacja edukacji społeczeństwa dotyczącej przygotowania obronnego oraz prowadzenia szkolenia i ćwiczeń obronnych[159].

Inne kompetencje wojewody, których podstawę stanowi ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*, określają:
- art. 18 ust. 4 – wojewodowie organizują wykonywanie zadań w ramach powszechnego obowiązku obrony przez urzędy wojewódzkie, podporządkowane i nadzorowane jednostki organizacyjne oraz przedsiębiorców, dla których są organami założycielskimi, a ponadto przez organy samorządu terytorialnego, organizacje społeczne oraz przedsiębiorców niebędących jednostkami organizacyjnymi podporządkowanymi lub nadzorowanymi przez ministrów;
- art. 207a – wojewoda koordynuje na obszarze województwa działalność organów samorządu terytorialnego w zakresie planowania i nakładania obowiązku świadczeń osobistych, w tym:
  - prowadzi zbiorczy wykaz świadczeń osobistych przewidzianych do realizacji na obszarze województwa,
  - planuje wydatki finansowe związane z nakładaniem obowiązku świadczeń osobistych na obszarze województwa,
  - nadzoruje zadania związane z planowaniem, typowaniem i nakładaniem świadczeń osobistych na obszarze województwa,
  - analizuje potrzeby i możliwości realizacji świadczeń osobistych przez organy gminy na obszarze województwa, a w razie potrzeby wskazuje wójta lub burmistrza (prezydenta miasta), który może zrealizować zadania nałożenia tych świadczeń;
- art. 215a – wojewoda koordynuje na obszarze województwa działalność organów samorządu terytorialnego w zakresie planowania i nakładania obowiązku świadczeń rzeczowych, w tym:
  - prowadzi zbiorczy wykaz świadczeń rzeczowych przewidzianych do realizacji na obszarze województwa,

[159] Ibidem, Ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.).

– planuje wydatki finansowe związane z nakładaniem obowiązku świadczeń rzeczowych na obszarze województwa,
– nadzoruje zadania związane z planowaniem, typowaniem i nakładaniem świadczeń rzeczowych na obszarze województwa,
– analizuje potrzeby i możliwości realizacji świadczeń rzeczowych przez organy gminy na obszarze województwa, a w razie potrzeby wskazuje wójta lub burmistrza (prezydenta miasta), który może zrealizować zadania nałożenia tych świadczeń,
– może wystąpić do wójta lub burmistrza (prezydenta miasta) z wnioskiem o przeznaczenie nieruchomości na cele świadczeń rzeczowych w związku z użyciem ich w czasie poboru.

7.6. Starosta

Zgodnie z art. 17 ust. 1 ustawy *o zarządzaniu kryzysowym*[160] na obszarze powiatu organem właściwym w sprawach zarządzania kryzysowego jest starosta jako przewodniczący zarządu powiatu dla zagrożeń występujących na obszarze większym niż obszar jednej gminy wchodzącej w skład powiatu.

Do zadań starosty w sprawach zarządzania kryzysowego należy:

- kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie powiatu,
- realizacja zadań z zakresu planowania cywilnego, w tym:
  a) opracowywanie i przedkładanie wojewodzie do zatwierdzenia powiatowego planu zarządzania kryzysowego,
  b) realizacja zaleceń do powiatowych planów zarządzania kryzysowego,
  c) wydawanie organom gminy zaleceń do gminnego planu zarządzania kryzysowego,
  d) zatwierdzanie gminnego planu zarządzania kryzysowego,
- zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego,
- wykonywanie przedsięwzięć wynikających z planu operacyjnego funkcjonowania powiatów i miast na prawach powiatu,
- zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym,
- współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym,

[160] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

- organizacja i realizacja zadań z zakresu ochrony infrastruktury krytycznej[161].

Powyższe zadania starosta wykonuje przy pomocy powiatowej administracji zespolonej i jednostek organizacyjnych powiatu[162].

Starosta wykonuje zadania zarządzania kryzysowego przy pomocy Powiatowego Zespołu Zarządzania Kryzysowego (PZZK) powołanego przez starostę, który określa jego skład, organizację, siedzibę oraz tryb pracy[163]. Powiatowy Zespół Zarządzania Kryzysowego wykonuje na obszarze powiatu zadania przewidziane dla zespołu wojewódzkiego. W skład PZZK, którego pracami kieruje starosta, wchodzą osoby powołane spośród osób zatrudnionych w starostwie powiatowym, powiatowych jednostkach organizacyjnych lub jednostkach organizacyjnych stanowiących aparat pomocniczy kierowników zespolonych służb, inspekcji i straży powiatowych przedstawicieli społecznych organizacji ratowniczych. W jego skład mogą wchodzić także inne osoby zaproszone przez starostę. Powiatowy Zespół Zarządzania Kryzysowego składa się z szefa, zastępcy, grup roboczych o charakterze stałym i czasowym. Zespół działa na podstawie planu zarządzania kryzysowego zatwierdzonego przez wojewodę. Do innych dokumentów zalicza się: roczne plany pracy, plany ćwiczeń, raporty posiedzeń grup roboczych o charakterze stałym i czasowym, raporty bieżące i okresowe, karty zdarzeń w przypadku uruchomienia grup roboczych o charakterze czasowym, raporty odbudowy.

Tabela 73. Skład Powiatowego Zespołu Zarządzania Kryzysowego

Powiatowy Zespół Zarządzania Kryzysowego	
Szef Powiatowego Zespołu Zarządzania Kryzysowego	
Grupy robocze o charakterze stałym	Grupy robocze o charakterze czasowym
grupa planowania cywilnego grupa monitorowania, prognoz i analiz	grupa operacji i organizacji działań grupa zabezpieczenia logistycznego grupa opieki zdrowotnej i pomocy socjalno-bytowej
Zadania grup roboczych	
Grupa planowania cywilnego – na bieżąco uaktualnia plan zarządzania kryzysowego, opracowuje roczne plany ćwiczeń, prowadzi protokoły z posiedzeń grup roboczych, określa potrzeby w zakresie środków ostrzegania i alarmowania, ustala strefy ostrzegania, opracowuje specjalny system ostrzegania i alarmowania dla osób niepełnosprawnych, ustala ze stacjami telewizyjnymi i radiowymi potrzeby w zakresie ostrzegania i informowania ludności, ustala potrzeby planistyczne z kierownikiem Centrum Zarządzania Kryzysowego, dokonuje oceny zagrożeń,	Grupa operacji i organizacji działań – prowadzi dokumentację odbudowy zawierającą opisy i analizy skutków zaistniałego zdarzenia oraz propozycję odbudowy, sporządza szczegółowy wykaz strat w infrastrukturze oraz potencjale ratowniczym, prowadzi projekt harmonogramu likwidacji strat i odbudowy, współdziała z grupą planowania cywilnego, utrzymuje bazę danych o zasobach, zapewnia przygotowanie niezbędnych porozumień z przedsiębiorstwami (instytucjami) i sąsiednimi gminami w zakresie wykorzystania ich zasobów w sytuacjach kryzysowych.

[161] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 17 ust. 2.

[162] Ibidem, art. 17 ust. 3.

[163] Ibidem, art. 17 ust. 4.

w fazie przygotowania podejmuje działania planistyczne dotyczące sposobu zarządzania na czas wystąpienia klęsk żywiołowych.	
Grupa monitorowania, prognoz i analiz – prowadzi karty zdarzeń zawierające chronologiczny opis zdarzeń i wdrożonych działań, a także analizuje decyzje podejmowane w celu likwidacji zagrożeń, pomocy poszkodowanym i ograniczenia strat oraz zarządzania informacjami.	Grupa zabezpieczenia logistycznego: – opracowuje sposób udzielania pomocy i zabezpieczeń logistycznych w czasie zarządzania kryzysowego, utrzymuje kontakty z lokalnymi mediami, współdziała z Powiatowym Centrum Zarządzania Kryzysowego w zakresie opracowania informacji dla ludności i przedstawia je staroście/wójtowi do akceptacji, opracowuje i rozpowszechnia informacje dotyczące realizacji fazy odbudowy, prowadzi opiekę nad zwierzętami.
	Grupa opieki zdrowotnej i pomocy socjalno-bytowej: – przedstawia sposób udzielania pomocy socjalno-bytowej poszkodowanym, opracowuje i rozpowszechnia informacje na temat prowadzenia opieki zdrowotnej, typuje organizacje publiczne i prywatne posiadające odpowiednie wyposażenie i urządzenia z przeznaczeniem do udzielania pomocy poszkodowanym, przedstawia wstępny bilans potrzeb finansowych w zakresie udzielania przez nich pomocy poszkodowanym, podejmuje działania polegające na dostarczaniu pomocy poszkodowanym, zahamowaniu występujących zagrożeń oraz ograniczaniu strat i zniszczeń.
W skład grup roboczych mogą wchodzić również specjaliści, eksperci, osoby zaufania społecznego, a także przedstawiciele organów administracji publicznej lub społecznych organizacji ratowniczych.	

Źródło: Opracowano na podstawie J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego*, Kraków 2010, s. 159 i 161

Na poziomie powiatu tworzy się Powiatowe Centra Zarządzania Kryzysowego (PCZK)[164], które zapewniają przepływ informacji na potrzeby zarządzania kryzysowego oraz wykonują odpowiednio zadania przewidziane dla Wojewódzkich Centrów Zarządzania Kryzysowego[165].

Do zakresu zadań Powiatowego Centrum Zarządzania Kryzysowego należy przede wszystkim ocenianie występujących i potencjalnych zagrożeń mających wpływ na bezpieczeństwo publiczne oraz prognozowanie tych zagrożeń, a także przygotowanie propozycji działań i przedstawianie staroście wniosków dotyczących wykonania, zmiany lub zaniechania działań ujętych w powiatowym planie zarządzania kryzysowego. Centrum jest właściwe także w sprawach przekazywania do wiadomości publicznej informacji związanych z zagrożeniami. Ono również opiniuje powiatowe plany zarządzania kryzysowego oraz plany ochrony infrastruktury krytycznej. PCZK

[164] Ibidem, art. 18 ust. 1.

[165] Ibidem, art. 16 ust. 2.

jest odpowiedzialne za pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego oraz współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej. Centra te sprawują również nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności. Zajmują się współpracą z podmiotami realizującymi monitoring środowiska. Współpracują z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne oraz dokumentują podejmowane przez siebie działania. Centrum jest odpowiedzialne za zapewnienie stałego dyżuru na potrzeby podwyższonej gotowości obronnej państwa oraz pełnienie całodobowego dyżuru lekarza koordynatora ratownictwa medycznego[166].

Organizację, siedzibę oraz tryb pracy Powiatowego Centrum Zarządzania Kryzysowego, w tym sposób całodobowego alarmowania członków zespołu zarządzania kryzysowego oraz sposób zapewnienia całodobowego obiegu informacji w sytuacjach kryzysowych, określa starosta[167]. W miejscowościach będących jednocześnie siedzibami powiatów i miast na prawach powiatu na podstawie porozumienia zawartego między tymi jednostkami samorządu terytorialnego może być tworzone wspólne centrum zarządzania kryzysowego obejmujące zasięgiem działania obszar obu jednostek samorządu terytorialnego[168].

Starosta, poza zadaniami wykonywanymi w ramach samorządu terytorialnego, jest organem administracji rządowej, co wynika z art. 2 pkt 5 ustawy z dnia 23 stycznia 2009 roku *o wojewodzie i administracji rządowej w województwie*[169]. Zgodnie z art. 35 ust. 1 ustawy z dnia 5 czerwca 1998 roku *o samorządzie powiatowym*[170], starosta organizuje pracę zarządu powiatu i starostwa powiatowego, kieruje bieżącymi sprawami powiatu oraz reprezentuje powiat na zewnątrz. Opracowuje plan operacyjny ochrony przed powodzią oraz ogłasza i odwołuje pogotowie i alarm przeciwpowodziowy. W sprawach nie cierpiących zwłoki, związanych z zagrożeniem interesu publicznego, zagrażających bezpośrednio zdrowiu i życiu oraz w sprawach mogących spowodować znaczne straty materialne starosta podejmuje niezbędne czynności należące do właściwości zarządu powiatu. Jest również zwierzchnikiem powiatowych służb, inspekcji i straży, i tak: jest kierownikiem starostwa powiatowego oraz zwierzchnikiem służbowym pracowników starostwa i kierowników jednostek organizacyjnych powiatu oraz zwierzchnikiem powiatowych służb, inspekcji i straży[171], sprawując zwierzchnictwo powołuje i odwołuje kierowników tych jednostek, w uzgodnieniu z wojewodą, a także wykonuje wobec nich czynności w sprawach z zakresu prawa pracy, jeżeli przepisy szczególne nie stanowią inaczej,

166 J. Ziarko, J. Walas-Trębacz, op. cit., s. 161.

167 Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 18 ust. 3.

168 Ibidem, art. 18 ust. 4.

169 Dz. U. z 2009 r. Nr 31, poz. 206.

170 Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.

171 Ustawa z dnia 5 czerwca 1998 roku *o samorządzie powiatowym* (Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.), art. 35 ust. 2 i 3.

zatwierdza programy ich działania, uzgadnia wspólne działanie tych jednostek na obszarze powiatu, w sytuacjach szczególnych kieruje wspólnymi działaniami tych jednostek, zleca w uzasadnionych przypadkach przeprowadzenie kontroli.

Narzędziem pozwalającym na współpracę starosty z wójtami (burmistrzami, prezydentami miast) jest możliwość udzielania sobie wzajemnej pomocy. Zgodnie z art. 7a ustawy *o samorządzie powiatowym*[172], powiaty, związki i stowarzyszenia powiatów mogą sobie wzajemnie bądź innym jednostkom samorządu terytorialnego udzielać pomocy, w tym pomocy finansowej.

Stan klęski żywiołowej

Ustawa z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej*, w art. 10 ust. 1 stanowi, że w czasie stanu klęski żywiołowej właściwy miejscowo starosta kieruje działaniami prowadzonymi na obszarze powiatu w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia[173]. W związku z tym starosta może wydawać polecenia wiążące wójtom (burmistrzom, prezydentom miast niebędących miastami na prawach powiatu), kierownikom jednostek organizacyjnych utworzonych przez powiat, kierownikom powiatowych służb, inspekcji i straży, kierownikom jednostek ochrony przeciwpożarowej działających na obszarze powiatu oraz kierownikom jednostek organizacyjnych czasowo przekazanych przez właściwe organy do jego dyspozycji i skierowanych do wykonywania zadań na obszarze powiatu[174]. Ponadto starosta może występować do kierowników innych jednostek organizacyjnych działających na obszarze powiatu z wnioskami o wykonanie czynności niezbędnych w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia. W razie odmowy wykonania tych czynności lub ich niewłaściwego wykonywania starosta niezwłocznie zawiadamia organ, któremu podlega kierownik lub który sprawuje nadzór nad nim. W razie niezdolności do kierowania lub niewłaściwego kierowania działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia wojewoda może zawiesić uprawnienia starosty oraz wyznaczyć pełnomocnika do kierowania tymi działaniami[175].

Starosta albo pełnomocnik wykonuje czynności kierownicze na właściwym dla siebie obszarze wobec podmiotów takich jak wójt (burmistrz, prezydent miasta), może wydawać polecenia wiążące organom jednostek pomocniczych, kierownikom jednostek organizacyjnych utworzonych przez gminę, kierownikom jednostek ochrony przeciwpożarowej działających na obszarze gminy oraz kierownikom jednostek organizacyjnych czasowo przekazanych przez właściwe organy do jego dyspozycji i skierowanych do wykonywania zadań na obszarze gminy.

[172] Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.

[173] Dz. U. z 2002 r. Nr 62, poz. 558.

[174] Ustawa z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej* (Dz. U. z 2002 nr 62 poz. 558), art. 10 ust. 2.

[175] Ibidem, art. 10 ust. 5.

Na podstawie art. 14 ust. 3 ustawy z dnia 24 sierpnia 1991 roku o *Państwowej Straży Pożarnej*[176] w przypadku bezpośredniego zagrożenia bezpieczeństwa wspólnoty samorządowej, w szczególności życia lub zdrowia, starosta może wydać komendantowi powiatowemu (miejskiemu) Państwowej Straży Pożarnej polecenie podjęcia działań w zakresie właściwości Państwowej Straży Pożarnej, zmierzających do usunięcia tego zagrożenia. Na polecenie starosty (prezydenta miasta) komendant powiatowy (miejski) Państwowej Straży Pożarnej obowiązany jest składać w każdym czasie informacje o stanie bezpieczeństwa powiatu (miasta na prawach powiatu) w zakresie ochrony przeciwpożarowej[177]. Starosta na obszarze powiatu określa zadania krajowego systemu ratowniczo-gaśniczego, koordynuje jego funkcjonowanie i kontroluje wykonywanie wynikających stąd zadań, a w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia lub środowiska kieruje tym systemem[178]. Starosta może żądać informacji związanych z wykonywaniem zadań w zakresie ochrony przeciwpożarowej na terenie danego powiatu od: związku ochotniczych straży pożarnych, ochotniczej straży pożarnej pozostającej poza strukturami związku ochotniczych straży pożarnych, organów wykonawczych gmin i powiatów, instytucji, organizacji, osób prawnych i fizycznych, które utworzyły jednostki ochrony przeciwpożarowej informacji związanych z wykonywaniem ich zadań w zakresie ochrony przeciwpożarowej na terenie danego powiatu[179].

7.7. Wójt (burmistrz, prezydent miasta)

Na terenie gminy organem właściwym w sprawach zarządzania kryzysowego jest wójt, burmistrz, prezydent miasta[180]. Należy mieć świadomość tego, że wójt (burmistrz, prezydent miasta) nie realizuje zadań organu administracji rządowej. Jego kompetencje wynikają z ustawy z dnia 8 marca 1990 roku *o samorządzie gminnym*[181]. Zgodnie z jej postanowieniami wójt wykonuje zadania przy pomocy urzędu gminy, posiada uprawnienia zwierzchnika służbowego zarówno w stosunku do pracowników gminy, jak i gminnych jednostek organizacyjnych. Dla tego poziomu zarządzania kryzysowego ustawa z dnia 26 kwietnia 2007 roku

[176] T. j.: Dz. U. 2009 Nr 12, poz. 68 z późn. zm.

[177] Ustawa *o Państwowej Straży Pożarne* (T. j.: Dz. U. 2009 Nr 12, poz. 68 z późn. zm.), art. 14 ust. 1.

[178] Ibidem, art. 14 ust. 3.

[179] Ustawa z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej* (T. j.: Dz. U. 2009 Nr 178, poz. 1380 z późn. zm.), art. 21.

[180] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 19 ust. 1.

[181] Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.

o zarządzaniu kryzysowym przewiduje komórki urzędu właściwe w przedmiotowej sprawie.

Do zadań wójta (burmistrza, prezydenta miasta) w sprawach zarządzania kryzysowego należy:

- kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie gminy,
- realizacja zadań z zakresu planowania cywilnego, w tym realizacja zaleceń do gminnego planu zarządzania kryzysowego, opracowywanie i przedkładanie staroście do zatwierdzenia gminnego planu zarządzania kryzysowego,
- zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego,
- wykonywanie przedsięwzięć wynikających z planu operacyjnego funkcjonowania gmin i gmin o statusie miasta,
- zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym,
- współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym,
- organizacja i realizacja zadań z zakresu ochrony infrastruktury krytycznej[182].

Powyższe zadania wójt (burmistrz, prezydent miasta) wykonuje przy pomocy komórki organizacyjnej urzędu gminy (miasta) właściwej w sprawach zarządzania kryzysowego.

Organem pomocniczym wójta (burmistrza, prezydenta miasta) w zapewnieniu wykonywania zadań zarządzania kryzysowego jest Gminny Zespół Zarządzania Kryzysowego (GZZK) powoływany przez wójta (burmistrza, prezydenta miasta), który określa jego skład, organizację, siedzibę oraz tryb pracy[183]. GZZK wykonuje na obszarze gminy zadania przewidziane dla zespołu wojewódzkiego. Pracami zespołu kieruje wójt (burmistrz, prezydent miasta), a w jego składzie znajdują się osoby powołane spośród osób zatrudnionych w urzędzie gminy, gminnych jednostkach organizacyjnych lub jednostkach pomocniczych, pracowników zespolonych służb, inspekcji i straży, skierowanych przez przełożonych do wykonywania zadań w tym zespole na wniosek wójta (burmistrza, prezydenta miasta), przedstawicieli społecznych organizacji ratowniczych[184].

Gminny Zespół Zarządzania Kryzysowego składa się z szefa, zastępcy i grup roboczych zarówno o charakterze stałym, jak i czasowym. Szefa gminnego zespołu i jego zastępców wyznacza wójt spośród zatrudnionych w urzędzie gminy, gminnych jednostkach organizacyjnych lub jednostkach pomocniczych, które posiadają właściwe przygotowanie specjalistyczne przydatne w procesie zarządzania kryzysowego. Grupy robocze o charakterze stałym i czasowym również

[182] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 19 ust. 2.

[183] Ibidem, art. 19 ust. 4.

[184] J. Ziarko, J. Walas-Trębacz, op. cit., s. 162.

tworzone są na bazie osób zatrudnionych w urzędzie gminy, gminnych jednostkach organizacyjnych lub jednostkach pomocniczych.

Gminny Zespół Zarządzania Kryzysowego działa na podstawie planu zarządzania kryzysowego zatwierdzonego przez starostę. Ponadto dokumentami działań i pracy zespołu są roczne plany pracy, plany ćwiczeń, protokoły posiedzeń grup roboczych o charakterze stałym i czasowym, raporty bieżące i okresowe, karty zdarzeń w przypadku uruchomienia grup roboczych o charakterze czasowym, raporty odbudowy.

Tabela 74. Skład Gminnego Zespołu Zarządzania Kryzysowego

<table>
<tr><td colspan="2">Gminny Zespół Zarządzania Kryzysowego</td></tr>
<tr><td colspan="2">Szef Gminnego Zespołu Zarządzania Kryzysowego</td></tr>
<tr><td>Grupy robocze o charakterze stałym
– grupa planowania cywilnego
– grupa monitorowania, prognoz i analiz</td><td>Grupy robocze o charakterze czasowym
– grupa operacji i organizacji działań
– grupa zabezpieczenia logistycznego
– grupa opieki zdrowotnej i pomocy socjalno-bytowej</td></tr>
<tr><td>Ich zadania są tożsame z zadaniami grup roboczych o charakterze stałym i są wykonywane przez PZZK. Siedziba GZZK powinna być w odpowiedni sposób oznakowana, a jego lokalizacja podana do publicznej wiadomości w sposób umożliwiający poinformowanie wszystkich mieszkańców gminy.</td><td>Ich zadania są tożsame z zadaniami grup roboczych o charakterze stałym i są wykonywane przez PZZK.</td></tr>
<tr><td colspan="2">W skład grup roboczych mogą wchodzić również specjaliści, eksperci, osoby zaufania społecznego, a także przedstawiciele organów administracji publicznej lub społecznych organizacji ratowniczych.</td></tr>
</table>

Źródło: Opracowano na podstawie J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego*, Kraków 2010, s. 163 i 164

W skład Gminnego Zespołu Zarządzania Kryzysowego mogą wchodzić inne osoby zaproszone przez wójta (burmistrza, prezydenta miasta).

Wójt (burmistrz, prezydent miasta) zapewnia na obszarze gminy (miasta):

- całodobowe alarmowanie członków gminnego zespołu zarządzania kryzysowego, a w sytuacjach kryzysowych całodobowy dyżur w celu zapewnienia przepływu informacji oraz dokumentowania prowadzonych czynności,
- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej;
- funkcjonowanie systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,
- współpracę z podmiotami realizującymi monitoring środowiska,
- współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne,

- realizację zadań stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa[185].

W celu realizacji zadań związanych z zarządzaniem kryzysowym wójt (burmistrz, prezydent miasta) może tworzyć Gminne (Miejskie) Centra Zarządzania Kryzysowego (GCZK/MCZK)[186].

Do zadań Gminnego Centrum Zarządzania Kryzysowego należy w szczególności:

- pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego,
- współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej,
- nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,
- współpraca z podmiotami realizującymi monitoring środowiska,
- zapewnienie stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa,
- dokonywanie wstępnej oceny sytuacji oraz powiadamianie wójta (burmistrza, prezydenta miasta),
- przygotowywanie ostrzeżeń, komunikatów dla środków masowego przekazu,
- przekazywanie informacji o zdarzeniach do Powiatowego Centrum Zarządzania Kryzysowego.

W sytuacjach kryzysowych do Gminnego Centrum Zarządzania Kryzysowego należy:

- współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne,
- dokumentowanie działań podejmowanych przez centrum,
- śledzenie przebiegu prowadzonych przez władze samorządowe akcji ratunkowych o małym zasięgu,
- zbieranie informacji o rozwoju sytuacji, przetwarzanie ich i przekazywanie do poszczególnych grup roboczych,
- przekazywanie zadań sposobów współdziałania zgodnie z decyzją szefa grupy do wykonawców (instytucji), przedsiębiorstw wydzielających siły i środki ratownicze i materiałowe,
- nadzór nad przebiegiem realizacji zadań przez poszczególnych wykonawców.

Art. 31b ust. 1 ustawy z dnia 8 marca 1990 roku *o samorządzie gminnym*[187] stanowi, że jeżeli w inny sposób nie można usunąć bezpośredniego niebezpieczeństwa dla życia ludzi lub dla mienia, wójt może zarządzić ewakuację z obszarów bezpośrednio zagrożonych. Takiego uprawnienia nie posiada starosta, natomiast

[185] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 20 ust. 1.

[186] Ibidem, art. 20 ust. 2.

[187] T. j.: Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.

wojewoda w ograniczonym zakresie. Ustawa nie zawęża tych kompetencji ani do rodzaju zagrożenia, ani do jego wielkości[188].

Ustawa w art. 14 ust. 3 ustawy z dnia 24 sierpnia 1991 roku *o Państwowej Straży Pożarnej*[189] określa, że w przypadku bezpośredniego zagrożenia bezpieczeństwa wspólnoty samorządowej, w szczególności życia lub zdrowia, wójt (burmistrz, prezydent miasta) może wydać komendantowi powiatowemu (miejskiemu) Państwowej Straży Pożarnej polecenie podjęcia działań w zakresie właściwości Państwowej Straży Pożarnej, zmierzających do usunięcia tego zagrożenia. Na polecenie prezydenta miasta komendant miejski Państwowej Straży Pożarnej obowiązany jest składać w każdym czasie informacje o stanie bezpieczeństwa powiatu (miasta na prawach powiatu) w zakresie ochrony przeciwpożarowej, co wynika z postanowienia art. 14 ust. 1 tejże ustawy.

Zgodnie z art. 14 ust. 5 ustawy z dnia z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej*[190], wójt (burmistrz, prezydent miasta) koordynuje funkcjonowanie krajowego systemu ratowniczo-gaśniczego na obszarze gminy w zakresie ustalonym przez wojewodę. Zadanie to może być wykonywane przy pomocy komendanta gminnego ochrony przeciwpożarowej, jeżeli komendant taki został zatrudniony przez wójta (burmistrza, prezydenta miasta), albo przy pomocy komendanta gminnego związku ochotniczych straży pożarnych.

W procesie zarządzania kryzysowego należy zwrócić uwagę na rolę wójta i samorządu gminnego. Szczególny charakter zadań realizowanych na tym szczeblu wynika z faktu, że zadaniem własnym samorządu gminnego jest udzielanie pomocy społecznej. Pomoc ta udzielana jest m.in. w przypadku zdarzeń losowych oraz klęski żywiołowej i ekologicznej, co wynika z treści art. 7 pkt 14 i 15 ustawy z dnia 12 marca 2004 roku *o pomocy społecznej*[191]. W jej zakres wchodzi m.in. udzielanie schronienia, zapewnienie posiłku oraz niezbędnego ubrania osobom tego pozbawionym, przyznawanie i wypłacanie zasiłków okresowych, zasiłków celowych, zasiłków celowych na pokrycie wydatków powstałych w wyniku zdarzeń losowych[192] (przyznawanie i wypłacanie zasiłków celowych na pokrycie wydatków związanych z klęską żywiołową lub ekologiczną jest zadaniem zleconym z zakresu administracji rządowej realizowanym przez gminę, co oznacza, że podlega refundacji z budżetu państwa).

Obronność państwa

Kompetencje wójta lub burmistrza (prezydenta miasta) w sferze obronności państwa zostały określone w ustawie z dnia 21 listopada 1967 roku *o powszechnym*

[188] W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Warszawa 2010, s. 132.

[189] Dz. U. z 1991 r. Nr 88, poz. 400 z późn. zm.

[190] T. j.: Dz. U. z 2009 r. Nr 178, poz. 1380 z późn. zm.

[191] Dz. U. z 2004 r. Nr 64, poz. 593 z późn. zm.

[192] Ustawa z dnia 12 marca 2004 roku *o pomocy społecznej* (T. j.: Dz. U. z 2009 r. Nr 175, poz. 1362 z późn. zm.), art. 17 ust. 1.

obowiązku obrony Rzeczypospolitej Polskiej[193], i tak wójt lub burmistrz (prezydent miasta):

- art. 202 ust. 1 – nakłada, w drodze decyzji administracyjnej, obowiązek świadczeń osobistych na wniosek wojskowego komendanta uzupełnień, kierownika jednostki organizacyjnej stanowiącej bazę formowania specjalnie tworzonej jednostki zmilitaryzowanej, kierownika jednostki organizacyjnej wykonującej zadania na potrzeby obrony państwa, o której mowa w art. 208 ust. 2 albo właściwego organu obrony cywilnej;
- art. 203 ust. 1 – wydaje w czasie pokoju decyzję administracyjną o przeznaczeniu osoby do wykonania świadczeń osobistych, w tym planowanych do wykonania w razie ogłoszenia mobilizacji i w czasie wojny, na wniosek organów i jednostek organizacyjnych, o których mowa w art. 202 ust. 1;
- art. 210 ust. 1 – wydaje decyzję administracyjną o przeznaczeniu nieruchomości lub rzeczy ruchomej na cele świadczeń rzeczowych, w tym planowanych do wykonania w razie ogłoszenia mobilizacji i w czasie wojny, na wniosek organów i kierowników jednostek organizacyjnych, o których mowa w art. 202 ust. 1;
- art. 219. ust. 1 – nakłada obowiązek świadczeń osobistych i rzeczowych na podstawie doraźnie zgłoszonych wniosków przez organy i kierowników jednostek organizacyjnych, o których mowa w art. 202 ust. 1, a także dowódców jednostek wojskowych;
- art. 219 ust. 3 – w szczególnych sytuacjach może nakładać obowiązek świadczeń osobistych lub rzeczowych również w drodze obwieszczeń lub w inny sposób.

[193] T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

ROZDZIAŁ 8

Podsystem wykonawczy

8.1. Istota podsystemu wykonawczego

W systemie zarządzania kryzysowego obok podsystemów informacyjnego, planowania i kierowania najważniejszy jest podsystem wykonawczy, którego podstawowym zadaniem jest niesienie natychmiastowej pomocy dla osób poszkodowanych i oczekujących na wsparcie w sytuacji nieszczęścia, zagrożenia, awarii, katastrofy czy kataklizmu. Podsystem wykonawczy to szeroko rozumiane ratownictwo, ewakuacja i pomoc w różnych sytuacjach życiowych, społecznych i technicznych. Jest elementem solidarności społecznej i nawet w wymiarze międzynarodowym jest zawsze aktem szlachetnej woli, często ogromnego zrywu, który przebiega ponad wszelkimi podziałami i różnicami społecznymi, politycznymi czy obyczajowymi[1].

Podsystem wykonawczy obejmuje działania ratownicze, przez które należy rozumieć każdą czynność podjętą w celu ochrony życia, zdrowia i mienia lub środowiska, a także likwidacji przyczyn powstawania pożaru, wystąpienia klęski żywiołowej lub innego miejscowego zdarzenia[2]. Wielu specjalistów uważa jednak, że działania ratownicze to każda czynność podjęta w celu likwidacji nagłego zagrożenia życia, zdrowia, mienia i środowiska realizowana w trybie pilnym. Przy współczesnych zagrożeniach, ich skali i dynamice ta definicja przy dużym stopniu uogólnienia jest najbardziej trafna. Do działań ratowniczych zalicza się:
- informowanie, alarmowanie i ostrzeganie ludności o zagrożeniach,
- ratownictwo,
- pomoc humanitarną i socjalną,
- opiekę psychologiczną,
- opiekę medyczną,
- zapewnienie niezbędnych warunków życia (przetrwania),
- zapewnienie porządku publicznego i przestrzeganie prawa,
- inne elementy i zadania w sferze bezpieczeństwa[3].

[1] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 259.

[2] D. Marczyński, *Dokąd zmierza Państwowa Straż Pożarna*, „Przegląd Pożarniczy" 2008, nr 1, s. 34.

[3] Ibidem, s. 34.

Stosując kryterium zakresu i wielkości działań ratowniczych, można wyróżnić trzy poziomy organizacyjne działań ratowniczych:

- akcję ratowniczą, polegającą na udzielaniu pomocy doraźnej w krótkim czasie i przy małym nakładzie sił,
- działania ratownicze, a więc każdą czynność podjętą w celu ochrony zdrowia, życia, mienia i środowiska, wystąpienia klęski żywiołowej lub innego miejscowego zagrożenia,
- operację ratowniczą, czyli kompleks kolejno po sobie następujących i jednoczesnych działań ratowniczych, wymagających użycia różnorodnych, specjalistycznych sił i środków w myśl jednolitego planu działania.

Z powyższego wynika, że podsystem wykonawczy w systemie zarządzania kryzysowego stanowi złożony i mobilny organizm składający się z ludzi, sprzętu technicznego i specjalistycznego wyposażenia dodatkowego, który wspierany jest przez komórki kierownicze i przygotowane rezerwy i zapasy materiałowe.

Omawiany podsystem wykonuje najbardziej ciężką i odpowiedzialną i z reguły niebezpieczną pracę fizyczną bezpośrednio w terenie, na miejscu zdarzenia, katastrofy czy innego nieszczęścia. Jednostki ratownicze działają najczęściej w ekstremalnych warunkach zagrożenia dla własnego bezpieczeństwa, dlatego współczesna technika i technologia stwarza im coraz doskonalsze systemy i procedury fizycznego bezpieczeństwa służb ratowniczych[4].

Podsystem wykonawczy powinien stanowić jednolity i spójny układ, skupiający powiązane ze sobą różne podmioty ratownicze, tak aby można było podjąć skutecznie każde działanie ratownicze. Ideą przewodnią tego podsystemu jest stworzenie takiego zespołu działań, w którym człowiek bez względu na rodzaj i wielkość zagrożenia daje jeden sygnał, a system ma tak funkcjonować, aby zagrożeniu udzielić wszechstronnej, skutecznej pomocy[5].

Na podsystem wykonawczy zarządzania kryzysowego składają się cztery podstawowe komponenty:

- ratownictwo medyczne, którego podstawowym zadaniem jest ratowanie życia i zdrowia ludzi oraz udzielanie im wszelkiej, niezbędnej pomocy lekarskiej i sanitarnej czy nawet humanitarnej, także w zakresie szybkiej i sprawnej ewakuacji z miejsc zagrożonych do rejonów bardziej bezpiecznych;
- ratownictwo techniczne obejmujące szeroką gamę rozmaitych procedur, czynności i usług wykonywanych mniej lub bardziej rutynowo podczas różnych akcji antykryzysowych; z reguły jest to torowanie bezpiecznej drogi do ofiar i poszkodowanych, usuwanie różnych konstrukcji i obiektów z miejsca zdarzenia oraz likwidowanie różnorodnych skutków awarii i katastrof, głównie technicznych, w miejscu zdarzenia;
- ratownictwo ekologiczne, to szczególna forma ratowania ocalałych i zagrożonych zasobów przyrodniczych i ograniczania negatywnych następstw wszel-

[4] K. Ficoń, op. cit., s. 259.

[5] Z. Socha, *Krajowy system ratowniczo-gaśniczy w przyszłym powszechnym systemie ratowniczym,* „Towarzystwo Wiedzy Obronnej" 1999, nr 1, s. 33.

kich zagrożeń w stosunku do środowiska naturalnego w celu przywrócenia tych miejsc do stanu pierwotnego;

- ratownictwo specjalne dotyczące wysoce specjalistycznych, często nietypowych form działań ratowniczych podejmowanych w stosunku do ludzi, środowiska cywilizacyjnego i przyrodniczego; głównym jego celem jest eliminowanie skutków i następstw szczególnie groźnych zagrożeń czy katastrof klimatycznych, technicznych bądź terrorystycznych; bardzo groźne rezultaty mogą wystąpić na przykład w przypadku skażenia chemicznego, bakteriologicznego, promieniotwórczego czy sanitarnego generujących niebezpieczeństwo wystąpienia nieodwracalnych skutków i następstw społecznych, cywilizacyjnych lub przyrodniczych[6].

Na rzecz podsystemu wykonawczego pracują wszystkie inne struktury wchodzące w skład systemu zarządzania kryzysowego. Powinny one zabezpieczać przede wszystkim jego potrzeby: ludzkie, informacyjne, materiałowo-techniczne, finansowe, a także wspierać poprzez odpowiednie regulacje prawne, koordynować wysiłki wszystkich podmiotów zaangażowanych w zarządzanie kryzysowe.

Podstawę podsystemu wykonawczego w zarządzaniu kryzysowym stanowi poziom gminny, powiatowy, wojewódzki i krajowy, co ma ścisły związek z podziałem administracyjnym państwa. Należy podkreślić, że im niższy poziom administracji publicznej, tym większy zakres zarządzania kryzysowego. Z kolei przy wyższym szczeblu administracji funkcja zarządzania zastępowana jest przez funkcję koordynacji działań i udzielania wsparcia.

Skuteczność podsystemu wykonawczego: Krajowego Systemu Ratowniczo-Gaśniczego, Państwowego Ratownictwa Medycznego, Obrony Cywilnej, Sił Zbrojnych RP, Policji, Żandarmerii Wojskowej, Straży Granicznej, Biura Ochrony Rządu, służb specjalnych innych służb, straży i instytucji w dużym stopniu zależy od sprawności systemu powiadamiania alarmowego oraz systemu powiadamiania ratunkowego.

Wymienione systemy to zorganizowany układ wzajemnie powiązanych elementów organizacyjno-technicznych przeznaczonych do gromadzenia informacji, ich przetwarzania i udostępniania dla uprawnionych odbiorców (podmioty kierujące na wszystkich poziomach zarządzania kryzysowego w państwie, podmioty wykonawcze, społeczeństwo itp.). Systemy te realizują swoje zadania w czasie rzeczywistym pod kątem natychmiastowego uruchomienia czynności określonych w obowiązujących przepisach. Należy zaznaczyć, że niezawodność, sprawność i czułość systemów stanowi warunek podjęcia jakiejkolwiek akcji czy działań przez uprawnione podmioty[7]. Systemy te inicjują reakcję całego systemu zarządzania kryzysowego i warunkują jego funkcjonalną aktywność, co oznacza, że stanowią jego odpowiedni bodziec informacyjny. Rola tych systemów jest kluczowa z punktu widzenia bezpieczeństwa państwa i obywateli. Jeżeli systemy te nie rozpoznają i nie zidentyfikują na czas zaistniałego zagrożenia i nie uruchomią

[6] K. Ficoń, op. cit., s. 259 i 261.

[7] Ibidem, s. 251.

odpowiedniego alarmu, to dane zagrożenie może stanowić poważne niebezpieczeństwo często z trudnymi do przewidzenia następstwami.

Podsystem wykonawczy zarządzania kryzysowego powinien integrować wszystkie dziedziny ratownictwa, organy władzy i podmioty ratownicze w ramach jednego celu, jakim jest służenie poszkodowanym, szczególnie w obliczu zdarzeń złożonych, masowych czy katastrof.

Budowanie podsystemu wykonawczego nie jest przedsięwzięciem jednorazowym, ale procesem, któremu muszą towarzyszyć czytelne regulacje prawne, gdzie powinny być zawarte zarówno zobowiązania, jak i uprawnienia poszczególnych organów władzy rządowej i samorządowej, a siły i środki ratownicze będące w dyspozycji różnych podmiotów powinny być tak przygotowane, aby ich działanie było optymalne i zapewniało możliwie ciągłość ratowania[8].

8.2. System powiadamiania alarmowego

Polska z uwagi na swoje położenie geograficzne, przynależność do organizacji międzynarodowych (np. Sojusz Północnoatlantycki i Unia Europejska), a także na międzynarodowe zaangażowanie m.in. w zwalczanie terroryzmu narażona jest na zagrożenia zarówno o charakterze militarnym jak i pozamilitarnym. W związku z tym w ocenie swojego bezpieczeństwa powinna uwzględniać polityczno-militarne wyzwania czasu pokoju, zagrożenia kryzysowe i wojenne. Dlatego tak ważna jest współpraca cywilno-wojskowa obejmująca współdziałanie organów cywilnych i wojskowych tak w czasie pokoju jak i stanach zagrożenia.

> Dotychczasowe zdolności wojska w zakresie wspierania władz cywilnych i społeczeństwa należy rozwijać i wzbogacać o nowe drogą ewolucji, przyjmując strategię długoterminowego przystosowania wojska do zadań wsparcia. Potrzebna jest też upubliczniona cywilno-wojskowa dyskusja o roli, misjach i zadaniach Sił Zbrojnych RP w ochronie kraju, ludności i infrastruktury w czasie pokoju przed współczesnymi zagrożeniami niewojennymi[9].

Sprawne działanie i przetrwanie w warunkach kryzysu i wojny wymaga przygotowania społeczeństwa w czasie pokoju. Działalność tego charakteru ma na celu ochronę ludności, zakładów pracy, urządzeń użyteczności publicznej, dóbr kultury, ratowanie i udzielanie pomocy poszkodowanym.

W celu zminimalizowania czynnika zaskoczenia ze strony zagrożeń znanych i tych, które mogą pojawić się w następstwie postępujących przeobrażeń cywilizacyjnych, stworzony został system składający się ze służb pełniących dyżury na

[8] D. Marczyński, op. cit., s. 33.

[9] K. Gąsiorek, W. Kitler, *Wojskowe wsparcie władz cywilnych i społeczeństwa*, Warszawa 2005, s. 169.

różnych szczeblach władz cywilnych i wojskowych. Ich podstawowe zadanie to wykrywanie zagrożeń, ostrzeganie i alarmowanie.

Wykrywanie zagrożeń, ostrzeganie[10] i alarmowanie[11], to przede wszystkim:

- uzyskiwanie informacji o zbliżaniu się lub stwierdzenie faktu zaistnienia na określonym terenie niebezpieczeństwa dla zdrowia i życia ludności, związanego z zastosowaniem środka rażenia, wystąpienia klęski żywiołowej, katastrof naturalnych, awarii obiektów technicznych, skażeń i zakażeń lub innych zdarzeń, których skutki mogą wpłynąć negatywnie na poziom bezpieczeństwa ludności;
- określanie rodzaju, miejsca, skali i skutków zaistniałych zagrożeń oraz oznaczanie stref niebezpiecznych;
- ostrzeganie i alarmowanie ludności o zbliżającym się niebezpieczeństwie oraz informowanie o zalecanych zasadach postępowania (zachowania się) obywateli w określonej sytuacji[12].

Podmioty wchodzące w skład systemu wczesnego ostrzegania:

- Rządowe Centrum Bezpieczeństwa (RCB),
- Centrum Zarządzania Kryzysowego wymienione w rozporządzeniu Rady Ministrów z dnia 15 grudnia 2009 roku *w sprawie określenia organów administracji rządowej, które tworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania,*
- Centrum Antyterrorystyczne,
- Wojewódzkie Centrum Zarządzania Kryzysowego,
- Powiatowe Centrum Zarządzania Kryzysowego,
- Gminne (Miejskie) Centrum Zarządzania Kryzysowego,
- jednostki organizacyjne przyjmujące zgłoszenia na numery alarmowe oraz prowadzące działania interwencyjne w sytuacjach wystąpienia zagrożeń, nadzorowane odpowiednio przez Ministra Spraw Wewnętrznych,
- Centrum Powiadamiania Ratunkowego przyjmujące zgłoszenia pod numer telefonu alarmowego 112,
- państwowe i regionalne Zarządy Gospodarki Wodnej,
- jednostki nadzoru epidemiologicznego i kontroli chorób zakaźnych – nadzorowane przez Państwową Inspekcję Sanitarną,
- jednostki państwowej służby hydrologiczno-meteorologicznej,

[10] „Ostrzeganie, to przekazywanie komunikatów i informacji uprzedzających o prawdopodobnych zagrożeniach i zalecających podjęcie działań zabezpieczających i ochronnych oraz instruujące o sposobach wykonywania tych działań" – rozporządzenie Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach* (Dz. U. z 2006 r. Nr 191, poz. 1415), § 2 pkt 6.

[11] „Alarmowanie, działania mające na celu natychmiastowe przekazanie sygnału do właściwych terytorialnie władz, służb i ludności na danym terenie, informującego o zagrożeniu skażeniami, skażeniu lub o innym zagrożeniu wymagającym natychmiastowego działania" – ibidem, § 2 pkt 2.

[12] J. Zwoliński, *Koncepcja wykrywania zagrożeń, ostrzegania i alarmowania*, ock.gov.pl [pobrano 10.03.2012].

- jednostki monitorowania chorób odzwierzęcych i odzwierzęcych czynników chorobotwórczych oraz badań kontroli zakażeń zwierząt – nadzorowane przez Państwowego Inspektora Weterynarii,
- jednostki monitoringu środowiska – nadzorowane przez Państwowego Inspektora Ochrony Środowiska,
- nadawcy programów radiowych i telewizyjnych,
- operatorzy telekomunikacji,
- jednostki organizacyjne zobowiązane w myśl przepisów o ochronie środowiska do sporządzania planów ratowniczych,
- Aeroklub,
- Państwowa Agencja Atomistyki.

Dla systemu alarmowania ważne są wytyczne Szefa Obrony Cywilnej Kraju z dnia 17 grudnia 2010 roku *w sprawie ogólnych zasad przygotowania i zapewnienia działania systemu wykrywania i alarmowania (SWA) oraz systemu wczesnego ostrzegania o zagrożeniach (SWO) w województwach, powiatach i gminach*. Niniejsze wytyczne określają ogólne zasady tworzenia wojewódzkich SWA i SWO, ich współdziałanie z elementami składowymi funkcjonującymi w powiatach i gminach oraz koordynację w realizacji zadań z zakresu alarmowania i ostrzegania ludności o zagrożeniach z Krajowym Systemem Wykrywania Skażeń i Alarmowania oraz systemem powszechnego ostrzegania wojsk i ludności cywilnej o zagrożeniu uderzeniami z powietrza.

Uwzględniając powyższe wytyczne, szefowie obrony cywilnej województw opracowują wytyczne w sprawie ogólnych zasad przygotowania i zapewnienia działania SWA oraz SWO w województwach i przesyłają je do powiatów. Z kolei szefowie obrony cywilnej powiatów opracowują wytyczne w sprawie ogólnych zasad przygotowania i zapewnienia działania SWA oraz SWO w powiatach i przesyłają je do gmin, uwzględniając występowanie charakterystycznych zagrożeń dla terenu, odpowiednio województwa, powiatu i gminy. System wykrywania i alarmowania (SWA) oraz system wczesnego ostrzegania o zagrożeniach (SWO) organizują szefowie obrony cywilnej województw. SWA oraz SWO w województwie powinny zapewnić możliwości skutecznego reagowania na zagrożenia występujące na jego terenie oraz zdolność do efektywnej współpracy wszystkich jednostek organizacyjnych wchodzących w ich skład we wszelkich rodzajach zagrożeń.

Powszechne ostrzeganie i alarmowanie ludności o zagrożeniach obejmuje funkcjonujące w czasie pokoju SWO i systemy wykrywania skażeń i alarmowania wchodzące w skład Krajowego Systemu Wykrywania Skażeń i Alarmowania oraz system powszechnego ostrzegania wojsk i ludności cywilnej o zagrożeniu uderzeniami z powietrza, funkcjonujące lub uruchamiane i rozwijane w celu zapobieżenia skutkom katastrofy naturalnej, awarii technicznej lub działań terrorystycznych, w przypadku wprowadzenia stanu nadzwyczajnego, w szczególności stanu klęski żywiołowej, a także w przypadku przeprowadzania ćwiczeń i treningów.

System wczesnego ostrzegania o zagrożeniach stanowią jednostki organizacyjne, służby, inspekcje posiadające całodobową służbę dyżurną lub osoby dyżurne wyposażone w środki łączności, a także służby dyżurne lub osoby dyżurne w zakładach, obiektach oraz na terenie instalacji stanowiących potencjalne zagrożenie dla ludności i środowiska w przypadku ich uszkodzenia lub awarii. Podmioty te działają w sposób zapewniający jednolitość funkcjonowania, zdolność do efektywnej współpracy we wszystkich rodzajach zagrożeń oraz są zobowiązane na podstawie powszechnie obowiązującego prawa lub aktów prawa miejscowego stanowionego przez właściwy organ administracji publicznej lub samorządowej do wzajemnej wymiany informacji uzyskanych w czasie własnej działalności statutowej.

Do podstawowych celów systemu wczesnego ostrzegania o zagrożeniach należy:

- ostrzeganie i alarmowanie ludności o zbliżającym się niebezpieczeństwie na tyle wcześnie, aby było możliwe podjęcie działań ograniczających potencjalne straty,
- informowanie o zalecanych zasadach postępowania (zachowania się) obywateli w sytuacji określonego zagrożenia.

System wykrywania i alarmowania obejmuje systemy funkcjonujące lub uruchamiane i rozwijane w ramach jednolitego Krajowego Systemu Wykrywania Skażeń i Alarmowania w celu zapobiegania skutkom katastrofy naturalnej, awarii technicznej lub działaniom terrorystycznym, mogącym spowodować wystąpienie skażeń chemicznych, biologicznych lub promieniotwórczych, a także w przypadku wprowadzenia stanu nadzwyczajnego, stanu klęski żywiołowej oraz w przypadku przeprowadzania ćwiczeń i treningów. Z kolei system powszechnego ostrzegania wojsk i ludności cywilnej o zagrożeniu uderzeniami z powietrza obejmuje zespół sił i środków przeznaczonych do terminowego uprzedzenia jednostek wojskowych Sił Zbrojnych Rzeczypospolitej Polskiej oraz organów administracji publicznej w celu zminimalizowania ich skutków. Włączenie jednostek i instytucji do SWA i SWO na podstawie wydanych przez wojewodów, starostów i wójtów zarządzeń w sprawie tworzenia i funkcjonowania na danym terenie SWA i SWO nie zmienia ich służbowego podporządkowania i zadań.

Do wykonywania czynności związanych z wykrywaniem zagrożeń, przekazywaniem informacji o ich zaistnieniu, opracowywaniem danych oraz ostrzeganiem i alarmowaniem są zobowiązane:

- jednostki organizacyjne obrony cywilnej/systemu ochrony ludności, odpowiednio do nałożonych na nie zadań,
- zakłady, obiekty, które w przypadku awarii mogą stanowić źródło zagrożenia dla ludności i środowiska,
- jednostki organizacyjne, których statutowa działalność przewiduje wykonywanie takich czynności w zakresie ustalonym przez właściwe terenowo organy administracji publicznej/organy obrony cywilnej.

Podmioty te mają obowiązek przekazywania informacji o stwierdzonym zagrożeniu właściwym terenowym organom administracji publicznej.

Wytyczne Szefa Obrony Cywilnej Kraju określają ogólne zasady ostrzegania i alarmowania:

- rodzaje alarmów, treść komunikatów ostrzegawczych, sygnały alarmowe i sposób ich ogłaszania określa załącznik do rozporządzenia Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach*[13],
- doprecyzowuje się sposób ogłoszenia alarmu o skażeniach akustycznym systemem alarmowym w przywołanym w ust. 1 rozporządzenia – o przerywany modulowany dźwięk syreny nadawany przez czas 3 (trzech) minut,
- za upowszechnienie sygnału wśród ludności czyni się odpowiedzialnym szefa obrony cywilnej województwa,
- przekazywanie informacji o zagrożeniach komunikatów ostrzegawczych i sygnałów alarmowych odbywa się w pierwszej kolejności za pośrednictwem dostępnych środków łączności oraz środków masowego przekazu,
- dopuszcza się przekazywanie ostrzeżeń i alarmowanie ludności w sposób zwyczajowo przyjęty na danym terenie,
- organy administracji publicznej oraz inni dysponenci systemów lub środków łączności zapewniają możliwość ich wykorzystania na potrzeby przekazywania informacji o zagrożeniach i alarmowania,
- gromadzenie informacji o zagrożeniach oraz ostrzeganie organizuje są na szczeblu zakładów, miast, gmin, powiatów oraz województw.

Za stworzenie warunków do działania oraz przygotowanie do działania systemów wykrywania skażeń i alarmowania odpowiadają organy administracji publicznej wymienione w rozporządzeniu Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach* w zakresie określonym w tym rozporządzeniu. Natomiast zasady i tryb przygotowania podmiotów do powszechnego ostrzegania wojsk oraz ludności cywilnej o zagrożeniu uderzeniami z powietrza określa *instrukcja funkcjonowania systemu powszechnego ostrzegania wojsk oraz ludności cywilnej o zagrożeniu uderzeniami z powietrza* wprowadzona decyzją Nr 2864/ON Ministra Obrony Narodowej z dnia 13 sierpnia 2009 roku[14].

Powszechne ostrzeganie o zagrożeniu uderzeniami z powietrza służy w szczególności:

- wprowadzaniu przedsięwzięć dotyczących właściwego obiegu informacji o zagrożeniu uderzeniami z powietrza,
- monitorowaniu, wykrywaniu i rozpoznaniu rejonu uderzenia, umożliwiających wykonanie w danym rejonie niezbędnych przedsięwzięć eliminujących lub zmniejszających skutki ewentualnych uderzeń.

[13] Dz. U. z 2006 r. Nr 191, poz. 1415.

[14] Dz. Urz. MON z 2009 r. Nr 15, poz. 153, instrukcja została opublikowana w Wojskowym Wydawnictwie Specjalistycznym, sygn. WLOP 41212009.

Problematyka wykrywania skażeń i organów uprawnionych do realizowania zadań tego charakteru została uregulowana w drodze rozporządzenia Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach*[15]. Rozporządzenie określa organizację i warunki przygotowania oraz sposób funkcjonowania systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania o skażeniach na terytorium Rzeczypospolitej Polskiej oraz właściwość organów w tych sprawach dla zapewnienia zewnętrznego bezpieczeństwa państwa i sprawowania ogólnego kierownictwa w dziedzinie obronności kraju.

W przypadku wprowadzenia stanu nadzwyczajnego, w szczególności stanu klęski żywiołowej, w celu zapobieżenia skutkom katastrofy naturalnej, awarii technicznej lub działań terrorystycznych, mogących spowodować wystąpienie skażeń chemicznych, biologicznych lub promieniotwórczych, a także w przypadku przeprowadzania ćwiczeń i treningów, systemy funkcjonują lub są uruchamiane i rozwijane w ramach jednolitego krajowego systemu wykrywania skażeń i alarmowania[16]. Nadzór i funkcje koordynacyjne nad funkcjonowaniem krajowego systemu sprawuje Minister Obrony Narodowej przy pomocy centrum dyspozycyjnego, którego rolę pełni Centralny Ośrodek Analizy Skażeń Sił Zbrojnych. Minister Obrony Narodowej we współpracy z ministrami właściwymi do spraw wewnętrznych, zdrowia, gospodarki morskiej, środowiska oraz gospodarki wodnej opracowuje, aktualizuje i uruchamia stosowne plany i procedury współdziałania jednostek organizacyjnych podległych i nadzorowanych przez tych ministrów w realizacji zadań w ramach krajowego systemu.

Skład krajowego systemu wykrywania skażeń i alarmowania[17]

1. System wykrywania i alarmowania o skażeniach:
   a) system wykrywania skażeń Sił Zbrojnych Rzeczypospolitej Polskiej – nadzorowany przez Ministra Obrony Narodowej,
   b) sieci i systemy nadzoru epidemiologicznego i kontroli chorób zakaźnych w kraju oraz krajowe punkty kontaktowe dla międzynarodowych systemów nadzoru nad zagrożeniami zdrowia lub życia dużych grup ludności – nadzorowane przez ministra właściwego do spraw zdrowia,

[15] Dz. U. z 2006 r. Nr 191, poz. 1415.

[16] „System wykrywania skażeń (SWS) jest to zorganizowany układ elementów powiązanych wzajemnymi relacjami organizacyjno-technicznymi, przeznaczonych do zdobywania, gromadzenia, przetwarzania i analizowania informacji o uderzeniach BMR oraz powstałych w ich wyniku skażeniach, a także o skażeniach środkami promieniotwórczymi, biologicznymi i chemicznymi spowodowanych zdarzeniami innymi niż uderzenie bronią masowego rażenia oraz o potencjalnych źródłach tych zagrożeń", K. Budyn, *Funkcjonowanie systemu wykrywania skażeń w Siłach Zbrojnych RP. Systemy wykrywania skażeń w wybranych państwach Sojuszu Północnoatlantyckiego oraz w państwach sąsiadujących z Polską*, [w:] *Kurs podstawowy dla specjalistów Krajowego Systemu Wykrywania Skażeń*, praca zbiorowa, Warszawa 2005, s. 13.

[17] Rozporządzenie Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach* (Dz. U. z 2006 r. Nr 191, poz. 1415).

c) system stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych, których działania koordynuje Prezes Państwowej Agencji Atomistyki,
d) nadzorowane przez wojewodów wojewódzkie systemy wykrywania i alarmowania oraz wojewódzkie systemy wczesnego ostrzegania o zagrożeniach, o których mowa w § 3 pkt 6 rozporządzenia Rady Ministrów z dnia 25 czerwca 2002 r. *w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin*[18],
e) system wykrywania i alarmowania określony w Krajowym Planie Zwalczania Zagrożeń i Zanieczyszczeń Środowiska Morskiego opracowany na podstawie rozporządzenia Rady Ministrów z dnia 3 grudnia 2002 r. *w sprawie organizacji i sposobu zwalczania zagrożeń i zanieczyszczeń na morzu*[19].

2. Organy i jednostki organizacyjne dokonujące analizy i oceny sytuacji skażeń oraz dokonujące opracowywania, ogłaszania i wprowadzania działań interwencyjnych, obejmujące:
   a) jednostki organizacyjne prowadzące działania interwencyjne w sytuacji wystąpienia skażeń – nadzorowane przez ministra właściwego do spraw wewnętrznych,
   b) formacje obrony cywilnej przeznaczone do monitoringu, wykrywania i rozpoznania skażeń oraz alarmowania o skażeniach – tworzone i nadzorowane przez podmioty wymienione w art. 138 ust. 3 i 4 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej,
   c) inne organy i jednostki organizacyjne dokonujące obserwacji, pomiarów i powiadamiania o skażeniach na terenie kraju włączone do systemów, o których mowa w § 1, na podstawie umów i porozumień – zgodnie z tymi porozumieniami.

Systemy obserwacji, pomiarów, analiz, prognozowania i powiadamiania o skażeniach na terytorium Rzeczypospolitej Polskiej powinny działać w sposób zapewniający jednolitość funkcjonowania oraz wzajemną interoperacyjność, w szczególności przez stosowanie:

- takich samych metodyk i procedur obserwacji i pomiarów skażeń,
- takich samych formatów meldunków i informacji o skażeniach,
- identycznych procedur przekazywania meldunków i informacji o skażeniach,
- jednolitego schematu obiegu i wymiany informacji o skażeniach.

Jednolitość i interoperacyjność funkcjonowania systemów wchodzących w skład krajowego systemu zapewniają organy, którym te systemy podlegają lub które je nadzorują. Koordynację w zakresie jednolitości i interoperacyjności funkcjonowania systemów wchodzących w skład krajowego systemu zapewnia Minister Obrony Narodowej.

[18] Dz. U. z 2002 r. Nr 96, poz. 850.

[19] Dz. U. z 2002 r. Nr 239, poz. 2026.

Zadania systemów wchodzących w skład krajowego systemu wykrywania skażeń i alarmowania to:

- realizacja sojuszniczych zobowiązań Rzeczypospolitej Polskiej oraz zobowiązań wynikających z ratyfikowanych porozumień międzynarodowych w zakresie obserwacji, pomiarów, analiz prognozowania i powiadamiania o skażeniach na terytorium Rzeczypospolitej Polskiej,
- wprowadzanie przedsięwzięć dotyczących ochrony przed skażeniami i związanych z tym stanów alarmowych zgodnie z obowiązującymi procedurami,
- monitorowanie, wykrywanie i rozpoznanie skażeń, umożliwiające natychmiastowe stwierdzenie wzrostu poziomu skażeń w oparciu o standardy i normy krajowe,
- ostrzeganie i alarmowanie ludności lub Sił Zbrojnych Rzeczypospolitej Polskiej o skażeniach,
- opracowywanie ocen eksperckich stanu zagrożenia skażeniami i przygotowywanie zaleceń postępowania ochronnego,
- doradztwo specjalistyczne w zakresie metodyki ograniczania zasięgu i skutków oddziaływania skażeń,
- uruchamianie systemów wykrywania i alarmowania o skażeniach ludności lub Sił Zbrojnych Rzeczypospolitej Polskiej oraz uruchamianie działań interwencyjnych[20].

Przygotowanie systemów wchodzących w skład krajowego systemu wykrywania skażeń i alarmowania do realizacji zadań wykonują w zakresie swoich kompetencji organy i jednostki organizacyjne w stosunku do podlegających im systemów, w szczególności przez:

- działania planistyczne, organizacyjne i szkoleniowe dotyczące:
  a) aktualizacji danych o potencjalnych źródłach zagrożenia skażeniami,
  b) doskonalenia procedur podnoszenia gotowości tych systemów – stosownie do poziomu zagrożenia skażeniami,
  c) aktualizacji planów rozmieszczenia punktów wykonujących pomiary skażeń w zależności od stanu gotowości systemu i danych wynikających z analizy potencjalnych zagrożeń,
  d) doskonalenia sposobów i procedur współdziałania w zakresie monitoringu, prognozowania, rozpoznania i oceny sytuacji skażeń,
  e) sposobów organizacji i utrzymania łączności i wymiany informacji o skażeniach w warunkach pokoju i w stanach nadzwyczajnych,
  f) tworzenia warunków do preferencyjnego przekazu informacji w systemach wykrywania i alarmowania,
  g) doskonalenia procedur uruchamiania i wdrażania zadań,
- organizowanie szkoleń i doskonalenie osób funkcyjnych w zakresie: wiedzy o właściwościach źródeł skażeń, systemów ochrony przed skażeniami, sposobów i metodyki dokonywania pomiarów skażeń, oceny sytuacji skażeń,

[20] Rozporządzenie Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach* (Dz. U. z 2006 r. Nr 191, poz. 1415).

usuwania skutków skażeń oraz prawnych rozwiązań dotyczących zagadnień ochrony przed skażeniami,

- organizowanie oraz prowadzenie ćwiczeń i treningów sprawdzających i doskonalących funkcjonowanie tych systemów i procedur oraz udział w takich ćwiczeniach i treningach.

Podmioty, o których mowa w rozporządzeniu Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach*, w przypadku wykrycia zagrożenia skażeniami lub stwierdzenia wystąpienia skażeń przez podległe im systemy niezwłocznie powiadamiają właściwy terytorialnie dla miejsca takiego zdarzenia organ administracji publicznej.

Sygnały alarmowe i komunikaty ostrzegawcze powszechnie obowiązujące na terytorium Rzeczypospolitej Polskiej określa załącznik do omawianego rozporządzenia. Sygnały alarmowe i komunikaty ostrzegawcze mogą być wykorzystane, z zastrzeżeniem wyłącznie na potrzeby systemów, o których mowa jest w rozporządzeniu i w sytuacji rzeczywistego zagrożenia. Decyzje o wprowadzeniu lub ogłoszeniu sygnału lub komunikatu ostrzegawczego, a także o ich odwołaniu podejmuje właściwy terytorialnie organ administracji publicznej. Z kolei wykorzystanie sygnałów alarmowych i komunikatów ostrzegawczych w ramach treningów i ćwiczeń systemów wykrywania i alarmowania możliwe jest po ogłoszeniu tego faktu przez właściwe terytorialnie organy administracji publicznej z 24-godzinnym wyprzedzeniem w środkach masowego przekazu i w sposób zwyczajowo przyjęty na danym terenie. Ogłoszenie zawiera informacje o zakresie i zasięgu terytorialnym prowadzonego treningu lub ćwiczenia.

Minister Obrony Narodowej, minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw wewnętrznych we współpracy z wojewodami prowadzą ogólnokrajowe treningi uruchamiania systemów i ich pracy w ramach krajowego systemu nie rzadziej niż raz w roku i ogólnokrajowe ćwiczenia systemów nie rzadziej niż raz na trzy lata. Przygotowania i przeprowadzanie treningów i ćwiczeń finansuje się odpowiednio z budżetów: Ministra Obrony Narodowej, ministra właściwego do spraw gospodarki morskiej oraz ministra właściwego do spraw wewnętrznych i wojewodów. Program treningów i ćwiczeń ogólnokrajowych ma w szczególności na celu sprawdzenie i doskonalenie przygotowania systemów do działania w ramach krajowego systemu w sytuacji pokoju i stanach nadzwyczajnych, a także sprawdzenie przygotowania do realizacji zadań związanych z zarządzaniem kryzysowym oraz weryfikację i doskonalenie procedur i mechanizmów funkcjonowania systemów.

Należy podkreślić, że funkcjonowanie systemu, organu lub jednostki organizacyjnej w krajowym systemie nie zmienia ich podległości organizacyjnej, w szczególności podległości systemu Sił Zbrojnych Rzeczypospolitej Polskiej oraz systemów określonych w przepisach dotyczących prawa atomowego, administracji rządowej w województwie, chorób zakaźnych i zakażeń oraz zapobiegania zanieczyszczaniu morza przez statki.

Do zadań systemu wykrywania skażeń w Siłach Zbrojnych Rzeczypospolitej Polskiej należy:

- monitorowanie skażeń w wyznaczonych obiektach, rejonach i strefach,
- wykrywanie uderzeń bronią jądrową, chemiczną i biologiczną oraz uwolnień środków promieniotwórczych, chemicznych lub biologicznych spowodowanych zdarzeniami typu ROTA[21],
- prognozowanie sytuacji skażeń promieniotwórczych, chemicznych i biologicznych powstałych w wyniku BMR[22] lub zdarzeń typu ROTA,
- ostrzeganie i alarmowanie jednostek wojskowych o skażeniach powstałych w wyniku uderzeń BMR lub zdarzeniach typu ROTA,
- wykrywanie w terenie skażeń promieniotwórczych, chemicznych i biologicznych,
- prowadzenie rozpoznania w celu określenia charakteru i stopnia skażenia promieniotwórczego, chemicznego i biologicznego i oraz określenie obszarów niebezpiecznych,
- oznakowanie rejonów skażonych i niebezpiecznych,
- odtworzenie i ocena rzeczywistych sytuacji promieniotwórczych, chemicznych i biologicznych na podstawie danych z rozpoznania,
- ocena sytuacji promieniotwórczych, chemicznych i biologicznych oraz ich wpływ na działanie wojsk,
- meldowanie przełożonym wniosków i propozycji działań wypływających z oceny sytuacji uderzeń BMR oraz uwolnień środków promieniotwórczych, chemicznych oraz biologicznych spowodowanych zdarzeniami typu ROTA,
- organizowanie pobierania, przygotowanie do transportu oraz analiza próbek skażonego powietrza, gleby, wody i innych materiałów,
- prowadzenie baz danych o uderzeniach BMR, skażeniach oraz substancjach niebezpiecznych stwarzających zagrożenia dla SZ RP,
- określenie warunków atmosferycznych w przyziemnej warstwie powietrza oraz zbieranie i opracowywanie danych o średnich wiatrach w górnych warstwach atmosfery,
- wymiana informacji pomiędzy jednostkami wojskowymi, siłami NATO i układem pozamilitarnym o uderzeniach BMR, a także uwolnieniach środków promieniotwórczych, chemicznych i biologicznych spowodowanych zdarzeniami typu ROTA oraz powstałych w ich wyniku skażeniach,
- udział w wykonywaniu zadań związanych z ochroną środowiska naturalnego, zgodnie z obowiązującymi dokumentami normatywnymi[23].

Strukturę organizacyjną systemu wykrywania skażeń w Siłach Zbrojnych RP tworzą: jednostki wykrywania zagrożeń (monitoringu), laboratoria analityczne, ośrodki analizy skażeń.

[21] ROTA – incydent z udziałem Toksycznych Środków Przemysłowych (TŚP).

[22] BMR – broń masowego rażenia.

[23] K. Budyn, op. cit., s. 15.

Tabela 75. Struktura szczegółowa systemu wykrywania skażeń w SZ RP

Podmioty podstawowe	Podmioty szczegółowe
Jednostki wykrywania zagrożeń (monitoringu)	drużyny (sekcje) rozpoznania skażeń klucze śmigłowców powietrznego rozpoznania skażeń okręty marynarki wojennej stacjonarne punkty monitoringu jednostek wojskowych stacje (urządzenia) do automatycznej rejestracji parametrów uderzeń jądrowych, chemicznych i biologicznych, skażeń i zakażeń oraz warunków meteorologicznych pododdziały radiotechniczne i posterunki lotniskowe wojsk lotniczych i obrony powietrznej pododdziały rozpoznania artylerii zespoły wykrywania i monitorowania skażeń kompanii (równorzędnych)
Laboratoria analityczne	laboratoria pododdziałów wojsk obrony przeciwchemicznej oraz laboratoria chemiczne i radiometryczne pozostałych rodzajów wojsk i służb jednostki organizacyjne, których statutowa działalność przewiduje wykonywanie laboratoryjnych analiz radiometrycznych, chemicznych i mikrobiologicznych
Ośrodki analizy skażeń	Centralny Ośrodek Analizy Skażeń ośrodki analizy skażeń rodzajów sił zbrojnych ośrodki analizy skażeń okręgów wojskowych i korpusów ośrodki analizy skażeń wojewódzkich sztabów wojskowych, dywizji, flotylli i brygad (równorzędnych)

Źródło: K. Budyn, *Funkcjonowanie systemu wykrywania skażeń w Siłach Zbrojnych RP. Systemy wykrywania skażeń w wybranych państwach Sojuszu Północnoatlantyckiego oraz w państwach sąsiadujących z Polską*, [w:] *Kurs podstawowy dla specjalistów Krajowego Systemu Wykrywania Skażeń*, praca zbiorowa, Warszawa 2005, s. 13–15

W systemie wykrywania skażeń w Siłach Zbrojnych Rzeczypospolitej Polskiej ważną rolę odgrywa podsystem wczesnego ostrzegania (PWO). Do podstawowych zadań tego podsystemu należy:

- monitorowanie źródeł zagrożeń skażeniami, powodujących zagrożenia dla jednostek i instytucji wojskowych,
- wykrywanie skażeń promieniotwórczych, chemicznych i biologicznych,
- ostrzeganie i powiadamianie wojsk i instytucji wojskowych o zagrożeniach skażeniami,
- rozpoznanie skażeń promieniotwórczych, chemicznych i biologicznych oraz określenie rzeczywistych stref skażeń, oznakowanie rejonów skażonych i niebezpiecznych, wymiana informacji z innymi systemami obronnymi państwa,
- meldowanie przełożonym wniosków i propozycji wypływających z oceny zagrożenia[24].

Podsystem wczesnego ostrzegania składa się z sił i środków wytypowanych jednostek oraz instytucji wojskowych i obejmuje:

[24] K. Budyn, op. cit., s. 13–16.

– sieć stacjonarnych punktów monitoringu działających w oparciu o służby dyżurne jednostek i instytucji wojskowych,
– sieć stacji do automatycznej rejestracji parametrów uderzeń BMR oraz warunków meteorologicznych,
– jednostki organizacyjne zbioru i analizy danych: Centralny Ośrodek Analizy Skażeń, ośrodki analizy skażeń rodzajów sił zbrojnych, ośrodki analizy skażeń okręgów wojskowych, korpusów i Ośrodków Dowodzenia i Naprowadzania (ODN) Sił Zbrojnych RP[25].

Alarmy, sygnały alarmowe i komunikaty ostrzegawcze zostały wprowadzone rozporządzeniem Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach*[26].

Tabela 76. Rodzaje alarmów, sygnały alarmowe

Rodzaj alarmu	Sposób ogłaszania alarmów			Sposób odwoływania alarmów	
	Akustyczny system alarmowy	Środki masowego przekazu	Wizualny sygnał alarmowy	Akustyczny system alarmowy	Środki masowego przekazu
Alarm powietrzny	– ciągły modulowany dźwięk syreny w okresie jednej minuty – następujące po sobie sekwencje długich dźwięków sygnałów dźwiękowych pojazdów, gwizdków, trąbek lub innych przyrządów na sprężone powietrze w stosunku 3:1; w przybliżeniu 3 sekundy dźwięku oraz 1 sekunda przerwy	powtarzana trzykrotnie zapowiedź słowna: Uwaga! Uwaga! Ogłaszam alarm powietrzny dla...	znak czerwony, najlepiej w kształcie kwadratu	dźwięk ciągły trwający 3 minuty	powtarzana trzykrotnie zapowiedź słowna: Uwaga! Uwaga! Odwołuję alarm powietrzny dla...
Alarm o skażeniach	– przerywany modulowany dźwięk syreny – sekwencja krótkich sygnałów wydawanych sygnałem dźwiękowym pojazdu lub innym podobnym urządzeniem lub też uderzenia metalem czy też innym przedmiotem w stosunku 1:1, w przybliżeniu jedna sekunda wydawania dźwięku oraz 1 sekunda przerwy	powtarzana trzykrotnie zapowiedź słowna: Uwaga! Uwaga! Ogłaszam alarm o skażeniach... (podać rodzaj skażenia) dla...	znak czarny, najlepiej w kształcie trójkąta	dźwięk ciągły trwający 3 minuty	powtarzana trzykrotnie zapowiedź słowna: Uwaga! Uwaga! Odwołuję alarm o skażeniach dla…

Źródło: Rozporządzeniem Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach* (Dz. U. z 2006 r. Nr 191, poz. 1415)

[25] Ibidem.

[26] Dz. U. z 2006 r. Nr 191, poz. 1415.

Tabela 77. Komunikaty ostrzegawcze

Rodzaj komunikatu	Sposób ogłaszania komunikatu		Sposób odwoływania komunikatu	
	Akustyczny system alarmowy	Środki masowego przekazu	Akustyczny system alarmowy	Środki masowego przekazu
Uprzedzenie o zagrożeniu skażeniami		powtarzana trzykrotnie zapowiedź słowna: Uwaga! Uwaga! Osoby znajdujące się na terenie... około godziny... min... może nastąpić skażenie... (podać rodzaj skażenia) w kierunku... (podać kierunek)		powtarzana trzykrotnie zapowiedź słowna: Uwaga! Uwaga! Odwołuję uprzedzenie o zagrożeniu... (rodzaj skażenia) dla...
Uprzedzenie o zagrożeniu zakażeniami	Formę i treść komunikatu uprzedzenia o zagrożeniu zakażeniami ustalają organy Państwowej Inspekcji Sanitarnej			
Uprzedzenie o klęskach żywiołowych i zagrożeniu środowiska		powtarzana trzykrotnie zapowiedź słowna: informacja o zagrożeniu i sposób postępowania mieszkańców...		powtarzana trzykrotnie zapowiedź słowna: Uwaga! Uwaga! Odwołuję alarm o klęskach... dla...

Źródło: Rozporządzeniem Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach* (Dz. U. z 2006 r. Nr 191, poz. 1415)

8.3. System powiadamiania ratunkowego

System powiadamiania ratunkowego stanowi jednostkę, której podstawowym zadaniem jest integracja Krajowego Systemu Ratowniczo-Gaśniczego i Systemu Państwowego Ratownictwa Medycznego. Podstawę prawną systemu powiadamiania ratunkowego stanowi ustawa z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej*[27]. Zadaniem tego systemu jest:

– bieżąca analiza zasobów ratowniczych,
– przyjmowanie zgłoszeń oraz obsługa numeru alarmowego 112,
– kwalifikacja zgłoszeń,
– podejmowanie działań zgodnie z określonymi procedurami, w szczególności:
  a) dysponowania sił ratowniczych i zespołów ratownictwa medycznego,
  b) koordynowania oraz monitorowania działań ratowniczych i medycznych czynności ratunkowych,
  c) powiadamiania o zdarzeniu szpitalnych oddziałów ratunkowych lub jeżeli wymaga tego sytuacja na miejscu zdarzenia jednostek organizacyjnych

[27] Ustawa z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej* (Dz. U. z 1991 r. Nr 81, poz. 351 z późn. zm.), art. 14a ust. 1.

szpitali wyspecjalizowanych w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego,

d) inicjowania procedur reagowania kryzysowego.

Zadania systemu powiadamiania ratunkowego wykonują na terenie województwa:

- wojewódzkie centrum powiadamiania ratunkowego, przez które rozumie się wspólne stanowisko kierowania, w skład którego wchodzą stanowisko kierowania komendanta wojewódzkiego Państwowej Straży Pożarnej, stanowisko lekarza koordynatora ratownictwa medycznego,
- centra powiadamiania ratunkowego, przez które rozumie się wspólne stanowiska kierowania, w skład których wchodzą: stanowiska kierowania komendantów powiatowych (miejskich) Państwowej Straży Pożarnej, dyspozytorzy medyczni zatrudnieni przez dysponentów jednostek funkcjonujących na terenie działania centrum powiadamiania ratunkowego,
- pozostałe stanowiska kierowania Państwowej Straży Pożarnej,
- stanowiska kierowania Policji obsługujące numery alarmowe[28].

Tworzenie i rozwijanie centrum powiadamiania ratunkowego (CPR) pozwala na realizację zadań w zakresie nagłego wypadku, zagrożenia życia, zdrowia, mienia oraz środowiska naturalnego. Zadania centrum powiadamiania ratunkowego jest:

- przyjmowanie, kwalifikacja i selekcja wywołań alarmowych dotyczących nagłych stanów zagrożenia życia i zdrowia, mienia i środowiska, wymagających działań ratowniczych realizowanych w trybie pilnym,
- uruchamianie Zespołu Zarządzania Kryzysowego w czasie powstania katastrofy lub w innych sytuacjach nadzwyczajnych zagrożenia życia, zdrowia, mienia, środowiska,
- dysponowanie do działań sił i środków na podstawie przyjętych planów ratowniczych, uwzględniających możliwości podmiotów systemu ratowniczego i współdziałanie,
- koordynowanie działań podmiotów ratowniczych w zakresie wspomagania i dysponowania siłami i środkami na podstawie informacji kierującego działaniem ratowniczym lub koordynatora medycznych działań ratowniczych,
- stałe analizowanie i ocenianie gotowości systemu ratowniczego do prowadzenia działań ratowniczych, w zakresie ratownictwa medycznego, chemicznego, technicznego i gaszenia pożarów,
- monitorowanie powstawania i rozwoju zagrożeń,
- ostrzeganie służb ratowniczych i ludności o możliwości powstania nadzwyczajnych zagrożeń i informowanie o podjętych formach i sposobach zachowania się ludności,
- informowanie o podjętych formach ochrony, przebiegu działań ratowniczych i sposobach zachowania ludności, zarządzeniach prewencyjnych władz obowiązujących wszystkich obywateli,

[28] Ibidem, art. 14a ust. 2.

- współdziałanie ze Szpitalnymi Oddziałami Ratunkowymi,
- współpraca z podmiotami ratowniczymi spoza obszaru chronionego w razie potrzeby spowodowanej rodzajem i skalą zdarzenia,
- analizowanie i dokumentowanie powstałych zdarzeń i ich oddziaływania na ludzi i środowisko, podjętych decyzji i zastosowanych w konkretnych sytuacjach działań, w celu przedstawienia propozycji zmian planu ratowniczego,
- tworzenie baz danych na użytek systemu ratowniczego, gromadzących informacje od podmiotów ratowniczych i innych powiatowych instytucji[29].

Skuteczność działania centrum powiadamiania ratunkowego (CPR) osiąga się poprzez realizację określonych funkcji:

- skrócenie czasu powiadamiania i dysponowania do działań podmiotów właściwych dla danego rodzaju zagrożenia,
- szybki obieg informacji w sieci CPR na obszarze województwa w przypadku wystąpienia zdarzeń o zasięgu wykraczającym poza obszar powiatu,
- ukształtowanie korzystnych warunków koordynacji działań ratowniczych dla wszystkich podmiotów ratowniczych z terenu powiatu,
- stworzenie jednolitej bazy danych zawierających informacje o zdarzeniach, użytych środkach, poniesionych stratach, liczbie poszkodowanych itp.,
- optymalny dobór i wykorzystanie sił i środków niezbędnych do skutecznego prowadzenia działań ratowniczych,
- podniesienie skuteczności koordynacji działań medycznych o zasięgu ponadpowiatowym i przekraczającym możliwości ratownicze powiatu,
- efektywniejsze wykorzystywanie potencjału ratowniczego i infrastruktury komunikacyjnej Państwowej Straży Pożarnej i Państwowego Ratownictwa Medycznego[30].

Jednostkami współpracującymi z systemem powiadamiania ratunkowego są ponadto służby ustawowo powołane do realizacji przedsięwzięć mających na celu ochronę życia, zdrowia oraz bezpieczeństwa obywateli, mienia i środowiska, a także społeczne organizacje ratownicze.

W centrach powiadamiania ratunkowego i wojewódzkich centrach powiadamiania ratunkowego mogą być zatrudnieni operatorzy numerów alarmowych, do przyjmowania zgłoszeń alarmowych oraz podejmujący określone procedurami czynności[31]. Centrum powiadamiania ratunkowego działa na terenie co najmniej jednego powiatu lub miasta na prawach powiatu, na obszarze którego wykonywane są zadania centrum powiadamiania ratunkowego. Komendant Główny Państwowej Straży Pożarnej koordynuje oraz kontroluje funkcjonowanie systemu powiadamiania ratunkowego na obszarze kraju, w szczególności poprzez analizę funkcjonowania systemu powiadamiania ratunkowego w woje-

[29] W. Lidwa, W. Krzeszowski, W. Więcek, *Zarządzanie w sytuacjach kryzysowych*, Warszawa 2010, s. 67 i 68.

[30] Opracowano na podstawie J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego*, Kraków 2010, s. 213.

[31] Ibidem, art. 14a ust. 5.

wództwach oraz inicjowanie przedsięwzięć w zakresie systemu powiadamiania ratunkowego, z wyłączeniem świadczeń zdrowotnych, o których mowa w ustawie z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym*[32]. Wojewoda przy pomocy komendanta wojewódzkiego Państwowej Straży Pożarnej oraz komendantów powiatowych (miejskich) Państwowej Straży Pożarnej na obszarze województwa organizuje oraz koordynuje funkcjonowanie systemu powiadamiania ratunkowego. Wojewoda także kontroluje oraz nadzoruje funkcjonowanie systemu powiadamiania ratunkowego na obszarze województwa. Dysponent jednostki, w rozumieniu ustawy z dnia 8 września 2006 r. *o Państwowym Ratownictwie Medycznym*, zapewnia środki łączności umożliwiające komunikację z centrum powiadamiania ratunkowego i pomiędzy jednostkami systemu Państwowego Ratownictwa Medycznego oraz zatrudnienie dyspozytorów medycznych[33]. Komendant wojewódzki Policji zapewnia jednostkom podległym środki łączności umożliwiające komunikację z centrum powiadamiania ratunkowego.

Zgodnie z ustawą z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej*[34] wojewódzkie centrum powiadamiania ratunkowego oraz centra powiadamiania ratunkowego organizowane są odpowiednio przez komendantów wojewódzkich i komendantów powiatowych (miejskich) Państwowej Straży Pożarnej. Komendant wojewódzki Państwowej Straży Pożarnej w uzgodnieniu z wojewodą określa liczbę, lokalizację i teren działania centrów powiadamiania ratunkowego oraz liczbę stanowisk dyspozytorów medycznych i stanowisk operatorów numerów alarmowych. Wojewoda może w drodze porozumienia powierzyć organizowanie centrów powiadamiania ratunkowego starostom lub prezydentom miast na prawach powiatów[35]. Porozumienie określa prawa i obowiązki stron oraz zasady współfinansowania centrów powiadamiania ratunkowego. Centra powiadamiania ratunkowego w zakresie realizacji zadań[36] mogą wykonywać zadania innych podmiotów oraz jednostek samorządu terytorialnego na podstawie porozumienia zawartego z wojewodą. Porozumienie określa zakres i zasady wykonywania zadań oraz ich finansowanie. Wojewódzkie centra powiadamiania ratunkowego są finansowane z budżetu państwa, z części, której dysponentem jest właściwy wojewoda[37]. Centra powiadamiania ratunkowego organizowane przez komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej są finansowane z budżetu państwa w formie dotacji celowej na zadania z zakresu administracji rządowej.

[32] Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.

[33] Ibidem, art. 14b ust. 1.

[34] Ibidem, art. 14c ust. 1.

[35] Ibidem, art. 14c ust. 3.

[36] Ibidem, art. 14a ust. 1.

[37] Ibidem, art. 14d ust. 1.

Minister Spraw Wewnętrznych i Administracji rozporządzeniem z dnia 31 lipca 2009 roku *w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego i wojewódzkich centrów powiadamiania ratunkowego*[38] określił:

- 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,
- 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 – uwzględniając potrzeby systemu powiadamiania ratunkowego w zakresie jego sprawnego funkcjonowania.

Skuteczność realizacji zadań przez centrum powiadamiania ratunkowego wykonania wielu wzajemnie powiązanych przedsięwzięć to:

- opracowanie planów postępowania na wypadek wystąpienia sytuacji awaryjnych,
- określenie zasad prowadzenia i archiwizacji dokumentacji,
- określenie zasady i zakresu przekazywania informacji niezbędnych do prawidłowego funkcjonowania,
- opracowanie szczegółowych procedur przyjmowania zgłoszeń alarmowych, w tym obcojęzycznych,
- określenie zasad organizacji pracy dyspozytorów medycznych i operatorów numerów alarmowych oraz pełnienia służby dyspozytorów Państwowej Straży Pożarnej,
- opracowanie planu zwiększania obsad osobowych centrum w sytuacjach nadzwyczajnych,
- opracowanie regulaminu wewnętrznego centrum,
- sporządzenie wykazu podmiotów ratowniczych i służb funkcjonujących na terenie działania centrum,
- opisanie struktury systemu powiadamiania ratunkowego na terenie działania centrum wraz ze schematem przepływu informacji[39].

Centrum w celu wykonania zadania systemu powiadamiania ratunkowego uzyskuje informacje od:

- dyspozytorów jednostek, zakładów opieki zdrowotnej i jednostek współpracujących z systemem Państwowego Ratownictwa Medycznego w zakresie:

[38] Dz. U. z 2009 r. Nr 130, poz. 1073.

[39] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2009 roku *w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego i wojewódzkich centrów powiadamiania ratunkowego* (Dz. U. z 2009 r. Nr 130, poz. 1073), § 3 ust. 6.

- liczby i rozmieszczenia dostępnych podstawowych i specjalistycznych zespołów ratownictwa medycznego, w tym lotniczych zespołów ratownictwa medycznego,
- liczby i wyposażenia oraz rodzaju i rozmieszczenia dostępnych zastępów i grup ratowniczych zdolnych do udzielenia kwalifikowanej pierwszej pomocy,
- czasowego lub całkowitego braku możliwości udzielenia świadczeń opieki zdrowotnej przez komórki organizacyjne szpitala, wraz z informacją o przyczynie i przewidywanym okresie trwania tych ograniczeń,
- gotowości szpitalnych oddziałów ratunkowych i innych jednostek organizacyjnych szpitali do przyjęcia osób znajdujących się w sytuacji nagłego zagrożenia zdrowotnego,

- podmiotów krajowego systemu ratowniczo-gaśniczego i podmiotów współpracujących z tym systemem,
- innych podmiotów ratowniczych, które współpracują z systemem powiadamiania ratunkowego w zakresie niezbędnym do realizacji zadań ratowniczych[40].

Centrum w procesie realizowania zadań w systemie powiadamiania ratunkowego wykonuje następujące zadania:

- przyjmuje zgłoszenia alarmowe, w szczególności:
  - kierowane na numery alarmowe 112, 998 i 999,
  - kierowane na numery alarmowe innych podmiotów oraz jednostek samorządu terytorialnego, które na podstawie porozumienia realizują zadania systemu powiadamiania ratunkowego w danym centrum,
  - z systemów monitoringu,
  - przy wykorzystaniu innych dostępnych w centrum środków komunikacji,
  - od Policji,
  - od dyspozytorów Państwowej Straży Pożarnej spoza centrum,
  - z innych centrów lub wojewódzkich centrów,
  - od podmiotów ratowniczych i służb zlokalizowanych poza centrum,
- zapewnia obsługę numerów alarmowych, w tym numeru alarmowego 112,
- zapewnia obsługę zgłoszeń obcojęzycznych, w tym kierowanych na numer alarmowy 112,
- zapewnia wymianę informacji w czasie rzeczywistym między operatorami numerów alarmowych i dyspozytorami centrum oraz wymianę informacji między centrum a dyspozytorami spoza centrum[41].

Centrum powiadamiania ratunkowego i wojewódzkie centrum powiadamiania ratunkowego mają prawo uzyskać, za pośrednictwem centralnego punktu systemu centrów powiadamiania ratunkowego albo własnego punktu centralnego, o których mowa w art. 78 ust. 4 pkt 1 ustawy z dnia 16 lipca 2004 roku *Prawo*

[40] Ibidem, § 4 ust. 1.

[41] Ibidem, § 6.

telekomunikacyjne[42], informacje dotyczące lokalizacji zakończenia sieci, z którego zostało wykonane połączenie do numeru alarmowego 112 albo innego numeru alarmowego oraz dane dotyczące abonenta lub zarejestrowanego użytkownika końcowego usługi przepłaconej, o których mowa w art. 169 ust. 1 ustawy z dnia 16 lipca 2004 roku *Prawo telekomunikacyjne*.

Telefon alarmowy 112

Numer alarmowy 112 jest jednolitym numerem alarmowym obowiązującym na terenie wszystkich krajów Unii Europejskiej. W sytuacji zagrożenia zdrowia, życia lub mienia osoby przebywające na terenie całej UE wybierając numer 112 mają gwarancję połączenia się ze służbami ratowniczymi powołanymi do niesienia pomocy. Obowiązek wdrożenia w Polsce rozwiązań umożliwiających korzystanie z numeru 112 wynika z postanowień Dyrektywy 2002/22/WE Parlamentu Europejskiego z dnia 7 marca 2002 roku *w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników* (dyrektywa o usłudze powszechnej). Obowiązek ten nakłada również ustawa z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym* w oparciu o upoważnienie z delegacji ustawowej – minister właściwy do spraw wewnętrznych w porozumieniu z ministrem właściwym do spraw zdrowia określił w drodze rozporządzenia szczegółową organizację centrów powiadamiania ratunkowego, ich liczbę oraz sposób rozmieszczenia, mając na uwadze realizację zadań centrów oraz potrzeby krajowego systemu ratowniczo-gaśniczego.

System 112 stanowi jednolity krajowy system odbioru zgłoszeń na ten numer alarmowy. Obejmuje on sieć centrów powiadamiania ratunkowego, którego celem jest przyjmowanie, przetwarzanie i obsługa zgłoszeń na numer alarmowy 112, a w szczególności przekazywanie szczegółowych informacji o zdarzeniu do właściwych terytorialnie stanowisk kierowania służb ustawowo powołanych do niesienia pomocy w celu podjęcia interwencji, a w razie potrzeby utrzymanie ciągłego połączenia osoby zgłaszającej zdarzenie oraz przekierowanie zgłoszenia do dyspozytora medycznego.

W ramach systemu telefonu alarmowego 112 funkcjonują takie podmioty, jak Policja, Straż Pożarna, pogotowie ratunkowe, a także inne podmioty ratownicze, do których przekierowywane są zgłoszenia alarmowe i które potwierdzają podjęcie akcji ratowniczej lub innej interwencji.

Powyższy system został uruchomiony w 2010 roku i funkcjonuje w 16 wojewódzkich centrach powiadamiania ratunkowego. Funkcjonowanie CPR ma być spójne pod względem technicznym z wymogami Unii Europejskiej dotyczącymi usługi E-Call i E-112. Zgodnie z obowiązującymi założeniami wszystkie rozmowy mają być rejestrowane wraz z informacjami na temat właściciela telefonu i miejsca, z którego dzwoni. Numer 112 ma być obsługiwany także w kilku językach obcych. Kiedy zgłoszenie nastąpi w języku obcym, operator będzie posiadał możliwość przekierowania rozmowy do osoby znającej dany język.

[42] Dz. U. z 2004 r. Nr 171, poz. 1800, z późn. zm.

Zbudowanie systemu 112 pozwala na skrócenie czasu oczekiwania na pomoc, a także samych czynności ratowniczych, właściwy dobór sił i środków do działania, usprawnienie przepływu informacji, jak również stworzenie jednolitej bazy danych, ponadto na integrację dyspozytorów, koordynację działań i usprawnienie współpracy między jednostkami podejmującymi działania ratownicze.

Połączenia wykonywane na numer alarmowy 112 obecnie odbierane są przez Powiatowe/Miejskie Stanowiska Kierowania Straży Pożarnej (dla telefonii stacjonarnej) oraz w Komendach Powiatowych Policji (dla telefonii mobilnej). Operatorzy 112 dysponują właściwe służby ratownicze na podstawie przekazanych informacji lub/jeśli zachodzi taka konieczność mogą przełączyć rozmowę do dyspozytorów poszczególnych służb ratunkowych. W miastach, gdzie już zostały wybudowane lokalne centra powiadamiania ratunkowego, połączenia alarmowe z numerem 112 są tam kierowane. Obecnie toczą się prace nad modelem docelowym systemu dobierania połączeń z numeru 112 i innych numerów alarmowych. Ze względu na przyzwyczajanie, komfort obywateli i specyfikę niektórych wezwań zachowane będą numery 997, 998, 999.

Numer alarmowy 112 służy wyłącznie do powiadamiania w nagłych sytuacjach zagrożenia zdrowia, życia lub mienia, np. w przypadku pożaru, wypadku drogowego, kradzieży, włamania, użycia przemocy, nagłego omdlenia i utraty świadomości, poważnego uszkodzenia ciała i silnego krwawienia, porażenia prądem, rozpoznania osoby poszukiwanej przez Policję, inną nagłą sytuację zagrażającą zdrowiu lub życiu.

Czynności po wybraniu numeru 112:

1. Miejsce rozmowy powinno znajdować się w pobliżu miejsca zdarzenia i pozwalać na przeprowadzenie spokojnej rozmowy z operatorem (bez zakłóceń).
2. Jeśli to możliwe, połączenie z operatorem numeru 112 powinno być wykonane przez osobę znajdującą się bezpośrednio w miejscu zagrożenia lub inną osobą będącą świadkiem danego zdarzenia.
3. Należy czekać cierpliwie do momentu zgłoszenia się operatora, nie odkładać słuchawki do czasu, aż połączenie zostanie podjęte (połączenie jest bezpłatne, więc nie generuje kosztów dla zgłaszającego zdarzenie).
4. Przedstawić się z imienia i nazwiska, krótko opisać zdarzenie lub sytuację, której było się świadkiem w celu wezwania przez operatora CPR właściwej służby.
5. Wskazać miejsce przebywania/adres w którym miało miejsce zdarzenie lub sytuacja; jeśli to możliwe wskazać najszybszą drogę dojazdu do miejsca zdarzenia.
6. Udzielać dodatkowych informacji na zadawane przez operatora pytania.
7. Wykonywać polecenia/instrukcje przekazywane przez operatora.
8. Nie rozłączać się do czasu wyraźnego polecenia operatora z uwagi na konieczność przekazania najważniejszych informacji o zdarzeniu.
9. Jeśli sytuacja nagle się zmieni lub pogorszy, należy szybko o tym powiadomić operatora numeru 112.

Czego można spodziewać się dzwoniąc na 112?

Zgłoszenie zostanie skierowane do najbliższego centrum powiadamiania ratunkowego właściwego ze względu na miejsce lokalizacji osoby zgłaszającej zdarzenie lub – w przypadku problemów z łącznością – może być przekierowane do następnego centrum powiadamiania ratunkowego, które przyjmie zgłoszenie i powiadomi właściwe służby.

Co robi operator odbierający połączenie na numer alarmowy 112?

Zapyta o rodzaj zdarzenia, miejsce zdarzenia, wstępnie dokona oceny sytuacji i wytypuje odpowiednią służbę, która powinna być skierowana do miejsca zdarzenia, poinformuje o rodzaju zdarzenia właściwe służby ratunkowe najbliższe miejscu zdarzenia (dlatego tak istotne jest precyzyjne wskazanie miejsca/lokalizacji), jeśli zajdzie potrzeba, operator może połączyć osobę zgłaszającą zdarzenie bezpośrednio z dyspozytorem danej służby, np. z dyspozytorem medycznym. Należy pamiętać, że w przypadku zagrożenia kilka osób może dzwonić jednocześnie na numer alarmowy 112, zgłaszając to samo zdarzenie. Nie należy się irytować, kiedy operator dokona przyjęcia zgłoszenia i po dokonaniu weryfikacji oraz zadaniu jednego lub dwóch pytań, szybko zakończy rozmowę. Działanie to ma na celu uniknięcie blokowania linii oraz powielania tych samych informacji o zdarzeniu, do którego zostały już zadysponowane właściwe służby.

Nie należy dzwonić na numer 112, kiedy zaistniała sytuacja nie jest niebezpieczna i nie stwarza zagrożenia dla zdrowia, życia lub mienia lub w innych sytuacjach, takich jak:

- zgłoszenie fikcyjnego zdarzenia lub tylko dla zabawy,
- poinformowanie, że nie potrzebujesz pomocy,
- sprawdzenie, czy numer 112 naprawdę działa,
- ustalenie danych kontaktowych firmy lub osoby (telefon, faks, cennik usług, działalność itp.),
- poinformowanie o ograniczeniach i utrudnieniach w ruchu drogowym lub o złym stanie technicznym dróg,
- uzyskanie informacji o rozkładzie jazdy komunikacji miejskiej, kolejowej lub lotniczej,
- uzyskanie połączenia międzynarodowego,
- wezwanie taksówki, zamówienie kwiatów, dania z restauracji, baru, pizzerii itp.,
- wyrażenie opinii na temat wydarzenia lub na temat osoby publicznej,
- uzyskanie konsultacji i porady lekarskiej.

Użycie numeru alarmowego 112 bez potrzeby i uzasadnienia blokuje linię telefoniczną osobie, która właśnie w tej chwili może potrzebować natychmiastowej pomocy, a nie może połączyć się z operatorem w CPR.

8.4. Krajowy System Ratowniczo-Gaśniczy

Do prowadzenia działań ratowniczych na miejscu zdarzenia potrzebne są profesjonalne służby i podmioty ratownicze, wyposażone w odpowiednie środki, zorganizowane i działające w ramach systemu ratowniczego na danym terenie oraz dobre procedury ratownicze przewidziane w planach ratowniczych[43].

Zgodne z art. 14 ust. 1 ustawy z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej*[44] krajowy system ratowniczo-gaśniczy (KSRG) ma na celu ochronę życia, zdrowia, mienia lub środowiska poprzez:

- walkę z pożarami lub innymi klęskami żywiołowymi,
- ratownictwo techniczne,
- ratownictwo chemiczne,
- ratownictwo ekologiczne,
- ratownictwo medyczne,
- współpracę z jednostkami systemu Państwowego Ratownictwa Medycznego, o których jest mowa w art. 32 ust. 1 ustawy z dnia 8 września 2006 r. *o Państwowym Ratownictwie Medycznym*[45], oraz systemem powiadamiania ratunkowego; jednostkami systemu Państwowego Ratownictwa Medycznego są szpitalne oddziały ratunkowe i zespoły ratownictwa medycznego (w tym lotnicze zespoły ratownictwa medycznego); z systemem współpracują centra urazowe oraz jednostki organizacyjne szpitali wyspecjalizowane w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego.

Minister Spraw Wewnętrznych pełni nadzór nad funkcjonowaniem krajowego systemu ratowniczo-gaśniczego i systemu powiadamiania ratunkowego[46]. Komendant Główny Państwowej Straży Pożarnej, wojewoda lub starosta odpowiednio na obszarze kraju, województwa lub powiatu określają zadania krajowego systemu ratowniczo-gaśniczego, koordynują jego funkcjonowanie i kontrolują wykonywanie wynikających stąd zadań, a w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia lub środowiska kierują tym systemem. Wojewoda i starosta wykonują swoje zadania przy pomocy odpowiednio wojewódzkiego i powiatowego zespołu zarządzania kryzysowego, działających na podstawie ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[47]. Wójt (burmistrz, prezydent miasta) koordynuje funkcjonowanie krajowego systemu ratowniczo-gaśniczego na obszarze gminy w zakresie ustalonym przez wojewodę. Zadanie to może być wykonywane przy pomocy komendanta gminnego ochrony przeciwpożarowej, jeżeli komendant taki został zatrudniony przez wójta (burmistrza,

[43] S. Kwiatkowski, *Zarządzanie bezpieczeństwem w sytuacjach kryzysowych*, Pułtusk 2011, s. 143.

[44] Dz. U. z 1991 r. Nr 81, poz. 351 z późn. zm.

[45] Dz. U. z 2006 r. Nr 191, poz. 1410, z późn. zm.

[46] Ustawa z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej* (Dz. U. z 1991 r. Nr 81, poz. 351 z późn. zm.), art. 12.

[47] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

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

Minister Spraw Wewnętrznych i Administracji na podstawie art. 14 ust 2 ustawy *o ochronie przeciwpożarowej* wydał rozporządzenie z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego*[48]. W rozporządzeniu tym zostały wskazane zasady organizacji krajowego systemu ratowniczo-gaśniczego, i tak:

- podmioty tworzące poszczególne poziomy systemu (na poziomie: krajowym, wojewódzkim, powiatowym),
- dysponowania do działań ratowniczych,
- kierowania działaniami ratowniczymi,
- prowadzenia dokumentacji działań ratowniczych oraz dokumentacji funkcjonowania systemu ratowniczego,
- organizacji odwodów operacyjnych,
- organizacji stanowiska kierowania[49].

Krajowy system ratowniczo-gaśniczy (KSTG) funkcjonuje na trzech poziomach odpowiednich do obszarów podziału administracyjnego państwa:

- powiatowym – wykonawczym,
- wojewódzkim – wspomaganie i koordynacja działań ratowniczych w sytuacjach wspomagających użycie sił i środków spoza terenu danego powiatu,
- krajowym – koordynacja działań i wspomaganie w sytuacjach użycia dodatkowych sił i środków spoza obszaru danego województwa oraz w przypadku zagrożeń szczególnych, tzn. zdarzeń, niezależnie od zasięgu terytorialnego i skutku, które znajdują się w kompetencjach organu administracji rządowej szczebla centralnego[50].

Organizację krajowego systemu ratowniczo-gaśniczego na poziomie powiatowym, wojewódzkim i krajowym przedstawiono w tabeli 78.

Tabela 78. Systemu ratowniczo-gaśniczy

Poziom systemu	Podmioty systemu
Powiatowy	komenda powiatowa (miejska) Państwowej Straży Pożarnej
	jednostki ochrony przeciwpożarowej mające siedzibę na obszarze powiatu włączone do systemu
	powiatowy zespół do spraw ochrony przeciwpożarowej i ratownictwa
	włączone do systemu inne służby, inspekcje, straże i instytucje
	specjaliści w sprawach ratownictwa i inne podmioty, włączeni do systemu w drodze umowy cywilnoprawnej

[48] Dz. U. z 1999 r. Nr 111, poz. 1311, z 2001 r. Nr 81, poz. 877.

[49] S. Kwiatkowski, op. cit., s. 144.

[50] Ibidem, s. 145.

Wojewódzki	komenda wojewódzka Państwowej Straży Pożarnej
	wydzielone siły i środki z poziomów powiatowych stanowiące wojewódzki odwód operacyjny
	ośrodki szkolenia Państwowej Straży Pożarnej
	wojewódzki zespół do spraw ochrony przeciwpożarowej i ratownictwa
	krajowa baza sprzętu specjalistycznego Państwowej Straży Pożarnej
Krajowy	Komenda Główna Państwowej Straży Pożarnej
	wydzielone siły i środki z wojewódzkich odwodów operacyjnych stanowiące centralny odwód operacyjny
	szkoły Państwowej Straży Pożarnej
	krajowe bazy sprzętu specjalistycznego Państwowej Straży Pożarnej
	jednostki badawczo-rozwojowe ochrony przeciwpożarowej

Źródło: Rozporządzenie MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311)

Komendanci powiatowy (miejski) i wojewódzki Państwowej Straży Pożarnej opracowują plany ratownicze odpowiednio dla obszarów powiatu i województwa[51], które poprzedza się:

- analizą zagrożeń występujących na danym obszarze, przy uwzględnieniu gęstości zaludnienia, warunków geograficzno-topograficznych, stanu infrastruktury oraz zagrożeń z obszarów sąsiadujących, w tym terenów objętych prawem górniczym, poligonów, wód przybrzeżnych oraz terenów państw ościennych,
- analizą zabezpieczenia operacyjnego podległego obszaru, określającą siły i środki niezbędne do ratowania życia, zdrowia, mienia i środowiska oraz ograniczenia, likwidacji lub usuwania potencjalnych zagrożeń, przy uwzględnieniu sił i środków własnych systemu oraz współdziałających z systemem na poszczególnych poziomach jego funkcjonowania.

Powyższe plany sprawdza się w drodze ćwiczeń aplikacyjnych i praktycznych z udziałem podmiotów systemu oraz poddaje się aktualizacji co najmniej raz w roku[52]. Podmioty wchodzące w skład systemu na poszczególnych poziomach są obowiązane do przekazywania odpowiednio komendantowi powiatowemu (miejskiemu) i wojewódzkiemu Państwowej Straży Pożarnej niezbędnych informacji do sporządzenia oraz aktualizacji analizy i planów. Komendant powiatowy (miejski) i wojewódzki uzgadnia plan z podmiotami systemu w części dotyczącej zakresu ich zadań. Plany zatwierdzają, po zasięgnięciu opinii właściwych terenowo zespołów do spraw ochrony przeciwpożarowej i ratownictwa: starosta – dla obszaru powiatu, wojewoda – dla obszaru województwa.

[51] Rozporządzenia MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311), § 4 ust. 1.

[52] Ibidem, § 6 ust. 1.

Walka z pożarami i innymi klęskami żywiołowymi

Organizacja walki z pożarami obejmuje zespół działań planistyczno-organizacyjnych i stosowanie technik gaśniczych niezbędnych do zmniejszenia i likwidacji zagrożenia pożarowego[53], a w szczególności:

- rozpoznawanie i analizowanie zagrożeń pożarowych,
- ocenę rozmiarów powstałego pożaru i prognozowanie jego rozwoju,
- ratowanie ludzi i zwierząt przed skutkami zagrożenia pożarowego,
- dostosowanie sprzętu oraz technik gaśniczych do rodzaju i miejsca pożaru,
- zlokalizowanie pożaru,
- ugaszenie pożaru.

Walka z pożarami w ramach systemu prowadzona jest siłami i środkami jednostek ochrony przeciwpożarowej włączonych do systemu na wszystkich poziomach jego funkcjonowania, a także wydzielonymi siłami i środkami pozostałych podmiotów włączonych do systemu w zakresie ustalonym w decyzji o włączeniu do systemu lub umowie cywilnoprawnej o współdziałaniu z systemem.

Organizacja walki z innymi klęskami żywiołowymi obejmuje zespół działań planistyczno-organizacyjnych i działań ratowniczych niezbędnych do ratowania życia, zdrowia, mienia lub środowiska, a także oceny zagrożenia i jego eliminacji[54]. Do walki z klęskami żywiołowymi są przeznaczone wszystkie jednostki ochrony przeciwpożarowej włączone do systemu oraz pozostałe podmioty włączone do systemu w zakresie wynikającym z ich możliwości sprzętowo-technicznych, ze szczególnym uwzględnieniem środków ochrony osobistej.

Ratownictwo techniczne, chemiczne, ekologiczne i medyczne

Organizacja ratownictwa technicznego obejmuje zespół działań planistyczno-organizacyjnych i stosowanie środków technicznych niezbędnych do ratowania, poszukiwania lub ewakuacji ludzi i zwierząt oraz ratowania mienia i środowiska[55] – zob. tabela 79.

Tabela 79. Ratownictwo techniczne

Organizacja ratownictwa technicznego obejmuje	Ratownictwo techniczne w ramach systemu prowadzą
analizowanie awarii oraz katastrof technicznych	specjalistyczne grupy poszukiwawczo-ratownicze Państwowej Straży Pożarnej stosujące techniki poszukiwawcze oraz wykorzystujące do działań ratowniczych zwierzęta i sprzęt do poszukiwania i ewakuacji osób zasypanych lub unieruchomionych w wyniku katastrofy budowlanej, zawału, osunięcia ziemi lub innych awarii technicznych

[53] Ibidem, § 7 ust. 1.

[54] Ibidem, § 8 ust. 1.

[55] Ibidem, § 9 ust. 1.

ocenę rozmiarów powstałego zdarzenia i prognozowanie jego rozwoju	specjalistyczne grupy wysokościowe Państwowej Straży Pożarnej stosujące techniki alpinistyczne i wykorzystujące do działań ratowniczych specjalistyczny sprzęt ratowniczy, w tym statki powietrzne
dostosowanie sprzętu oraz wdrożenie technik stosowanych do poszukiwania, uwalniania i ewakuacji poszkodowanych i zagrożonych ludzi oraz zwierząt w zależności od rodzaju i miejsca zdarzenia	specjalistyczne grupy wodno-nurkowe Państwowej Straży Pożarnej stosujące techniki nurkowe i wykorzystujące do działań ratowniczych specjalistyczny sprzęt, w tym łodzie ratunkowe
ratowanie życia ludzi i zwierząt zagrożonych awarią techniczną	specjalistyczne grupy techniczne Państwowej Straży Pożarnej stosujące techniki ratownicze i wykorzystujące specjalistyczny sprzęt do działań ratowniczych podczas katastrof i wypadków budowlanych, komunikacyjnych oraz infrastruktury technicznej
oznakowanie i wydzielenie strefy bezpośrednich działań ratowniczych sił systemu oraz stref zagrożenia	wydzielone siły i środki pozostałych podmiotów systemu w zakresie ustalonym w decyzji o włączeniu do systemu lub umowie cywilnoprawnej o współdziałaniu z systemem
przewietrzanie lub wentylowanie stref zagrożenia oraz stref bezpośrednich działań ratowniczych sił systemu	
oświetlenie oraz zabezpieczenie miejsca zdarzenia przed osobami postronnymi	
wykonywanie przejść i dojść do poszkodowanych lub zagrożonych ludzi i zwierząt	
usuwanie przeszkód naturalnych i sztucznych utrudniających niesienie pomocy poszkodowanym lub zagrożonym ludziom oraz ratowanie środowiska	
wypompowywanie, obwałowywanie lub uszczelnianie miejsc wycieku substancji stwarzającej zagrożenie	

Źródło: Rozporządzenia MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311), § 9 ust. 2 i 3

Organizacja ratownictwa chemicznego obejmuje zespół działań planistyczno-organizacyjnych i stosowanie technik ratowniczych niezbędnych do ratowania środowiska oraz wszelkich innych czynności podejmowanych w celu ratowania życia i zdrowia ludzi w wyniku likwidacji bezpośrednich zagrożeń stwarzanych przez toksyczne środki przemysłowe lub inne niebezpieczne materiały chemiczne[56].

Organizacja ratownictwa ekologicznego obejmuje zespół działań planistyczno-organizacyjnych i stosowanie technicznych zabezpieczeń niezbędnych do ratowania środowiska oraz stosowania środków neutralizujących ograniczających lub eliminujących powstałe skażenie.

[56] Ibidem, § 10 ust. 1.

Tabela 80. Ratownictwo chemiczne i ekologiczne

Organizacja ratownictwa chemicznego i ekologicznego obejmuje	Ratownictwo chemiczne i ekologiczne w ramach systemu prowadzą
rozpoznawanie zagrożeń oraz ocenę i prognozowanie ich rozwoju oraz skutków dla ludzi i środowiska	specjalistyczne grupy ratownictwa chemicznego i ekologicznego Państwowej Straży Pożarnej
analizowanie powstałych awarii oraz katastrof chemicznych i ekologicznych	specjalistyczne grupy wodno-nurkowe Państwowej Straży Pożarnej stosujące techniki nurkowe i wykorzystujące do działań ratowniczych specjalistyczny sprzęt ratowniczy
ratowanie życia ludzi i zwierząt zagrożonych skażeniem substancją niebezpieczną	jednostki ochrony przeciwpożarowej włączone do systemu w zakresie wynikającym z ich możliwości sprzętowo-technicznych, ze szczególnym uwzględnieniem środków ochrony osobistej
identyfikację substancji stwarzającej zagrożenie w czasie powstałego zdarzenia	wydzielone siły i środki pozostałych podmiotów systemu w zakresie ustalonym w decyzji o włączeniu do systemu lub umowie cywilnoprawnej o współdziałaniu z systemem
prognozowanie rozwoju skażenia środowiska i ocenę rozmiarów zagrożenia oraz zmian wielkości strefy zagrożenia dla ludności	
dostosowanie sprzętu oraz technik ratowniczych do miejsca zdarzenia i rodzaju substancji stwarzającej zagrożenie	
przepompowywanie i przemieszczanie substancji niebezpiecznej do nowych lub zastępczych zbiorników	
obwałowywanie lub uszczelnianie miejsc wycieku substancji niebezpiecznej	
ograniczanie parowania substancji niebezpiecznej	
zatrzymanie emisji toksycznych środków przemysłowych	
stawianie kurtyn wodnych	
neutralizację substancji niebezpiecznej substancjami chemicznymi	
związywanie substancji niebezpiecznej sorbentami	
stawianie zapór na ciekach lub obszarach wodnych zagrożonych skutkami rozlania substancji toksycznych hydrofobowych	
zbieranie substancji niebezpiecznej z powierzchni wody lub gleby	

Źródło: Rozporządzenie MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311), § 10 ust. 3 i 4

Organizacja ratownictwa medycznego obejmuje zespół działań planistyczno-organizacyjnych i stosowanie technik z zakresu pomocy medycznej w warunkach pozaszpitalnych mających na celu ratowanie życia i zdrowia, podczas zda-

rzeń prowadzących do nagłej groźby utraty życia ludzkiego lub pogorszenia się stanu zdrowia[57] – zob. tabela 81.

Tabela 81. Ratownictwo medyczne

Organizacja ratownictwa medycznego obejmuje	Ratownictwo medyczne może być realizowane przez podmioty systemu, jeżeli:
bieżące analizowanie rodzaju i liczby zagrożeń prowadzących do nagłego pogarszania się stanu zdrowia lub groźby utraty życia ludzkiego	dysponują podstawowym zespołem ratownictwa medycznego, w którego skład wchodzą co najmniej dwie osoby uprawnione do udzielania pomocy przedlekarskiej wyposażone w środek transportu i sprzęt medyczny, środki łączności i leki, działające na polecenie i w porozumieniu z lekarzem
ocenę groźby utraty życia ludzkiego lub pogorszenia się stanu zdrowia w wyniku zdarzenia i prognozowanie rozwoju zagrożenia	dysponują specjalistycznym zespołem ratownictwa medycznego, w którego skład wchodzą co najmniej jeden lekarz i dwie osoby uprawnione do udzielania pomocy przedlekarskiej wyposażone w środek transportu i sprzęt medyczny, środki łączności i leki
dostosowanie sprzętu oraz technik niezbędnych do ratowania życia i zdrowia ludzi w zależności od rodzaju i miejsca zdarzenia oraz liczby poszkodowanych i zagrożonych	dysponują izbami przyjęć lub oddziałami szpitalnymi wyspecjalizowanymi w zakresie medycyny ratunkowej
zapewnienie ciągłości procesu ratowania poszkodowanych i zagrożonych ludzi na miejscu zdarzenia oraz właściwych procedur przekazywania poszkodowanych kwalifikowanej pomocy medycznej, wynikających z powiatowych i wojewódzkich planów ratowniczych	
zapewnienie prowadzenia działań z zakresu ratownictwa medycznego przez osoby posiadające odpowiednie kwalifikacje, określone w odrębnych przepisach	

Źródło: Rozporządzenie MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311), § 11 ust. 2

Ratownictwo medyczne w warunkach pozaszpitalnych w czasie walki z pożarami, klęskami żywiołowymi lub organizowania ratownictwa technicznego, chemicznego i ekologicznego prowadzą uprawnieni strażacy z jednostek ochrony przeciwpożarowej oraz uprawnieni ratownicy z innych podmiotów włączonych do systemu w sytuacji:

- braku kwalifikowanej pomocy medycznej, gdy personel służby zdrowia nie dotarł do miejsca zdarzenia,
- braku możliwości wykorzystania personelu służby zdrowia na miejscu zdarzenia, gdy dostęp do poszkodowanych jest możliwy tylko dla strażaków-ratowników przy wykorzystaniu sprzętu specjalistycznego,

[57] Ibidem, § 11 ust. 1.

- gdy zdarzenie ma cechy nagłego zagrożenia z dużą liczbą poszkodowanych, którego skutki przekraczają możliwości ich opanowania w ramach rutynowej działalności właściwych terytorialnie służb medycznych.

Organizacja ratownictwa medycznego w ramach systemu obejmować może również działania planistyczno-organizacyjne i stosowanie technik z zakresu pomocy medycznej mających na celu ratowanie życia i zdrowia w czasie transportu poszkodowanych i we wczesnej fazie leczenia szpitalnego, podczas zdarzeń prowadzących do nagłej groźby utraty życia lub pogorszenia się stanu zdrowia. Działania tego rodzaju obejmują w szczególności zapewnienie ciągłości i spójności procesu ratowania poszkodowanych i zagrożonych ludzi na miejscu zdarzenia, w czasie transportu oraz w warunkach szpitalnych.

W działaniach z zakresu ratownictwa medycznego w warunkach pozaszpitalnych uczestniczy koordynator medycznych działań ratowniczych lub inny lekarz, który przybył pierwszy na miejsce zdarzenia[58]. Lekarz koordynujący medyczne działania ratownicze, oznakowany w sposób widoczny dla innych uczestników działań ratowniczych, wspomaga kierującego działaniem ratowniczym w zakresie ratownictwa medycznego, a w szczególności:

- nadzorowania ratownictwa medycznego w zakresie pomocy lekarskiej i przedlekarskiej prowadzonej przez podmioty i ratowników systemu na miejscu zdarzenia oraz w czasie transportu,
- prowadzenia i ewentualnego nadzorowania segregacji, jako procesu określania priorytetów terapeutyczno-transportowych,
- realizowania procedur organizacyjno-medycznych wynikających z rodzaju zdarzenia i liczby poszkodowanych oraz wybór czasu i miejsca hospitalizacji poszkodowanych lub zagrożonych utratą życia i zdrowia ludzi,
- przedstawiania kierującemu działaniem ratowniczym opinii dotyczących zabezpieczenia uczestników działań ratowniczych pod względem medycznym,
- wykorzystania możliwości transportowych oraz sprzętowych podmiotów realizujących ratownictwo medyczne oraz innych podmiotów biorących udział w działaniu ratowniczym,
- współdziałania z punktami informacyjnymi placówek służby zdrowia w zakresie informacji co do liczby i stanu poszkodowanych, rozwoju i potrzeb działań z zakresu ratownictwa medycznego,
- realizowania innych zadań organizacyjnych wynikających z potrzeb działań ratowniczych lub poleceń kierującego działaniem ratowniczym.

Organizacja walki z pożarami i innymi klęskami żywiołowymi oraz ratownictwa technicznego, chemicznego, ekologicznego i medycznego obejmuje również:

- ujednolicanie zasad powiadamiania i dysponowania podmiotów systemu oraz podmiotów współdziałających z systemem,
- ujednolicanie metodyki ostrzegania i informowania ludności o aktualnych i prognozowanych zagrożeniach oraz kierunkach i zasadach ewakuacji podczas prowadzenia działań ratowniczych,

[58] Ibidem, § 13 ust. 1.

- ujednolicanie zasad postępowania w zdarzeniach z dużą liczbą poszkodowanych,
- ujednolicanie metodyki planowania transportu poszkodowanej lub zagrożonej ludności do izb przyjęć lub szpitalnych oddziałów wyspecjalizowanych w zakresie medycyny ratunkowej lub innych podmiotów prowadzących ratownictwo medyczne w warunkach szpitalnych,
- wspomaganie kierującego działaniem ratowniczym w podejmowaniu decyzji dotyczących organizacji i prowadzenia działań ratowniczych,
- wspomaganie lekarza koordynującego medyczne działania ratownicze w podejmowaniu decyzji dotyczących prowadzenia ratownictwa medycznego w warunkach pozaszpitalnych i szpitalnych,
- wsparcie psychologiczne osób uczestniczących w działaniach ratowniczych,
- wsparcie logistyczne podmiotów systemu w czasie działań ratowniczych,
- prowadzenie działań w zakresie edukacji ratowniczej oraz badań naukowych na potrzeby ratownictwa,
- realizowanie stałej współpracy podmiotów systemu w zakresie wymiany informacji dotyczących występujących zagrożeń na danym obszarze, unowocześniania łączności dla celów ratowniczych, prowadzenia ćwiczeń w celu weryfikacji i modyfikowania planów oraz postępowania poszczególnych podmiotów systemu podczas prognozowanych zagrożeń lub w czasie prowadzonych działań ratowniczych, analizowania dokumentacji z prowadzonych działań ratowniczych, standardów sprzętowych i zasad postępowania podmiotów systemu w czasie działań ratowniczych w zależności od dziedziny ratownictwa i rodzaju zdarzenia, analizowania i ujednolicania programów szkolenia, zasad doskonalenia oraz zachowania bezpieczeństwa osób biorących udział w działaniach ratowniczych[59].

Organizacja stanowisk kierowania oraz dysponowanie sił i środków systemu do działań ratowniczych. Podstawowym elementem systemu przyjmującym informacje o zdarzeniach są stanowiska kierowania w komendach Państwowej Straży Pożarnej[60]. Stanowiskami kierowania na poszczególnych poziomach systemu są odpowiednio powiatowe (miejskie) stanowisko kierowania na poziomie powiatowym, wojewódzkie stanowisko koordynacji ratownictwa na poziomie wojewódzkim, Krajowe Centrum Koordynacji Ratownictwa na poziomie krajowym. Powiatowe (miejskie) stanowiska kierowania i wojewódzkie stanowiska koordynacji ratownictwa stanowią również bazę techniczną i informacyjną właściwych terenowo zespołów do spraw ochrony przeciwpożarowej i ratownictwa. Natomiast Krajowe Centrum Koordynacji Ratownictwa zapewnia obsługę techniczną i informacyjną sztabowi Komendanta Głównego Państwowej Straży Pożarnej. Stanowiska kierowania dokonują bieżącej wymiany informacji niezbędnej do prognozowania zagrożeń i prowadzenia działań ratowniczych oraz stanowią centrum powiadamiania ratunkowego sił i środków podmiotów systemu lub

[59] Ibidem, § 14 ust. 1.

[60] Ibidem, § 15 ust. 1.

wspomagających system. Stanowiska kierowania na poszczególnych poziomach systemu zorganizowane są w sposób zapewniający ciągłość funkcjonowania.

Zasady funkcjonowania stanowiska kierowania:

- stałe współdziałanie z dyspozytorami lub innymi osobami z poszczególnych podmiotów systemu,
- zapewnienie stosownych informacji kierującemu działaniem ratowniczym,
- alarmowanie odwodów operacyjnych,
- alarmowanie członków sztabu kierującego działaniem ratowniczym oraz innych osób ujętych w planie ratowniczym,
- korzystanie z telefonów alarmowych, poczty elektronicznej i faksów, mapy cyfrowej i innych map operacyjnych, monitoringu pożarowego i monitoringu innych zagrożeń, planów operacyjnych oraz dokumentacji operacyjnej, pomocniczej lub specjalnej,
- korzystanie z łączności przywoławczej, selektywnego wywoływania i alarmowania podmiotów systemu do działań ratowniczych, łączności satelitarnej, radiowej, komórkowej oraz przewodowej,
- współdziałanie ze specjalistami w sprawach ratownictwa,
- wykorzystanie baz danych operacyjnych,
- współdziałanie z podmiotami zajmującymi się monitorowaniem oraz prognozowaniem zagrożeń, a także z innymi podmiotami działającymi na rzecz systemu,
- korzystanie ze sprzętu niezbędnego do rejestracji rozmów telefonicznych oraz analizowanie czasu wyjazdu i pobytu zadysponowanych sił i środków do działań ratowniczych,
- stosowanie innych środków, urządzeń, systemów łączności i metod analizy danych, których wykorzystanie lub użycie może usprawnić działania ratownicze oraz realizację zadań poszczególnych stanowisk kierowania[61].

W organizacji stanowiska kierowania należy uwzględnić również awaryjne zasilanie urządzeń elektroenergetycznych, awaryjne plany ewakuacji w miejsca zastępcze, procedury funkcjonowania w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia lub środowiska.

Podmioty systemu z obszaru powiatu są obowiązane regularnie przekazywać szczegółowe dane do właściwego terenowo powiatowego (miejskiego) stanowiska kierowania o stanie oraz dyspozycyjności swych sił i środków oraz informować o ich zadysponowaniu do działań ratowniczych w zakresie określonym przez właściwego komendanta powiatowego (miejskiego)[62]. Mają również obowiązek zbierania i przekazywania do właściwego terenowo wojewódzkiego stanowiska koordynacji ratownictwa zbioru informacji o stanie sił i środków systemu na swym obszarze oraz informacji o ich zadysponowaniu do działań ratowniczych w zakresie określonym przez właściwego komendanta wojewódzkiego. Wojewódzkie stanowiska koordynacji ratownictwa przekazują do Krajowego

[61] Ibidem, § 16.

[62] Ibidem, § 17 ust. 1.

Centrum Koordynacji Ratownictwa informacje w zakresie określonym przez Komendanta Głównego Państwowej Straży Pożarnej. Uruchomienie sił i środków podmiotów systemu do działań ratowniczych na obszarze powiatu, województwa lub kraju następuje poprzez stanowiska kierowania i należy do komendanta powiatowego (miejskiego) na poziomie powiatowym, komendanta wojewódzkiego na poziomie wojewódzkim, Komendanta Głównego Państwowej Straży Pożarnej na poziomie krajowym[63]. Wymienni komendanci mogą upoważnić dyżurnych i dyspozytorów stanowisk kierowania do uruchamiania systemu na jego poszczególnych poziomach.

Dysponowanie sił i środków podmiotów systemu dla obszaru powiatu, województwa i kraju odbywa się z uwzględnieniem rodzaju i wielkości zdarzenia oraz liczby poszkodowanych, a także następujących czynników:

- możliwości podjęcia działań ratowniczych w najkrótszym czasie,
- aktualnego potencjału sił i środków będących w dyspozycji odpowiednio na poziomie powiatu, województwa i kraju,
- możliwości wykorzystania w działaniach ratowniczych sił i środków spoza systemu,
- możliwości wykorzystania odwodów operacyjnych systemu,
- możliwości techniczno-logistycznego wsparcia działań ratowniczych,
- procedur i uzgodnień zawartych w planach działań ratowniczych na poziomie powiatu, województwa i kraju,
- lokalnych zagrożeń i warunków naturalnych na terenie działania podmiotów systemu, takich jak gęstość zaludnienia, infrastruktura komunalna i przemysłowa, przeszkody naturalne: rzeki, jeziora, lasy, tereny bagienne, góry, i sztuczne: linie kolejowe, kanały, autostrady, instalacje transportujące media niebezpieczne, charakterystyka istniejących szlaków komunikacyjnych, tereny zajmowane przez poligony wojskowe.

Wykorzystanie sił i środków podmiotów systemu poza granice kraju określają odrębne umowy i porozumienia międzynarodowe.

Kierowanie działaniami ratowniczymi prowadzone jest jednoosobowo przez uprawnioną osobę odpowiednio oznakowaną, w sposób widoczny dla innych uczestników działań ratowniczych[64], zgodnie z przyjętymi procedurami i planami ratowniczymi, w celu wykonania określonych czynności ratowniczych. Kierujący posiada uprawnienia do określania rodzaju działań ratowniczych, wydawania rozkazów lub poleceń, ostrzegania podległych sił o wielkości i rodzajach zagrożenia oraz ewentualnym stopniu ryzyka planowanego działania ratowniczego. Kierujący w procesie organizowania działań ratowniczych musi uwzględnić rodzaj i wielkość zdarzenia, występujące zagrożenia oraz prognozę ich rozwoju, a w szczególności ustalić, czy w wyniku zdarzenia są osoby poszkodowane lub bezpośrednio zagrożone.

[63] Ibidem, § 18 ust. 1.

[64] Ibidem, § 20 ust. 2.

Kierowanie działaniami ratowniczymi ustaje po spełnieniu następujących warunków:

- zakończeniu ewakuacji ludzi, zwierząt i mienia ze strefy zagrożenia,
- udzieleniu pomocy medycznej poszkodowanym na miejscu zdarzenia oraz ich przekazaniu specjalistycznym zespołom ratownictwa medycznego lub podstawowym zespołom ratownictwa medycznego,
- ugaszeniu pożaru,
- zatrzymaniu emisji lub wypływu substancji niebezpiecznej oraz usunięciu spowodowanego przez nią bezpośredniego zagrożenia dla ludzi i środowiska,
- wykonaniu wszelkich innych czynności mających wpływ na ograniczenie lub likwidację zagrożenia.

Zgodnie § 22 ust. 1 rozporządzenia MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego*[65] wprowadza się trzy typy kierowania w czasie działania ratowniczego:

- interwencyjny – realizowany w strefie zagrożenia lub bezpośrednich działań ratowniczych, w której istnieje zagrożenie dla zdrowia i życia ludzi oraz mienia i środowiska lub prawdopodobieństwo jego wystąpienia, w celu likwidacji lub usunięcia skutków zdarzenia oraz zapewnienia bezpieczeństwa ratownikom; kierowaniu interwencyjnemu podlegają siły nie przekraczające wielkością jednej kompanii,
- taktyczny – realizowany na granicy strefy zagrożenia lub poza nią w celu wykonania przyjętej taktyki lub określonej strategii oraz nadzoru nad kierowaniem interwencyjnym; kierowaniu taktycznemu podlegają siły nie przekraczające wielkością jednego batalionu,
- strategiczny – realizowany w celu określenia i przyjęcia niezbędnej strategii w likwidowaniu zagrożenia oraz nadzoru nad kierowaniem taktycznym; kierowaniu strategicznemu podlegają siły wojewódzkich brygad odwodowych albo siły przekraczające wielkością jeden batalion.

Tabela 82. Typy kierowania w czasie działań ratowniczych

Typ kierowania	Podejmowane czynności
Interwencyjny	ustalenie rodzaju zagrożenia przydzielanie zadań dla rot, pododdziałów lub specjalistycznych grup ratowniczych ustalenie sposobów i metod poszukiwania poszkodowanych i zagrożonych oraz niesienia im pomocy medycznej ustalenie sposobów i metod ewakuacji poszkodowanych lub zagrożonych wyznaczenie i wydzielenie strefy bezpośrednich działań ratowniczych planowanie rozmieszczenia sprzętu ratowniczego na terenie działań ratowniczych analizowanie czasu pracy poszczególnych zespołów w strefie bezpośrednich działań ratowniczych, w szczególności czasu pracy w ubraniach ochronnych i sprzęcie izolującym drogi oddechowe ratowników nadzorowanie skuteczności działania ratowniczego oraz zachowania bezpiecznych warunków jego prowadzenia

[65] Dz. U. z 1999 r. Nr 111, poz. 1311.

	organizowanie łączności na potrzeby kierowania interwencyjnego i współdziałania podmiotów biorących udział w działaniu ratowniczym analizowanie zużycia sprzętu i środków gaśniczych, neutralizujących lub sorbentów organizowanie kierowania sekcjami i plutonami w strefie bezpośrednich działań ratowniczych współdziałanie z lekarzem-koordynatorem medycznych działań ratowniczych do czasu uruchomienia kierowania taktycznego wzywanie niezbędnych sił i środków zorganizowanie wsparcia logistycznego do czasu uruchomienia kierowania taktycznego wydzielenie strefy zagrożenia do czasu uruchomienia kierowania taktycznego
Taktyczny	ocena zagrożenia poprzez ustalenie jego charakteru i prognozowanie rozwoju podział terenu działania ratowniczego na odcinki bojowe i wyznaczenie zadań dla osób prowadzących kierowanie interwencyjne zorganizowanie ewakuacji zagrożonej ludności poza strefę zagrożenia współdziałanie z lekarzem-koordynatorem medycznych działań ratowniczych ocena wielkości sił i środków oraz wzywanie ich według potrzeb ewentualne wprowadzenie na teren działania ratowniczego innych podmiotów i służb ratowniczych wyznaczenie punktu kierowania i jego oznakowanie tworzenie systemu wspomagania decyzji kierowania taktycznego tworzenie, w miarę możliwości, odwodu taktycznego lub wezwanie odwodów operacyjnych wydzielenie strefy zagrożenia koordynowanie zmian sił ratowniczych, w tym ich wprowadzania i wyprowadzania z rejonu działania ratowniczego zorganizowanie niezbędnego wsparcia logistycznego nadzorowanie skuteczności działania ratowniczego oraz zachowanie bezpiecznych warunków jego prowadzenia analiza i korygowanie wydzielonej strefy bezpośrednich działań ratowniczych organizowanie punktu przyjęcia sił i środków współdziałanie ze sztabem kierowania taktycznego i strategicznego współdziałanie ze środkami masowego przekazu zorganizowanie łączności kierowania strategicznego oraz współdziałania podmiotów uczestniczących w działaniu ratowniczym współdziałanie z organami administracji samorządowej oraz z organizacjami pozarządowymi eliminowanie lub minimalizowanie wśród ratowników stresu pourazowego powstałego podczas zdarzenia
Strategiczny	ocena zagrożenia poprzez ustalenie jego charakteru i prognozowanie rozwoju określenie strategii działania ratowniczego podział terenu działania ratowniczego na odcinki bojowe oraz wyznaczenie zadań dla osób prowadzących kierowanie taktyczne nadzorowanie zadań prowadzonych przez podległe siły wyznaczenie punktu kierowania i jego oznakowanie informowanie ewakuowanej ludności o miejscach organizowanej pomocy humanitarnej wzywanie sił centralnego lub wojewódzkiego odwodu operacyjnego oraz ich wprowadzanie na wyznaczone odcinki bojowe eliminowanie lub minimalizowanie wśród ratowników stresu pourazowego powstałego podczas zdarzenia koordynowanie łączności na potrzeby sztabu, kierowania taktycznego oraz podmiotów uczestniczących w działaniu ratowniczym

	koordynowanie działań zaplecza logistycznego, medycznego, technicznego oraz podmiotów wspomagających działanie ratownicze współdziałanie ze środkami masowego przekazu współdziałanie z organami administracji rządowej współdziałanie z organami administracji samorządowej oraz z organizacjami pozarządowymi

Źródło: Rozporządzenie MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311), § 24 ust. 1, 2, 3

Rozporządzenie MSWiA wskazuje osoby funkcyjne zobowiązane do przejęcia kierowania w czasie działań ratowniczych na poziomach: interwencyjnym, taktycznym i strategicznym – zob. tabela 83.

Tabela 83. Osoby funkcyjne zobowiązane do przejęcia kierowania w czasie działań ratowniczych

Lp.	Poziom kierowania	Osoby funkcyjne
1.	Interwencyjne	uprawniony dowódca z jednostki ochrony przeciwpożarowej włączonej do systemu, dla której miejsce zdarzenia stanowi własny teren strażak wyznaczony przez komendanta jednostki ochrony przeciwpożarowej włączonej do systemu strażak wyznaczony przez komendanta miejskiego (powiatowego) kierowanie interwencyjne może przejąć również: – naczelnik ochotniczej straży pożarnej, właściwej dla miejsca zdarzenia, jeżeli w działaniu ratowniczym biorą udział tylko ochotnicze straże pożarne włączone do systemu, – komendant, kierownik, szef bądź inny kierujący, jeżeli w działaniu ratowniczym biorą udział tylko siły i środki jednostki ochrony przeciwpożarowej włączonej do systemu
2.	Taktyczne	dowódca jednostki ratowniczo-gaśniczej Państwowej Straży Pożarnej właściwej dla miejsca zdarzenia komendant, kierownik lub szef jednostki ochrony przeciwpożarowej włączonej do systemu dla zdarzenia mającego miejsce na terenie własnego działania oficer wyznaczony przez komendanta miejskiego (powiatowego) do kierowania w jego imieniu komendant powiatowy (miejski)
Kierowanie taktyczne jest realizowane ze stałego lub ruchomego stanowiska dowodzenia, usytuowanego w miejscu umożliwiającym ocenę rozwoju sytuacji oraz nadzorowanie i współdziałanie z kierowaniem interwencyjnym.		
3.	Strategiczne	oficer wyznaczony przez komendanta wojewódzkiego do kierowania w jego imieniu komendant wojewódzki oficer wyznaczony przez Komendanta Głównego Państwowej Straży Pożarnej do kierowania w jego imieniu Komendant Główny Państwowej Straży Pożarnej
Kierowanie strategiczne realizowane jest ze stałego stanowiska dowodzenia, w którym występuje możliwość funkcjonowania sztabu oraz współdziałania ze specjalistami określonych dziedzin ratownictwa, usytuowanego poza strefą kierowania taktycznego lub ze stanowisk kierowania Państwowej Straży Pożarnej.		
Kierowanie strategiczne, z wykorzystaniem batalionów centralnego odwodu operacyjnego, prowadzone jest przez właściwego terytorialnie komendanta wojewódzkiego lub dowódcę wojewódzkiej brygady odwodowej.		

Źródło: Rozporządzenie MSWiA z dnia 29 grudnia 1999 r. *w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego* (Dz. U. z 1999 r. Nr 111, poz. 1311), § 26, 27 i 28

Na potrzeby działania ratowniczego jednostki ochrony przeciwpożarowej włączone do systemu tworzą następującą strukturę:

- rota – dwuosobowy zespół ratowników, wchodzący w skład tego samego zastępu lub specjalistycznej grupy ratowniczej, wykonujący zadania ratownicze lub zabezpieczające, wyposażony w sprzęt ochrony osobistej,
- zastęp – pododdział liczący od trzech do sześciu ratowników, w tym dowódca, wyposażony w pojazd przystosowany do realizacji zadania ratowniczego,
- sekcja – pododdział w sile dwóch zastępów, liczący od dziewięciu do dwunastu ratowników, w tym dowódca,
- pluton – pododdział w sile od trzech do czterech zastępów lub dwóch sekcji, liczący od piętnastu do dwudziestu jeden ratowników, w tym dowódca,
- kompania – pododdział w sile trzech plutonów lub czterech sekcji oraz dowódca,
- batalion – oddział w sile od trzech do pięciu kompanii oraz dowódca,
- brygada – związek pododdziałów i oddziałów realizujący w granicach administracyjnych województwa wielkoobszarowe działanie ratownicze,
- specjalistyczna grupa ratownicza – pododdział ratowników posiadających specjalistyczne przeszkolenie i uprawnienia, wyposażony w sprzęt dostosowany do wykonania specjalistycznego zadania ratowniczego, w sile uzależnionej od specyfiki danej specjalności[66].

Pododdziały organizowane przez szkoły i ośrodki szkolenia Państwowej Straży Pożarnej mogą być tworzone również w innym składzie. Podmioty systemu, bez względu na strukturę sił przewidzianych do działań ratowniczych, posiadają jednolite oznakowanie osób funkcyjnych, pojazdów, kontenerów, przyczep, sprzętu ratowniczego i ewakuacyjno-logistycznego w sposób widoczny dla innych uczestników działań ratowniczych w zakresie określonym przez Komendanta Głównego Państwowej Straży Pożarnej. Po zakończeniu działania ratowniczego kierujący przekazuje teren, obiekt lub mienie objęte tym działaniem właścicielowi, zarządcy, użytkownikowi obiektu lub mienia, a w przypadku braku możliwości ich ustalenia przedstawicielowi Policji, straży gminnej (miejskiej) bądź organom samorządu terytorialnego[67].

Komendant powiatowy (miejski), wojewódzki i Komendant Główny Państwowej Straży Pożarnej prowadzą ewidencję podmiotów tworzących krajowy system ratowniczo-gaśniczy odpowiednio na poziomie powiatowym, wojewódzkim i krajowym[68]. Na polecenie komendanta powiatowego (miejskiego), wojewódzkiego lub Komendanta Głównego Państwowej Straży Pożarnej sporządza się analizę zdarzenia z udziałem kierującego i przedstawicieli podmiotów systemu biorących udział w działaniu ratowniczym.

Dla likwidowania skutków zdarzeń przekraczających możliwości operacyjne powiatów lub województw, z sił i środków podmiotów systemu formuje się

[66] Ibidem, § 21 ust. 1.

[67] Ibidem, § 31 ust. 1.

[68] Ibidem, § 34 ust. 1.

odwody operacyjne[69]. Uprawnienia do formowania odwodów operacyjnych posiadają Komendant Główny Państwowej Straży Pożarnej w odniesieniu do centralnego odwodu operacyjnego systemu tworzonego z sił i środków Państwowej Straży Pożarnej, komendanci wojewódzcy w odniesieniu do wojewódzkich odwodów operacyjnych systemu tworzonych z sił i środków podmiotów systemu na obszarze województwa, komendanci szkół Państwowej Straży Pożarnej w odniesieniu do kompanii szkolnych centralnego odwodu operacyjnego i specjalistycznych grup ratowniczych, tworzonych z sił i środków tych szkół. Wymienione podmioty odpowiedzialne są za wyszkolenie i gotowość do działań obwodów operacyjnych. Wojewódzkie odwody operacyjne systemu są organizowane jako wojewódzkie brygady odwodowe[70]. Oddziały i pododdziały brygad formują dowódcy brygad w celu:

- zwalczania pożarów o dużych rozmiarach,
- usuwania skutków innych miejscowych zagrożeń o dużych rozmiarach,
- usuwania skutków innych miejscowych zagrożeń wymagających specjalistycznych umiejętności lub wyposażenia.

Wyznaczone oddziały i pododdziały brygad stanowią centralny odwód operacyjny systemu ratowniczo-gaśniczego.

8.5. Państwowe Ratownictwo Medyczne

W celu realizacji zadań państwa polegających na zapewnieniu pomocy każdej osobie znajdującej się w stanie nagłego zagrożenia zdrowotnego tworzy się system Państwowe Ratownictwo Medyczne, którego podstawę prawną działania stanowi ustawa z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym*[71], która określa zasady organizacji, funkcjonowania i finansowania systemu oraz zasady zapewnienia edukacji w zakresie udzielania pierwszej pomocy.

W ramach systemu Państwowego Ratownictwa Medycznego działają:

- organy administracji rządowej właściwe w zakresie wykonywania zadań systemu, tj. minister właściwy do spraw zdrowia, wojewoda,
- jednostki systemu, do których zalicza się szpitalne oddziały ratunkowe, zespoły ratownictwa medycznego, w tym lotnicze zespoły ratownictwa medycznego, na których świadczenia zawarto umowy o udzielanie świadczeń opieki zdrowotnej[72].

[69] Ibidem, § 35 ust. 1.

[70] Ibidem, § 36. ust. 1.

[71] Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.

[72] Ustawa z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym* (Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.), art. 2 ust. 2.

Ich podstawowym zadaniem jest zapewnienie utrzymania gotowości ludzi, zasobów i jednostek organizacyjnych. Z systemem współpracują centra urazowe oraz jednostki organizacyjne szpitali wyspecjalizowane w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego, które zostały ujęte w planie.

Ponadto jednostkami współpracującymi z systemem są służby ustawowo powołane do niesienia pomocy osobom w stanie nagłego zagrożenia zdrowotnego, w szczególności:

- jednostki organizacyjne Państwowej Straży Pożarnej,
- jednostki ochrony przeciwpożarowej włączone do krajowego systemu ratowniczo-gaśniczego,
- Górskie Ochotnicze Pogotowie Ratunkowe (GOPR), Tatrzańskie Ochotnicze Pogotowie Ratunkowe (TOPR), Wodne Ochotnicze Pogotowie Ratunkowe (WOPR),
- inne jednostki podległe lub nadzorowane przez Ministra Spraw Wewnętrznych i Ministra Obrony Narodowej[73].

Jednostkami współpracującymi z systemem mogą być także społeczne organizacje ratownicze, które w ramach swoich zadań ustawowych lub statutowych są obowiązane do niesienia pomocy osobom w stanie nagłego zagrożenia zdrowotnego, jeżeli zostaną wpisane do rejestru jednostek współpracujących z systemem.

Nadzór nad systemem Państwowe Ratownictwo Medyczne na terenie kraju sprawuje minister właściwy do spraw zdrowia, który zatwierdza wojewódzki plan działania systemu i jego aktualizacje, może żądać od wojewody wszelkich informacji dotyczących funkcjonowania systemu na terenie województwa, może przeprowadzać kontrolę dysponentów jednostek na zasadach określonych w przepisach o działalności leczniczej. Nadzór nad powyższym systemem na terenie województwa sprawuje wojewoda, który ponadto odpowiedzialny jest za jego planowanie, organizowanie i koordynowanie. W ramach nadzoru wojewoda jest uprawniony do przeprowadzania kontroli jednostek współpracujących z systemem, dysponentów jednostek działających na obszarze województwa w trybie i na zasadach określonych w przepisach o zakładach opieki zdrowotnej, podmiotów prowadzących kursy.

System Państwowego Ratownictwa Medycznego działa na obszarze województwa na podstawie wojewódzkiego planu działania systemu, sporządzanego przez wojewodę, który w razie potrzeby zostaje zaktualizowany. Plan działania Systemu Państwowego Ratownictwa Medycznego zawiera:

- charakterystykę potencjalnych zagrożeń życia lub zdrowia mogących wystąpić na obszarze województwa, w tym analiza ryzyka wystąpienia katastrof naturalnych i awarii technicznych w rozumieniu przepisów o stanie klęski żywiołowej,

[73] Ibidem, art. 15 ust. 1.

- liczbę i rozmieszczenie na obszarze województwa jednostek wchodzących w skład systemu,
- obszary działania i rejony operacyjne,
- kalkulację kosztów działalności zespołów ratownictwa medycznego,
- sposób koordynowania działań jednostek systemu,
- sposób współpracy z organami administracji publicznej i jednostkami systemu z innych województw, zapewniający sprawne i skuteczne ratowanie życia i zdrowia bez względu na przebieg granic województw,
- sposób współpracy jednostek systemu,
- informacje o lokalizacji wojewódzkich centrów powiadamiania ratunkowego i centrów powiadamiania ratunkowego w rozumieniu ustawy z dnia 24 sierpnia 1991 r. *o ochronie przeciwpożarowej*[74] i terenach przez nie obsługiwanych,
- opis struktury systemu powiadamiania o stanach nagłego zagrożenia zdrowotnego w celu dokonania przez przedsiębiorców telekomunikacyjnych zestawienia koniecznych łączy telekomunikacyjnych, zapewniających możliwość niezbędnych przekierowań połączeń z centrum powiadamiania ratunkowego do właściwych jednostek organizacyjnych Policji, Państwowej Straży Pożarnej i dysponenta zespołów ratownictwa medycznego[75].

W planie umieszcza się ponadto:

- odpowiednią do potrzeb liczbę szpitalnych oddziałów ratunkowych i ich rozmieszczenie, kierując się kryterium zapewnienia odpowiedniego czasu dotarcia z miejsca zdarzenia do szpitalnego oddziału ratunkowego oraz liczbą zdarzeń,
- wykaz jednostek organizacyjnych szpitali wyspecjalizowanych w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego,
- centrum urazowe wraz z informacją o zakresie świadczeń opieki zdrowotnej, niezbędnych do realizacji jego zadań, jeżeli centrum urazowe znajduje się na obszarze danego województwa.

W planie umieszcza się również elementy dotyczące uzgodnień z dyrektorem właściwego wojewódzkiego oddziału Narodowego Funduszu Zdrowia sposobu współpracy jednostek systemu. Plan wymaga uzgodnienia z właściwym Szefem Wojewódzkiego Sztabu Wojskowego, Komendantem Wojskowego Obwodu Profilaktyczno-Leczniczego, komendantem wojewódzkim Państwowej Straży Pożarnej, komendantem wojewódzkim Policji, komendantem oddziału Straży Granicznej, którego zakres działania obejmuje strefę nadgraniczną[76].

Projekt aktualizacji planu uzgodniony z właściwymi podmiotami, o których mowa w ustawie, wojewoda przekazuje do zaopiniowania właściwym powiatowym i wojewódzkim jednostkom samorządu terytorialnego. Jednostki te

[74] T. j.: Dz. U. z 2009 r. Nr 178, poz. 1380 oraz z 2010 r. Nr 57, poz. 353.

[75] Ustawa z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym* (Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.), art. 21 ust. 1.

[76] Ibidem, art. 21 ust. 4.

przedstawiają opinię w terminie 14 dni od dnia otrzymania projektu aktualizacji planu. Ponadto organy jednostek samorządu terytorialnego i inne podmioty są zobowiązane dostarczyć na pisemne żądanie wojewody wszelkich informacji niezbędnych do sporządzenia projektu aktualizacji planu.

Wojewoda przekazuje projekt aktualizacji planu ministrowi właściwemu do spraw zdrowia w celu zatwierdzenia. Minister w terminie 30 dni od dnia otrzymania projektu aktualizacji planu może zgłosić zastrzeżenia do poszczególnych postanowień projektu aktualizacji planu, uzupełnia projekt aktualizacji planu o część dotyczącą lotniczych zespołów ratownictwa medycznego. Zatwierdzony plan jest podstawą do zawierania przez dyrektorów oddziałów wojewódzkich Narodowego Funduszu Zdrowia umów na wykonywanie medycznych czynności ratunkowych[77]. Wojewoda prowadzi w formie elektronicznej lub pisemnej ewidencję jednostek systemu z obszaru województwa[78].

Minister właściwy do spraw zdrowia, po zawarciu umowy na wykonywanie medycznych czynności ratunkowych z dysponentem lotniczych zespołów ratownictwa medycznego, przekazuje wojewodzie następujące dane o tych zespołach: liczbę zespołów na terenie województwa, na których medyczne czynności ratunkowe zawarto umowę z dysponentem lotniczych zespołów ratownictwa medycznego, miejsce stacjonowania i zasięg działania poszczególnych zespołów, czas pozostawania w gotowości[79].

Wojewoda podejmuje działania organizacyjne zmierzające do zapewnienia następujących parametrów czasu dotarcia na miejsce zdarzenia dla zespołu ratownictwa medycznego od chwili przyjęcia zgłoszenia przez dyspozytora medycznego:

- mediana czasu dotarcia – w skali każdego miesiąca – jest nie większa niż 8 minut w mieście powyżej 10 tysięcy mieszkańców i 15 minut poza miastem powyżej 10 tysięcy mieszkańców,
- trzeci kwartyl czasu dotarcia – w skali każdego miesiąca – jest nie większy niż 12 minut w mieście powyżej 10 tysięcy mieszkańców i 20 minut poza miastem powyżej 10 tysięcy mieszkańców,
- maksymalny czas dotarcia nie może być dłuższy niż 15 minut w mieście powyżej 10 tysięcy mieszkańców i 20 minut poza miastem powyżej 10 tysięcy mieszkańców[80].

Dysponent jednostki właściwy dla miejsca lokalizacji centrum powiadamiania ratunkowego, w rozumieniu ustawy z dnia 24 sierpnia 1991 roku *o ochronie przeciwpożarowej*, zatrudnia dyspozytora medycznego albo zawiera z nim umowę cywilnoprawną[81].

[77] Ibidem, art. 22.

[78] Ibidem, art. 23.

[79] Ibidem, art. 23 ust. 2.

[80] Ibidem, art. 24 ust. 1.

[81] Ibidem, art. 26 ust. 1.

Zadania dyspozytorów medycznych:

- przyjmowanie powiadomień o zdarzeniach, ustalanie priorytetów i niezwłoczne dysponowanie zespołów ratownictwa medycznego na miejsce zdarzenia, zgodnie z obowiązującymi przepisami,
- przekazywanie niezbędnych informacji osobom udzielającym pierwszej pomocy,
- przekazywanie osobie kierującej akcją prowadzenia medycznych czynności ratowniczych, niezbędnych informacji ułatwiających prowadzenie medycznych czynności ratunkowych w miejscu zdarzenia,
- zbieranie aktualnych informacji o dostępnych w rejonie operacyjnym jednostkach systemu, ich gotowości oraz przekazywanie tych informacji lekarzowi koordynatorowi ratownictwa medycznego,
- zbieranie i archiwizowanie bieżących informacji o zdarzeniach i prowadzonych medycznych czynnościach ratunkowych,
- powiadamianie o zdarzeniu szpitalnych oddziałów ratunkowych lub, jeżeli wymaga tego sytuacja na miejscu zdarzenia, centrów urazowych lub jednostek organizacyjnych szpitali wyspecjalizowanych w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego,
- powiadamianie o zdarzeniu jednostek współpracujących z systemem, jeżeli wymaga tego sytuacja na miejscu zdarzenia[82].

W razie konieczności użycia jednostek systemu spoza rejonu operacyjnego, dyspozytor medyczny powiadamia o tym fakcie lekarza-koordynatora ratownictwa medycznego, który wyznacza dyspozytorów medycznych do realizacji zadań i koordynuje działania dysponentów jednostek.

W wojewódzkim centrum powiadamiania ratunkowego działają lekarze-koordynatorzy ratownictwa medycznego w liczbie niezbędnej do zapewnienia całodobowej realizacji zadań. Do zadań lekarza-koordynatora ratownictwa medycznego należy w szczególności:

- nadzór merytoryczny nad pracą dyspozytorów medycznych,
- koordynacja współpracy dyspozytorów medycznych w przypadku zdarzeń wymagających użycia jednostek systemu spoza jednego rejonu operacyjnego,
- udzielanie dyspozytorom medycznym niezbędnych informacji i merytorycznej pomocy,
- udział w pracach wojewódzkiego zespołu zarządzania kryzysowego,
- pełnienie całodobowego dyżuru[83].

W przypadku wystąpienia katastrof naturalnych i awarii technicznych w rozumieniu ustawy z dnia 18 kwietnia 2002 r. *o stanie klęski żywiołowej*[84] lub gdy w ocenie lekarza-koordynatora ratownictwa medycznego skutki zdarzenia mogą spowodować stan nagłego zagrożenia zdrowotnego znacznej liczby osób, lekarz ten informuje niezwłocznie wojewodę o potrzebie postawienia w stan podwyż-

[82] Ibidem, art. 27 ust. 1.

[83] Ibidem, art. 29 ust. 2.

[84] Dz. U. z 2002 r. Nr 62, poz. 558 i Nr 74, poz. 676 oraz z 2006 r. Nr 50, poz. 360.

szonej gotowości wszystkich lub niektórych zakładów opieki zdrowotnej działających na obszarze danego województwa[85]. W tym przypadku wojewoda może nałożyć w drodze decyzji administracyjnej na zakłady opieki zdrowotnej obowiązek pozostawania w stanie podwyższonej gotowości w celu przyjęcia osób znajdujących się w stanie nagłego zagrożenia zdrowotnego. Decyzji tej nadaje się rygor natychmiastowej wykonalności.

Jednostkami systemu Państwowego Ratownictwa Medycznego, obok szpitalnych oddziałów ratunkowych, zespołów ratownictwa medycznego (w tym lotniczych zespołów ratownictwa medycznego), są także szpitalne oddziały ratunkowe, centra urazowe oraz jednostki organizacyjne szpitala wyspecjalizowanego w zakresie udzielania świadczeń zdrowotnych niezbędnych dla ratownictwa medycznego, które niezwłocznie udzielają niezbędnych świadczeń opieki zdrowotnej pacjentowi urazowemu albo osobie w stanie nagłego zagrożenia zdrowotnego[86].

Zgodnie z ustawą z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym*, zespoły ratownictwa medycznego dzielą się na:

- zespoły specjalistyczne, w skład których wchodzą co najmniej trzy osoby uprawnione do wykonywania medycznych czynności ratunkowych, w tym lekarz systemu oraz pielęgniarka systemu lub ratownik medyczny,
- zespoły podstawowe, w skład których wchodzą co najmniej dwie osoby uprawnione do wykonywania medycznych czynności ratunkowych, w tym pielęgniarka systemu lub ratownik medyczny[87].

Lotniczy zespół ratownictwa medycznego składa się co najmniej z trzech osób, w tym co najmniej z jednego pilota zawodowego, lekarza systemu oraz ratownika medycznego lub pielęgniarki systemu. Jest wyposażony w specjalistyczny środek transportu sanitarnego, spełniający cechy techniczne i jakościowe określone w Polskich Normach przenoszących europejskie normy zharmonizowane oraz wymogi określone w ustawie z dnia 3 lipca 2002 r. *Prawo lotnicze*[88] w systemie przez oznaczone osoby i jednostki.

Z systemem współdziałają uczelnie medyczne, placówki kształcenia ustawicznego dorosłych, stowarzyszenia lekarskie o zasięgu ogólnokrajowym prowadzące działalność w zakresie medycyny ratunkowej – w zakresie edukacji i przygotowywania kadr systemu, opracowywania zaleceń proceduralnych funkcjonowania systemu, inicjowania i realizacji zadań naukowo-badawczych w zakresie medycyny ratunkowej, oceny jakości systemu oraz wytyczania kierunków jego rozwoju[89].

[85] Ustawa z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym* (Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.), art. 30 ust. 1.

[86] Ibidem, art. 33 ust. 1.

[87] Ibidem, art. 36 ust. 1.

[88] Dz. U. z 2006 r. Nr 100, poz. 696, z późn. zm.

[89] Ustawa z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym* (Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.), art. 39.

8.5. Obrona Cywilna

Obrona Cywilna w Rzeczypospolitej Polskiej funkcjonuje na wszystkich poziomach organizacyjnych państwa. Szczegółowy katalog zadań Obrony Cywilnej zawiera Pierwszy Protokół Dodatkowy do Konwencji Genewskich z dnia 12 sierpnia 1949 roku, dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych, sporządzony w Genewie dnia 8 czerwca 1977 roku, który Rzeczpospolita Polska przyjęła 19 września 1991 roku[90]. W rozumieniu Protokołu określenie *obrona cywilna* oznacza wypełnianie wszystkich lub niektórych wymienionych niżej zadań humanitarnych, mających na celu ochronę ludności cywilnej przed niebezpieczeństwami wynikającymi z działań zbrojnych lub klęsk żywiołowych i przezwyciężanie ich bezpośrednich następstw, jak też zapewnienie warunków koniecznych do przetrwania.

Do obowiązujących regulacji prawnych w zakresie obrony cywilnej należy zaliczyć:

- ustawę z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczpospolitej Polskiej*[91],
- ustawę z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[92],
- ustawę z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej*[93],
- rozporządzenia, dekrety, wytyczne.

Zgodnie z treścią art. 137 ustawy z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczpospolitej Polskiej*[94] Obrona Cywilna ma na celu:

- ochronę ludności, zakładów pracy i urządzeń użyteczności publicznej, dóbr kultury,
- ratowanie i udzielanie pomocy poszkodowanym w czasie wojny,
- współdziałanie w zwalczaniu klęsk żywiołowych i zagrożeń środowiska oraz usuwaniu ich skutków.

Zadaniami Obrony Cywilnej w czasie pokoju jest działalność planistyczna i prowadzenie prac organizacyjnych oraz działalność szkoleniowa, a także upowszechniająca w zakresie problematyki obrony cywilnej. Do zadań Obrony Cywilnej w czasie pokoju należy również przygotowanie ludności do uczestnictwa w powszechnej samoobronie[95].

Zadania Obrony Cywilnej w czasie wojny:

- wykrywanie zagrożeń oraz ostrzeganie i alarmowanie,
- prowadzenie zabiegów specjalnych,

90 Dz. U. z 1992, Nr 41, poz. 175 z późn. zm.

91 T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

92 Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

93 Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.

94 T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

95 B. Wiśniewski, *Obrona Cywilna w krajowym porządku prawnym. Zbiór dokumentów,* Bielsko-Biała 2008, s. 5 i 6.

- organizowanie ewakuacji ludności,
- prowadzenie ewakuacji załóg zakładów pracy,
- przygotowanie budowli ochronnych,
- zaopatrywanie ludności w sprzęt i środki ochrony indywidualnej,
- organizowanie i prowadzenie akcji ratunkowych,
- walka z pożarami,
- udzielanie poszkodowanym pomocy medycznej,
- organizowanie doraźnych pomieszczeń i zaopatrzenia dla poszkodowanej ludności,
- zabezpieczenie dóbr kultury, użyteczności publicznej i ważnej dokumentacji,
- doraźne przywracanie działania niezbędnych służb użyteczności publicznej, w tym pomoc w budowie i odbudowie awaryjnych ujęć wody pitnej,
- doraźna pomoc w przywracaniu i utrzymaniu porządku w strefach dotkniętych klęskami,
- wyposażenie zakładów pracy w indywidualne środki ochrony przed skażeniami,
- zabezpieczenie dostaw wody pitnej dla ludności,
- doraźna pomoc w grzebaniu zmarłych.

W zakresie obrony cywilnej ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[96] określa również:

- organy administracji w sprawach obrony cywilnej,
- skład oraz sposób tworzenia formacji Obrony Cywilnej,
- obowiązki obywateli w zakresie obrony cywilnej (służba w OC, szkolenia w zakresie powszechnej samoobrony ludności),
- przysposobienie obronne młodzieży szkolnej i studentów.

Zgodnie z art. 17 ust. 1 tej ustawy centralnym organem administracji rządowej w sprawach obrony cywilnej jest Szef Obrony Cywilnej Kraju, którego powołuje Prezes Rady Ministrów na wniosek ministra właściwego do spraw wewnętrznych, któremu bezpośrednio podlega.

Do zakresu działania Szefa Obrony Cywilnej Kraju należy:

- przygotowywanie projektów założeń i zasad działania obrony cywilnej,
- ustalanie ogólnych zasad realizacji zadań obrony cywilnej,
- koordynowanie określonych przedsięwzięć i sprawowanie kontroli realizacji przez organy administracji rządowej i organy samorządu terytorialnego zadań obrony cywilnej,
- sprawowanie nadzoru nad odbywaniem zasadniczej służby w obronie cywilnej[97].

Terenowymi organami Obrony Cywilnej są wojewodowie, starostowie, wójtowie lub burmistrzowie (prezydenci miast). Do zakresu działania szefów Obrony Cywilnej województw, powiatów i gmin należy kierowanie oraz koordyno-

[96] T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

[97] Ustawa z 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczpospolitej Polskiej* (T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.), art. 17 ust. 4.

wanie przygotowań i realizacji przedsięwzięć obrony cywilnej przez instytucje państwowe, przedsiębiorców i inne jednostki organizacyjne oraz organizacje społeczne działające na ich terenie[98].

Podstawowymi jednostkami organizacyjnymi przeznaczonymi do wykonywania zadań obrony cywilnej są formacje obrony cywilnej, które składają się z oddziałów przeznaczonych do wykonywania zadań ogólnych lub specjalnych oraz innych jednostek tych formacji[99]. Formacje Obrony Cywilnej tworzą w drodze rozporządzenia ministrowie, a wojewodowie, starostowie, wójtowie lub burmistrzowie (prezydenci miast) w drodze zarządzenia, uwzględniając w szczególności: skalę występujących zagrożeń, rodzaj formacji, ich przeznaczenie oraz stan osobowy i organizację wewnętrzną. Formacje takie mogą tworzyć także pracodawcy.

Rada Ministrów w drodze rozporządzenia z dnia 25 czerwca 2002 roku określiła szczegółowy zakres działania Szefa Obrony Cywilnej Kraju oraz szefów Obrony Cywilnej województw, powiatów i gmin, jak również zasady i tryb kierowania oraz koordynowania przez nich przygotowań i realizacji przedsięwzięć obrony cywilnej[100].

Zakres działania Szefa Obrony Cywilnej Kraju:

- inicjowanie, przygotowanie, wydawanie i opiniowanie projektów aktów normatywnych dotyczących obrony cywilnej,
- uzgadnianie projektu planu obrony cywilnej państwa z Ministrem Obrony Narodowej oraz z innymi właściwymi ministrami,
- określanie założeń do planów OC województw, powiatów, gmin i przedsiębiorców,
- opracowanie założeń programowych oraz kierunków kształcenia i szkolenia pracowników, ratowników i ludności w zakresie obrony cywilnej,
- dokonywanie oceny stanu przygotowań obrony cywilnej województw, powiatów i gmin,
- planowanie potrzeb w zakresie środków finansowych i materiałowych niezbędnych do realizacji zadań własnych w zakresie obrony cywilnej,
- określanie założeń dotyczących ewakuacji ludności i mienia na wypadek masowego zagrożenia,
- inicjowanie działalności naukowo-badawczej dotyczącej obrony cywilnej, a także udział w pracach unifikacyjno-normalizujących w tej dziedzinie,
- opracowywanie, na potrzeby ministra właściwego do spraw wewnętrznych i Prezesa Rady Ministrów, informacji dotyczących obrony cywilnej,
- organizowanie i koordynowanie ćwiczeń w zakresie obrony cywilnej,
- kontrolowanie przygotowania formacji Obrony Cywilnej i ratowników do prowadzenia działań ratowniczych,
- kontrolowanie warunków odbywania zasadniczej służby w Obronie Cywilnej,

98 Ibidem, art. 17 ust. 7.

99 Ibidem, art. 138.

100 Dz. U. z 1996 r. Nr 2, poz. 850.

- ustalanie normatywów w zakresie zaopatrywania organów i formacji Obrony Cywilnej w sprzęt, środki techniczne i umundurowanie niezbędne do wykonywania zadań obrony cywilnej[101].

Zakres działania szefów Obrony Cywilnej województw, powiatów i gmin, na ich obszarze działania:

- dokonywanie oceny stanu przygotowań obrony cywilnej,
- opracowywanie i opiniowanie planów,
- opracowywanie i uzgadnianie planów działania,
- organizowanie i koordynowanie szkoleń oraz ćwiczeń,
- organizowanie szkolenia ludności w zakresie obrony cywilnej,
- przygotowanie i zapewnienie działania systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania o zagrożeniach,
- tworzenie i przygotowanie do działań jednostek organizacyjnych obrony cywilnej,
- przygotowanie i organizowanie ewakuacji ludności na wypadek powstania masowego zagrożenia dla życia i zdrowia na znacznym obszarze,
- planowanie i zapewnienie środków transportowych, warunków bytowych oraz pomocy przedmedycznej, medycznej i społecznej dla ewakuowanej ludności,
- planowanie i zapewnienie ochrony płodów rolnych i zwierząt gospodarskich oraz produktów żywnościowych i pasz, a także ujęć i urządzeń wodnych na wypadek zagrożenia zniszczeniem,
- planowanie i zapewnienie ochrony oraz ewakuacji dóbr kultury i innego mienia na wypadek zagrożenia zniszczeniem,
- wyznaczanie zakładów opieki zdrowotnej zobowiązanych do udzielania pomocy medycznej poszkodowanym w wyniku masowego zagrożenia życia i zdrowia ludności oraz nadzorowanie przygotowania tych zakładów do niesienia tej pomocy,
- zapewnienie dostaw wody pitnej dla ludności i wyznaczonych zakładów przemysłu spożywczego oraz wody dla urządzeń specjalnych do likwidacji skażeń i do celów przeciwpożarowych,
- zaopatrywanie formacji Obrony Cywilnej w sprzęt, środki techniczne i umundurowanie niezbędne do wykonywania zadań obrony cywilnej, a także zapewnienie odpowiednich warunków przechowywania, konserwacji, eksploatacji, remontu i wymiany tego sprzętu, środków technicznych i umundurowania,
- integrowanie sił Obrony Cywilnej oraz innych służb, w tym sanitarno-epidemiologicznych i społecznych organizacji ratowniczych do prowadzenia akcji ratunkowych oraz likwidacji skutków klęsk żywiołowych i zagrożeń środowiska,

[101] Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 roku *w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin* (Dz. U. z 1996 r. Nr 2, poz. 850), § 2.

- opiniowanie projektów aktów prawa miejscowego dotyczących obrony cywilnej i mających wpływ na realizację zadań obrony cywilnej,
- inicjowanie działalności naukowo-badawczej i standaryzacyjnej dotyczącej obrony cywilnej,
- współpraca z terenowymi organami administracji wojskowej,
- zapewnienie warunków do odbywania zasadniczej służby w obronie cywilnej,
- opiniowanie wniosków w sprawie tworzenia formacji Obrony Cywilnej, w których jest odbywana zasadnicza służba w Obronie Cywilnej,
- opracowywanie informacji dotyczących realizowanych zadań,
- współpraca z pełnomocnikami wojewodów do spraw ratownictwa medycznego i z terenowymi organami administracji wojskowej w zakresie dotyczącym realizowanych zadań,
- kontrolowanie przygotowania formacji Obrony Cywilnej i ratowników do prowadzenia działań ratowniczych,
- ustalanie wykazu instytucji państwowych, przedsiębiorców i innych jednostek organizacyjnych oraz społecznych organizacji ratowniczych funkcjonujących na ich terenie, przewidzianych do prowadzenia przygotowań i realizacji przedsięwzięć w zakresie obrony cywilnej,
- organizowanie i prowadzenie szkolenia ratowników odbywających zasadniczą służbę w Obronie Cywilnej,
- przygotowanie i zapewnienie niezbędnych sił do doraźnej pomocy w grzebaniu zmarłych[102].

Szefowie Obrony Cywilnej ustalają zadania i kontrolują ich realizację oraz koordynują i kierują działalnością w zakresie przygotowania i realizacji przedsięwzięć obrony cywilnej:

- Szef Obrony Cywilnej Kraju – szefów obrony cywilnej województw,
- szef Obrony Cywilnej województwa – szefów obrony cywilnej powiatów,
- szef Obrony Cywilnej powiatu – szefów obrony cywilnej gmin,
- szef Obrony Cywilnej gminy – szefów obrony cywilnej w instytucjach, u przedsiębiorców, w społecznych organizacjach ratowniczych i w innych jednostkach organizacyjnych działających na obszarze gminy[103].

Szefowie Obrony Cywilnej województw, powiatów, gmin oraz instytucje, przedsiębiorcy i inne jednostki organizacyjne i społeczne organizacje ratownicze opracowują wieloletnie i roczne plany działania w zakresie obrony cywilnej które podlegają uzgodnieniu z właściwymi dla swojego terenu działania organami Obrony Cywilnej[104].

Informacje o realizacji zadań obrony cywilnej składają:

- Szef Obrony Cywilnej Kraju – na żądanie Ministra Spraw Wewnętrznych lub Prezesa Rady Ministrów,

[102] Ibidem, § 3.

[103] Ibidem, § 4.

[104] Ibidem, § 5 ust. 1.

- szef Obrony Cywilnej Województwa – na wystąpienie Szefa Obrony Cywilnej Kraju,
- szef Obrony Cywilnej Powiatu – na wystąpienie szefa Obrony Cywilnej Województwa,
- szef Obrony Cywilnej Gminy – na wystąpienie szefa Obrony Cywilnej Powiatu,
- przedsiębiorcy, kierownicy instytucji i innych jednostek organizacyjnych i społecznych organizacji ratowniczych, działających na obszarze gminy, które prowadzą przygotowania i realizują przedsięwzięcia w zakresie obrony cywilnej – na wystąpienie szefa Obrony Cywilnej Gminy[105].

Szef Obrony Cywilnej Kraju oraz szefowie obrony cywilnej województw, powiatów i gmin, koordynując przygotowania i realizację przedsięwzięć obrony cywilnej, uwzględniają również działalność w zakresie obrony cywilnej przedsiębiorstw, dla których Minister Obrony Narodowej jest organem założycielskim, oraz jednostek organizacyjnych podległych Ministrowi Spraw Wewnętrznych lub przez niego nadzorowanych, w szczególności w zakresie systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania, ewakuacji ludności oraz sił i środków wydzielanych do prowadzenia akcji ratunkowych[106]. Szef Obrony Cywilnej Kraju na podstawie art. 17 ust. 4 pkt 2 i ust. 5 *ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[107], w związku z rozporządzeniem Rady Ministrów z dnia 25 czerwca 2002 roku *w sprawie szczegółowego działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin*[108], co roku wydaje wytyczne do działalności obrony cywilnej na następny rok.

Zasadniczym celem działania obrony cywilnej w 2012 roku jest doskonalenie mechanizmów ochrony ludności w warunkach zagrożenia bezpieczeństwa państwa, w tym w zakresie ostrzegania i alarmowania o zagrożeniach, współdziałania podmiotów realizujących zadania ochrony ludności w czasie pokoju, a także dążenie do zapewnienia warunków realizacji zadań w sytuacjach katastrof naturalnych, klęsk żywiołowych oraz zagrożenia państwa i w czasie wojny[109]. W tym okresie główny wysiłek realizacji zadań obrony cywilnej przedstawiono następująco:

– kontynuowanie procesu przebudowy systemu ochrony ludności pod kątem aktualnych wyzwań bezpieczeństwa ludności cywilnej,
– integracja przedsięwzięć z zakresu obrony cywilnej z planami zarządzania kryzysowego poprzez realizację wytycznych szefa obrony cywilnej kraju w sprawie zasad opracowania planu obrony cywilnej województw, powiatów i gmin,

[105] Ibidem, § 6.

[106] Ibidem, § 7.

[107] Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

[108] Dz. U. z 2002 r. Nr 96, poz. 850.

[109] Wytyczne Szefa Obrony Cywilnej Kraju z dnia 12 grudnia 2011 roku *do działalności w dziedzinie obrony cywilnej w 2012 roku* (www.uw.olsztyn.pl [pobrano 12.03.2012]).

- doskonalenie współpracy z siłami zbrojnymi RP na rzecz ochrony ludności,
- doskonalenie ewakuacji ludności, zwierząt i mienia na wypadek masowego zagrożenia,
- upowszechnianie zadań z zakresu ochrony ludności i obrony cywilnej, w tym poprzez realizację szkoleń z zakresu powszechnej samoobrony,
- zapewnienie warunków w ramach programów doskonalenia obrony cywilnej na lata 2009–2018 do modernizacji techniki i infrastruktury, szkolenia personelu, a także ludności w zakresie powszechnej samoobrony, stosownie do priorytetów wytycznych Szefa Obrony Cywilnej Kraju na 2012 rok,
- doskonalenie współpracy z ochotniczymi strażami pożarnymi w odniesieniu do zadań z zakresu ochrony ludności i obrony cywilnej,
- realizowanie zadań z zakresu ochrony ludności, związanych z uczestnictwem Polski w pracach grup roboczych i komitetów Unii Europejskiej i wynikających z przewodnictwa Polski w Grupie Wyszehradzkiej.

8.6. Siły zbrojne

Siły zbrojne stanowią jeden z nielicznych podmiotów w państwie, które posiadają największą siłę oraz zorganizowaną strukturę przygotowaną do działań w czasie pokoju, kryzysu i wojny. Podstawy prawne, struktura organizacyjna, wyposażenie, wyszkolenie i odpowiednie środki finansowe przekładają się na ich gotowość do natychmiastowego działania. Sytuacje kryzysowe, gdzie ma miejsce bezpośrednie wsparcie władz i społeczeństwa, są praktycznym sprawdzianem skuteczności działania sił zbrojnych.

W podsystemie militarnym do elementów wykonawczych zalicza się Siły Zbrojne RP, w tym pododdziały i oddziały wydzielone do realizacji zadań w sytuacjach kryzysowych, a do elementów kierowania organa Systemu Zarządzania Kryzysowego MON.

Elementy kierowania podsystemem militarnym:

- Minister Obrony Narodowej przy współudziale kierownictwa Ministerstwa Obrony Narodowej, poszerzonego w razie potrzeby o dowódców rodzajów sił zbrojnych, Dowódcę Dowództwa Operacyjnego oraz dyrektorów (szefów, dowódców, komendantów, kierowników) komórek organizacyjnych Ministerstwa Obrony Narodowej i jednostek organizacyjnych resortu obrony narodowej,
- zespół i centrum zarządzania kryzysowego w Ministerstwie Obrony Narodowej,
- grupy reagowania kryzysowego (GRK) Dowództwa Operacyjnego, dowódców rodzajów Sił Zbrojnych Rzeczypospolitej Polskiej (wojsk lądowych, sił

powietrznych, marynarki wojennej, wojsk specjalnych), Inspektoratu Wsparcia Sił Zbrojnych, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Komendy Głównej Żandarmerii Wojskowej),

- grupy operacyjne (GO) dowództw okręgów wojskowych, Dowództwa Garnizonu Warszawa, wojskowej ochrony przeciwpożarowej, dowództw korpusów i związków taktycznych, baz lotniczych, oddziałów Żandarmerii Wojskowej, Wojewódzkich Sztabów Wojskowych,
- zespoły operacyjne (ZO) jednostek wojskowych (brygad, pułków)[110].

Występujące zagrożenia w otoczeniu wewnętrznym i zewnętrznym państwa celowe i naturalne oznaczają, że zadaniem Sił Zbrojnych jest reagowanie nie tylko na zagrożenia o charakterze militarnym, ale i na zagrożenia pozamilitarne.

Podstawy prawne udziału Sił Zbrojnych RP w zarządzaniu kryzysowym:

- Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku[111],
- ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[112],
- ustawa z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej*[113],
- ustawa z dnia 21 czerwca 2002 roku *o stanie wyjątkowym*[114],
- ustawa z dnia 29 sierpnia 2002 roku *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*[115],
- ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[116],
- *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2007,
- *Strategia Obronności Rzeczypospolitej Polskiej* z 2009 roku.

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku w art. 26 stanowi, że Siły Zbrojne Rzeczypospolitej Polskiej służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic. W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej (art. 228). W razie zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić stan wojenny na części albo na całym terytorium państwa (art. 229). W razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić, na czas oznaczony,

[110] W. Lidwa, W. Krzeszowski, W. Więcek, *Zarządzanie w sytuacjach kryzysowych*, Warszawa 2010, s. 75.

[111] Dz. U. z 1997 r. Nr 78, poz. 483.

[112] T. j.: Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

[113] Dz. U. z 2002 r. Nr 62 poz. 558 z późn. zm.

[114] Dz. U. z 2002 r. Nr 113 poz. 985 z późn. zm.

[115] Dz. U. 2002 r. Nr 156 poz.1301 z późn. zm.

[116] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

nie dłuższy niż 90 dni, stan wyjątkowy na części albo na całym terytorium państwa (art. 230). W celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia Rada Ministrów może wprowadzić na czas oznaczony, nie dłuższy niż 30 dni, stan klęski żywiołowej na części albo na całym terytorium państwa. Przedłużenie tego stanu może nastąpić za zgodą Sejmu (art. 232).

Art. 3 ust. 2 ustawy 21 listopada 1967 r. *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* stanowi, że Siły Zbrojne RP mogą ponadto brać udział w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działaniach antyterrorystycznych i z zakresu ochrony mienia, akcjach poszukiwawczych oraz ratowania lub ochrony zdrowia i życia ludzkiego, oczyszczaniu terenów z materiałów wybuchowych i niebezpiecznych pochodzenia wojskowego oraz ich unieszkodliwianiu, a także w realizacji zadań z zakresu zarządzania kryzysowego. Siły Zbrojne RP, realizując zadania konstytucyjne w zakresie ochrony niepodległości państwa, niepodzielności jego terytorium oraz zapewnienia bezpieczeństwa i nienaruszalności jego granic, mają prawo stosowania środków przymusu bezpośredniego, użycia broni i innego uzbrojenia, z uwzględnieniem konieczności i celu wykonania tych zadań, w sposób adekwatny do zagrożenia oraz w granicach zasad określonych w wiążących Rzeczpospolitą Polską ratyfikowanych umowach międzynarodowych oraz międzynarodowym prawie zwyczajowym.

Zgodnie z art. 18 ustawy z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej*, jeżeli użycie innych sił i środków jest niemożliwe lub niewystarczające, Minister Obrony Narodowej może przekazać do dyspozycji wojewody, na którego obszarze działania występuje klęska żywiołowa, pododdziały lub odziały Sił Zbrojnych RP, wraz ze skierowaniem ich do wykonywania zadań związanych z zapobieżeniem skutkom klęski żywiołowej lub ich usunięciem. Pododdziały i oddziały Sił Zbrojnych RP pozostają pod dowództwem przełożonych służbowych i wykonują zadania określone przez wojewodę.

Zgodnie z art. 11 ust. 1 ustawy z dnia 21 czerwca 2002 roku *o stanie wyjątkowym* Prezydent RP na wniosek Prezesa Rady Ministrów może postanowić o użyciu oddziałów i pododdziałów Sił Zbrojnych RP do przywrócenia normalnego funkcjonowania państwa, jeżeli dotychczas zastosowane siły i środki zostały wyczerpane. Oddziały i pododdziały SZ RP pozostają pod dowództwem przełożonych służbowych. Przepis § 3 rozporządzenia Rady Ministrów z dnia 6 maja 2003 r. *w sprawie szczegółowych zasad użycia oddziałów i pododdziałów Sił Zbrojnych RP w czasie stanu wyjątkowego* ustala, że Minister Obrony Narodowej kieruje oddziały Sił Zbrojnych RP w celu wykonania postanowienia Prezydenta RP do realizacji zadań w czasie stanu wyjątkowego. Minister Obrony Narodowej wydaje decyzję, w której wyznacza zadania oddziałów Sił Zbrojnych i przekazuje je dowódcom w trybie obowiązującym w Siłach Zbrojnych.

Zgodnie z art. 10 ust. 2 ustawy z dnia 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej,* Prezydent Rzeczypospolitej Polskiej w czasie stanu wojennego w szczególności:

- postanawia, na wniosek Rady Ministrów, o przejściu organów władzy publicznej na określone stanowiska kierowania,
- postanawia, na wniosek Rady Ministrów, o stanach gotowości bojowej Sił Zbrojnych Rzeczypospolitej Polskiej,
- określa, na wniosek Rady Ministrów, zadania Sił Zbrojnych w czasie stanu wojennego,
- może mianować, na wniosek Prezesa Rady Ministrów, Naczelnego Dowódcę Sił Zbrojnych,
- zatwierdza, na wniosek Naczelnego Dowódcy Sił Zbrojnych, plany operacyjnego użycia Sił Zbrojnych,
- uznaje, na wniosek Naczelnego Dowódcy Sił Zbrojnych, określone obszary Rzeczypospolitej Polskiej jako strefy bezpośrednich działań wojennych.

Art. 25 ust. 1 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* stanowi, jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, o ile inne przepisy nie stanowią inaczej, Minister Obrony Narodowej na wniosek wojewody może przekazać do jego dyspozycji pododdziały lub oddziały Sił Zbrojnych Rzeczypospolitej Polskiej wraz ze skierowaniem ich do wykonywania zadań z zakresu zarządzania kryzysowego.

Zgodnie ze *Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2007 roku jednym z zadań Sił Zbrojnych RP jest wspieranie organów państwa w zapewnianiu bezpieczeństwa wewnętrznego Polski i udzielanie niezbędnej pomocy wojskowej właściwym instytucjom i służbom rządowym oraz samorządowym, organizacjom cywilnym i społeczeństwu w reagowaniu na zagrożenia.

Rozwinięcie powyższej Strategii stanowi *Strategia Obronności Rzeczypospolitej Polskiej* z 2009 roku, która porusza kwestie regulujące zadania Sił Zbrojnych Rzeczypospolitej Polskiej w czasie kryzysu. W celu wypełnienia misji związanej ze wspieraniem bezpieczeństwa wewnętrznego i pomocy społeczeństwu Siły Zbrojne RP utrzymują zdolność do realizacji zadań polegających na:

- monitorowaniu i ochronie przestrzeni powietrznej oraz wsparciu ochrony granicy lądowej i wód terytorialnych,
- prowadzeniu działalności rozpoznawczej i wywiadowczej,
- monitorowaniu skażeń promieniotwórczych, chemicznych i biologicznych na terytorium kraju,
- oczyszczaniu terenu z materiałów wybuchowych i przedmiotów niebezpiecznych pochodzenia wojskowego,
- prowadzeniu działań poszukiwawczo-ratowniczych,
- pomocy władzom państwowym, administracji publicznej oraz społeczeństwu w reagowaniu na zagrożenia.

Oprócz tego siły zbrojne utrzymują gotowość do prowadzenia samodzielnie bądź we współpracy z innymi organami i służbami państwowymi operacji poszukiwawczo-ratowniczych.

Podstawowym aktem prawnym, w którym zawarto regulacje z zakresu zarządzania kryzysowego z udziałem Sił Zbrojnych RP, jest ustawa z dnia 26 kwietnia

2007 roku *o zarządzaniu kryzysowym*[117]. W realizacji zadań z zakresu zarządzania kryzysowego mogą uczestniczyć oddziały Sił Zbrojnych stosownie do ich przygotowania specjalistycznego, zgodnie z wojewódzkim planem reagowania kryzysowego.

W art. 25 ust. 3 tej ustawy określone zostały zadania Sił Zbrojnych RP w zakresie zarządzania kryzysowego:

- współudział w monitorowaniu zagrożeń,
- wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń,
- wykonywanie zadań poszukiwawczo-ratowniczych,
- ewakuowanie poszkodowanej ludności i mienia,
- wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach,
- współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń,
- izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej,
- wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych i zabytkach,
- prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach Sił Zbrojnych RP,
- usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących na wyposażeniu Sił Zbrojnych RP,
- likwidowanie skażeń chemicznych oraz skażeń i zakażeń biologicznych,
- usuwanie skażeń promieniotwórczych,
- wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej,
- współudział w zapewnieniu przejezdności szlaków komunikacyjnych,
- udzielanie pomocy medycznej i wykonywanie zadań sanitarno-higienicznych i przeciwepidemicznych,
- wykonywanie zadań ujętych w wojewódzkim planie reagowania kryzysowego.

Działania Sił Zbrojnych RP są prowadzone na podstawie wojewódzkiego planu zarządzania kryzysowego, który podlega uzgodnieniu z właściwymi organami wskazanymi przez Ministra Obrony Narodowej. Oddziały Sił Zbrojnych mogą być przekazane do dyspozycji wojewody w składzie etatowym albo jako tworzone doraźnie zgrupowania zadaniowe[118].

Za koordynację udziału oddziałów Sił Zbrojnych RP w realizacji zadań w zakresie zarządzania kryzysowego na obszarze województwa, powiatu i gminy odpowiadają odpowiednio: wojewodowie, starostowie, wójtowie, burmistrzowie

[117] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

[118] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 25 ust. 5.

i prezydenci miast. Koordynacja obejmuje przedsięwzięcia mające na celu sprawne włączenie oddziałów Sił Zbrojnych do realizacji zadań, z uwzględnieniem czasu i miejsca ich użycia oraz sposobu współdziałania z innymi podmiotami. Wojewodowie, starostowie, wójtowie, burmistrzowie i prezydenci miast zadania dla oddziałów przekazują wyłącznie ich dowódcom.

Dowodzenie oddziałami Sił Zbrojnych RP odbywa się na zasadach określonych w regulaminach wojskowych i według procedur obowiązujących w Siłach Zbrojnych RP. Należy podkreślić, że użycie tych oddziałów w sytuacji kryzysowej nie może zagrozić ich zdolności do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej i ratyfikowanych umów międzynarodowych[119].

Udział Sił Zbrojnych w zapobieganiu skutkom klęsk żywiołowych lub ich usuwaniu został określony przez Radę Ministrów rozporządzeniem z dnia 20 lutego 2003 roku *w sprawie szczegółowych zasad udziału pododdziałów i oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu*. Określono w nim:

- rodzaje działań ratowniczych lub prewencyjnych wykonywanych w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia, w których mogą brać udział pododdziały i oddziały Sił Zbrojnych Rzeczypospolitej Polskiej,
- sposób koordynowania i dowodzenia oddziałami Sił Zbrojnych biorącymi udział w działaniach,
- sposób zabezpieczenia logistycznego oddziałów Sił Zbrojnych biorących udział w działaniach[120].

Zakres działań ratowniczych lub prewencyjnych został enumeratywnie wymieniony w art. 25 ustawy *o zarządzaniu kryzysowym*.

Udział oddziałów Sił Zbrojnych w realizacji działań ratowniczych lub prewencyjnych odbywa się na podstawie planu reagowania kryzysowego, opracowanego przez wojewódzki zespół reagowania kryzysowego oraz planu reagowania kryzysowego, opracowanego przez Rządowy Zespół Koordynacji Kryzysowej, o ile stan klęski żywiołowej jest wprowadzony na obszarze większym niż jedno województwo.

Powyższe plany podlegają uzgodnieniu z Ministrem Obrony Narodowej w zakresie:

- warunków użycia oddziałów Sił Zbrojnych w działaniach ratowniczych lub prewencyjnych,
- składu i wyposażenia oddziałów Sił Zbrojnych, a także zabezpieczenia logistycznego wymaganego do realizacji powierzonych zadań,
- przedsięwzięć realizowanych przez działające na terenie województwa jednostki organizacyjne, których celem będzie zabezpieczenie logistyczne oddziałów Sił Zbrojnych, w tym w zakresie zakwaterowania, wyżywienia, pomocy medycznej, zabezpieczenia materiałowo-technicznego i łączności,
- korzystania przez oddziały Sił Zbrojnych z elementów infrastruktury technicznej w czasie realizacji powierzonych zadań.

[119] Ibidem, art. 25 ust. 9.

[120] Dz. U. z 2003 r. Nr 41, poz. 347.

W strukturze Ministerstwa Obrony Narodowej znajduje się Centrum Zarządzania Kryzysowego Ministerstwa Obrony Narodowej, które rozpoczęło funkcjonowanie z dniem 1 stycznia 2011 roku. Na podstawie art. 13 ust. 1 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[121] oraz w związku z § 2 pkt 14 i 16 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 roku *w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej*[122], Minister Obrony Narodowej Decyzją Nr 245/MON z dnia 7 lipca 2010 roku utworzył Centrum Zarządzania Kryzysowego Ministerstwa Obrony Narodowej[123]. Centrum jest jednostką organizacyjną podległą Ministrowi Obrony Narodowej, bezpośrednio podporządkowaną Szefowi Sztabu Generalnego Wojska Polskiego.

Centrum realizuje w resorcie obrony narodowej zadania określone w art. 13 ust. 2 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*, do którego właściwości ponadto należy:

- obsługa prac Zespołu Zarządzania Kryzysowego w Ministerstwie Obrony Narodowej pod względem merytorycznym, techniczno-organizacyjnym oraz ochrony informacji niejawnych i obsługi kancelaryjnej,
- planowanie i koordynowanie działania Sił Zbrojnych RP w sytuacjach kryzysowych,
- opracowywanie dokumentów normatywnych Ministerstwa Obrony Narodowej oraz monitorowanie realizacji zadań z zakresu zarządzania kryzysowego przez jednostki i komórki organizacyjne resortu obrony narodowej,
- monitorowanie działalności szkoleniowo-operacyjnej wojsk, uczestniczenie w systemie meldowania o wypadkach i rażących naruszeniach dyscypliny wojskowej oraz uruchamianie procedur w zakresie aktywowania sił i środków wydzielonych z Sił Zbrojnych RP w sytuacjach kryzysowych,
- zapewnienie wymiany informacji z wojskowymi strukturami dowodzenia oraz zarządzania kryzysowego Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej.

Zadanie utworzenia Centrum powierzono Szefowi Sztabu Generalnego Wojska Polskiego.

W przeciwdziałaniu zagrożeniom niemilitarnym oraz w przypadku potrzeby usuwania skutków katastrof i klęsk żywiołowych Siły Zbrojne są w gotowości do użycia ponad 20 tys. żołnierzy, w tym wyposażone w odpowiedni sprzęt wyspecjalizowane pododdziały[124], których zadania przedstawiono w tabeli 83.

Podstawę do wydzielenia sił i środków Sił Zbrojnych RP stanowi *Plan użycia oddziałów i pododdziałów Sił Zbrojnych RP w przypadku wystąpienia sytuacji kryzysowych*, który zawiera procedury, organizację łączności, zasady aktywacji, a także w formie załączników rejestr zagrożeń oraz procedury działań podejmowanych przez Siły Zbrojne RP w przypadku wystąpienia sytuacji kryzyso-

[121] Dz. U. Nr 89, poz. 590, z późn. zm.

[122] Dz. U. z 1996 r. Nr 94, poz. 426 z późn. zm.

[123] Dz. Urz. MON z 2010 r. Nr 14, poz. 183.

[124] W. Lidwa, W. Krzeszowski, W. Więcek, op. cit., s. 87.

wych oraz szczegółowe plany udziału pododdziałów i oddziałów Sił Zbrojne RP w przypadku wystąpienia sytuacji kryzysowych: w obronie przed terroryzmem, w zwalczaniu powodzi i zjawisk lodowych, w akcji odśnieżania, w akcjach ratowniczo-gaśniczych i usuwaniu skutków pożarów przestrzennych, w likwidacji skutków awarii technicznych z TŚP i wypadków radiacyjnych, w akcjach poszukiwawczo-ratowniczych, w oczyszczaniu terenu z przedmiotów wybuchowych i niebezpiecznych, w działaniach przeciwepidemicznych[125].

Tabela 84. Zadania wyspecjalizowanych pododdziałów biorących udział w usuwaniu skutków katastrof i klęsk żywiołowych

Nazwa pododdziału	Zadania
pododdziały ratownictwa inżynieryjnego	prowadzenie akcji ewakuacyjno-ratunkowych i prac drogowo-inżynieryjnych podczas usuwania skutków klęsk żywiołowych
zespoły rozpoznania biologicznego	rozpoznawanie rodzaju środka biologicznego i oznaczanie granic rejonu objętego działaniem tego czynnika
chemiczno-radiacyjne zespoły awaryjne	usuwanie skutków oddziaływania toksycznych środków przemysłowych (TŚP) i bojowych środków trujących (BŚT) oraz prowadzenie prac odkażających i dezaktywujących, środki chemiczne i radiacyjne
grupy ratownictwa lotniczego	ratowanie życia załóg lotniczych środków wojskowych, jak również udzielanie pomocy w przypadku wystąpienia wypadków lotnictwa cywilnego
grupy naziemnego poszukiwania	wspieranie akcji poszukiwawczo-ratowniczych
minerskie patrole oczyszczania	rozpoznawanie i unieszkodliwianie sprzętu, amunicji oraz przedmiotów wybuchowych niewiadomego pochodzenia

Źródło: W. Lidwa, W. Krzeszowski, W. Więcek, *Zarządzanie w sytuacjach kryzysowych*, Warszawa 2010, s. 87

Plan użycia pododdziałów i oddziałów Sił Zbrojnych RP w przypadku wystąpienia sytuacji kryzysowych jest aktualizowany raz na dwa lata i stanowi podstawowy dokument do opracowania planów szczegółowych. Z kolei w planach szczegółowych uwzględnia się zagrożenia, regulacje prawne dotyczące udziału Sił Zbrojnych w działaniach w zarządzaniu kryzysowym. Plany te zawierają zadania, procedury użycia odpowiednich sił i środków, sposoby działania, zabezpieczenie logistyczne działań, zakres współpracy, wykaz ilościowy sił i środków przeznaczonych do tych działań.

Zgodnie z obowiązującymi przepisami Siły Zbrojne RP mogą także działać poza granicami państwa. Użycie Sił Zbrojnych poza granicami państwa oznacza obecność jednostki wojskowej poza granicami państwa w celu udziału w konflikcie zbrojnym lub dla wzmocnienia sił państwa oraz państw sojuszniczych, misji pokojowej i akcji zapobieżenia aktom terroryzmu lub ich skutkom. Pobyt Sił Zbrojnych Rzeczypospolitej Polskiej poza granicami państwa oznacza obecność jednostki wojskowej poza granicami państwa w celu udziału w szkoleniach i ćwiczeniach wojskowych, akcjach ratowniczych, poszukiwawczych lub humanitar-

[125] Ibidem, s. 87 i 88.

nych; przepisu tego nie stosuje się do akcji ratowniczych regulowanych przepisami o ratownictwie na morzu oraz w przedsięwzięciach reprezentacyjnych.

Należy podkreślić, że wykorzystanie potencjału Siła Zbrojnych do działań w sytuacjach kryzysowych tak w państwie, jak i poza jego granicami wymaga spełnienia wielu warunków, do których należy zaliczyć: właściwe regulacje prawne, finanse, wydzielenie odpowiednich sił i środków, wyszkolenie, system alarmowania, system kierowania i kolejności ich użycia.

Specyfika wojska, przede wszystkim wysoki poziom wyszkolenia żołnierzy, utrzymywanie jednostek w gotowości do podjęcia działań oraz wyposażenie w dobry, specjalistyczny sprzęt powoduje, że instytucje cywilne bardzo chętnie korzystają z jego usług. Zauważalne jest to w polskim systemie prawnym, w którym znaleźć można wiele norm pozwalających na wykorzystanie wojska do realizacji zróżnicowanych zadań.

Do przepisów prawa regulujących użycie wojska w sytuacjach innych niż w opisanych powyżej zalicza się:

– ustawę z dnia 6 kwietnia 1990 roku *o Policji*[126],
– ustawę z dnia 12 października 1990 roku *o Straży Granicznej*[127],
– ustawę z dnia 12 października 1990 roku *o ochronie granicy państwowej*[128],
– ustawę z dnia 24 sierpnia 1991 roku *o Państwowej Straży Pożarnej*[129],
– ustawę z dnia 29 listopada 2000 roku *Prawo atomowe*[130],
– ustawę z dnia 8 września 2006 roku *o Państwowym Ratownictwie Medycznym*[131],
– rozporządzenie Rady Ministrów z dnia 14 grudnia 2004 roku *w sprawie postępowania przy stosowaniu środków obrony powietrznej w stosunku do obcych statków powietrznych niestosujących się do wezwań państwowego organu zarządzania ruchem lotniczym*[132],
– rozporządzenie Rady Ministrów z dnia 19 lipca 2005 roku *w sprawie szczegółowych warunków i sposobu użycia oddziałów i poddziałów Policji oraz Sił Zbrojnych Rzeczypospolitej Polskiej w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego*[133],
– rozporządzenie Rady Ministrów z dnia 16 października 2006 roku *w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach*[134].

126 T. j.: Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.

127 Dz. U. z 2011 r. Nr 116, poz. 675 z późn. zm.

128 Dz. U. z 2005 r. Nr 226, poz. 1944 z późn. zm.

129 T. j.: Dz. U. z 2009 r. Nr 12, poz. 68 z późn. zm.

130 T. j.: Dz. U. z 2004 r. Nr 161, poz. 1689 z późn. zm.

131 Dz. U. z 2006 r. Nr 191, poz. 1410 z późn. zm.

132 Dz. U. z 2004 r. Nr 279, poz. 2757.

133 Dz. U. z 2005 r. Nr 131, poz. 1134.

134 Dz. U. z 2006 r. Nr 191, poz. 1415.

ROZDZIAŁ 9

Inni uczestnicy zarządzania kryzysowego

9.1. Policja

Policja jest uzbrojoną i umundurowaną formacją służącą społeczeństwu i przeznaczoną do ochrony bezpieczeństwa ludzi oraz do utrzymania bezpieczeństwa i porządku publicznego[1]. Ta ogólna dyspozycja w odniesieniu do działań w sytuacjach kryzysowych została przełożona na poziom wykonawczy, co zostało uszczegółowione w zarządzeniach Komendanta Głównego Policji. Podstawę prawną działania Policji stanowi ustawa z dnia 6 kwietnia 1990 roku *o Policji*. Centralnym organem administracji rządowej właściwym w sprawach ochrony bezpieczeństwa ludzi oraz utrzymania bezpieczeństwa i porządku publicznego jest Komendant Główny Policji, który podlega Ministrowi Spraw Wewnętrznych[2]. W granicach swoich uprawnień Policja w celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń wykonuje czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-procesowe[3]. W systemie zarządzania kryzysowego podstawowym zadaniem Policji jest chronić ludność przed skutkami klęsk żywiołowych i katastrof.

Organami administracji rządowej na obszarze województwa w sprawach, o których mowa wyżej, są:

- wojewoda przy pomocy komendanta wojewódzkiego Policji działającego w jego imieniu albo komendant wojewódzki Policji działający w imieniu własnym w sprawach:
  - wykonywania czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych i z zakresu ścigania wykroczeń,
  - wydawania indywidualnych aktów administracyjnych, jeżeli ustawy tak stanowią,
- komendant powiatowy (miejski) Policji,
- komendant komisariatu Policji[4].

1 Ustawa z dnia 6 kwietnia 1990 roku *o Policji* (T. j.: Dz. U. z 2007 r. Nr 43, poz. 277 z późn. zm.), art. 1 ust. 1.

2 Ibidem, art. 5 ust. 1.

3 Ibidem, art. 14 ust. 1.

4 Ibidem, art. 6 ust. 1.

Zadania i obowiązki podstawowych elementów bezpieczeństwa wewnętrznego państwa są realizowane przez centralne organy administracji rządowej podporządkowane Ministrowi Spraw Wewnętrznych. W zależności od rodzaju zdarzenia (pożar, katastrofa, wypadek drogowy, akt terroryzmu, niepokoje społeczne itp.) odpowiedni system (formacja) przejmuje organizację i kierowanie działaniami. Podstawowe elementy systemu bezpieczeństwa wewnętrznego państwa to:

- Krajowy System Ratowniczo-Gaśniczy, funkcjonujący w oparciu o siły i środki Państwowej Straży Pożarnej i Ochotniczej Straży Pożarnej,
- System Utrzymania Ładu i Porządku Publicznego, opierający się na siłach i środkach Policji,
- System Zabezpieczenia i Ochrony Granic, którego bazę stanowi Straż Graniczna,
- System Alarmowania i Ostrzegania Ludności, w którym najważniejszą rolę odgrywają formacje Obrony Cywilnej.

Poszczególne systemy stanowią integralną część bezpieczeństwa wewnętrznego państwa i są zobowiązane do współpracy z innymi systemami, do których należą Wojskowe Systemy Ratownicze obejmujące ratownictwo ogólne oraz specjalistyczne, np. w zakresie likwidacji materiałów wybuchowych, Resortowe Systemy Ratownicze obejmujące ratownictwo górnicze (Stacje Ratownictwa Górniczego), kolejowe (Techniczne Służby PKP), morskie (Polskie Ratownictwo Okrętowe), radiacyjne (Państwowa Agencja Atomistyki), medyczne (Państwowe Ratownictwo Medyczne), Społeczne Systemy Ratownicze obejmujące ratownictwo górskie i jaskiniowe (Górskie Ochotnicze Pogotowie Ratunkowe, Tatrzańskie Ochotnicze Pogotowie Ratunkowe), medyczne (Polski Czerwony Krzyż) i wodne (Wodne Ochotnicze Pogotowie Ratunkowe)[5].

Policja w sytuacjach zagrożenia wykonuje czynności ochronno-porządkowe, czyli przedsięwzięcia organizacyjno-taktyczne w celu ochrony bezpieczeństwa i porządku publicznego, w tym zapewnienia spokoju w miejscach publicznych, w środkach transportu publicznego i komunikacji publicznej. Są one realizowane na podstawie opracowanych planów określających formy i metody stosowane w sytuacjach kryzysowych lub wykonywane doraźnie. W ramach tych czynności Policja zajmuje się izolowaniem miejsca akcji ratowniczej, zabezpieczenia mienia, ewakuacją ludności, organizacją ruchu drogowego[6].

W trakcie prowadzenia działań ratowniczych zadaniem Policji jest m.in.: pilnowanie porządku w rejonie prac, niedopuszczenie do tworzenia się skupisk obserwatorów i powstawania paniki, oznakowanie obszaru prowadzenia działań ratowniczych. Istotnym zadaniem w sytuacjach katastrof, awarii i innych zagrożeń jest zapewnienie warunków płynnego i niezakłóconego ruchu drogowego dla jednostek ratowniczych (pilotowanie kolumn pojazdów, zorganizowanie

[5] H. Tokarski, *Dowodzenie jednostkami Policji w sytuacjach kryzysowy*ch – http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/BEZPIECZENSTWO/Tokarskic.pdf [pobrano 27.02.2012].

[6] *Współczesny wymiar funkcjonowania policji*, red. B. Wiśniewski, Z. Piątek, Warszawa 2009, s. 90.

objazdów). W sytuacjach zagrożeń Policja podejmuje także działania ratownicze w przypadkach nieobecności służb, których zadaniem jest udzielanie pomocy.

Natomiast czynności dochodzeniowo-śledcze podejmowane w sytuacjach kryzysowych obejmują: oględziny miejsca zdarzenia, zabezpieczenie śladów, przesłuchanie świadków, identyfikację ofiar, analizę przyczyn wystąpienia zdarzenia.

W zarządzaniu kryzysowym Policja analogicznie jak inne służby ratownicze realizuje zadania w czterech fazach: zapobiegania, przygotowania, reagowania i odbudowy[7].

W zarządzaniu kryzysowym istotną rolę odgrywa sztab Policji, który jest komórką organizacyjną o charakterze pomocniczym i wykonawczym dowódcy operacji z zakresem zadań dostosowanych do rodzaju operacji. W zakresie ochrony strefy działań ratowniczych kierownicy jednostek Policji zapewniają ochronę porządku w miejscach prac ekip ratowniczych oraz zabezpieczenie miejsc, które mogą stwarzać dodatkowe źródła zagrożenia dla bezpieczeństwa ludzi[8].

Na poziomie krajowym za realizację zadań związanych z zarządzaniem kryzysowym odpowiedzialny jest Główny Sztab Policji, i tak:

- kierownicy wszystkich jednostek organizacyjnych Policji są obowiązani do stosowania procedur zarządzania kryzysowego oraz ich bieżącego aktualizowania, stosownie do aktualnego stanu prawnego,
- kierownicy wszystkich jednostek organizacyjnych Policji, stosownie do potrzeb, uszczegóławiają i dostosowują procedury do zakresu działania i kompetencji poszczególnych i podległych komórek organizacyjnych[9].

Zadania Głównego Sztabu Policji zostały określone w Zarządzeniu Nr 2 Komendanta Głównego Policji z dnia 17 stycznia 2006 roku *w sprawie regulaminu Komendy Głównej Policji*[10]. Do zadań Głównego Sztabu Policji należy:

- opracowywanie procedur i planów operacyjnych,
- przygotowanie zasobów do reagowania w sytuacjach kryzysowych (w warunkach zewnętrznych zagrożeń bezpieczeństwa państwa i wojny, zarządzania działaniami Policji, w tym o zasięgu ogólnokrajowym w warunkach zagrożenia bezpieczeństwa i porządku publicznego.

Skład sztabu określa się już w planie zamierzonej operacji policyjnej, a jego struktura składa się z następujących ogniw: szefa sztabu, rozpoznawczo-informacyjnego, taktycznego, analityczno-sprawozdawczego, materiałowo-technicznego[11]. Rozmiar sił zaangażowanych w operację, jej rodzaj, a zwłaszcza stojące przed nią cele determinują stan osobowy sztabu, w tym rodzaj i ilość ogniw.

[7] Rozporządzenie Rady Ministrów z dnia 3 grudnia 2002 r. *w sprawie sposobu tworzenia gminnego zespołu reagowania, powiatowego, wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji Kryzysowej i ich koordynacji* (Dz. U. z 2002 r., Nr 215, poz. 1818).

[8] *Współczesny wymiar funkcjonowania Policji*, red. B. Wiśniewski, Z. Piątek, Warszawa 2009, s. 91.

[9] Zarządzenie Nr 1429 Komendanta Głównego Policji z dnia 31 grudnia 2004 roku *w sprawie wprowadzenia w Policji procedur reagowania w sytuacjach kryzysowych* (Dz. Urz. KGP z 2006 r. Nr 2, poz. 8).

[10] Ibidem.

[11] H. Tokarski, op. cit.

Sztab przygotowuje wszelkie materiały niezbędne dowódcy operacji do podjęcia decyzji, nadaje jego decyzjom odpowiednią formę, organizuje przekazanie decyzji wykonawcom oraz nadzoruje ich wykonanie. Poza wymienionymi funkcjami spełnia również zadanie precyzowania decyzji dowódcy w ramach swych uprawnień[12]. Taka konstrukcja sztabu nie narusza zasady jednoosobowego dowodzenia i odpowiedzialności. W zależności od potrzeb, jeżeli wymaga tego sytuacja operacyjna, dowódca organizuje wysunięte lub ruchome stanowisko dowodzenia. Jest to odpowiednio przygotowane miejsce, pomieszczenie lub pojazd w rejonie działań, co usprawnia proces dowodzenia.

Struktura sztabu Policji na szczeblu Komendy Głównej Policji (KGP) i Komendy Wojewódzkiej Policji (KWP)

Sytuacje kryzysowe, których rodzaj wymaga działań aktywnych ze strony Policji jako formacji właściwej do ich rozwiązania (samodzielnie lub współdziałając z innymi służbami bądź instytucjami), z istoty rzeczy rodzą potrzebę działań szczególnych, czasem nieporównywalnych z rutynowymi, zwłaszcza zaś użycia znacznych sił i środków, w tym także niestandardowych. Stąd też dowodzenie tymi środkami i ich użycie rodzi zapotrzebowanie na wsparcie. W tym celu w Komendzie Głównej Policji i Komendach Wojewódzkich oraz Komendzie Stołecznej Policji powołuje się sztaby, czyli komórki organizacyjne wspierające kierowanie siłami policyjnymi w ramach całego systemu zarządzania kryzysowego w państwie lub na części jego terytorium.

Generalnie na szczeblu centralnym organem dowodzącym siłami policyjnymi w ramach zarządzania kryzysowego jest Komendant Główny Policji, a na szczeblu wojewódzkim Komendant Wojewódzki Policji. Zatem odpowiednio powołuje się sztaby Komendanta Głównego Policji i Komendanta Wojewódzkiego (Stołecznego) Policji.

Standardowo w skład sztabu Komendanta Głównego Policji powinni wchodzić: kierownik (szef sztabu) – wyznaczony przez Komendanta Głównego Policji, zastępca szefa sztabu, członkowie sztabu, reprezentujący odpowiednie służby stosownie do potrzeb, Naczelny Lekarz Kraju, jeśli istnieje taka potrzeba[13]. Natomiast w skład sztabu Komendanta Wojewódzkiego Policji powinni wchodzić: kierownik (szef sztabu) – wyznaczony przez Komendanta Wojewódzkiego Policji, zastępca szefa sztabu, członkowie sztabu, policjanci KWP reprezentujący służby i specjalności w zależności od potrzeb, przedstawiciele służb i innych podmiotów współdziałających z Policją, przedstawiciele organów administracji rządowej i samorządowej oraz organizacji społecznych współuczestniczących w działaniach, Lekarz Wojewódzki, jeśli istnieje taka potrzeba.

W celu pozyskiwania informacji o stanie bezpieczeństwa i porządku publicznego na terenie kraju oraz monitorowania i koordynowania działań policyjnych Komendant Główny Policji Zarządzeniem nr 1401/2004 z dnia 16 grudnia 2004

[12] M. Dąbrowski, J. Gampf, *Wybrane zagadnienia pracy sztabowej w Policji*, Szczytno 2004, s. 8–9.

[13] Ibidem, s. 14–15.

roku *w sprawie utworzenia w Komendzie Głównej Policji Centrum Operacyjnego Komendanta Głównego Policji*[14] utworzył w Komendzie Głównej Policji Centrum Operacyjne Komendanta Głównego Policji.

Zadania Centrum Operacyjnego Komendanta Głównego Policji:

- systematyczne analizowanie uzyskiwanych informacji o stanie bezpieczeństwa i porządku publicznego oraz aktualizowanie danych o siłach i środkach policyjnych wykorzystywanych do działań,
- ocena sytuacji i kalkulacja sił niezbędnych do utrzymania bezpieczeństwa i porządku publicznego,
- przyjmowanie meldunków o wydarzeniach, realizowanych przedsięwzięciach i podjętych decyzjach,
- weryfikacja zapotrzebowań na siły i środki zgłaszanych przez komendy wojewódzkie Policji,
- opracowywanie projektów decyzji, postanowień oraz innych dokumentów, w szczególności dotyczących wykonywania zadań oraz użycia sił,
- zapewnienie właściwego obiegu informacji,
- przekazywanie właściwym adresatom do wykonania decyzji podjętych przez kierownictwo KGP,
- współdziałanie z innymi zaangażowanymi instytucjami pozapolicyjnymi,
- prowadzenie dokumentacji rejestrującej przebieg działań.

Centrum jest nieetatowym ogniwem organizacyjnie podległym kierownikowi Biura KGP właściwego do spraw sztabowych. W aktualnej strukturze organizacyjnej jest to Biuro Głównego Sztabu Policji. Zgodnie z treścią cytowanego zarządzenia Centrum Operacyjne podejmuje działania zarówno w sytuacjach zarządzenia operacji, kiedy działa sztab Komendanta Głównego Policji, a także może być powołane w innych sytuacjach, kiedy sztab Komendanta Głównego nie został powołany. Jest uruchamiane w przypadku zagrożenia bezpieczeństwa i porządku publicznego na terenie kraju. Ogniwo to wspiera działania Komendanta Głównego Policji podejmującego działania w charakterze organu, niezależnie od tego czy w danym czasie została zarządzona operacja, ustanowiony jej dowódca oraz wspomagający jego czynności sztab.

Doskonalenie przygotowań Policji do działań w sytuacjach kryzysowych przedstawiono następująco:

- osiąganie przez Policję pełnej funkcjonalności w obowiązującym systemie zarządzania kryzysowego w państwie (KWP, KGP),
- unowocześnienie systemu kierowania Policją w ramach systemu kierowania bezpieczeństwem narodowym, stanowiska kierowania Policji w dotychczasowym i zapasowym miejscu pracy (KWP, KGP),
- doskonalenie współdziałania z siłami zbrojnymi i innymi systemu obronnego Rzeczypospolitej Polskiej poprzez wspólną realizację zadań w zakresie obronności RP, w tym w zakresie wykonywania zadań wsparcia przez państwo gospodarza – HNS (KGP),

[14] Dz. Urz. KGP z 2004 r. Nr 24, poz. 151.

- podnoszenie poziomu przygotowania oraz realizacji zadań w ramach przygotowań obronnych Policji (KWP, KGP),
- wypracowanie założeń do efektywnego wykorzystywania sił i środków Policji w sytuacji katastrof, klęsk żywiołowych, zbiorowego naruszenia porządku publicznego i działań pościgowych (KWP, KGP),
- podnoszenie poziomu organizacji pracy oraz realizowanie przedsięwzięć gwarantujących prawidłowe funkcjonowanie służby dyżurnej Policji (KWP, KGP),
- doskonalenie procedur oraz przygotowanie funkcjonariuszy do reagowania w sytuacjach zagrożenia terrorystycznego (KWP, KGP),
- wprowadzanie rozwiązań systemowych dotyczących funkcjonowania pododdziałów i oddziałów Policji, pozwalających na lepsze wykorzystanie zasobów (KGP),
- współdziałanie z pozostałymi służbami państwowymi, a także organami innych państw celem pozyskania najlepszych wzorców, wymiany informacji i doświadczeń, zharmonizowania wysiłków na rzecz ograniczania zagrożeń terrorystycznych (KGP),
- koordynowanie operacji policyjnych oraz podnoszenie standardów dowodzenia działaniami Policji, m.in. poprzez:
  - wypracowanie nowych założeń w ramach organizowania, koordynowania i zabezpieczenia imprez charakterze masowym (KGP),
  - zweryfikowanie i uzgodnienie zasad współdziałania oraz programów realizowanych z organami, agencjami i służbami państwowymi, przedstawicielami administracji państwowej i samorządowej oraz innymi podmiotami w zakresie poprawy bezpieczeństwa i porządku publicznego (KGP),
- organizowanie szkoleń, ćwiczeń sztabowych z udziałem podmiotów pozapolicyjnych oraz zaangażowanie organów administracji państwowej i samorządowej, w przypadku wystąpienia różnego rodzaju zagrożeń i sytuacji kryzysowych (KWP, KGP)[15].

W zależności od rodzaju i okoliczności zdarzenia, wobec którego wymagane jest działanie policyjne, wyodrębnione zostały trzy formy organizacyjne tych przedsięwzięć:

- interwencje – polegające na reagowaniu wobec określonych zdarzeń czy sytuacji przy użyciu tych sił i środków, którymi w danym czasie zarządza dyżurny właściwej terytorialnie jednostki Policji i są one optymalne w stosunku do zaistniałego zdarzenia,
- akcje – czyli działania relatywne w stosunku do zdarzenia, którego zakres przekracza możliwości sił i środków będących w dyspozycji dyżurnego jednostki, zarządza je Komendant Powiatowy (Miejski) Policji,
- operacje – czyli działania adekwatne do zaistniałej sytuacji, która wykracza poza obszar terytorialny jednej KPP lub KMP albo jej rozmiary i charakterystyka wymagają dłuższego oddziaływania i użycia większych sił i środków albo zorganizowania specjalnego zaplecza logistycznego.

[15] H. Tokarski, op. cit.

Operację zarządza Komendant Główny Policji, Komendant Wojewódzki Policji lub Komendant Powiatowy (Miejski) Policji w zależności od zasięgu terytorialnego sytuacji, która jest powodem jej zorganizowania. Ulokowanie odpowiednio wysoko ośrodka dowodzenia może być podyktowane także innymi względami. W ramach operacji mogą być podejmowane czynności dotyczące różnych zdarzeń lub specyficznych i różnorodnych zadań operacji, jeśli dotyczą zasadniczego celu operacji. Takie działanie obejmuje się odpowiednimi podoperacjami.

Dowodzenie operacją polega na:

- ocenie zagrożenia poprzez ustalenie jego rodzaju i przewidywanego rozwoju,
- określeniu oraz koncentracji sił i środków niezbędnych do usunięcia zagrożenia,
- zorganizowaniu stacjonarnego lub ruchomego stanowiska dowodzenia i sztabu,
- zorganizowaniu systemów łączności i obiegu informacji,
- wyznaczeniu dowódców podoperacji i określeniu ich zadań,
- koordynowaniu przygotowania zaplecza logistycznego, medycznego i technicznego,
- nadzorowaniu i koordynowaniu przebiegu operacji zgodnie z planem działania dowódcy,
- wyznaczeniu policjanta uprawnionego do kontaktów ze środkami masowego przekazu w zakresie przebiegu operacji,
- współdziałaniu ze służbami specjalistycznymi i instytucjami właściwymi dla rodzaju zdarzenia oraz z właściwymi terytorialnie organami administracji publicznej,
- przygotowywaniu i przekazywaniu właściwemu przełożonemu meldunków o sytuacji i realizowanych działaniach[16].

Policja jest ważnym elementem w krajowym systemie rozpoznawania, przeciwdziałania i reagowania na przestępstwa o charakterze terrorystycznym. W jej skład wchodzą wyspecjalizowane jednostki organizacyjne obejmujące zakresem swoich działań m.in.:

- fizyczne zwalczanie przestępstw o charakterze terrorystycznym, w tym prowadzenie negocjacji policyjnych – Biuro Operacji Antyterrorystycznych Komendy Głównej Policji[17],
- rozpoznawanie operacyjne przestępczości o charakterze terrorystycznym – Centralne Biuro Śledcze Komendy Głównej Policji[18],
- zabezpieczanie imprez masowych, nadzór nad bezpieczeństwem obiektów infrastruktury krytycznej – Główny Sztab Policji Komendy Głównej Policji,

[16] M. Dąbrowski, J. Gampf, op. cit., s. 23.

[17] Decyzja nr 372 z dnia 14 kwietnia 2008 r. Komendanta Głównego Policji *w sprawie zmiany regulaminu Komendy Głównej Policji*.

[18] Zarządzenie nr 749 Komendanta Głównego Policji z dnia 27 maja 2010 roku *w sprawie zmiany regulaminu Komendy Głównej Policji* (Dz. Urz. Komendy Głównej Policji z 2010 r. Nr 6, poz. 20), § 29 ust. 1.

- edukację społeczną na rzecz przeciwdziałania przestępczości, w tym zagrożeniom o charakterze terrorystycznym – funkcjonariusze służby prewencyjnej jednostek policji na szczeblu komend wojewódzkich policji/Komendy Stołecznej Policji oraz komend miejskich/rejonowych i powiatowych policji – Biuro Prewencji Komendy Głównej Policji.

Ponadto w Policji zadania w ramach operacji antyterrorystycznych realizują: Samodzielne Pododdziały Antyterrorystyczne Policji Komendy Wojewódzkiej w Gdańsku, Białymstoku, Wrocławiu, Łodzi, Szczecinie, Poznaniu, Krakowie, Katowicach, Rzeszowie, Sekcje Antyterrorystyczne Komendy Wojewódzkiej Policji w Lublinie, Olsztynie, Bydgoszczy, Kielcach, Opolu, Gorzowie Wielkopolskim i Radomiu[19].

Konieczność zapewnienia optymalnej sprawności i efektywności w zarządzaniu siłami i środkami w sytuacjach kryzysowych w państwie wymaga szczególnych rozwiązań odnoszących się do całej administracji oraz poszczególnych jej działów. Wymóg ten dotyczy wszystkich służb państwowych, a szczególnie Policji, która dysponuje największym potencjałem, zwłaszcza ludzkim. Jest także wyposażona w szerokie kompetencje i zakres obowiązków. Stąd w zasadzie w każdej sytuacji kryzysowej jej udział jest wymagalny. Podejmowane w takich sytuacjach działania będą przebiegały w formie operacji policyjnych organizowanych na szczeblu Komend Głównej i Wojewódzkich Policji.

W sytuacjach, o których mowa, zmieniają się zadania Policji tak pod względem ilościowym, jak i jakościowym. Z tych względów:

- powstaje nieadekwatność standardowo używanych sił i środków Policji w stosunku do zwiększonych zadań,
- struktury organizacyjne jednostek Policji spełniające swoje funkcje w normalnych warunkach stają się niewystarczające,
- istnieje uzasadniona potrzeba użycia do działań znacznie większych sił, często też innych jakościowo, co z reguły wiąże się z koniecznością ich przemieszczania,
- zachodzi konieczność powołania doraźnych struktur, w tym zwłaszcza wspomagających, dowodzenie, to jest sztabów wykonujących zadania na rzecz dowódców operacji[20].

Wymienione czynniki stwarzają więc określone problemy w funkcjonowaniu systemu kierowania i dowodzenia przystosowanego do działania w normalnych warunkach. Zatem niezwykle ważne staje się wówczas rozbudowanie istniejącego systemu dowodzenia, przez który należy rozumieć uporządkowaną zgodnie z zasadami kierowania (dowodzenia) siłami Policji w sytuacjach kryzysowych (szczególnych) całość złożoną z organów i środków dowodzenia sprzężonych ze sobą informacyjnie i zapewniającą podejmowanie stosownych decyzji na wszystkich szczeblach organizacyjnych sił Policji oraz ich sprawną, terminową i bezwzględną realizację[21].

[19] *Współczesny wymiar…*, s. 116.

[20] H. Tokarski, op. cit.

[21] M. Dąbrowski, *Działania Policji podczas niebezpiecznego zbiorowego naruszenia porządku publicznego*, Szczytno 2004, s. 5.

Trudno jest zakładać powodzenie operacji policyjnej bez sprawnego zarządzania tego rodzaju przedsięwzięciem, a to w przeważającej mierze warunkuje profesjonalny i sprawny system dowodzenia.

Skuteczność działania Policji w zarządzaniu kryzysowym wymaga określenia zakresu i zasad współpracy z innymi uprawnionymi podmiotami w tej dziedzinie. Zadania związane z zarządzaniem kryzysowym Policja realizuje wspólnie z Siłami Zbrojnymi Rzeczypospolitej Polskiej, Żandarmerią Wojskową, Strażą Graniczną, Państwową Strażą Pożarną, Strażą Ochrony Kolei, Pogotowiem Ratunkowym i innymi.

9.2. Straż Graniczna

Do ochrony granicy państwowej na lądzie i na morzu oraz kontroli ruchu granicznego utworzona została Straż Graniczna (SG). Podstawą prawną działania Straży Granicznej jest ustawa z dnia 12 października 1990 roku *o Straży Granicznej*[22]. Straż Graniczna jako jednolita, umundurowana i uzbrojona formacja[23] stanowi w ramach resortu spraw wewnętrznych jedno z ogniw ochronnych podsystemu pozamilitarnego w systemie obronnym państwa. Centralny organem administracji rządowej właściwym w sprawach ochrony granicy państwowej i kontroli ruchu granicznego jest Komendant Straży Granicznej, który podlega Ministrowi Spraw Wewnętrznych.

Należy podkreślić, że od 1 maja 2004 roku na Straży Granicznej spoczywa znacznie większa odpowiedzialność za bezpieczeństwo nie tylko granic RP, lecz także w ograniczonym zakresie Unii Europejskiej[24]. Polska jest odpowiedzialna za ochronę najdłuższego odcinka zewnętrznej granicy Unii Europejskiej (1185,47 km) z Federacją Rosyjską, Republiką Białorusi i Ukrainą[25].

Podstawowym zadaniem Straży Granicznej[26] jest ochrona granicy państwowej oraz organizowanie i dokonywanie kontroli ruchu granicznego, w tym wydawanie zezwoleń na przekraczanie granicy, łącznie z wizami. Straż Graniczna wykonuje także zadania związane z rozpoznawaniem, zapobieganiem i wykrywaniem przestępstw oraz wykroczeń objętych zakresem właściwości tej służby, jak również ściganie ich sprawców[27]. Ponadto Straż Graniczna wykonuje zadania

22 T. j.: Dz. U. z 2011 r. Nr 116, poz. 675.

23 Ibidem, art. 1 ust. 1.

24 *Współczesny wymiar…*, s. 23.

25 Ibidem, s. 27.

26 Ustawa z dnia 12 października 1990 roku *o Straży Granicznej* (T. j.: Dz. U. z 2011 r. Nr 116, poz. 675) art. 1 ust. 2.

27 Ibidem, art. 1 ust. 2 pkt 4.

dotyczące bezpieczeństwa w komunikacji międzynarodowej i porządku publicznego w zasięgu terytorialnym przejścia granicznego, jak również w strefie nadgranicznej[28].

> Straż Graniczna, zgodnie z przypisanymi jej zadaniami, przeciwdziała transportowaniu przez granicę państwową odpadów, szkodliwych substancji chemicznych oraz materiałów jądrowych i promieniotwórczych bez zezwolenia wymaganego w myśl odrębnych przepisów, a także zanieczyszczania wód granicznych. Zapobiegać ma także nielegalnemu przemieszczaniu przez granicę środków odurzających i substancji psychotropowych oraz broni, amunicji i materiałów wybuchowych[29].

Zadania Straży Granicznej określają także ustawy o stanach nadzwyczajnych:

- art. 17 ustawy z dnia 18 kwietnia 2002 roku *o stanie klęski żywiołowej*[30] stanowi: w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu uczestniczy Straż Graniczna,
- art. 21 ustawy z dnia 21 czerwca 2002 roku *o stanie wyjątkowym*[31] stanowi: w czasie stanu wyjątkowego Straż Graniczna ma prawo złożyć wniosek do właściwego wojewody o wszczęcie postępowania o odosobnienie osoby pełnoletniej, w stosunku do której zachodzi uzasadnione podejrzenie, że będąc na wolności będzie prowadziła działalność, która zagraża państwu, bezpieczeństwu obywateli i porządkowi publicznemu, albo gdy odosobnienie jest konieczne, aby zapobiec popełnienia czynu karalnego lub uniemożliwić ucieczkę po jego popełnieniu,
- art. 28 ustawy z dnia 29 sierpnia 2002 roku *o stanie wojennym oraz kompetencjach naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*[32] stanowi, że czasie stanu wojennego można:
  - zamykać lub ograniczać ruch osobowy i towarowy przez przejścia graniczne,
  - wprowadzić szczególne zasady wydawania dokumentów uprawniających obywateli polskich do przekraczania granicy państwowej,
  - wprowadzić szczególne zasady wydawania dokumentów uprawniających cudzoziemców do przekraczania granicy państwowej oraz przebywania na terytorium Rzeczypospolitej Polskiej.

Powyższe ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniu wprowadza i stosuje, w drodze rozporządzenia, minister właściwy do spraw wewnętrznych w porozumieniu z ministrem właściwym do spraw zagranicznych i Ministrem Obrony Narodowej, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń.

[28] Ustawa z dnia 12 października 1990 r. *o ochronie granicy państwowej* (Dz. U. z 1990 r. Nr 78, poz. 461 z późn. zm.).

[29] Ustawa z 12 października 1990 roku *o Straży Granicznej* (T. j.: Dz. U. z 2011 r. Nr 116, poz. 675) art. 1 ust. 2 pkt 13 i 14.

[30] Dz. U. z 2002 r. Nr 62, poz. 558 z późn. zm.

[31] Dz. U. z 2002 r. Nr 113, poz. 985 z późn. zm.

[32] Dz. U. z 2002 r. Nr 156, poz. 1301 z późn. zm.

Proces zarządzania kryzysowego w Straży Granicznej obejmuje następujące etapy działania:

- zapobieganie, działania eliminujące lub redukujące prawdopodobieństwo wystąpienia danego zagrożenia oraz ograniczające jego skutki,
- przygotowanie, planowanie, w jaki sposób i jakimi środkami należy reagować w razie wystąpienia zagrożenia,
- reagowanie, dążenie do maksymalnego ograniczenia skutków zagrożenia oraz niesienie pomocy poszkodowanym,
- odbudowa, mająca na celu przywrócenie stanu poprzedniego lub lepszego niż stan poprzedni[33].

W czasie wystąpienia sytuacji kryzysowych struktury organizacyjne Straży Granicznej wykonują zadania przedstawione w tabeli 85.

Tabela 85. Zadania wykonywane przez struktury Straży Granicznej w czasie sytuacji kryzysowych

Struktury	Zadania
Placówki Straży Granicznej	planowanie, organizowanie i koordynowanie działań organizacja zabezpieczenia logistycznego dokonywanie odprawy granicznej zgłoszonych środków pomocowych pomoc przy zapewnieniu warunków bytowych poszkodowanym (uchodźcom) udział w likwidacji skutków kryzysu
Oddziały Straży Granicznej	określanie operacyjnych kierunków działań planowanie, organizowanie i koordynowanie wzmocnienia działań (uruchomienie sił specjalistycznych lub własnych sił odwodowych) planowanie, organizowanie i koordynowanie współdziałania z innymi podmiotami
Komenda Główna Straży Granicznej	nadzorowanie, organizacja i koordynacja działań prowadzonych w terenie planowanie, organizowanie i koordynowanie współdziałania oddziałów straży granicznej z innymi podmiotami logistyczne zabezpieczenie operacji dysponowanie odwodem centralnego podporządkowania Komendanta Głównego wystąpienie o wzmocnienie przez policję, siły zbrojne, zgodnie z zawartymi porozumieniami

Źródło: *Współczesny wymiar funkcjonowania Straży Granicznej*, red. B. Wiśniewski, Z. Piątek, Warszawa 2006, s. 79

Straż Graniczna realizuje również czynności związane z rozpoznawaniem i przeciwdziałaniem zagrożeniom terrorystycznym. Działania wyspecjalizowanych komórek organizacyjnych Straży Granicznej w walce z terroryzmem przestawiono następująco:

- zapobieganie nielegalnemu przekroczeniu granicy państwowej przez osoby i pojazdy, zapobieganie i wykrywanie przestępstw i wykroczeń oraz ściga-

[33] *Współczesny wymiar…*, s. 79.

nie ich sprawców, a w szczególności przestępstw pozostających w związku z przekraczaniem granicy państwowej,

- przeciwdziałanie przemytowi materiałów wybuchowych, broni i amunicji, materiałów promieniotwórczych (przejścia graniczne wyposażone są w urządzenia do wykrywania promieniowania jonizującego, niebezpiecznych środków chemicznych, towarów podwójnego zastosowania (stosuje się przy tym dodatkowe formy wtórnej kontroli bezpieczeństwa przy wykorzystaniu psów służbowych i testerów do określania składu chemicznego przewożonych substancji),
- zapewnienie bezpieczeństwa w międzynarodowej komunikacji lotniczej poprzez prowadzenie kontroli bezpieczeństwa pasażerów, bagaży, ładunków i statków powietrznych realizujących loty wysokiego ryzyka oraz prowadzenia działań minersko-pirotechnicznych,
- wykonywanie wart ochronnych na pokładach samolotów,
- utrzymanie ładu i porządku publicznego w zasięgu terytorialnym przejść granicznych, w tym poprzez ochronę obiektów należących lub użytkowanych przez Straż Graniczną przed aktami terrorystycznymi,
- zabezpieczanie imprez masowych i ochronie obiektów infrastruktury krytycznej,
- ochrona szlaków komunikacyjnych,
- monitorowanie środowisk i skupisk cudzoziemców i ich przestępczej aktywności na terytorium RP,
- gromadzenie, przetwarzanie i analizowanie informacji dotyczących potencjalnych zagrożeń terroryzmem,
- realizacja czynności operacyjno-rozpoznawczych w zakresie rozpoznawania i przeciwdziałania zagrożeniu terroryzmem,
- współdziałanie w zakresie przeciwdziałania zagrożeniom terrorystycznym z Agencją Bezpieczeństwa Wewnętrznego, Agencją Wywiadu, Policją, Służbą Kontrwywiadu Wojskowego, Służbą Wywiadu Wojskowego i Żandarmerią Wojskową oraz z organami ochrony granicy[34].

Ustawowe zadania w zakresie ochrony granicy państwowej Straż Graniczna realizuje w okresie pokoju. W przypadku narastania napięć, powstania kryzysu lub rozpoczęcia działań wojennych realizować ona będzie zadania okresu pokojowego, odpowiednio poszerzone o te zadania, które są przewidziane do wykonania w przygotowanych planach w ramach współdziałania z Siłami Zbrojnymi RP. Wspólne wykonywanie zadań w sytuacji zagrożenia bezpieczeństwa państwa lub wojny Straży Granicznej z jednostkami Sił Zbrojnych RP wymaga współdziałania także w czasie pokoju, m.in. w zakresie określenia terminów i miejsca realizacji wspólnych zadań, określenia sposobów i zakresu wymiany informacji, a także określenia zakresu udzielania wzajemnej pomocy w sytuacjach

[34] Opracowano na podstawie ustawy z dnia 12 października 1990 roku *o Straży Granicznej* (T. j.: Dz. U. z 2011 r. Nr 116, poz. 675).

szczególnych, ustalenia możliwości realizacji zadań na rzecz organu współdziałającego. Ogólne obszary współdziałania obejmują rozpoznawanie zagrożeń dla bezpieczeństwa i nienaruszalności granicy państwowej, wymianę informacji, system ostrzegania i alarmowania, zabezpieczenie łączności, zabezpieczenie logistyczne oraz działalność szkoleniową.

Ponadto w sprawie organizacji systemu wsparcia wojsk sojuszniczych przebywających na terytorium Rzeczypospolitej Polskiej lub przemieszczających się przez to terytorium oraz wsparcia wojsk własnych wysyłanych poza terytorium kraju Straż Graniczna realizuje zadania wsparcia państwa-gospodarza (HNS) w zakresie zabezpieczenia przegrupowania wojsk własnych i sojuszniczych oraz ich pobytu na terenie kraju, poprzez:

- zapewnienie sprawnego przekraczania granicy państwowej wojskom własnym i sojuszniczym,
- organizację działań w zakresie rozpoznania potencjalnych zagrożeń w strefie nadgranicznej,
- udzielanie pomocy pododdziałom wojskowym podczas wprowadzania do rejonów rozmieszczenia w strefie nadgranicznej,
- udostępnianie wojskom własnym i sojuszniczym informacji dotyczących strefy nadgranicznej o terenie, miejscowych zasobach, ruchach ludności itp.,
- uczestniczenie w osłonie antyterrorystycznej rejonów rozmieszczenia wojsk w ramach współdziałania z organami Sił Zbrojnych RP,
- skierowanie przedstawicieli Straży Granicznej do udziału w pracach Narodowego Centrum Koordynacji Ruchu Wojsk, a także w zależności od potrzeb innych struktur organizacyjnych realizujących zadania HNS,
- zapewnienie pomocy w zabezpieczeniu bezkolizyjnego przemieszczania się kolumn wojskowych po drogach w strefie nadgranicznej.

Zakres współdziałania Straży Granicznej z Siłami Zbrojnymi RP w okresie zewnętrznego zagrożenia bezpieczeństwa państwa lub czasie wojny obejmuje przedsięwzięcia wspierające działania jednostek wojska przyjmujących zadanie obrony granic Polski przed agresją zewnętrzną. Szczegóły dotyczące rodzaju i zakresu tych przedsięwzięć, uregulowane stosowną dokumentacją planistyczną, mają charakter niejawny.

Ponadto Straż Graniczna współdziała z Policją, Agencją Bezpieczeństwa Wewnętrznego, z Szefem Krajowego Centrum Informacji Kryminalnych, Państwową Inspekcją Pracy, Służbą Celną, Zakładem Ubezpieczeń Społecznych, urzędami kontroli skarbowej oraz związkami zawodowymi i organizacjami pracodawców, Siłami Powietrznymi w zakresie ochrony granicy państwowej w przestrzeni powietrznej i Marynarką Wojenną w zakresie ochrony morskiej granicy państwowej.

Tabela 86. Współdziałanie Straży Granicznej w zakresie zarządzania kryzysowego

Podmioty	Zakres współdziałania
Policja	zwalczanie przestępczości, zwłaszcza rozpoznawanie zagrożeń terrorystycznych, ochrona granicy państwowej, ochrona prewencyjna bezpieczeństwa i porządku publicznego, doskonalenie metodyki wykonywania zadań i czynności służbowych oraz wsparcie logistyczne*
Agencja Bezpieczeństwa Wewnętrznego	organizacja i prowadzenie wspólnych przedsięwzięć służących ochronie bezpieczeństwa wewnętrznego państwa, jego porządku konstytucyjnego i ochronie granicy państwowej, zwłaszcza w zakresie wykonywania czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych oraz wymiany informacji i łączności**
Państwowa Straż Pożarna	organizowanie następujących przedsięwzięć: wykrywania, rozpoznawania oraz monitorowania zaistniałych zagrożeń w ramach realizacji działań własnych, alarmowania i informowania przez podległe jednostki organizacyjne o zaistniałych pożarach, klęskach żywiołowych i innych miejscowych zagrożeniach powstałych w strefie nadgranicznej, wspomagania działań ratowniczych, gaśniczych i poszukiwawczych prowadzonych przez jednostki ochrony przeciwpożarowej w terytorialnym zasięgu działania Oddziałów Straży Granicznej***
Państwowa Inspekcja Sanitarna	ochrona zdrowia
Państwowa Inspekcja Ochrony Roślin i Nasiennictwa oraz Inspekcja Weterynaryjna	ochrona roślin i zwierząt
Służba Celna	przestrzeganie przepisów celnych
Generalna Dyrekcja Dróg Krajowych i Autostrad, Polskie Koleje Państwowe	utrzymanie infrastruktury

* *Porozumienie Komendanta Głównego Straży Granicznej i Komendanta Głównego Policji w sprawie współdziałania Straży Granicznej i Policji* z dnia 17 czerwca 2004 roku.

** *Porozumienie Szefa Agencji Bezpieczeństwa Wewnętrznego i Komendanta Głównego Straży Granicznej o współdziałaniu Agencji Bezpieczeństwa Wewnętrznego i Straży Granicznej* z dnia 10 czerwca 2003 roku.

*** *Porozumienie Komendanta Głównego Straży Granicznej i Komendanta Głównego Państwowej Straży Pożarnej – Szefa Obrony Cywilnej Kraju o współdziałaniu i wzajemnej współpracy w zakresie zapobiegania i likwidacji zagrożeń* z dnia 6 maja 2001 roku.

Źródło: Obowiązujące przepisy prawa

Współpraca Straży Granicznej obejmuje formy aktywności służbowej sprowadzające się w ujęciu ogólnym do wymiany informacji sytuacyjnych charakteryzujących przedmiot wspólnych zainteresowań, przekazywania informacji o występujących zagrożeniach i zaistniałych przestępstwach oraz udostępniania informacji z posiadanych baz danych, przeprowadzania doskonalących szkoleń i ćwiczeń, udostępniania środków transportu lądowego, wodnego i powietrznego, środków łączności, specjalistycznego sprzętu technicznego, umożliwiania korzystania z pomieszczeń służbowych, przeprowadzania wspólnych patroli, kon-

troli i inspekcji, wspomagania akcji ratowniczych i ewakuacyjnych, wspierania działań interwencyjnych i realizacyjnych, przekazywania ocen i opinii, udzielania pomocy prawnej.

9.3. Żandarmeria Wojskowa

Żandarmeria Wojskowa (ŻW) jest wyodrębnioną i wyspecjalizowaną służbą, która wchodzi w skład Sił Zbrojnych Rzeczypospolitej Polskiej. Utworzona została na podstawie ustawy z dnia 24 sierpnia 2001 roku *o Żandarmerii Wojskowej i wojskowych organach porządkowych*[35]. Jej misją jest zapewnienie przestrzegania prawa, porządku i dyscypliny wojskowej w Siłach Zbrojnych Rzeczypospolitej Polskiej oraz bezpieczeństwa wojsk i prowadzonych operacji militarnych. Żandarmeria Wojskowa zgodnie z obowiązującymi przepisami wykonuje zadania zarówno na terytorium Rzeczypospolitej Polskiej, jak i poza granicami kraju[36].

Żandarmeria Wojskowa z uwagi na usytuowanie podejmuje działania w niemilitarnych sytuacjach kryzysowych w ramach systemu zarządzania kryzysowego resortu obrony narodowej, ponadto jest częścią systemu krajowego i sojuszniczego. Realizacja zadań wynikających z tego systemu wymaga ścisłej koordynacji oraz współdziałania wszystkich uczestniczących w nim podmiotów, w tym również w ramach działalności bieżącej przed wystąpieniem określonej sytuacji kryzysowej, i to zarówno w układzie pionowym, jak i poziomym.

Użycie ŻW w czasie kryzysu niemilitarnego następuje w sytuacjach po wyczerpaniu możliwości niemilitarnego podsystemu bezpieczeństwa państwa. Ponadto jednostki Żandarmerii Wojskowej mogą być użyte do wykonywania zadań w przypadku zagrożenia bezpieczeństwa publicznego, niebezpiecznego zakłócania porządku lub klęski żywiołowej, zwłaszcza w sytuacjach niebezpieczeństwa powszechnego dla życia, zdrowia lub wolności obywateli oraz bezpośredniego i powodującego duże straty zagrożenia mienia, w tym obiektów i urządzeń ważnych dla bezpieczeństwa lub obronności państwa. Celem działań o tym charakterze jest przede wszystkim wsparcie działań przeciwterrorystycznych Policji, ochrona i obrona obiektów i urządzeń ważnych dla bezpieczeństwa lub obronności państwa, wspieranie działań Policji przywracającej bezpieczeństwo i porządek publiczny, gdy jej siły są niewystarczające.

Zgodnie z postanowieniem ustawy z dnia 24 sierpnia 2001 roku *o Żandarmerii Wojskowej* do zadań Żandarmerii Wojskowej w zarządzaniu kryzysowym należy zwalczanie klęsk żywiołowych, nadzwyczajnych zagrożeń środowiska i likwidowanie ich skutków oraz czynne uczestniczenie w akcjach poszukiwawczych,

[35] Dz. U. z 2001 r. Nr 123, poz. 1353 z późn. zm.

[36] Ibidem, art. 5.

ratowniczych i humanitarnych, mających na celu ochronę życia i zdrowia oraz mienia, wykonywanie innych zadań określonych w odrębnych przepisach[37].

ŻW może być użyta w celu przeciwdziałania negatywnym zjawiskom oraz wsparcia innych służb w sytuacjach kryzysowych. Do zadań Żandarmerii Wojskowej w sytuacjach kryzysowych należy:

- kontrola osób i mienia,
- wsparcie działań antyterrorystycznych policji,
- wzmocnienie systemu zewnętrznej ochrony obiektów i instalacji mających szczególne znaczenie dla bezpieczeństwa i obronności państwa,
- udział w akcjach poszukiwawczo-ratowniczych,
- udział w akcjach ratowniczo-gaśniczych oraz usuwania skutków pożarów,
- likwidacja skutków awarii technicznych obiektów z toksycznymi środkami przemysłowymi oraz wypadków radiacyjnych,
- likwidacja wypadków drogowych,
- udział w akcjach odśnieżania,
- udział w zwalczaniu powodzi i likwidacji ich skutków,
- udział w oczyszczaniu terenu z przedmiotów wybuchowych i niebezpiecznych,
- udział w działaniach przeciwepidemiologicznych[38].

Działania Żandarmerii Wojskowej w zarządzaniu kryzysowym przebiegają w trzech fazach: monitorowania, aktywacji sił i środków, działania (w tym usuwania skutków).

W fazie pierwszej utrzymywane są w gotowości do działania wydzielone siły i środki przeznaczone do prowadzenia działań dochodzeniowo-śledczych, prewencyjnych i operacyjno-rozpoznawczych ukierunkowane na wykrywanie zagrożeń we współdziałaniu z innymi służbami odpowiedzialnymi za bezpieczeństwo i porządek publiczny w kraju. W fazie tej są wykonywane zadania mające na celu zapewnienie bezpośredniej ochrony osobom zajmującym kluczowe stanowiska w MON oraz przedstawicielom dowództw NATO przebywającym w Polsce.

W fazie drugiej wydzielane są siły i środki do wykonania zadań prewencyjnego oraz do dochodzeniowo-śledczego zabezpieczenia zagrożonych terenów i obiektów wojskowych we współdziałaniu z wydzielonymi siłami Policji, Straży Granicznej oraz innych służb odpowiedzialnych za zapewnienie bezpieczeństwa i utrzymanie porządku publicznego w kraju.

W fazie trzeciej jest realizowane zabezpieczenie przegrupowania sił przeznaczonych do udziału w sytuacjach kryzysowych oraz w przeszukiwaniu i izolowaniu terenu. W fazie tej kierowane są do działania określone siły i środki oraz usuwane ewentualne skutki sytuacji kryzysowych.

[37] Ustawa z dnia 24 sierpnia 2001 roku *o Żandarmerii Wojskowej i wojskowych organach porządkowych* (Dz. U. z 2001 r. Nr 123, poz. 1353 z późn. zm.), art. 4 ust. 1 pkt 7 i 8.

[38] G. Wasilewski, *Żandarmeria Wojskowa w niemilitarnych sytuacjach kryzysowych*, [w:] *Wojsko w niemilitarnych sytuacjach kryzysowych*, red. W.S. Krzeszowski, Warszawa 2008, s. 77–78.

Kierowanie i dowodzenie siłami oraz ich użycie operacyjne, a także zabezpieczenie logistyczne podczas bieżącego funkcjonowania oraz w okresie kryzysu jest zadaniem wiodących pionów funkcjonalnych: dochodzeniowo-śledczego, prewencyjnego, administracyjno-logistyczno-technicznego[39].

Po wyczerpaniu możliwości niemilitarnego podsystemu bezpieczeństwa państwa w celu zapobiegania, zwalczania i usuwania skutków sytuacji kryzysowych organy władzy państwowej mogą się zwrócić o pomoc do Żandarmerii Wojskowej. W tej sytuacji stosuje się jedną z procedur: nakazową, podstawową, alarmową.

Procedura nakazowa polega na włączaniu wyznaczonych jednostek ŻW do danego typu akcji na podstawie decyzji Ministra Obrony Narodowej lub rozkazu szefa Sztabu Generalnego WP. Podstawą wydania tej decyzji lub rozkazu jest postanowienie, które zapada na szczeblu centralnym (prezydent, premier). W przypadku procedury podstawowej przedstawiciel określonego szczebla organów administracji publicznej powiadamia w sytuacji kryzysowej ogniwa nadrzędne do wojewody włącznie, a ten przez właściwego terytorialnie szefa wojewódzkiego sztabu wojskowego składa pisemny wniosek o użycie określonych jednostek organizacyjnych Sił Zbrojnych RP, w tym Żandarmerii Wojskowej. Procedura alarmowa jest stosowana w sytuacjach nagłych, niespodziewanych zagrożeń. Decyzję o użyciu określonych jednostek ŻW podejmują ich dowódcy, po czym niezwłocznie meldują o tym fakcie swoim przełożonym. Szczeblem, który ma prawo podjąć decyzję o użyciu podległych sił, jest dowódca rodzaju Sił Zbrojnych oraz dowódca okręgu wojskowego. O podjętych decyzjach przekazuje się informację do szefa Sztabu Generalnego WP. Wykonywanie zadań związanych z zarządzaniem kryzysowym wymaga koordynacji oraz współdziałania między wszystkimi elementami biorącymi w tym udział. Użycie oddziałów i pododdziałów ŻW powinno następować zgodnie z ich przeznaczeniem i posiadanym wyposażeniem.

Żandarmeria Wojskowa w celu realizacji ustawowych zadań współdziała z dowódcami wszystkich rodzajów Sił Zbrojnych i wszystkich jednostek wojskowych oraz ze służbami odpowiedzialnymi za zapewnienie bezpieczeństwa państwa oraz przestrzeganie prawa i porządku, a także za bezpieczeństwo i ochronę ludności. Podstawę współdziałania stanowią porozumienia zawarte z szefami oraz komendantami instytucji odpowiedzialnych za bezpieczeństwo i porządek publiczny w kraju.

Współpraca ta polega na:

- ciągłej wymianie informacji o zagrożeniach występujących na określonym terenie odnoszących się do bezpieczeństwa ludzi i mienia oraz porządku publicznego,
- organizowaniu i prowadzeniu wspólnych działań,

[39] Ustawa z dnia 24 sierpnia 2001 *o Żandarmerii Wojskowej i wojskowych organach porządkowych* (Dz. U. z 2001 r. Nr 123, poz. 1353 z późn. zm.), art. 8 ust. 1.

- podejmowaniu przedsięwzięć w celu zapewnienia bezpieczeństwa w ruchu drogowym,
- wspólnym prowadzeniu działań porządkowych w celu zapewnienia spokoju i porządku w miejscach zgromadzeń, organizowanych imprez artystycznych itd.,
- współpracy przy zabezpieczaniu miejsc popełnienia przestępstw – udzielaniu w miarę potrzeby pomocy przy doprowadzaniu do właściwych organów sprawców przestępstw i wykroczeń.

Specjalne uprawnienia nadano Żandarmerii Wojskowej ustawą z dnia 6 kwietnia 1990 roku *o Policji*. Zgodnie z jej postanowieniami może ona być użyta niezależnie od pozostałych Sił Zbrojnych RP do udzielania pomocy Policji w sytuacjach zagrożenia bezpieczeństwa i porządku publicznego. Do zadań tych można zaliczyć:

- wykonywanie czynności operacyjno-rozpoznawczych i procesowych w granicach jej kompetencji,
- prewencyjne i dochodzeniowo-śledcze zabezpieczenie miejsc, obiektów i obszarów oraz kontrola dostępu do nich,
- izolowanie terenu, organizowanie objazdów i posterunków kontrolno-blokadowych, a także przeszukiwanie i patrolowanie terenu,
- zwalczanie terroryzmu,
- ochronę osób,
- podejmowanie czynności poszukiwania osób, mienia i przedmiotów.

Zgodnie z art. 18a. ust 1. ustawy z dnia 6 kwietnia 1990 roku *o Policji*[40] w razie klęski żywiołowej lub nadzwyczajnego zagrożenia środowiska, gdy siły Policji są niewystarczające do wykonania ich zadań w zakresie ochrony bezpieczeństwa i porządku publicznego, Prezes Rady Ministrów, na wniosek ministra właściwego do spraw wewnętrznych uzgodniony z Ministrem Obrony Narodowej, może zarządzić użycie żołnierzy Żandarmerii Wojskowej do udzielania pomocy Policji.

Kwestię działań Żandarmerii Wojskowej w ramach wsparcia jednostek Policji należy rozpatrywać w dwóch przypadkach:

- kiedy ŻW wspiera inne podmioty uprawnione do prowadzenia działań w celu zapewnienia bezpieczeństwa wewnętrznego (Policję, Straż Graniczną, Straż Ochrony Kolei),
- kiedy ŻW jest samodzielnym i jedynym podmiotem prowadzącym działania bądź kiedy jest podmiotem wiodącym, wspieranym przez inne organy porządku prawnego (Policję, Straż Ochrony Kolei, Straż Graniczną).

Wskazane jest realizowanie wspólnych przedsięwzięć (ćwiczenia, treningi, szkolenia itp.) z udziałem wszystkich podsystemów systemu bezpieczeństwa państwa. Istotny jest również sprawny system obiegu informacji w ramach krajowego jak i sojuszniczego systemu zarządzania kryzysowego.

Jednym z czynników gwarantujących ochronę Rzeczypospolitej Polskiej przed nagłym i niespodziewanym wzrostem zagrożenia zewnętrznego lub

[40] Dz. U. z 2002 r. Nr 7, poz. 58 z późn. zm.

wewnętrznego, np. aktem terroru, jest sprawność funkcjonowania m.in. Żandarmerii Wojskowej. W związku z przydzieleniem Żandarmerii Wojskowej do wykonywania zadań w systemie zarządzania kryzysowego, wynikających z wojewódzkich planów zarządzania kryzysowego, konieczny jest wgląd do przedmiotowych dokumentów, co umożliwi właściwe przygotowanie i wyposażenie określonych jednostek organizacyjnych ŻW, a tym samym pozwala skrócić czas reakcji na powstałe zagrożenie i zapewnia szybsze wsparcie władz cywilnych i społeczeństwa.

Szczególny nacisk kładzie się na przygotowanie Żandarmerii Wojskowej oraz innych podmiotów odpowiedzialnych za bezpieczeństwo i porządek publiczny do zapobiegania aktom terrorystycznym i ich negatywnym następstwom.

> Działania antyterrorystyczne to m.in. utrzymanie kontroli na obszarach podatnych na ataki terrorystyczne. Działania te mogą obejmować ocenę podatności obiektów na ataki, rozwijania i wdrażania procedur wykrywania akcji terrorystycznych, wzmocnienia potencjalnych celów ataku i podejmowania akcji ofensywnych w celu zlikwidowania zagrożenia terrorystycznego[41].

Wykorzystanie potencjału Żandarmerii Wojskowej w realizacji zadań zarządzania kryzysowego ma bezpośredni związek z tworzonym na poziomie państwa systemem, który pozwalałby m.in. na:

- prognozowanie zagrożeń patologiami społecznymi wynikającymi z liberalizacji przepisów granicznych, bezrobocia i pauperyzacji społeczeństwa,
- wskazanie kierunków, trendów, dynamiki i przedziałów czasowych erupcji patologii oraz na wyprzedzające powiadamianie o konieczności zapewnienia odpowiednich instrumentów prawnych, technicznych, finansowych i funkcjonalnych organów ochrony bezpieczeństwa wewnętrznego.

9.4. Biuro Ochrony Rządu

Osoby zajmujące najwyższe stanowiska w państwie muszą mieć zapewnione właściwe warunki dla realizacji swoich ustawowych obowiązków zarówno w kraju, jak i poza jego granicami. Dotyczy to również pracowników placówek dyplomatycznych i konsularnych w państwach akredytacji. Występujące zagrożenia związane z terroryzmem, przestępczością zorganizowaną, a także niestabilnością polityczną, społeczną, gospodarczą, wojskową, działalnością wywiadowczą i kontrwywiadowczą czy też miejscami o szczególnie wysokim ryzyku, gdzie takie osoby przebywają, uzasadniają podjęcie działań zapewniających im bezpieczeństwo. Ponadto należy mieć na uwadze zagrożenia wynikające z ewentualnej

[41] *APP – 12 (policja wojskowa NATO. Doktryna procedury*), projekt ratyfikacyjny, Warszawa 2000, s. 6–3.

spontanicznej reakcji braku poparcia społecznego, która może przybrać postać czynnej napaści, jak i wcześniej zaplanowanego, przygotowanego oraz przeprowadzonego zamachu[42]. Oznacza to, że szczególnym wyzwaniem dla funkcjonariuszy Biura Ochrony Rządu są sytuacje kryzysowe w kraju i poza jego granicami.

W Polsce wyspecjalizowaną służbą właściwą w sferze ochrony najwyższych osób w państwie jest Biuro Ochrony Rządu (BOR). Jest to jednolita, umundurowana i uzbrojona formacja, wykonującą zadania z zakresu ochrony osób, obiektów i urządzeń[43]. BOR jest podporządkowane Ministrowi Spraw Wewnętrznych. Podstawę prawną jego działania stanowi ustawa z dnia 16 marca 2001 roku *o Biurze Ochrony Rządu*[44].

Szef BOR kieruje Biurem Ochrony Rządu i zapewnia sprawne oraz efektywne wykonywanie jego zadań, w szczególności poprzez organizowanie ochrony, współdziałanie z centralnymi organami administracji rządowej podległymi ministrowi właściwemu do spraw wewnętrznych, jednostkami organizacyjnymi podporządkowanymi, podległymi oraz nadzorowanymi przez ministra właściwego do spraw wewnętrznych lub Ministra Obrony Narodowej oraz innymi organami administracji rządowej i samorządu terytorialnego w zakresie zadań realizowanych przez BOR i te organy[45].

Do zadań Biura Ochrony Rządu należy ochrona:

- Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu, Marszałka Senatu, Prezesa Rady Ministrów, wiceprezesa Rady Ministrów, ministra właściwego do spraw wewnętrznych oraz ministra właściwego do spraw zagranicznych,
- innych osób ze względu na dobro państwa,
- byłych prezydentów Rzeczypospolitej Polskiej na podstawie ustawy z dnia 30 maja 1996 roku o uposażeniu byłego Prezydenta Rzeczypospolitej Polskiej (wyłącznie na terytorium RP)[46],
- delegacji państw obcych przebywających na terytorium Rzeczypospolitej Polskiej,
- polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych poza granicami Rzeczypospolitej Polskiej,
- obiektów i urządzeń o szczególnym znaczeniu oraz zapewnienie ich funkcjonowania,
- prowadzenie rozpoznania pirotechniczno-radiologicznego obiektów Sejmu i Senatu,

[42] K. Zeidler, *Zadania Biura Ochrony Rządu wobec zagrożeń przestępczością zorganizowaną i terroryzmem,* [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 959.

[43] Ustawa z dnia 16 marca 2001 r. *o Biurze Ochrony Rządu* (Dz. U. z 2004 r. Nr 163, poz. 1712 z późn. zm.), art. 1 ust. 1.

[44] Dz. U. z 2004 r. Nr 163, poz. 1712 z późn. zm.

[45] Ibidem, art. 7.

[46] Dz. U. z 1996 r. Nr 75, poz. 356 oraz z 1998 r. Nr 160, poz. 1065.

- obiektów służących Prezydentowi Rzeczypospolitej Polskiej, Prezesowi Rady Ministrów, ministrowi właściwemu do spraw wewnętrznych oraz ministrowi właściwemu do spraw zagranicznych[47].

W celu zapewnienia ochrony, o której mowa w ustawie o Biurze Ochrony Rządu, BOR w szczególności: planuje zabezpieczenie osób, obiektów i urządzeń, rozpoznaje i analizuje potencjalne zagrożenia, zapobiega powstawaniu tych zagrożeń, koordynuje realizację działań ochronnych i wykonuje bezpośrednią ochronę, zabezpiecza obiekty i urządzenia, doskonali metody pracy[48].

W zakresie swoich zadań Biuro wykonuje czynności administracyjno-porządkowe oraz podejmuje działania profilaktyczne[49]. Korzysta z pomocy i informacji uzyskanych w szczególności przez: Policję, Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Straż Graniczną, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Żandarmerię Wojskową. Prawa Funkcjonariuszy Biura Ochrony Rządu wykonujących swoje zadania to:

- wydawanie polecenia osobom, których zachowanie może stworzyć zagrożenie dla bezpieczeństwa osób, obiektów i urządzeń podlegających ochronie BOR, a w szczególności polecenia:
  a) opuszczenia przez osoby miejsca, w którym przebywanie może stanowić zagrożenie dla realizacji zadania,
  b) zatrzymania pojazdu,
  c) usunięcia pojazdu z miejsca postoju,
- legitymowanie osób w celu ustalenia ich tożsamości,
- zatrzymywanie osób stwarzających w sposób oczywisty bezpośrednie zagrożenie dla życia lub zdrowia ludzkiego oraz dla mienia, a także w sposób rażący naruszających porządek publiczny,
- dokonywanie kontroli osobistej, a także przeglądanie zawartości bagaży i sprawdzanie ładunków i pomieszczeń w sytuacjach, jeżeli jest to niezbędne dla zapewnienia bezpieczeństwa ochranianych osób, obiektów i urządzeń,
- żądanie niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i jednostki są obowiązane, w zakresie swojego działania, do udzielenia tej pomocy,
- zwracanie się o niezbędną pomoc do innych jednostek gospodarczych i organizacji społecznych, jak również w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy[50].

W przypadku niepodporządkowania się wydanym na podstawie prawa poleceniom, o których mowa w art. 13 ust. 1, funkcjonariusz może stosować środki

[47] Ustawa z dnia 16 marca 2001 r. *o Biurze Ochrony Rządu* (Dz. U. z 2004 r. Nr 163, poz. 1712 z późn. zm.), art. 2.

[48] Ibidem, art. 11.

[49] Ibidem, art. 12 ust. 1.

[50] Ibidem, art. 13 ust. 1.

przymusu bezpośredniego (siłę fizyczną w postaci chwytów obezwładniających oraz podobnych technik obrony lub ataku; urządzenia techniczne w postaci kajdanek, prowadnic, kaftanów bezpieczeństwa, pasów i siatek obezwładniających; urządzenia techniczne w postaci kolczatek drogowych i innych przeszkód umożliwiających zatrzymanie pojazdu; chemiczne środki obezwładniające; pałki służbowe zwykłe, teleskopowe i wielofunkcyjne, psy służbowe)[51]. Jeżeli środki, o których mowa w art. 14 ust. 1, okazały się niewystarczające lub jeżeli ich użycie ze względu na okoliczności danego zdarzenia nie jest możliwe, funkcjonariusz ma prawo użycia broni palnej[52].

Biuro Ochrony Rządu w zakresie działań, o których jest mowa w art. 12 ustawy:

- zapobiega popełnianiu przestępstw przeciwko osobom ochranianym,
- ujawnia osoby i zdarzenia oraz rozpoznaje miejsca i zjawiska mogące mieć związek z zagrożeniem osób ochranianych oraz bezpieczeństwa obiektów i urządzeń objętych ochroną,
- współdziała z Policją, Agencją Bezpieczeństwa Wewnętrznego, Agencją Wywiadu, Służbą Kontrwywiadu Wojskowego, Służbą Wywiadu Wojskowego, Żandarmerią Wojskową, Strażą Graniczną oraz Państwową Strażą Pożarną w zakresie uzyskiwania informacji o zagrożeniach dla osób lub obiektów i urządzeń chronionych,
- utrzymuje kontakty z osobami, które mogłyby udzielić mu pomocy[53].
- BOR prowadzi działania, o których mowa w art. 12 ustawy, poprzez:
- gromadzenie i przetwarzanie informacji mogących wpłynąć na realizację zadań,
- planowanie i systematyczne sprawdzanie obiektów i urządzeń objętych ochroną, w celu zapewnienia bezpiecznej realizacji zadań,
- korzystanie z informacji i danych przechowywanych w zbiorach ewidencji kryminalnej i zbiorach archiwalnych dla wyeliminowania potencjalnego zagrożenia dla osób, obiektów i urządzeń ochranianych[54].

Przetwarzanie danych osobowych BOR może prowadzić bez wiedzy i zgody osoby, której one dotyczą, o ile służy to realizacji zadań, o których mowa w ustawie.

Na uwagę zasługuje treść art. 2 ust. 1 pkt 5 ustawy *o Biurze Ochrony Rządu,* który stanowi, że do zadań BOR należy ochrona polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych poza granicami Rzeczypospolitej Polskiej. BOR zapewnia ochronę tylko placówkom w wysokim stopniu zagrożenia (m.in. atakiem terrorystycznym, działalnością obcych służb specjalnych lub umiejscowionych w państwach zagrożonych niepokojami i przestępczością). W tym obszarze zadania BOR pokrywają się z zadaniami Agencji Wywiadu, jednak są uregulowane

[51] Ibidem, art. 14 ust. 1.

[52] Ibidem, art. 15 ust. 1.

[53] Ibidem, art. 16.

[54] Ibidem, art. 17.

przepisami prawa i nie kolidują ze zobowiązaniami Agencji Wywiadu. O uznaniu placówki za placówkę wysokiego stopnia zagrożenia Szef BOR informowany jest przez Dyrektora Generalnego Służby Zagranicznej[55]. Rozporządzenie określa zakres, warunki i tryb kierowania funkcjonariuszy do wykonywania zadań oraz wymogi, jakie powinni spełnić funkcjonariusze skierowani do wykonywania zadań ochrony polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych poza granicami Rzeczypospolitej Polskiej.

Tabela 87. Działania w zakresie ochrony fizycznej w placówce

Działania w zakresie ochrony fizycznej	
Osoba funkcyjna	Zadania
Dowódca ochrony	jest bezpośrednim przełożonym wszystkich funkcjonariuszy skierowanych do ochrony placówki kieruje działaniami ochronnymi odpowiada za bieżącą dokumentację ochronną w zakresie ochrony fizycznej, jej tworzenie, przechowywanie i archiwizowanie, jak również prowadzi ewidencję obecności funkcjonariuszy w służbie w sprawach dotyczących wykonania nadzoru służbowego, w tym realizacji zadań ochronnych, przepisów, procedur oraz instrukcji Szefa Biura Ochrony Rządu, podlega Szefowi Biura Ochrony Rządu składa Szefowi Biura Ochrony Rządu, za pośrednictwem łączności Ministerstwa Spraw Zagranicznych, okresowe meldunki z realizacji zadań ochronnych, a w sytuacjach nadzwyczajnych melduje niezwłocznie, z zachowaniem przepisów o ochronie informacji niejawnych
Funkcjonariusze	zewnętrzne i wewnętrzne kontrolowanie stanu obiektów placówki obsługa techniczna systemów zabezpieczających obiekty placówki obserwacja otoczenia placówki zapobieganie wstępu osób nieuprawnionych na teren placówki kontrola i zapobieganie wnoszeniu na teren placówki przedmiotów mogących zagrażać bezpieczeństwu przebywających w niej osób, w tym sprawdzanie przesyłek otrzymywanych za pośrednictwem poczty obserwowanie ruchu pojazdów i zachowania osób za pośrednictwem luster, systemu telewizji przemysłowej oraz innych urządzeń zabezpieczanie śladów wskazujących na próbę lub dokonanie włamania lub penetracji dokumentowanie czynności związanych z ochroną placówki podejmowanie interwencji w przypadku zagrożenia

Źródło: Rozporządzenie Ministra Spraw Wewnętrznych z dnia 12 stycznia 2012 r. *w sprawie zakresu, warunków i trybu wykonywania zadań ochrony polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych poza granicami Rzeczypospolitej polskiej* (Dz. U. z 2012 r. Nr 0, poz. 92), § 6 ust 1 i § 7

[55] Rozporządzenie Ministra Spraw Wewnętrznych z dnia 12 stycznia 2012 r. *w sprawie zakresu, warunków i trybu wykonywania zadań ochrony polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych poza granicami Rzeczypospolitej polskiej* (Dz. U. z 2012 r. Nr 0, poz. 92).

Stopień zagrożenia placówek określa minister właściwy do spraw zagranicznych w porozumieniu z Szefem Agencji Wywiadu. Minister właściwy do spraw wewnętrznych na podstawie przekazanego przez Ministra Spraw Zagranicznych wniosku wraz z uzasadnieniem poleca Szefowi Biura Ochrony Rządu objęcie ochroną określonej placówki. Na tej podstawie Szef Biura Ochrony Rządu kieruje funkcjonariuszy BOR do ochrony placówki (decyduje również o jego odwołaniu). Za ochronę fizyczną placówki odpowiada Szef Biura Ochrony Rządu. Po przystąpieniu Polski do Unii Europejskiej Biuro Ochrony Rządu nawiązało stałą współpracę z organizacjami zajmującymi się zapewnieniem bezpieczeństwa osób publicznych. Biuro Ochrony Rządu jest członkiem następujących stowarzyszeń:

- Europejskiej Sieci Ochrony Osób Publicznych (European Network for the Protection of Public Figures) ENPPF. Sieć została powołana do życia decyzją Rady Unii Europejskiej z dnia 28 listopada 2002 roku z inicjatywy Królestwa Hiszpanii. W jej skład wchodzą krajowe służby policyjne i inne służby odpowiedzialne za ochronę osób publicznych. Do głównych zadań stowarzyszenia należą: wymiana informacji przy planowaniu zabezpieczeń wizyt osób ochranianych w krajach UE, wypracowanie wspólnych procedur w trakcie realizacji działań ochronnych i wspólnego stanowiska w zakresie metod działania celem zapewnienia maksimum bezpieczeństwa osób ochranianych;
- Stowarzyszenia Służb Ochrony Osobistej (Association of Personal Protection Services) APPS. Stowarzyszenie zrzesza instytucje publiczne z całego świata odpowiedzialne za bezpieczeństwo najważniejszych osób w poszczególnych państwach. Głównym celem organizacji jest wymiana poglądów, wiedzy, doświadczeń, informacji oraz promocja ścisłej współpracy pomiędzy poszczególnymi służbami ochrony podczas realizacji wspólnych zadań;
- Projektu Współpracy Bliźniaczej Twinning Project PL, prowadzącego międzyinstytucjonalną współpracę na rzecz zwalczania przestępczości zorganizowanej, powołanym w ramach Unii Europejskiej w celu prowadzenia i umacniania partnerstwa między Wielką Brytanią a Polską. Działania w ramach Projektu koncentrują się głównie na prowadzeniu szkoleń w dziedzinach takich jak walka z terroryzmem oraz walka z przestępczością zorganizowaną.

W ramach współpracy międzynarodowej Biuro Ochrony Rządu utrzymuje kontakty ze służbami ochronnymi z całego świata, które obejmują m.in. wymianę doświadczeń, działania ochronne, szkolenia międzynarodowe.

9.5. Służby specjalne

Globalizacja, rozwój społeczeństwa informacyjnego i towarzyszący im postęp naukowo-techniczny to szanse i zagrożenia, z przewagą tych drugich. W obliczu istniejących i ewoluujących zagrożeń ich skala, dynamika, a przede wszystkim

charakter sprawiają, że zwiększa się zakres działania służb specjalnych. Oznacza to, że państwo stopniowo poszerza zakres wartości chronionych, wskazując służbom wywiadu i kontrwywiadu nowe kierunki zainteresowania, które mają istotny wpływ na poziom jego bezpieczeństwa.

Obok tradycyjnych zagrożeń pojawiły się nowe, o których wiedza państwa jest niewystarczająca. Dotyczy to przede wszystkim informacji dotyczących wszelkich zagrożeń dla światowego pokoju, w tym ważnych dla bezpieczeństwa i obronności państwa i jego sojuszników. Jednocześnie wzrasta zapotrzebowanie na informacje gospodarcze związane z prowadzoną walką konkurencyjną o nowe rynki zbytu, rodzaje produkcji, technologie, źródła tanich zasobów surowców itp.[56] Osobnym rodzajem informacji znajdujących się w kręgu zainteresowania służb specjalnych są dane dotyczące nielegalnego handlu bronią, przemytu narkotyków, materiałów rozszczepialnych, technologii do produkcji broni masowego rażenia i środków do jej przenoszenia, handlu żywym towarem (organami i tkankami ludzkimi), terroryzmu, zorganizowanej przestępczości (w tym o charakterze transgranicznym), praniu brudnych pieniędzy, masowych migracji, a także zagrożeń płynących ze sfery ekologicznej, kulturowej czy psychospołecznej. Kolejne wyzwanie dla służb specjalnych to ochrona infrastruktury krytycznej państwa, w tym informacji w systemach i sieciach teleinformatycznych. Na uwadze należy mieć również zagrożenia dla bezpieczeństwa państwa, których źródłem są sprzeczności interesów grup społecznych, etnicznych i wyznaniowych, co może mieć tendencje wzrostowe. Może się tak dziać za sprawą mniejszości narodowych (niemieckiej, ukraińskiej lub białoruskiej) i wyznaniowych (przede wszystkim prawosławnej)[57].

> Występujące tu sprzeczności interesów mogą doprowadzić do kryzysu powodującego zagrożenie militarne. Za takim wnioskiem przemawia złożoność zjawisk, które przebiegają na gruncie psychosocjologicznym i bardzo łatwo mogą przybrać charakter międzynarodowy (zwłaszcza gdy dotyczą mniejszości narodowych, etnicznych i wyznaniowych)[58].

Na uwadze należy mieć również anarchizację życia społeczno-politycznego w państwach posiadających broń masowego rażenia, negowanie postanowień traktatowych i eksponowanie zaszłości historycznych, rozszerzający się krąg państw dysponujących i mogących wejść w przyszłości w posiadanie broni jądrowej, nieistniejącą kontrolę międzynarodowych organizacji bezpieczeństwa zbiorowego procesów militaryzacji niektórych państw czy regionów, nasilające się zjawiska nacjonalizmu, szowinizmu i fundamentalizmu religijnego oraz terroryzmu organizacji anarchistycznych czy ortodoksyjnych[59].

[56] Z.C. Michalski, *Dostosowanie regulacji prawno-organizacyjnych w ochronie tajemnicy państwowej i wojskowej do standardów NATO*, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 1999, nr 3, s. 6.

[57] S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, s. 38.

[58] Ibidem, s. 38.

[59] Szerzej ibidem, s. 25–26.

Służby specjalne wykonując ustawowe zadania w systemie bezpieczeństwa państwa w przypadku wystąpienia sytuacji kryzysowej i uruchomienia przedsięwzięć związanych z zarządzaniem kryzysowym, obok funkcji informacyjnej realizują także funkcje procesowe i ochronno-kontrolne.

W polskim systemie prawnym jedynie Agencja Bezpieczeństwa Wewnętrznego (ABW) posiada uprawnienia do wykonywania czynności procesowych (dochodzeniowo-śledczych) określonych w ustawie z dnia 6 czerwca 1997 roku *Kodeks postępowania karnego*[60].

Zgodnie z art. 21 ust. 1 ustawy z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[61] w granicach zadań określonych w art. 5 ust. 1 niniejszego aktu prawnego funkcjonariusze ABW wykonują czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców. Agencja Bezpieczeństwa Wewnętrznego wykonuje również czynności na polecenie sądu lub prokuratora w zakresie określonym w *Kodeksie postępowania karnego* oraz *Kodeksie karnym wykonawczym*[62]. Funkcjonariusze ABW wykonują czynności tylko w zakresie właściwości tej Agencji i w tym zakresie przysługują im uprawnienia procesowe Policji, wynikające z przepisów *Kodeksu postępowania karnego*[63].

Ustawowe zadania Agencji Bezpieczeństwa Wewnętrznego związane z wykonywaniem funkcji procesowej to zapobieganie i wykrywanie oraz ściganie:

- sprawców przestępstw,
- szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa oraz godzących w podstawy ekonomiczne państwa[64],
- korupcji osób pełniących funkcje publiczne, o których jest mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 roku *o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne*[65], jeśli to może godzić w bezpieczeństwo państwa,
- w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,
- nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi, substancjami psychotropowymi w obrocie międzynarodowym.

Jeżeli informacje i materiały uzyskane przez ABW albo AW wskazują na uzasadnione podejrzenie popełnienia przestępstwa lub przestępstwa skarbowego albo potwierdzają jego popełnienie, Szef właściwej Agencji przedstawia

60 Dz. U. z 1997 r. Nr 89, poz. 555 z późn. zm.

61 Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.

62 Ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.), art. 21 ust. 2.

63 Ibidem, art. 21 ust. 3.

64 Ibidem, art. 5 ust. 1 pkt 2.

65 Dz. U. z 2006 r. Nr 216, poz. 1584, 2008 r. Nr 223, poz. 1458 oraz z 2009 r. Nr 178, poz. 1375.

je uprawnionemu prokuratorowi w celu podjęcia decyzji w zakresie ich dalszego procesowego wykorzystania[66]. Należy zaznaczyć, że funkcjonariusze Agencji Wywiadu nie posiadają uprawnień do wykonywania czynności procesowych.

Uprawnień do wykonywania czynności procesowych nie posiadają żołnierze (funkcjonariusze) wojskowych służby specjalnych, jak: Służba Kontrwywiadu Wojskowego (SKW) i Służba Wywiadu Wojskowego (SWW). Zgodnie z art. 27 ust. 3 ustawy z dnia 9 czerwca z 2006 roku *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[67], jeżeli informacje i materiały uzyskane przez SKW albo SWW wskazują na uzasadnione podejrzenie popełnienia przestępstwa lub przestępstwa skarbowego albo potwierdzają jego popełnienie, SKW albo SWW przedstawia je właściwemu prokuratorowi w celu podjęcia decyzji w zakresie ich dalszego procesowego wykorzystania.

W systemie bezpieczeństwa wewnętrznego i zewnętrznego, a także zarządzania kryzysowego cywilne i wojskowe służby specjalne realizują także funkcję ochronno-kontrolną. Ta funkcja ma ścisły związek z przeciwdziałaniem naruszeniom informacji niejawnych, co wynika z postanowień ustawy z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*[68]. Niniejszy akt prawny wprowadza wiele rozwiązań organizacyjnych, wskazując służbom specjalnym zadania w zakresie ochrony informacji niejawnych.

Ustawa *o ochronie informacji niejawnych* w art. 1 ust. 1 określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, a także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażenia, to jest zasady:

- klasyfikowania informacji niejawnych,
- organizowania ochrony informacji niejawnych,
- przetwarzania informacji niejawnych,
- postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nimi objęta daje rękojmię zachowania tajemnicy,
- postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nimi objęty zapewnia warunki do ochrony informacji niejawnych,
- organizacji kontroli stanu zabezpieczenia informacji niejawnych,
- ochrony informacji niejawnych w systemach teleinformatycznych,
- stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych[69].

Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego nadzorują funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości określonej w ustawie:

[66] Ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.), art. 22a ust. 3.

[67] Dz. U. z 2006 r. Nr 104, poz. 709 z późn. zm.

[68] Dz. U. z 2010 r. Nr 182, poz. 1228.

[69] Ibidem.

- prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie,
- realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych,
- prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego,
- zapewniają ochronę informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi,
- prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych[70].

Agencja Bezpieczeństwa Wewnętrznego realizuje powyższe zadania w odniesieniu do jednostek organizacyjnych i osób podlegających ustawie, ale z wyłączeniem jednostek i osób znajdujących się we właściwości Służby Kontrwywiadu Wojskowego[71]. Służba Kontrwywiadu Wojskowego wykonuje powyższe zadania w odniesieniu do Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, ataszatów obrony w placówkach zagranicznych, żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienionych w pkt. 1 i 2[72].

Szef Agencji Bezpieczeństwa Wewnętrznego pełni funkcję krajowej władzy bezpieczeństwa, a w odniesieniu do podmiotów podlegających właściwości Służby Kontrwywiadu Wojskowego za pośrednictwem Szefa tej służby (SKW). Zgodnie z ustawą z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych* Szef ABW organizuje współdziałanie z Szefem SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa.

Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych Traktatu Północnoatlantyckiego, Unii Europejskiej lub innych organizacji międzynarodowych[73].

W zakresie niezbędnym do wykonywania funkcji krajowej władzy bezpieczeństwa odpowiednio Szef ABW lub upoważnieni przez niego funkcjonariusze ABW oraz Szef SKW lub upoważnieni przez niego żołnierze lub funkcjonariusze mają prawo do:

- wglądu do dokumentów związanych z ochroną informacji niejawnych międzynarodowych,
- wstępu do obiektów i pomieszczeń przeznaczonych do przetwarzania informacji niejawnych międzynarodowych,
- dostępu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych,

[70] Ustawa z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182, poz. 1228), art. 10 ust. 1.

[71] Ibidem, art. 10 ust. 3.

[72] Ibidem, art. 10 ust. 2.

[73] Ibidem, art. 11 ust. 2.

- uzyskiwania wyjaśnień i informacji dotyczących informacji niejawnych międzynarodowych[74].

W zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych upoważnieni pisemnie funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mają prawo do wykonywania czynności określonych w ustawie *o ochronie informacji niejawnych.*

Prawa funkcjonariuszy ABW, funkcjonariuszy lub żołnierzy SKW w trakcie prowadzenia kontroli stanu zabezpieczenia informacji niejawnych:

- wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są przetwarzane,
- wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej,
- żądania udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania tych informacji,
- przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji,
- żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień,
- zasięgania w związku z przeprowadzaną kontrolą informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek,
- powoływania oraz korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych,
- uczestniczenia w posiedzeniach kierownictwa organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej[75].

Jeżeli w czasie wykonywania kontroli, o której jest mowa w art. 12 ust. 1 ustawy z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*, zostanie w znacznym stopniu uprawdopodobnione podejrzenie możliwości przetwarzania informacji niejawnych w systemach teleinformatycznych nieposiadających akredytacji bezpieczeństwa teleinformatycznego, funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mogą żądać udostępnienia do kontroli tych systemów wyłącznie w celu i zakresie niezbędnym do ustalenia, czy przetwarzanie takie miało miejsce oraz wyjaśnienia okoliczności z tym związanych.

Postępowanie sprawdzające, kontrolne postępowanie sprawdzające oraz postępowania bezpieczeństwa przemysłowego z wyłączeniem postępowań, o których jest mowa w art. 23 ust. 5 ustawy z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*, podlegają kontroli w zakresie prawidłowości ich realizacji. Zgodnie

[74] Ibidem, art. 11 ust. 4.

[75] Ibidem, art. 12 ust. 1.

z art. 23 ust. 5 niniejszej ustawy Agencja Wywiadu, Biuro Ochrony Rządu, Policja, Służba Więzienna, Służba Wywiadu Wojskowego, Straż Graniczna oraz Żandarmeria Wojskowa przeprowadzają samodzielnie postępowania sprawdzające odpowiednio wobec własnych funkcjonariuszy, żołnierzy i pracowników oraz osób ubiegających się o przyjęcie do służby lub pracy, a także osób wykonujących na ich rzecz czynności zlecone lub ubiegających się o wykonywanie tych czynności, z zastrzeżeniem wskazanym w art. 23 ust. 3 i 4 niniejszej ustawy.

Ustawodawca przyjął, że:

- Agencja Bezpieczeństwa Wewnętrznego przeprowadza poszerzone postępowanie sprawdzające wobec:
  - Szefa Służby Kontrwywiadu Wojskowego, Szefa Agencji Wywiadu, Szefa Centralnego Biura Antykorupcyjnego, Szefa Biura Ochrony Rządu, Komendanta Głównego Policji, Dyrektora Generalnego Służby Więziennej, Komendanta Głównego Straży Granicznej oraz osób przewidzianych na te stanowiska,
  - pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w Służbie Kontrwywiadu Wojskowego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Biura Ochrony Rządu, Policji, Służby Więziennej, Straży Granicznej,
- Służba Kontrwywiadu Wojskowego przeprowadza poszerzone postępowanie sprawdzające wobec:
  - Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Żandarmerii Wojskowej oraz osób przewidzianych na te stanowiska,
  - pełnomocników ochrony, zastępców pełnomocników ochrony oraz osób przewidzianych na te stanowiska w Służbie Kontrwywiadu Wojskowego, Agencji Bezpieczeństwa Wewnętrznego, Służbie Wywiadu Wojskowego oraz Żandarmerii Wojskowej.

Służby specjalne jak: Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego i Agencja Wywiadu, posiadają ustawowe uprawnienia do wykonywania czynności operacyjno-rozpoznawczych, każda w zakresie swojej właściwości.

Obowiązująca ustawa z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych* tworzy system, gdzie służby specjalne o charakterze kontrwywiadowczym i wywiadowczym zajmują dominującą pozycję w procesach związanych z ochroną informacji niejawnych w państwie (w czasie pokoju, stanie kryzysu i wojny).

ROZDZIAŁ 10

Ochrona infrastruktury krytycznej państwa

10.1. Elementy infrastruktury krytycznej

Ludzkości na każdym etapie historii towarzyszył rozwój infrastruktury, która w znacznej mierze zależała od zmian zachodzących w sferze nauki i techniki. Z uwagi na to, że infrastruktura może być rozumiana na wiele sposobów, poniżej zostaną przedstawione definicje pochodzące z różnych źródeł.

Tabela 88. Definicje infrastruktury

Źródło	Treść
Wielka encyklopedia powszechna, t. 5, Warszawa 1965, s. 54	Infrastruktura to podstawowe urządzenia i instytucje świadczące usługi niezbędne do należytego funkcjonowania produkcyjnych działów gospodarki. Rozróżnia się infrastrukturę ekonomiczną, która obejmuje urządzenia świadczące usługi w zakresie transportu, komunikacji, energetyki, irygacji, melioracji itd., oraz infrastrukturę społeczną, w skład której wchodzą urządzenia i instytucje świadczące usługi w dziedzinie prawa, bezpieczeństwa, kształcenia, oświaty, służby zdrowia itd.
T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Wrocław 1978, s. 82	Infrastruktura, należące do otoczenia organizacje z aparaturą, których funkcjonowanie stwarza warunki powstania i rozwoju rozpatrywanej organizacji.
W. Grzywacz, *Infrastruktura transportu*, Warszawa 1982, s. 34	Infrastruktura to podstawowe urządzenia i instytucje, wraz z niezbędnym wyposażeniem rzeczowym i osobowym, służące do zapewnienia materialnych i społecznych warunków jakiejkolwiek działalności w ramach całej gospodarki narodowej lub jej poszczególnych działów, gałęzi i jednostek podstawowych.
W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1988, s. 229	Infrastruktura to podstawowe urządzenia, przedsiębiorstwa i instytucje usługowe nieodzownie potrzebne do właściwego funkcjonowania produkcyjnych działów gospodarki.
J. Penc, *Leksykon biznesu*, Warszawa 1997, s. 163	Infrastruktura to urządzenia i instytucje usługowe (na przykład w dziedzinie transportu, komunikacji, oświaty, ochrony zdrowia itp.) niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki.

Rozwój infrastruktury transportu, red. K. Wojewódzka-Król, Gdańsk 1999, s. 14–15	Infrastruktura zapewnia utrzymanie więzi w ujęciu terytorialnym (co jest uważane za historycznie najstarszy przejaw infrastruktury, istniejący od czasów przemieszczania się społeczności), przyciąga ludzi i działalność gospodarczą.
Słownik terminów i definicji NATO, Warszawa 1998, s. 164	Infrastruktura to ogólny termin stosowany do określenia wszystkich stałych instalacji, budowli lub urządzeń wykorzystywanych do zabezpieczenia i kontroli sił zbrojnych.
Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2009, s. 47	Infrastruktura to obiekty, urządzenia stałe i instytucje (krajowe i międzynarodowe) niezbędne do należytego funkcjonowania społeczeństw, tzn. produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności.
M. Ciesielski, A. Szudrowicz, *Ekonomia transportu*, Poznań 2000, s. 7	Infrastruktura służy wszystkim rodzajom mobilności ludzi, przepływowi materii i energii oraz dyfuzji informacji.
D.F. Schultz, *What is Infrastructure*, http://iti.acns.nwu.edu/def_infr.html	Infrastruktura to urządzenia materialne umożliwiające ruch towarów, wyrobów, wody, ścieków, energii i informacji, ale nie obejmująca budynków (z wyjątkiem terminali transportowych) oraz pojazdów, a podstawowym celem infrastruktury jest wspomaganie ludzkiej działalności.

Źródło: Opracowanie własne na podstawie literatury przedmiotu

Przedstawione powyżej pojęcia infrastruktury i jej zakres nie są jednoznaczne. Są one zbieżne, jednak różnią się co do szczegółów wynikających z potrzeby konkretnego obszaru zainteresowania. W zależności od przyjętego celu do pojęcia infrastruktura wprowadza się różne elementy. Z uwagi na charakterystyczne cechy obiektów i usług można wyróżnić infrastruktury szczegółowe zob. tabela 89.

Tabela 89. Infrastruktury szczegółowe

Nazwa	Treść
Bilateralna	Infrastruktura, która dotyczy jedynie dwóch członków NATO i jest finansowana na podstawie dwustronnego porozumienia pomiędzy nimi (na przykład: urządzenia, z których korzystają siły jednego z państw członków NATO, znajdujące się na terytorium innego państwa)[1].
Narodowa	Infrastruktura zabezpieczana i finansowana przez państwo członkowskie NATO, na jego własnym terytorium, wyłącznie na użytek jego własnych sił zbrojnych (włączając w to siły zbrojne przydzielone lub wyznaczone do NATO)[2].
Państwa	Część infrastruktury obejmująca obiekty, urządzenia stałe i instytucje usługowe niezbędne do należytego funkcjonowanie produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności kraju[3].
Obronna	Infrastruktura stanowiąca część infrastruktury państwa, obejmująca obiekty i urządzenia stałe oraz instytucje niezbędne do funkcjonowania systemu obronnego państwa. Tworzona jest głównie w czasie pokoju, ale rozwijana również w okresie zagrożenia i wojny, z punktu widzenia specyfiki wyróżnia się m.in. infrastrukturę wojskową[4].

Wojskowa	Infrastruktura to element infrastruktury obronnej obejmujący wszystkie stacjonarne (a w wyjątkowych wypadkach także ruchome) obiekty i urządzenia, które zgodnie ze swoim przeznaczeniem służą do zaspokajania potrzeb sił zbrojnych, a w szczególności dowodzenia, bytowania, szkolenia i przemieszczania wojsk[5].
Wojskowa wg poglądów niemieckich	Infrastruktura to wszystkie stacjonarne obiekty i urządzenia, służące bezpośrednio i pośrednio do obrony kraju, które zostały zbudowane w oparciu o przepisy obowiązujące siły zbrojne i których koszty są ujęte w budżecie sił zbrojnych[6].
Wojskowa wg poglądów amerykańskich	Infrastruktura – termin ogólny stosowany na oznaczenie wszystkich stacjonarnych urządzeń, instalacji lub wyrobów służących zaspokajaniu potrzeb sił zbrojnych[7].
Obrony cywilnej	Infrastruktura stanowiąca część infrastruktury państwa. Obiekty i urządzenia warunkujące skuteczne działanie obrony cywilnej – przede wszystkim ochronę ludności[8].
Obrony cywilnej w ujęciu słownikowym	Infrastruktura to obiekty, urządzenia i instytucje warunkujące skuteczność wykonania zadań obrony cywilnej (techniczne systemy alarmowe i łączności, budowle ochronne, punkty zabiegów sanitarnych, punkty zabiegów specjalnych, ośrodki szkolenia, magazyny, stanowiska kierowania)[9].
Publiczna	Infrastruktura są to dobra mające charakter dóbr podstawowych o strategicznym znaczeniu dla całej gospodarki i społeczeństwa, umożliwiające przemieszczanie mediów (energii, wody, informacji) osób i rzeczy, udostępniane bezpłatnie lub za odpłatnością częściową. Na całość infrastruktury publicznej składa się infrastruktura gospodarcza (zwana inaczej ekonomiczną, techniczną, techniczno-ekonomiczną) oraz infrastruktura społeczna odgrywająca różne funkcje tak samo ważne dla kraju, jak i społeczeństwa[10].
Komunalna	Infrastruktura to zbiór urządzeń (na przykład: sieci uzbrojenia podziemnego, drogi, mosty, trakcje elektryczne itp.), instytucji (przedsiębiorstwa komunalne) niezbędnych do prawidłowego funkcjonowania gospodarki i społeczeństwa na terenie ich zamieszkania. Na infrastrukturę komunalną składa się: infrastruktura komunalna naziemna, infrastruktura komunalna podziemna, infrastruktura komunalna napowietrzna[11].
Informacyjna	Infrastruktura odnosi się do zasobów informacyjnych, włącznie z systemami komunikacji, które działają w przemyśle, różnych instytucjach lub którymi posługują się ludzie. Przykładem może być infrastruktura informacji jakiejś firmy, infrastruktura informacji finansowej, infrastruktura informacji obrony, krajowa infrastruktura informacji, globalna infrastruktura informacji[12].
Krytyczna infrastruktura teleinformatyczna	Obejmuje systemy i sieci teleinformatyczne niezbędne dla prowadzenia podstawowych działań gospodarczych i funkcjonowania instytucji publicznych w państwie[13].
Krytyczna	Infrastruktura to fizyczne i wirtualne systemy o zasadniczym znaczeniu dla minimalnego funkcjonowania gospodarki, rządu i państwa[14].
Krytyczna	Infrastruktura ta oznacza składniki, system lub część infrastruktury zlokalizowanej 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[15].

Infrastruktura krytyczna wg Unii Europejskiej	Europejska infrastruktura krytyczna lub „EIK" oznacza infrastrukturę krytyczną zlokalizowaną 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[16].
Krytyczna wg ustawy o zarządzaniu kryzysowym	Infrastruktura 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[17].

[1] *Słownik terminów i definicji NATO*, Warszawa 1998, s. 49.

[2] Ibidem, s. 208.

[3] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2009, s. 48.

[4] Ibidem, s. 48.

[5] Ibidem, s. 49.

[6] *Handbuch zur Ökonomie der Verteidigungspolitik*, Regensburg 1986, s. 972.

[7] *Dictionary of Military and Associated Terms*, Departament of Defense, US Government Printing Office, Washington 1989, s. 189.

[8] J. Marczak, J. Pawłowski, *O obronie militarnej Polski przełomu XX–XXI wieku*, Warszawa 1995.

[9] *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2009, s. 48.

[10] K. Brzozowska, M. Łatuszyńska, *Infrastruktura informacyjna jako element infrastruktury publicznej*, http;//mikro.uiv.szczecin.pl [pobrano 9.09.2012].

[11] S. Denczew, *Podstawy gospodarki komunalnej. Współczesne zagadnienia sektorów inżynieryjnych*, Białystok 2004, s. 17.

[12] D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 24 i 25.

[13] P. Sienkiewicz, W. Błażejczyk, E. Lichocki, M. Jóźwiak, H. Świeboda, *Analiza systemowa cyberterroryzmu jako zagrożenia dla bezpieczeństwa państwa. Analiza systemowa zagrożeń informatycznych w środowisku bezpieczeństwa państwa*, Warszawa 2006, s. 63.

[14] E. Lichocki, K. Kasperska, *Krytyczna infrastruktura teleinformatyczna w Polsce*, „Terroryzm" 2001, nr 1, s. 17.

[15] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 roku *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony* (Dz. Urz. UE L 345/75 z 23 grudnia 2008 r.).

[16] Ibidem.

[17] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 3 ust. 2.

Źródło: Opracowanie własne na podstawie literatury przedmiotu

Obok wskazanych wyżej infrastruktur szczegółowych z punktu widzenia bezpieczeństwa warto również zwrócić uwagę na infrastrukturę techniczną, zaliczaną do infrastruktury globalnej, oraz infrastrukturę geopolityczną i społeczną. Infrastruktura techniczna reprezentuje tzw. operacyjne wyposażenie terenu do działań kryzysowych, natomiast infrastruktura geopolityczna i społeczna związana jest ze stosunkami społeczno-politycznymi panującymi w danym społeczeństwie[1]. Systemy łączności i telekomunikacji usytuowane są w globalnym systemie infrastruktury technicznej. Obok tych systemów ważna jest również tzw.

[1] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe,* Warszawa 2007, s. 264 i 265.

infrastruktura obiektowa i infrastruktura transportowa: państwa, województwa, powiatu, gminy, zakładu pracy itd.

Elementy składowe infrastruktury obiektowej:

- obiekty użyteczności publicznej (urzędy, poczta, sądy, szpitale, banki),
- placówki kulturalno-oświatowe (szkoły, uczelnie, kina, teatry, muzea),
- obiekty i placówki handlowe (hipermarkety, sklepy, hale targowe, hurtownie, pasaże handlowe, domy towarowe),
- obiekty komunikacji publicznej (dworce, przystanki, poczekalnie),
- publiczne jednostki służb porządkowych (miejskich, wiejskich),
- jednostki ratowniczo-gaśnicze straży pożarnej (państwowej i ochotniczej),
- miejsca wielkich imprez masowych (stadiony, amfiteatry, plaże),
- zakłady pracy i siedziby różnych firm i przedsiębiorstw,
- magazyny i składy surowców, materiałów i produktów,
- jednostki sił zbrojnych,
- jednostki właściwe w sferze bezpieczeństwa wewnętrznego i zewnętrznego państwa.

Infrastruktura obiektowa ma szczególne znaczenie dla dużych skupisk ludności (aglomeracje miejskie), zalicza się tu m.in. obiekty i budowle sektora gospodarki komunalnej[2] obsługujące systemy zaopatrzenia ludności w energię, wodę, gaz, odprowadzania ścieków i odpadów komunalnych, utylizacji śmieci i gospodarki surowcami wtórnymi, bezpieczeństwa i sygnalizacji drogowej, monitoringu bezpieczeństwa publicznego.

Na gospodarkę komunalną składa się infrastruktura komunalna podziemna, naziemna, napowietrzna – zob. tabela 90.

Tabela 90. Elementy infrastruktury komunalnej

Nazwa infrastruktury	Elementy infrastruktury
Podziemna	sieci wodociągowe sieci kanalizacyjne sieci energetyczne sieci cieplne sieci gazowe sieci telekomunikacyjne metro melioracja miejska (kanały miejskie, drenaże) drogi (podziemne, tunele)
Naziemna	drogi naziemne (mosty) komunikacja (tory tramwajowe) zieleń miejska melioracje miejskie (rowy otwarte, wały przeciwpowodziowe)

[2] „Gospodarka komunalna stanowi dział gospodarki narodowej zarządzanej przez samorząd terytorialny (wojewódzki, powiatowy, gminny), a jej celem jest zaspokajanie materialno-bytowych potrzeb ludności miast poprzez świadczenia usług materialnych i niematerialnych". S. Denczew, *Podstawy gospodarki komunalnej. Współczesne zagadnienia sektorów inżynieryjnych*, Białystok 2004, s. 16.

Napowietrzna	drogi nadziemne (estakady, wiadukty) sieci energetyczne napowietrzne trakcje elektryczne dla tramwajów napowietrzne sieci telefoniczne napowietrzne

Źródło: Opracowano na podstawie S. Denczew, *Podstawy gospodarki komunalnej. Współczesne zagadnienia sektorów inżynieryjnych*, Białystok 2004, s. 26

Dla funkcjonowania państwa, województwa, powiatu, gminy, miasta, wsi ważna jest wspomniana globalna infrastruktura transportowa, na którą składają się elementy punktowe i elementy liniowe, ich strukturę przedstawiono w tabeli 91.

Tabela 91. Struktura globalnej infrastruktury transportowej

Nazwa infrastruktury	Elementy infrastruktury
Punktowa	porty lądowe, morskie, lotnicze, śródlądowe rozumiane jako miejsca krzyżowania się szlaków komunikacyjnych punkty przeładunkowe surowców, towarów i funkcjonujących w technologiach tzw. centrów logistycznych albo centrów dystrybucji punkty przesiadkowe dla pasażerów różnych gałęzi transportowych, np. stacje i dworce kolejowe, samochodowe, morskie i lotnicze specjalistyczne stacje i punkty serwisowania i obsługi różnych środków transportowych, np. stacje paliw, stacje diagnostyczne, warsztaty naprawcze, serwisy firmowe
Liniowa	kołowe drogi samochodowe (autostrady, drogi ekspresowe, drogi utwardzone, nieutwardzone, drogi publiczne i niepubliczne itp.) szlaki kolejowe (magistrale kolejowe, drogi normalnotorowe, drogi wąskotorowe i in.) szlaki i tory wodne (szlaki oceaniczne, morskie, tory podejściowe do portów, kanały morskie) korytarze powietrzne (kontynentalne, transkontynentalne, krajowe)

Źródło: Opracowano na podstawie K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 265

Na uwagę zasługuje również występujący w podziale gałęziowym transportu tzw. transport przesyłowy, który jest oparty na koncepcji ciągłych masowych przepływów między dwoma punktami. Na formy transportu przesyłowego składają się:

- transport rurociągowy obejmujący przesyłanie wody (wodociągi) i różnych surowców i paliw płynnych (ropociągi) i gazowych (gazociągi),
- transport taśmociągowy służący do przemieszczania dużych mas towarowych, głównie surowców i materiałów sypkich, głównie w strukturach różnych instalacji technologicznych, produkcyjnych, magazynowych,
- transport instalacyjny dotyczący przede wszystkim przesyłania energii elektrycznej na różnych odległościach w terenie oraz w różnych obiektach i pomieszczeniach mieszkalnych,

– transport instalacyjny to także współczesna sieć łączności, zwłaszcza tzw. łączność przewodowa oraz transmisja różnych sygnałów medialnych (radio, telewizja, Internet)[3].

Na systemie transportu przesyłowego w dużym stopniu opiera się współczesna gospodarka komunalna, a jej symbolem są ciągnące się setki kilometrów podziemne sieci wodociągowe i kanalizacyjne, sieci energetyczne różnych napięć i prądów czy sieci gazowe. Tym systemom transportu przesyłowego muszą towarzyszyć odpowiednie obiekty techniczne, takie jak: różne zbiorniki i przepompownie, stacje transformatorowe, oczyszczalnie ścieków i inne. W państwach rozwiniętych, w wielkich aglomeracjach światowych transport przesyłowy służy coraz częściej do przemieszczania ludzi – ruchome schody, ruchome chodniki czy japońskie wizje kapsuł osobowych poruszających się specjalnych tunelach powietrznych. Szczególnym systemem transportu przesyłowego jest miejska kolej podziemna (metro), służąca do przewozu wielkiej liczby pasażerów w granicach dużej aglomeracji miejskiej. Systemy i instalacje transportu przesyłowego, ze względu na takie cechy jak zdeterminowana trasa przebiegu oraz regularne przepływy wielkich ilości materiałów albo pasażerów, są narażone na wiele zagrożeń (w tym zamachów terrorystycznych)[4].

Postęp naukowo-techniczny i technologiczny sprawia, że społeczeństwa stopniowo uzależniają się od zdobyczy cywilizacyjnych, w tym od infrastruktury technicznej. W określonych sytuacjach uzależnienie to prowadzi do ubezwłasnowolnienia ludności w przypadku wystąpienia awarii. Ponadto stopniowo pojawiają się nowe rozwiązania techniczne, bez których człowiek nie wyobraża sobie codziennego życia. Oznacza to, że społeczeństwa państw wysoko rozwiniętych są bardziej podatne na uszkodzenia infrastruktury technicznej (naturalne i celowe) niż społeczeństwa państw słabo rozwiniętych. Infrastruktura tego charakteru nosi nazwę infrastruktury krytycznej państwa (IKP).

Do cech infrastruktury, w tym i infrastruktury krytycznej, zaliczamy:

- służebny charakter – nie istnieje sama dla siebie, lecz świadczy usługi dotyczące obsługi sfery produkcyjnej bądź konsumpcyjnej,
- bryłowatość urządzeń – oznacza, iż istnieje konieczność tworzenia całych obiektów ze względu na kwestie ekonomiczne oraz technologiczne, nie da się ich budować etapami,
- wysoka kapitałochłonność – tworzenie urządzeń infrastruktury pociąga za sobą konieczność ponoszenia znacznych kosztów, które ze względu na bryłowatość zwracają się dopiero po długim okresie,
- skokowy sposób powstawania kosztów – oznacza, iż koszty infrastruktury rosną co pewien czas jako konsekwencja niepodzielności urządzeń infrastruktury,
- długowieczność – czas użytkowania urządzeń infrastruktury jest bardzo długi,

[3] K. Ficoń, op. cit., s. 266.

[4] Ibidem, s. 267.

- immobilność – nie da się przenosić urządzeń infrastruktury, zaś usługi świadczone przez urządzenia infrastruktury mogą być konsumowane na miejscu,
- urządzenia infrastruktury są względem siebie komplementarne, a nie substytucyjne.

Funkcje infrastruktury:

- transferowa – stwarza warunki przepływu w przestrzeni dóbr, energii oraz ludzi,
- usługowa – zaspokaja popyt na usługi zgłaszany poprzez sferę produkcyjną oraz konsumpcyjną,
- integracyjna – kształtuje więź społeczną, ekonomiczną i informacyjną w układach regionalnych,
- lokalizacyjna – poziom rozwoju infrastruktury na danym terenie świadczy o poziomie jego atrakcyjności (dostępność sieci transportowej, energii, zasobów wodnych itp.),
- akceleracyjna – poziom zagospodarowania infrastrukturalnego stanowi przesłankę rozwoju gospodarczego określonych regionów; rezerwa potencjału infrastruktury stanowi istotny czynnik rozwoju gospodarczego danego obszaru.

W Polsce problematyka dotycząca infrastruktury krytycznej została uregulowana ustawą z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[5], gdzie w art. 3 pkt 2 ujęta została definicja infrastruktury krytycznej, przez którą należy rozumieć: 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. W myśl art. 3 pkt 2 ustawy do infrastruktury krytycznej zaliczone zostały systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Unia Europejska Dyrektywą Rady 2008/114/WE z dnia 8 grudnia 2008 roku *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*[6] nałożyła na państwa członkowskie UE obowiązek uwzględnienia tej problematyki w prawie wewnętrznym. W następstwie tego ustawa z dnia 26 października 2007 roku *o zarządzaniu kryzysowym* została znowelizowana. Tym samym ustawodawca, ustawą z dnia 29 października 2010 roku *o zmianie ustawy o zarządzaniu kryzysowym* (Dz. U. z 2010 r. Nr 240, poz. 1600) dokonał transpozycji dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 roku *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz*

[5] Dz. U. z 2007 r. Nr 89, poz. 580 z późn. zm.

[6] Dz. Urz. UE L 345/75 z 23 grudnia 2008 r.

oceny potrzeb w zakresie poprawy jej ochrony[7], w następstwie tego w art. 3 po pkt 2 ustawy *o zarządzaniu kryzysowym* dodano pkt 2a w brzmieniu:

> europejska infrastruktura krytyczna, 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:
> a) energii elektrycznej,
> b) ropy naftowej i gazu ziemnego,
> c) 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.

Tabela 92. Wykaz sektorów europejskiej infrastruktury krytycznej

Sektor	Podsektor	
Energia	energia elektryczna	infrastruktura i urządzenia do wytwarzania i przesyłania energii elektrycznej w odniesieniu do dostaw energii elektrycznej
	ropa naftowa	produkcja, rafinacja, przetwarzanie, magazynowanie i przesyłanie rurociągami ropy naftowej
	gaz	produkcja, rafinacja, przetwarzanie, magazynowanie i przesyłanie gazociągami gazu terminale skroplonego gazu ziemnego (LNG)
Transport	drogowy kolejowy lotniczy wodny śródlądowy żegluga oceaniczna, żegluga morska bliskiego zasięgu i porty	

Źródło: Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 roku *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony* (Dz. Urz. UE L 345/75 z 23 grudnia 2008 r.)

Należy podkreślić, że w porównaniu do rozwiązań przyjętych przez Unię Europejską, strona polska w ustawie z 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* uwzględniła rozbudowany katalog infrastruktury krytycznej, który jest katalogiem otwartym. Oznacza to, że wraz z pojawiającymi nowymi zagrożeniami dla sektorów ważnych dla bezpieczeństwa państwa będzie uaktualniany. Rozbudowaną listę sektorów infrastruktury krytycznej w państwie przedstawiono w tabeli 92.

[7] Dz. Urz. UE L 345 z 23 grudnia 2008 r., s. 75.

Tabela 93. Lista sektorów infrastruktury krytycznej

Sektor	Składniki sektorów
Energia	gaz, ropa naftowa, paliwa płynne urządzenia do wydobywania, przetwarzania i przechowywania gazu, ropy naftowej i paliw płynnych elektrownie energetyczne sieci transmisyjne i dystrybucyjne dostarczające elektryczność, gaz, ropę naftową oraz paliwa płynne do użytkowników końcowych
Woda	zasoby wodne, rezerwuary i zbiorniki wodne systemy transportowania i dostarczania wody do domów i do celów przemysłowych urządzenia do filtrowania i uzdatniania wody oraz systemy kontroli jakości wody system odbioru wody zużytej wraz z oczyszczalniami ścieków system dostarczania wody do instalacji przeciwpożarowych
Transport	transport drogowy wraz z drogami, autostradami, ciężarówkami i samochodami osobowymi transport kolejowy wraz z siecią połączeń kolejowych, stacje kolejowe i tabor kolejowy transport lotniczy wraz z siecią połączeń z liniami lotniczymi, lotniska i samoloty transport wodny – morski i oceaniczny wraz z flotą handlową portami i drogami wodnymi transport wodny – śródlądowy wraz flotą handlową portami i drogami wodnymi system dystrybucji towarów krytycznych ważnych dla bezpieczeństwa i stabilności gospodarki wraz z infrastrukturą
Systemy i technologia teleinformatyczna, łączność, ICT	sieci teleinformatyczne, oprogramowanie, procesy i ludzie dbający o prawidłowe działanie i bezpieczeństwo, instalacje służące pierwotnemu przechowywaniu i przetwarzaniu danych systemy automatyki i kontroli Internet stacjonarne systemy telekomunikacyjne, centrale telefoniczne mobilne systemy telekomunikacyjne łączność i nawigacja radiowa łączność i nawigacja satelitarna systemy powiadamiania
Zdrowie	szpitale zdrowie publiczne stacje przechowujące zapasy krwi laboratoria i instytucje badawcze przemysł farmaceutyczny
Żywność	produkcja żywności magazynowanie i dystrybucja żywności
Bankowość i finanse	banki i bankowość ubezpieczenia giełda systemy rezerw finansowych

Administracja państwowa	ministerstwo obrony służba ochrony państwa parlament kluczowe ministerstwa państwowe gwarantujące ciągłość działań rządu służby ratunkowe elektrownie jądrowe usługi doręczycielskie, poczta i spedycja centra zarządzania kryzysowego
Narodowe pomniki i pamiątki	budynki, pomniki i muzea o znaczeniu ogólnonarodowym, obiekty sportowe
Istotny przemysł dla gospodarki	przemysł zbrojeniowy przemysł ciężki produkcja i magazynowanie substancji niebezpiecznych (chemicznych, biologicznych i jądrowych) składowanie odpadów niebezpiecznych
Wymiar sprawiedliwości	sądownictwo i wymiar sprawiedliwości
Przestrzeń kosmiczna, eksploracja kosmosu	przestrzeń kosmiczna prowadzenie prac badawczych i wprowadzenie nowych technologii w przestrzeni kosmicznej
Kluczowe zasoby	centra handlowe budynki biurowe stadiony, areny i obiekty sportowe parki rozrywki budynki szkolne przemysł turystyczny

Źródło: E. Lichocki, K. Kasperska, *Krytyczna infrastruktura teleinformatyczna w Polsce*, „Terroryzm" 2010, nr 1, s. 16

Początek XXI wieku to powszechny dostęp do komputerów.

Są one tanie, często niewielkie, często połączone między sobą, wbudowane we wszystko, od kuchenki mikrofalowej po precyzyjne pociski kierowane. Komputery uczestniczą we wszystkich rodzajach procesów, włącznie z procesami biznesowymi, bankowością i finansami, transportem, nawigacją, dystrybucją energii elektrycznej i wody, edukacją, rozrywką, administracją rządową, opieką zdrowotną, pogotowiem, działaniami militarnymi. Umożliwiły one handel elektroniczny, telemedycynę, telekonferencję i telekomunikację. W konsekwencji informacje wrażliwe, kiedyś ograniczone do rozmów i dokumentów trzymanych w biurach, zostały teraz skomputeryzowane i są przesyłane publicznymi sieciami. Przez to są potencjalnie podatne na kradzieże, wykorzystanie i sabotaż przez osoby i instytucje znajdujące się w znacznej odległości[8].

Analiza zagrożeń dla infrastruktury państwa, w tym infrastruktury krytycznej, pokazuje, że jest ona coraz bardziej zależna od postępującego rozwoju i wdrożenia nowoczesnych technologii (np. teleinformatycznej). Obecnie stanowi ona zasób strategiczny każdego państwa. Ataki terrorystyczne (cyberataki)

[8] D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 17.

czy cyberprzestępców na systemy i sieci teleinformatyczne, grożą totalnym paraliżem administracji państwowej i gospodarki narodowej.

Terroryści, cyberprzestępcy mogą zaatakować infrastrukturę krytyczną państwa, której funkcjonowanie zależy od techniki teleinformatycznej. Atak na systemy i sieci teleinformatyczne w połączeniu z atakiem konwencjonalnym, atomowym, biologicznym lub chemicznym nie tylko zakłóca funkcjonowanie infrastruktury krytycznej, ale ją niszczy. Współcześnie sprawne działanie systemów i sieci teleinformatycznych ma kluczowe znaczenie dla funkcjonowania infrastruktury krytycznej państwa.

W celu niedopuszczenia do ataku lub zminimalizowania jego negatywnych następstw państwa podejmują działania o charakterze prawno-organizacyjnym, których zadaniem jest ochrona infrastruktury krytycznej.

10.2. Organy właściwe w sferze bezpieczeństwa infrastruktury krytycznej

Realizacja zadań w sferze wewnętrznego i zewnętrznego bezpieczeństwa państwa zależy od sprawnej infrastruktury krytycznej, która wspierana jest przez nowoczesne technologie, w tym teleinformatyczne. Stanowi ona część jego strategii bezpieczeństwa. Poszczególne elementy infrastruktury krytycznej są zależne od siebie, a uszkodzenie jednego powoduje naruszenie lub zniszczenie kolejnego elementu. Takim przykładem może być uszkodzenie systemu energetycznego czy systemów i sieci teleinformatycznych. Postępująca zależność od technik teleinformatycznych oznacza, że jest podatna na wiele zagrożeń, wymaga więc szczególnej uwagi i ochrony.

Zabezpieczenie infrastruktury krytycznej wymaga wypracowania zasad i procedur, które zapewnią ciągłość świadczenia usług, niezawodność i stałą gotowość skutecznego reagowania, pozwalającą nabrać przekonania, że będzie ona mniej podatna na potencjalne zagrożenia[9]. Celem ochrony krytycznej infrastruktury teleinformatycznej w Polsce jest zapewnienie niezawodności i ciągłości działania systemów i sieci teleinformatycznych o szczególnie ważnym znaczeniu dla funkcjonowania i bezpieczeństwa państwa, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla struktur organizacyjnych państwa, obronności, życia lub zdrowia ludzi, dziedzictwa narodowego, środowiska naturalnego, a także spowodować poważne straty materialne w mieniu[10]. Dla celów ochrony krytycznej infrastruktury teleinformatycznej powinno wykorzystywać się Sys-

[9] E. Lichocki, K. Kasperska, op. cit., s. 17.

[10] *Projekt ustawy o ochronie Krytycznej Infrastruktury Teleinformatycznej*. Stan na dzień 15 kwietnia 2005 roku.

tem Reagowania na Incydenty Komputerowe[11]. Zakres działania tak w sferze wojskowo-militarnej, jak i cywilnej obejmuje: obszar Polski, kontakty z Sojuszem Północnoatlantyckim i państwami członkowskimi, kontakty z Unią Europejską i państwami członkowskimi.

Współcześnie szczególnym rodzajem zagrożenia dla bezpieczeństwa środowiska międzynarodowego jest terroryzm. Poszczególne państwa, jak i organizacje międzynarodowe (np. ONZ, NATO, Unia Europejska, Wspólnota Niepodległych Państw, Szanghajska Organizacja Współpracy**)** podejmują działania mające na celu walkę z tym negatywnym zjawiskiem. Przyjmuje się, iż szczególne niebezpieczeństwo stanowią rozbudowane organizacje terrorystyczne o sieciowej strukturze, dysponujące międzynarodowymi powiązaniami oraz wsparciem finansowym, informacyjnym, organizacyjnym, logistycznym i medialnym.

Sytuacje kryzysowe spowodowane działaniami terrorystycznymi (cyberterrorystycznymi) stanowią szczególne zagrożenie praktycznie dla bezpieczeństwa każdego państwa. Wymaga to zatem posiadania wypracowanych procedur uruchomianych w ramach zarządzania kryzysowego w przypadku pojawienia się bezpośredniego czy pośredniego zagrożenia. Miedzy terroryzmem a sytuacją kryzysową istnieje ścisła współzależność powodowana nie tylko samym atakiem, ale przede wszystkim strachem, zniszczeniami, chaosem i nieprzewidywalnością. Elementem, który również potęguje skalę zagrożenia, jest nieprzewidywalność co do rodzaju środka wykorzystanego podczas ataku terrorystycznego. Mogą to być środki konwencjonalne lub niekonwencjonalne (broń biologiczna, chemiczna, radiacyjna, jądrowa, a także środki komunikacyjne wypełnione wymienionymi rodzajami broni masowego rażenia itd.).

Mimo że Polska nie doświadczyła na swoim terytorium ataku terrorystycznego, to z uwagi na przynależność do Sojuszu Północnoatlantyckiego i Unii Europejskiej, a także udział w międzynarodowej krucjacie antyterrorystycznej stanowi obiekt potencjalnego ataku. W tych warunkach istnieje konieczność przygotowania państwa i społeczeństwa do sytuacji kryzysowych związanych z zagrożeniem terroryzmem.

Państwa członkowskie Unii Europejskiej podejmują kompleksowe działania mające na celu walkę z terroryzmem, uwzględniając instrumenty administracyjne, karne, policyjne, militarne. Uporządkowania, koordynacji i wzmocnienia tych przedsięwzięć dotyczą liczne dokumenty polityczne i programowe. Istotnym dokumentem Unii Europejskiej, który nakłada na państwa członkowskie obowiązek walki z terroryzmem, jest Decyzja Ramowa Rady 2002/474/WSiSW z 13 czerwca 2002 roku *w sprawie zwalczania terroryzmu* (Dz. Urz. WE l 164/3 z 22 czerwca 2002 r.). Zgodnie z przepisami art. 1 ust. 1 niniejszej decyzji ramowej państwa członkowskie UE zobowiązane zostały do uznania za przestępstwa terrorystyczne zamierzonych czynów, określonych zgodnie z prawem krajowym jako przestępstwa i wymienionych w tym przepisie w formie zamkniętego katalogu,

[11] E. Lichocki, K. Kasperska, op. cit., s. 18.

które ze względu na swój charakter i kontekst mogą wyrządzić poważne szkody krajowi lub organizacji międzynarodowej, gdy zostaną popełnione w celu:

- poważnego zastraszenia ludności,
- bezprawnego zmuszenia rządu lub organizacji międzynarodowej do podjęcia lub zaniechania działania,
- poważnej destabilizacji lub zniszczenia podstawowych politycznych, konstytucyjnych, gospodarczych lub społecznych struktur kraju lub organizacji międzynarodowej.

Określenie katalogu czynów zabronionych, zawartego w dalszej części przepisu art. 1 ust. 1 omawianej decyzji ramowej, jest zobowiązaniem do kryminalizacji objętych jego zakresem zachowań w ustawodawstwie wewnętrznych państwa członkowskich Unii Europejskiej i obejmuje takie czyny, jak:

a) ataki na życie ludzkie, które mogą powodować śmierć,
b) ataki na integralność cielesną osoby,
c) porwania lub branie zakładników,
d) spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, włącznie ze zniszczeniem systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego, mogące zagrozić życiu ludzkiemu lub mogące spowodować poważne straty gospodarcze,
e) zajęcie statku powietrznego, statku lub innego środka transportu publicznego lub towarowego,
f) wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie broni, materiałów wybuchowych lub jądrowych, broni biologicznej lub chemicznej, jak również badania i rozwój broni biologicznej i chemicznej,
g) uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, których rezultatem jest zagrożenie życia ludzkiego,
h) zakłócenia lub przerwy w dostawach wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, których rezultatem jest zagrożenie życia ludzkiego,
i) grożenie popełnieniem czynów wymienionych w lit. a)–h).

Podstawowym dokumentem UE jest *Strategia Unii Europejskiej w dziedzinie walki z terroryzmem*, przyjęta przez Radę Europejską podczas spotkania 15–16 grudnia 2005 roku. Podstawę strategii stanowi walka Unii Europejskiej z terroryzmem w skali globalnej, z uwzględnieniem praw człowieka, tak aby Europa była obszarem wolności, bezpieczeństwa i sprawiedliwości dla swoich obywateli. Zadania te realizowane są m.in. w sferze reagowania na ataki antyterrorystyczne i zarządzania kryzysowego. Ten cel strategiczny zakłada podjęcie przygotowań do zapewnienia zarządzania kryzysowego skutkami ataków terrorystycznych oraz ograniczenia i likwidacji ich następstw. W ramach tych działań zakłada się także udzielanie pomocy ofiarom terroryzmu i ich rodzinom.

Problematyka ochrony infrastruktury krytycznej jest uwzględniona w wielu przepisach prawa międzynarodowego i krajowego.

Podstawy prawne ochrony infrastruktury krytycznej:

- Dyrektywa 95/46/EC Parlamentu Europejskiego z dnia 25 października 1995 roku *w sprawie przetwarzania danych osobowych oraz swobodnego przepływu tych danych*,
- Decyzja Komisji z dnia 15 czerwca 2001 roku *w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich*, na mocy dyrektywy 95/46/WE (notyfikowana jako dokument nr C(2001) 1539),
- Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 roku *dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej* (dyrektywa o prywatności i łączności elektronicznej),
- Decyzja Ramowa Rady 2002/474/WSiSW z 13 czerwca 2002 roku *w sprawie zwalczania terroryzmu*[12],
- Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 roku *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*[13],
- ustawa z dnia 21 listopada 1967 roku *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[14],
- ustawa z dnia 8 marca 1990 roku *o samorządzie gminnym*[15],
- ustawa z dnia 6 kwietnia 1990 roku *o Policji*[16],
- ustawa z dnia 12 października 1990 roku *o Straży Granicznej*[17],
- ustawa z 22 sierpnia 1997 roku *o ochronie osób i mienia*[18],
- ustawa z dnia 29 sierpnia 1997 roku *o ochronie danych osobowych*[19],
- ustawa z dnia 6 czerwca 1997 roku *Kodeks karny*[20],
- ustawa z dnia 16 kwietnia 2004 roku *o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*[21],
- ustawa z dnia 5 czerwca 1998 roku *o samorządzie województwa*[22],
- ustawa z dnia 5 czerwca 1998 roku *o samorządzie powiatowym*[23],

12 Dz. Urz. WE l 164/3 z 22 czerwca 2002 r.

13 Dz. Urz. UE L 345 z 23 grudnia 2008, s. 75.

14 Dz. U. z 2004 r. Nr 241, poz. 2416 z późn. zm.

15 Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.

16 Dz. U. z 1990 r. Nr 30, poz. 179 z późn. zm.

17 Dz. U. z 2005 r. Nr 234, poz. 1997 z późn. zm.

18 Dz. U. z 2005 r. Nr 145, poz. 1221 z późn. zm.

19 Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.

20 Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.

21 Dz. U. z 2004 r. Nr 93, poz. 889.

22 Dz. U. z 2001 r. Nr 142, poz. 1590 z późn. zm.

23 Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.

- ustawa z dnia 16 listopada 2000 roku *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[24],
- ustawa z dnia 16 marca 2001 roku *o Biurze Ochrony Rządu*[25],
- ustawa z dnia 24 sierpnia 2001 roku *o Żandarmerii Wojskowej i wojskowych organach porządkowych*[26],
- ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[27],
- ustawa z dnia 9 czerwca 2006 roku *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[28],
- ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[29],
- ustawa z dnia 27 sierpnia 2009 roku *o Służbie Celnej*[30],
- ustawa z dnia 23 stycznia 2009 roku *o wojewodzie i administracji rządowej w województwie*[31],
- ustawa z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*[32],
- ustawa z dnia 29 października 2010 roku *o zmianie ustawy o zarządzaniu kryzysowym*[33],
- rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 roku *w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*[34],
- rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 roku *w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego*[35],
- rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego*[36],
- rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*[37],
- rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury* krytycznej[38],

[24] Dz. U. z 2010 r. Nr 46, poz. 276 z późn. zm.
[25] Dz. U. z 2001 r. Nr 27, poz. 298 z późn. zm.
[26] Dz. U. z 2001 r. Nr 123, poz. 1353 z późn. zm.
[27] Dz. U. z 2010 r. Nr 29, poz. 154 z późn zm.
[28] Dz. U. z 2006 r. Nr 104, poz. 709 z późn. zm.
[29] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.
[30] Dz. U. z 2009 r. Nr 168, poz. 1323 z późn. zm.
[31] Dz. U. z 2009 r. Nr 31, poz. 206 z późn. zm.
[32] Dz. U. z 2010 r. Nr 182, poz. 1228.
[33] Dz. U. z 2010 r. Nr 240, poz. 1600.
[34] Dz. U. z 2003 r. Nr 116, poz. 1090 z późn. zm.
[35] Dz. U. z 2009 r. Nr 226, poz. 1810.
[36] Dz. U. z 2010 r. Nr 540, poz. 540.
[37] Dz. U. z 2010 r. Nr 540, poz. 541.
[38] Dz. U. z 2010 r. Nr 540, poz. 542.

- rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 roku *w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*[39],
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*[40],
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 roku *w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych*[41].

Do innych dokumentów należy zaliczyć:

- Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 roku,
- Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016.

Podstawowym aktem prawnym regulującym kwestie dotyczące ochrony infrastruktury krytycznej jest ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*[42] wraz z przepisami wykonawczymi. Niniejsza ustawa w art. 3 pkt 3 definiuje pojęcie ochrony infrastruktury krytycznej, przez którą należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzyku 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.

Przyjęcie ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* skutkowało wypełnieniem istniejących luk prawnych dotyczących braku w naszym ustawodawstwie przepisów traktujących o przeciwdziałaniu terroryzmowi:

- po pierwsze, wprowadzono powszechny obowiązek informowania o zagrożeniach terrorystycznych,
- po drugie, wprowadzono obowiązek planowego przeciwdziałania spodziewanym następstwom zdarzeń o charakterze terrorystycznym,
- po trzecie, przypisano te zadania odpowiednio organom administracji publicznej na wszystkich poziomach zarządzania bezpieczeństwem państwa.

Wynika to z charakteru zagrożenia, jakim jest terroryzm, co oznacza, że trudno jest wskazać tylko jeden podmiot właściwy w walce z tym zjawiskiem.

Wskazanie i omówienie zadań dotyczących przeciwdziałania zagrożeniom terroryzmem należy zacząć od stwierdzenia, że Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku w art. 146 określa kierunki i charakter działania Rady Ministrów, a także jej kompetencje[43], które nie mają wyczerpującego charakteru.

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

[40] Dz. U. z 2004 r. Nr 100, poz. 1024.

[41] Dz. U. z 2008 r. Nr 229, poz. 1536.

[42] Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.

[43] Dz. U. z 1997 r. Nr 78, poz. 483.

Na podkreślenie zasługuje rola Rady Ministrów w sferze zewnętrznego i wewnętrznego bezpieczeństwa państwa, gdzie stykają się kompetencje zarówno Prezydenta RP, Rady Ministrów, jak i właściwych ministrów, którzy realizują w tym obszarze politykę określoną przez rząd. W procesie zarządzania bezpieczeństwem państwa na poziomie kraju do istotnych kompetencji Prezesa Rady Ministrów należy kierowanie pracami Rady Ministrów, które obejmuje zwoływanie posiedzeń rządu, przewodzenie jego obradom, dzięki czemu Premier posiada możliwość oddziaływania na przebieg jego prac i treść podejmowanych uchwał. Oznacza to, że Prezes Rady Ministrów w celu koordynacji działań m.in. w dziedzinie ochrony infrastruktury krytycznej państwa wydaje wiążące wytyczne oraz żąda informacji i opinii od następujących podmiotów:

- ministra właściwego do spraw wewnętrznych w odniesieniu do działalności Policji, Straży Granicznej, Biura Ochrony Rządu,
- Ministra Obrony Narodowej w odniesieniu do działalności Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Żandarmerii Wojskowej,
- Ministra Sprawiedliwości w odniesieniu do działalności Służby Więziennej,
- ministra właściwego do spraw finansów publicznych w odniesieniu do działalności Służby Celnej, urzędów i izb skarbowych, organów kontroli skarbowej oraz organów informacji finansowej,
- Szefa Agencji Bezpieczeństwa Wewnętrznego w odniesieniu do działalności Agencji,
- Szefa Agencji Wywiadu w odniesieniu do działalności Agencji.

Natomiast ministrowie kierują określonymi działami administracji rządowej lub wypełniają zadania wyznaczone im przez Prezesa Rady Ministrów. Zakres działania ministra kierującego działem administracji rządowej określają ustawy[44].

W polskim systemie prawnym zakres poszczególnych działów administracji rządowej określa ustawa z dnia 4 września 1997 roku o działach administracji rządowej[45]. Natomiast realizacja zadań związanych z ochroną infrastruktury krytycznej określa ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym*, i tak:

- zadania z zakresu planowania cywilnego obejmują m.in. przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej[46],
- zadania z zakresu ochrony infrastruktury krytycznej obejmują:
  - gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej,
  - opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej,
  - odtwarzanie infrastruktury krytycznej,

[44] Art. 149 ust. 1 Konstytucji Rzeczypospolitej Polskiej.

[45] Dz. U. z 1997 r. Nr 141, poz. 943 z późn. zm.

[46] Ustawa dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 4 ust. 1 pkt 5.

– współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony[47].

W celu realizacji zadań dotyczących ochrony infrastruktury krytycznej tworzone są następujące plany:

- Krajowy Plan Zarządzania Kryzysowego oraz wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego,
- na potrzeby Krajowego Planu Zarządzania Kryzysowego ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają *Raport o zagrożeniach bezpieczeństwa narodowego*,
- Narodowy Program Ochrony Infrastruktury Krytycznej[48].

Jeżeli dla obiektów, instalacji, urządzeń i usług infrastruktury krytycznej istnieją tworzone na podstawie innych przepisów plany odpowiadające wymogom planu ochrony infrastruktury krytycznej, uznaje się, iż wymóg posiadania takiego planu jest spełniony.

W proces ochrony infrastruktury krytycznej muszą być zaangażowane wszystkie uprawnione podmioty, począwszy od administracji rządowej, a kończąc na administracji samorządowej, które wykonują zadania dotyczące zarządzania kryzysowego – zob. tabela 94.

Tabela 94. Podmioty realizujące zadania dotyczące ochrony infrastruktury krytycznej

Podmioty	Zadania
Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych	zgodnie z zakresem swojej właściwości organizują realizację zadań z zakresu ochrony infrastruktury krytycznej (art. 12 ust. 2 pkt 4 ustawy)
Wojewoda	realizuje zadania z zakresu planowania cywilnego organizuje wykonanie zadań z zakresu ochrony infrastruktury krytycznej (art. 14 ust. 2 pkt 7 ustawy)
Zarząd województwa	uczestniczy w realizacji zadań z zakresu zarządzania cywilnego, w tym planowania cywilnego, co obejmuje ochronę infrastruktury krytycznej (art. 15 ustawy)
Starosta	realizuje zadania z zakresu planowania cywilnego organizuje i realizuje wykonanie zadań z zakresu ochrony infrastruktury krytycznej (art. 17 ust. 2 pkt 6 ustawy)
Wójt, burmistrz, prezydent miasta	w sprawach zarządzania kryzysowego realizuje zadania z zakresu planowania cywilnego, w tym organizuje i realizuje zadania z zakresu ochrony infrastruktury krytycznej (art. 19 ust. 2 pkt 6 ustawy)
Szef Agencji Bezpieczeństwa Wewnętrznego	zgodnie z art. 12a ustawy

Źródło: Opracowano na podstawie ustawy z dnia 27 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.)

[47] Ibidem, art. 6 ust. 1.

[48] Ibidem, art. 5, 5a ust. 1 i 5b ust. 1.

W polskim systemie ochrony antyterrorystycznej istnieją dwa poziomy: strategiczny i wykonawczy.

Na poziomie strategicznym zadania realizowane są przez Prezesa Rady Ministrów, Ministerstwo Spraw Wewnętrznych, Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego. Obok wymienionych podmiotów ważną rolę odgrywają Międzyresortowy Zespół ds. Zagrożeń Terrorystycznych i Kolegium ds. Służb Specjalnych.

Międzyresortowy Zespół ds. Zagrożeń Terrorystycznych został powołany zarządzeniem Nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 roku *w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych* na podstawie art. 12 ust. 1 pkt 3 i ust. 2 ustawy z dnia 8 sierpnia 1996 r. *o Radzie Ministrów*[49]. Zespół jest organem pomocniczym Rady Ministrów i zapewnia współdziałanie administracji rządowej w zakresie rozpoznawania, przeciwdziałania i zwalczania terroryzmu. Jego przewodniczącym jest Minister Spraw Wewnętrznych i Administracji. Do zadań Zespołu należy:

- monitorowanie zagrożeń o charakterze terrorystycznym, ich analiza i ocena, a także przedstawianie opinii i wniosków dla Rady Ministrów,
- opracowywanie projektów standardów i procedur w zakresie zwalczania terroryzmu, w szczególności standardów oceny występowania zagrożenia i określania jego poziomu,
- inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej, w szczególności w zakresie wykorzystania informacji oraz rozpoznawania, przeciwdziałania i zwalczania terroryzmu,
- występowanie z wnioskiem do właściwych ministrów w celu podjęcia działań legislacyjnych zmierzających do usprawnienia metod i form zwalczania terroryzmu; organizowanie współpracy z innymi państwami w zakresie zwalczania terroryzmu oraz koordynacja wymiany informacji i organizowanych wspólnych operacji,
- inicjowanie szkoleń i konferencji dotyczących zwalczania terroryzmu,
- opracowywanie propozycji zmierzających do usprawnienia metod i form zwalczania terroryzmu oraz występowanie z wnioskiem do właściwych organów o podjęcie w tym zakresie prac legislacyjnych[50].

  Skład Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych:
  - przewodniczący – Minister Spraw Wewnętrznych i Administracji,
  - zastępcy – Minister Finansów, Minister Obrony Narodowej, Minister Spraw Zagranicznych, Minister Sprawiedliwości, a także minister-członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, jeżeli został wyznaczony przez Prezesa Rady Ministrów,

[49] Dz. U. z 2003 r. Nr 24, poz. 199, z późn. zm.

[50] Zarządzenie Nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. *w sprawie utworzenia Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych* http://bip.kprm.gov.pl

członkowie:
- sekretarz lub podsekretarz stanu w Ministerstwie Spraw Wewnętrznych i Administracji sprawujący nadzór nad prowadzeniem spraw objętych działem administracji rządowej – sprawy wewnętrzne w zakresie ochrony bezpieczeństwa i porządku publicznego,
- sekretarz lub podsekretarz stanu w Ministerstwie Spraw Wewnętrznych i Administracji, sprawujący nadzór nad prowadzeniem spraw objętych działem administracji rządowej – sprawy wewnętrzne w zakresie zarządzania kryzysowego, obrony cywilnej, ochrony przeciwpożarowej, przeciwdziałania skutkom klęsk żywiołowych i innych podobnych zdarzeń zagrażających bezpieczeństwu powszechnemu,
- Sekretarz Kolegium do Spraw Służb Specjalnych lub osoba go zastępująca,
- Szef Obrony Cywilnej Kraju lub jego zastępca,
- Szef Agencji Bezpieczeństwa Wewnętrznego lub jego zastępca,
- Szef Agencji Wywiadu lub jego zastępca,
- Szef Biura Ochrony Rządu lub jego zastępca,
- Komendant Główny Policji lub jego zastępca,
- Komendant Główny Straży Granicznej lub jego zastępca,
- Komendant Główny Państwowej Straży Pożarnej lub jego zastępca,
- Szef Sztabu Generalnego Wojska Polskiego lub jego zastępca,
- Szef Służby Wywiadu Wojskowego lub jego zastępca,
- Szef Służby Kontrwywiadu Wojskowego lub jego zastępca,
- Komendant Główny Żandarmerii Wojskowej lub jego zastępca,
- Generalny Inspektor Kontroli Skarbowej lub osoba go zastępująca,
- Generalny Inspektor Informacji Finansowej lub osoba go zastępująca,
- Dyrektor Rządowego Centrum Bezpieczeństwa lub osoba go zastępująca,
- Szef Służby Celnej lub jego zastępca.

Członkowie Zespołu mogą zaprosić do udziału w pracach Zespołu osoby, których wiedza i doświadczenie może być przydatne, po uprzednim wyrażeniu zgody przez Przewodniczącego Zespołu.

Kolegium ds. Służb Specjalnych działa przy Radzie Ministrów, jest organem opiniodawczo-doradczym w sprawach programowania, nadzorowania i koordynowania działalności Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego oraz podejmowanych dla ochrony bezpieczeństwa państwa działań Policji, Straży Granicznej, Żandarmerii Wojskowej, Służby Więziennej, Biura Ochrony Rządu, Służby Celnej, urzędów skarbowych, izb skarbowych, organów kontroli skarbowej, organów informacji finansowej oraz służb rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej. Podstawę prawną działania Kolegium ds. Służb Specjalnych stanowi ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[51].

[51] T. j.: Dz. U. z 2010 r. Nr 29, poz. 154.

Do zadań Kolegium ds. Służb Specjalnych należy formułowanie ocen lub wyrażanie opinii w sprawach:
- kierunków i planów działania służb specjalnych,
- projektów aktów normatywnych i innych dokumentów rządowych dotyczących działalności służb specjalnych,
- wykonywania przez służby specjalne powierzonych im zadań zgodnie z kierunkami i planami działania tych służb,
- rocznych sprawozdań przedstawianych przez Szefów z działalności podległych im służb specjalnych,
- koordynowania działalności Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego, a także działalności służb specjalnych z Policją, Strażą Graniczną, Żandarmerią Wojskową, Biurem Ochrony Rządu, Służbą Celną, urzędami skarbowymi, izbami skarbowymi, organami kontroli skarbowej, organami informacji finansowej i służbami rozpoznania Sił Zbrojnych RP oraz ich współdziałania w dziedzinie ochrony bezpieczeństwa państwa,
- współdziałania organów administracji rządowej, organów samorządu terytorialnego, instytucji państwowych oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej ze służbami specjalnymi,
- współdziałania służb specjalnych z właściwymi organami i służbami innych państw,
- organizacji wymiany informacji istotnych dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej pomiędzy organami administracji rządowej[52].

W skład Kolegium ds. Służb Specjalnych wchodzą: przewodniczący – Prezes Rady Ministrów, sekretarz Kolegium, członkowie: minister właściwy do spraw wewnętrznych, minister właściwy do spraw zagranicznych, Minister Obrony Narodowej, minister właściwy do spraw finansów publicznych, Szef Biura Bezpieczeństwa Narodowego, minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, jeśli został wyznaczony przez Prezesa Rady Ministrów. W posiedzeniach Kolegium uczestniczą także Szefowie: Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Przewodniczący Sejmowej Komisji do Spraw Służb Specjalnych. Prezydent Rzeczypospolitej Polskiej może delegować swojego przedstawiciela do udziału w posiedzeniach Kolegium. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach przewodniczących właściwych komisji sejmowych, przedstawicieli organów państwowych oraz inne osoby, których uczestnictwo jest niezbędne ze względu na tematykę obrad.

[52] Ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (T. j.: Dz. U. z 2010 r. Nr 29, poz. 154), art. 12 ust. 1.

Na poziomie wykonawczym zadania dotyczące ochrony antyterrorystycznej wykonują podmioty właściwe w sferze bezpieczeństwa wewnętrznego państwa:

- Agencja Bezpieczeństwa Wewnętrznego[53],
- Agencja Wywiadu – rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej[54],
- Służba Kontrwywiadu Wojskowego – rozpoznawanie, zapobieganie oraz wykrywanie popełnionych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON przestępstw związanych z działalnością terrorystyczną, godzących w bezpieczeństwo potencjału obronnego państwa, Sił Zbrojnych RP, a także państw, które zapewniają wzajemność[55],
- Służba Wywiadu Wojskowego – rozpoznawanie i przeciwdziałanie zagrożeniom międzynarodowym terroryzmem[56],
- Policja – wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców[57],
- Straż Graniczna – prowadzenie czynności w celu rozpoznawania i przeciwdziałania zagrożeniom terroryzmem[58],
- Służba Celna – rozpoznawanie, wykrywanie, zapobieganie i zwalczanie przestępstw i wykroczeń związanych z naruszeniem przepisów dotyczących wprowadzania na terytorium Rzeczypospolitej Polskiej oraz wyprowadzania z jej terytorium towarów objętych ograniczeniami lub zakazami obrotu ze względu na bezpieczeństwo i porządek publiczny lub bezpieczeństwo międzynarodowe, w szczególności takich, jak odpady, substancje i preparaty chemiczne, materiały jądrowe i promieniotwórcze, środki odurzające i substancje psychotropowe, broń, amunicja, materiały wybuchowe oraz towary i technologie o znaczeniu strategicznym[59],
- Żandarmeria Wojskowa – zapewnienie porządku na terenie obiektów wojskowych oraz w miejscach publicznych, a przy tym ochrona życia i zdrowia ludzi oraz mienia wojskowego przed zamachami zakłócającymi te dobra[60],
- Generalny Inspektor Informacji Finansowej – uzyskiwanie, gromadzenie, przetwarzanie i analizowanie informacji w trybie określonym w ustawie oraz podejmowanie działań w celu przeciwdziałania praniu pieniędzy oraz finan-

[53] Ibidem, art. 5 ust. 2.

[54] Ibidem, art. 6 ust. 1 pkt 6.

[55] Ustawa z dnia 9 czerwca 2006 roku *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz. U. z 2006 r. nr 104, poz. 709 z późn. zm.), art. 5 ust. 1 lit. g.

[56] Ibidem, art. 6 ust. 1 pkt 2 lit. b.

[57] Ustawa z dnia 6 kwietnia 1990 roku *o Policji* (T. j.: Dz. U. z 2011 r. Nr 287, poz. 1687), art. 1 ust. 2 pkt 4.

[58] Ustawa z dnia 12 października 1990 roku *o Straży Granicznej* (T. j.: Dz. U. z 2011 r. Nr 116, poz. 675), art. 1 ust. 2 pkt 5d.

[59] Ustawa z dnia 27 sierpnia 2009 roku *o Służbie Celnej* (Dz. U. z 2009 r. Nr 168, poz. 1323 z późn. zm.), art. 2 ust. 1 pkt 4.

[60] Ustawa z dnia 24 sierpnia 2001 roku *o Żandarmerii Wojskowej i wojskowych organach porządkowych* (Dz. U. z 2001 r. Nr 123, poz. 1353 z późn. zm.), art. 4 ust. 1.

sowaniu terroryzmu, a w szczególności badanie przebiegu transakcji, co do których Generalny Inspektor powziął uzasadnione podejrzenia: przeprowadzanie procedury wstrzymania transakcji lub blokady rachunku, rozstrzyganie w przedmiocie zwolnienia zamrożenia wartości majątkowych, udostępnianie i żądanie przekazania informacji o transakcjach, przekazywanie uprawnionym organom dokumentów uzasadniających podejrzenie popełnienia przestępstwa, inicjowanie i podejmowanie innych działań w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, w tym szkolenie pracowników instytucji obowiązanych w zakresie zadań nałożonych na te instytucje, sprawowanie kontroli przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, współpraca z zagranicznymi instytucjami i międzynarodowymi organizacjami zajmującymi się przeciwdziałaniem praniu pieniędzy lub finansowaniu terroryzmu; nakładanie kar pieniężnych, o których mowa w ustawie[61].

- Służba Więzienna.

Na podkreślenie zasługują zbliżone składy: Rządowego Zespołu Zarządzania Kryzysowego, Kolegium do Spraw Służb Specjalnych i Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych, co w procesie ochrony infrastruktury krytycznej państwa ma istotne znaczenie praktyczne. Członkowie wymienionych podmiotów z uwagi na posiadaną wiedzę specjalistyczną i dostęp do określonych informacji mogą przedstawić Radzie Ministrów rozwiązania adekwatne do zagrożenia dla infrastruktury krytycznej.

W procesie ochrony infrastruktury krytycznej państwa obok wymienionych wyżej podmiotów ważną rolę odgrywają właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej, którzy mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia[62]. Wskazane podmioty mają obowiązek wyznaczyć w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie obiektów, instalacji lub usług osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej.

[61] Ustawa z dnia 16 listopada 2000 roku *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Dz. U. z 2010 r. Nr 46, poz. 276 z późn. zm.), art. 4 ust. 1.

[62] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 6 ust. 5.

10.3. Rola Agencji Bezpieczeństwa Wewnętrznego w ochronie infrastruktury krytycznej

Szczególne zadania w sytuacji zagrożeń terrorystycznych dla infrastruktury krytycznej ustawodawca powierzył Szefowi Agencji Bezpieczeństwa Wewnętrznego (ABW), który jest centralnym organem administracji rządowej właściwym w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Podstawę prawną działania Agencji stanowi ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[63]. Jednym z zadań Agencji Bezpieczeństwa Wewnętrznego jest rozpoznawanie, zapobieganie i wykrywanie przestępstw: szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo państwa[64]. Pozyskiwanie i analizowanie informacji dotyczących zagrożeń terrorystycznych pozwala na ocenę źródeł i skali zjawiska, wytypowanie grup potencjalnych zamachowców, rozpoznanie ich planów i zaplecza logistycznego. Walka z terroryzmem wymaga jednak ścisłej współpracy z innymi służbami i instytucjami państwowymi oraz organizacjami międzynarodowymi. Skuteczną koordynację działań podejmowanych przez jednostki odpowiedzialne za ochronę antyterrorystyczną Polski zapewnia utworzone 1 października 2008 roku powołane w ramach Agencji Bezpieczeństwa Wewnętrznego Centrum Antyterrorystyczne (CAT).

Centrum Antyterrorystyczne jest jednostką o charakterze koordynująco-analitycznym w zakresie przeciwdziałania działania terroryzmowi i jego zwalczania. CAT funkcjonuje w systemie całodobowym 7 dni w tygodniu. Służbę w nim pełnią, oprócz funkcjonariuszy ABW, oddelegowani funkcjonariusze, żołnierze i pracownicy m.in.: Policji, Straży Granicznej, Biura Ochrony Rządu, Agencji Wywiadu, Służby Wywiadu Wojskowego, Służby Kontrwywiadu Wojskowego oraz Służby Celnej. Ich oddelegowanie odbywa się na podstawie przepisów obowiązujących w jednostkach macierzystych i wykonują zadania w ramach kompetencji instytucji, którą reprezentują. Ponadto z Centrum Antyterrorystycznym aktywnie współpracują inne podmioty uczestniczące w systemie ochrony antyterrorystycznej RP, takie jak Rządowe Centrum Bezpieczeństwa, Ministerstwo Spraw Zagranicznych, Państwowa Straż Pożarna, Generalny Inspektor Informacji Finansowej, Sztab Generalny Wojska Polskiego, Żandarmeria Wojskowa.

Istotą systemu funkcjonowania Centrum Antyterrorystycznego ABW jest koordynacja procesu wymiany informacji między uczestnikami systemu ochrony antyterrorystycznej, co pozwala na wypracowanie i wdrażanie wspólnych procedur reagowania w przypadku:

[63] T. j.: Dz. z 2010 r. Nr 29, poz. 154 z późn. zm.

[64] Ustawa z dnia 24 maja 2002 roku o *Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (T. j.: Dz. z 2010 r. Nr 29, poz. 154 z późn. zm.), art. 5 ust. 2.

- zdarzenia terrorystycznego zaistniałego poza granicami Polski mającego wpływ na bezpieczeństwo RP i jej obywateli,
- zdarzenia terrorystycznego zaistniałego na terenie Polski mającego wpływ na bezpieczeństwo RP i jej obywateli,
- uzyskania informacji o potencjalnych zagrożeniach mogących wystąpić na terenie Polski i poza granicami RP,
- uzyskania informacji dotyczących prania pieniędzy lub transferów środków finansowych mogących świadczyć o finansowaniu działalności terrorystycznej.

Podstawową funkcją Centrum Antyterrorystycznego ABW jest koordynacja w zakresie analityczno-informacyjnym oraz działań służb i instytucji uczestniczących w zabezpieczeniu kraju przed zagrożeniami ze strony terroryzmu. Centrum wypełnia tę funkcję poprzez realizację następujących zadań:

- Wspomaganie procesów decyzyjnych w przypadku realnego zagrożenia atakiem terrorystycznym, CAT niezwłocznie po uzyskaniu informacji o możliwym zamachu przekazuje m.in. Prezesowi Rady Ministrów, Ministrowi Spraw Wewnętrznych oraz Dyrektorowi Rządowego Centrum Bezpieczeństwa wszelkie dane pozwalające na przygotowanie i zabezpieczenie sił i środków niezbędnych do prawidłowego reagowania kryzysowego.
- Koordynacja działań operacyjno-rozpoznawczych w zakresie zwalczania terroryzmu, obejmuje m.in.:
  - cykliczne lub doraźne narady osób szczebla decyzyjnego, w trakcie których określane są zadania do realizacji w ramach rozpoznawanych zagrożeń oraz wytyczane perspektywiczne kierunki i obszary aktywności służb i instytucji państwowych,
  - stałe przekazywanie sygnałów o potencjalnych zagrożeniach dla kierownictw instytucji współpracujących z CAT celem podejmowania na bieżąco działań zgodnie z algorytmami reagowania w sytuacjach zagrożenia,
  - monitoring aktywności organizacji terrorystycznych i ich członków oraz struktur wspierających,
  - monitoring poziomu bezpieczeństwa obiektów mogących stanowić potencjalne cele ataku terrorystycznego.
- Wykonywanie czynności analityczno-informacyjnych, które obejmują sporządzanie m.in.:
  - aktualnych, syntetycznych i całościowych informacji dla kierownictwa państwa (Prezydenta RP, Prezesa Rady Ministrów) na temat poziomu zagrożenia terrorystycznego kraju oraz działań podejmowanych przez służby i instytucje państwowe w celu zniwelowania niebezpieczeństw,
  - prognoz długo- i krótkookresowych poziomu zagrożenia terrorystycznego Polski,
  - analiz zagrożenia terrorystycznego w innych państwach w kontekście bezpieczeństwa strategicznych interesów i obywateli RP.

- Udział w opracowywaniu i nowelizowaniu procedur reagowania kryzysowego na wypadek ataku oraz sporządzanie algorytmów działań przed zamachem (Centrum Antyterrorystyczne uczestniczy w działaniach weryfikujących skuteczność aktualnie wykorzystywanych schematów postępowania w sytuacjach kryzysowych. Stara się także wykrywać i analizować słabe punkty zarządzania kryzysowego przy jednoczesnym wskazaniu potencjalnych strategii i kierunków dalszych działań).
- Monitoring zagranicznych mediów sympatyzujących z terrorystami.
- Wspomaganie po ewentualnym zamachu terrorystycznym działań służb i instytucji uczestniczących w ochronie antyterrorystycznej Polski.

Centrum Antyterrorystyczne ABW kontynuuje działalność koordynacyjną w zakresie analityczno-informacyjnym także po wystąpieniu sytuacji kryzysowej, jaką jest zamach terrorystyczny. Zgodnie z ustawą z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* Szef Agencji Bezpieczeństwa Wewnętrznego uczestniczy w realizacji czynności z zakresu likwidacji skutków zdarzeń o charakterze terrorystycznym. W centrali ABW funkcjonuje zespół reagowania podejmujący działania w przypadku uzyskania informacji o wystąpieniu lub możliwości wystąpienia zdarzenia o charakterze terrorystycznym. Ponadto CAT bierze udział w ocenianiu funkcjonowania systemów ochrony elementów infrastruktury krytycznej kraju pod kątem usunięcia ewentualnych nieprawidłowości. Współpraca Centrum Antyterrorystycznego z partnerami zagranicznymi jest prowadzona na płaszczyźnie dwustronnej i wielostronnej. Obejmuje przede wszystkim wymianę informacji, wspólną analizę globalnych zagrożeń oraz dzielenie się doświadczeniami i wiedzą.

Zadania z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym są realizowane we współpracy z organami administracji rządowej właściwymi w tych sprawach, w szczególności z Szefem Agencji Bezpieczeństwa Wewnętrznego[65]. Organy administracji publicznej, posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej są obowiązani niezwłocznie przekazywać Szefowi Agencji Bezpieczeństwa Wewnętrznego będące w ich posiadaniu informacje dotyczące zagrożeń o charakterze terrorystycznym dla tej infrastruktury krytycznej, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych istotnych z punktu widzenia bezpieczeństwa państwa, a także działań, które mogą prowadzić do zagrożenia życia lub zdrowia ludzi, mienia w znacznych rozmiarach, dziedzictwa narodowego lub środowiska[66].

Szef Agencji Bezpieczeństwa Wewnętrznego w przypadku podjęcia informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, życiu

[65] Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.), art. 12a ust. 1.

[66] Ibidem, art. 12a ust. 2.

lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku może udzielać zaleceń organom i podmiotom zagrożonym tymi działaniami oraz przekazywać im niezbędne informacje służące przeciwdziałaniu tym zagrożeniom[67]. O tych działaniach Szef ABW informuje dyrektora Rządowego Centrum Bezpieczeństwa.

Agencja Bezpieczeństwa Wewnętrznego w trakcie wykonywania zadań związanych z ochroną infrastruktury krytycznej współpracuje z posiadaczami samoistnymi i zależnymi obiektów, instalacji i urządzeń infrastruktury krytycznej oraz terenowymi organami zarządzania kryzysowego.

Posiadacz samoistny to osoba, która rzeczą faktycznie włada jak właściciel. Stan faktyczny (posiadanie) często idzie w parze z tytułem prawnym do rzeczy (własność), jednak można być posiadaczem samoistnym, nie będąc równocześnie właścicielem rzeczy. Ważna jest sama wola władania rzeczą we własnym imieniu, a nie tytuł prawny do niej. Posiadanie samoistne może prowadzić do nabycia własności poprzez zasiedzenie rzeczy. Natomiast posiadacz zależny to osoba, która faktycznie włada cudzą rzeczą jako użytkownik, najemca, dzierżawca, zastawnik itp. i jest podporządkowana właścicielowi lub posiadaczowi samoistnemu na podstawie stosunku prawnego uprawniającego go do władania rzeczą. Posiadacz zależny włada rzeczą zarówno we własnym imieniu i interesie (na podstawie np. umowy dzierżawy, najmu itd.), ale także w interesie właściciela lub posiadacza samoistnego. Posiadaczowi zależnemu przysługują roszczenia posesoryjne oraz ochrona własna i obrona konieczna z art. 343 *Kodeksu Cywilnego*. Posiadanie zależne nie może prowadzić do zasiedzenia.

Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia[68]. Podmioty te mają obowiązek wyznaczyć, w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej. Jeżeli dla obiektów, instalacji, urządzeń i usług infrastruktury krytycznej istnieją tworzone na podstawie innych przepisów plany odpowiadające wymogom planu ochrony infrastruktury krytycznej, uznaje się, iż wymóg posiadania takiego planu jest spełniony. Należy zaznaczyć, że posiadacze infrastruktury krytycznej mają obowiązek przekazywania informacji dotyczących zagrożeń terrorystycznych dla infrastruktury krytycznej (np. systemy i sieci teleinformatyczne, energetyczne, wodno-kanalizacyjne, ciepłownicze) mające istotne znaczenie dla bezpieczeństwa państwa do Agencji Bezpieczeństwa Wewnętrznego, a także poszczególnym organom zarządzania kryzysowego.

[67] Ibidem, art. 12a ust. 3.

[68] Ibidem, art. 6 ust. 5.

Szef Agencji Bezpieczeństwa Wewnętrznego w przypadku otrzymania informacji o możliwości wystąpienia sytuacji kryzysowej, będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, może udzielać zaleceń organom i podmiotom zagrożonym tymi działaniami oraz przekazywać im niezbędne informacje służące przeciwdziałaniu zagrożeniom[69].

W zależności od skali zagrożenia atakiem o charakterze terrorystycznym lub sabotażowym Prezes Rady Ministrów, ministrowie i kierownicy urzędów centralnych oraz wojewodowie w drodze zarządzenia mogą wprowadzić odpowiedni stopień alarmowy[70].

Organem właściwym w sprawach zarządzania kryzysowego na terenie województwa jest wojewoda[71]. Do zadań wojewody w sprawach zarządzania kryzysowego należy:

- 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.

Organem właściwym w sprawach zarządzania kryzysowego na obszarze powiatu jest starosta jako przewodniczący zarządu powiatu[72]. Do zadań starosty w sprawach zarządzania kryzysowego należy:

- zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym,
- współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym,
- organizacja i realizacja zadań z zakresu ochrony infrastruktury krytycznej.

Organem właściwym w sprawach zarządzania kryzysowego na terenie gminy jest wójt, burmistrz, prezydent miasta (art. 19 ust. 1 ustawy *o zarządzaniu kryzysowym*). Do zadań wójta, burmistrza, prezydenta miasta w sprawach zarządzania kryzysowego należy:

- zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym,
- współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym,
- organizacja i realizacja zadań z zakresu ochrony infrastruktury krytycznej.

[69] Ibidem, art. 12a ust. 3.

[70] Ibidem, art. 23 ust. 1.

[71] Ibidem, art. 14 ust. 1.

[72] Ibidem, art. 17 ust. 1.

Zadaniem Agencji Bezpieczeństwa Wewnętrznego jest zwalczanie terroryzmu, natomiast podmiotów zarządzania kryzysowego likwidacja skutków zdarzeń o charakterze terrorystycznym, i tak:

- zapobieganie skutkom zdarzeń o charakterze terrorystycznym,
- przeciwdziałanie skutkom zdarzeń o charakterze terrorystycznym,
- usuwanie skutków zdarzeń o charakterze terrorystycznym.

Skuteczne wykonywanie zadań przez organy zarządzania kryzysowego w procesie ochrony antyterrorystycznej wymaga współdziałania w sferze wymiany informacji. Podstawowym źródłem informacji dla tych organów jest Szef Agencji Bezpieczeństwa Wewnętrznego, który z uwagi na posiadane możliwości operacyjno-rozpoznawcze może zapewnić niezbędną wiedzę wojewodzie, staroście, wójtowi, burmistrzowi, prezydentowi miasta. Wiedza tego charakteru pozwoli wymienionym podmiotom na wprowadzenie odpowiedniego stopnia alarmowego.

W przeciwdziałaniu zagrożeniom terrorystycznym Agencja Bezpieczeństwa Wewnętrznego współpracuje z Rządowym Centrum Bezpieczeństwa.

Zgodnie z art. 11 ust. 2 pkt 10 i 10a ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* do zadań Rządowego Centrum Bezpieczeństwa należy realizacja zadań z zakresu przeciwdziałania, zapobiegania i likwidacji skutków zdarzeń o charakterze terrorystycznym, współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym. Tym samym Rządowe Centrum Bezpieczeństwa wpisuje się w system realizacji zadań z zakresu przeciwdziałania, zapobiegania i likwidacji skutków zdarzeń o charakterze terrorystycznym. Do podstawowych zadań Centrum, przy zastrzeżeniu właściwości Centrum Antyterrorystycznego ABW, należy dokonywanie analizy zagrożeń w oparciu o dane uzyskiwane ze wszystkich możliwych ośrodków kryzysowych funkcjonujących w ramach administracji publicznej oraz o dane od partnerów międzynarodowych. Zadania z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym są realizowane we współpracy z organami administracji rządowej właściwymi w tych sprawach, w szczególności z Szefem Agencji Bezpieczeństwa Wewnętrznego.

Bardzo ważnym zagadnieniem z punktu widzenia zagrożeń o charakterze terrorystycznym jest niewątpliwe ochrona infrastruktury krytycznej państwa. Dyrektor Rządowego Centrum Bezpieczeństwa na podstawie szczegółowych kryteriów we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy sporządza jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy oraz informuje o ujęciu w wykazie ich właścicieli, posiadaczy samoistnych i zależnych, którzy mają obowiązek ich ochrony.

Organy administracji publicznej, posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej są obowiązani niezwłocznie przekazywać Szefowi Agencji Bezpieczeństwa Wewnętrznego będące w ich po-

siadaniu informacje dotyczące zagrożeń o charakterze terrorystycznym dla tej infrastruktury krytycznej, istotnych z punktu widzenia bezpieczeństwa państwa, a także działań, które mogą prowadzić do zagrożenia życia lub zdrowia ludzi, mienia w znacznych rozmiarach, dziedzictwa narodowego lub środowiska. W ramach współdziałania Szef Agencji Bezpieczeństwa Wewnętrznego informuje Dyrektora Rządowego Centrum Bezpieczeństwa o uzyskaniu informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku.

ROZDZIAŁ 11

Ochrona cyberprzestrzeni państwa

11.1. Istota cyberprzestrzeni i podstawowe pojęcia

Otoczenie człowieka, które zmienia się wraz z postępem cywilizacyjnym, rozwój nauki, techniki i nowych technologii sprawiają, że świat stopniowo uzależnia się od wirtualnej rzeczywistości. Skala i dynamika tego zjawiska pozwala założyć, że w niedalekiej przyszłości granica między światem rzeczywistym a wirtualnym całkowicie zniknie. W wyścigu po nowe rozwiązania techniczne człowiek zapomina o przestrzeganiu prawa, o zasadach postępowania. W powstającym na naszych oczach cyberświecie konieczne jest wypracowanie nowych norm i zasad postępowania, ponieważ dotychczas obowiązujące już nie wystarczają. Argumentem, który przemawia za takim stanowiskiem, są zagrożenia towarzyszące czwartemu wymiarowi, jakim jest cyberprzestrzeń.

> Termin *cyberprzestrzeń* został użyty po raz pierwszy w 1984 roku przez Williama Gibsona w powieści *Neuromancer*. Na dobre spopularyzował go powszechny dostęp do Internetu oraz filmy opierające się na motywach gibsonowskich, takie jak *Johny Mnemonic*, czy trylogia *Matrix*. U Gibsona cyberprzestrzeń to – mówiąc jego poetyckim językiem – świat sieci cyfrowych traktowanych jako pole bitwy, na którym ścierają się światowe koncerny. Zanurzenie się w cyberprzestrzeń odsłania przed nami fortece tajnych informacji chronionych przez niedostępne programy, wyspy otoczone oceanami danych, które w szalonym tempie przekształcają się i wymieniają wokół planety. Niektórzy bohaterowie są w stanie fizycznie dostać się do tej przestrzeni danych, by przeżyć w niej najrozmaitsze przygody. Cyberprzestrzeń Gibsona uwidacznia zmienną, zazwyczaj ukrytą geografię informacji[1].

William Gibson w swojej powieści zatytułowanej *Neuromancer* napisał bowiem:

> to jest cyberprzestrzeń, konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność[2].

[1] C*yberprzestrzeń* – definicje, http://www.techsty.art.pl/hipertekst/cyberprzestrzen/cybe_696.htm [pobrano 13.09.2011].

[2] W. Gibson, *Neuromancer*, Warszawa 2009.

Pierre'a Delvy cyberprzestrzeń to przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie. Definicja ta uwzględnia wszystkie systemy komunikacji elektronicznej (w tym również sieci wykorzystujące fale Hertza i klasyczne sieci telefoniczne), które przesyłają informacje pochodzące ze źródeł numerycznych lub przeznaczone do numeryzacji. Podkreślam fakt numerycznego kodowania, gdyż warunkuje on charakter informacji. Charakter plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzany w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny. Uważam go za znamienną cechę cyberprzestrzeni. To nowe środowisko umożliwia współdziałanie i sprzęganie wszystkich narzędzi tworzenia informacji, rejestrowania, komunikacji i symulacji. Perspektywa powszechnej numeryzacji informacji i przekazów uczyni prawdopodobnie z cyberprzestrzeni główny kanał informacyjny i główny nośnik pamięciowy ludzkości, poczynając od pierwszych lat przyszłego stulecia.
Z kolei Marie Laure Ryan podciąga termin cyberprzestrzeń pod wirtualną rzeczywistość i jest to dla niej immersyjne i interaktywne doświadczenie świata wygenerowanego przez komputer. Umieszcza ona użytkownika wewnątrz samych danych, w trójwymiarowej przestrzeni wyprojektowanej przez cyfrowo zakodowaną informację[3].

Cyberprzestrzeń to cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[4].

Cyberprzestrzeń może być definiowana jako całość powiązań w sektorze ludzkiej działalności z udziałem technologii informacyjno-komunikacyjnych (ICT). Obszar ten, widziany przez pryzmat techniki, cechują inne jakości aniżeli tradycyjną przestrzeń geograficzną. [...] jej elementy pozbawione są wymiaru rozciągłości, lecz wpisane w specyficzny rodzaj czasowości związanej z procesem błyskawicznego rozpowszechniania[5].

Cyberprzestrzeń to nowe medium wzajemnych oddziaływań, gdzie skrępowanie czasem i odległością w znacznym stopniu zanikło; medium, gdzie wzajemne oddziaływania mają miejsce przez elektroniczne zakodowane bity informacji, mknące z prędkością światła przez miliony komputerów i łącza komunikacyjne[6].

Cyberprzestrzeń jest w rzeczywistości domeną fizyczną, będącą wynikiem utworzenia systemów informacyjnych i sieci, które umożliwiają wzajemne oddziaływanie drogą elektroniczną. [...] Działalność człowieka w tym środowisku wymaga świadomego sterowania przepływem energii. Do przesyłania obrazów komputerowych poprzez Internet potrzeba jedynie niewielkiej energii w porównaniu z przelotem samolotu do określonego miejsca przeznaczenia. Obydwa te działania wymagają jednak utworzenia materialnego pakietu, aby podjąć podróż: zrozumienia sposobu podróżowania w określonym środowisku, protokołów i przepisów ustanowionych w odniesieniu

[3] *Cyberprzestrzeń* – definicje, op. cit.

[4] *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, Warszawa 2010, s. 6.

[5] Z. Bauman, *Globalizacja,* Warszawa 2000, s. 24.

[6] L.R. Wilson, *The New Frontier. Cyberspace and the Telecoms*, „Vital Speech of the Day" LXIV, 1998, nr 6.

do takiej podróży oraz sposobu współdziałania z innymi systemami po przybyciu na miejsce[7].

Dlatego cyberterroryści i cyberprzestępcy prowadząc wojnę muszą polegać na znajomości zasad fizycznych i systemów rządzących środowiskiem informacyjnym.

> Cyberprzestrzeń jest dziełem człowieka i służy tworzeniu, przesyłaniu i używaniu różnorodnie sformułowanych informacji. [...] Sieci elektroniczne składające się na infrastrukturę informacyjną stanowią w istocie środowisko fizyczne dostarczające informację, jednak mogą jednocześnie być celami działań zmierzających do zakłócania tworzenia, przesyłania i używania informacji. [...] Zniekształcenie, zakłócenie lub zniszczenie składników cyfrowych sieci informacyjnych w rzeczywistości zmienia topografię cyberprzestrzeni[8].
>
> Czas i przestrzeń nie odgrywają roli w cyberprzestrzeni, a kontakty interpersonalne obejmują przedstawicieli różnych kultur, są nieprzerwane, niekontrolowane i bardzo intensywne. Kultury ekspansywne mają możliwość szczególnie efektywnego oddziaływania i kształtowania bardzo subtelnego wpływu w peryferyjnych albo konkurencyjnych regionach świata[9].

Cyberprzestrzeń i towarzyszący postęp techniczny kusi przede wszystkim brakiem ograniczeń, anonimowością, możliwością restartu, co oznacza rozpoczęcie wszystkiego od nowa. Cyberprzestrzeń stała się nową sferą wymiany informacji cyfrowych związanych z prowadzeniem handlu, rozrywką, kształceniem i szerokim zakresem innych działań, w tym uprawiania cyberterroryzmu czy cyberprzestępczości. Natura cyberprzestrzeni jako pola walki jest postrzegana jako wrogie działanie prowadzone w środowisku utworzonym przez systemy informacyjne[10]. Cyberprzestrzeń już samą nazwą jest związana z cybernetyką, tj. nauką o procesach sterowania oraz przekazywania i przekształcania informacji w systemach (maszynach, organizmach żywych i społeczeństwach)[11].

Analiza cech cybernetycznej przestrzeni prowadzi do wniosku, że jest to swoisty technosystem globalnej komunikacji społecznej, który odznacza się interaktywnością i multimedialnością. Został on ukształtowany w wyniku trzech procesów:

- integracji form przekazu i prezentacji informacji, która przyniosła ucyfrowienie tzw. infosfery,
- konwergencji systemów informatycznych i telekomunikacyjnych oraz mediów elektronicznych,

[7] G.J. Rattray, *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004, s. 30.

[8] Ibidem, s. 80.

[9] K.W. Grewlich, *Conflict and Good Governance in Cyberspace*, [w:] *Global Networks and Local Value. A Comparative Look at German and the United States,* New York 2002, s. 246.

[10] G.J. Rattray, op. cit., s. 95.

[11] J. Kisielnicki, *Systemy informatyczne zarządzania*, Warszawa 2008.

- integracji tzw. technosfery, która doprowadziła w rezultacie do powstania globalnej zintegrowanej platformy teleinformatycznej[12].

Cyberprzestrzeń stanowi zatem swego rodzaju przestrzeń komunikacyjną tworzoną przez system powiązań internetowych. Jak już wspomniano, jest obszarem zarówno kooperacji pozytywnej, prowadzącej do rozwoju w sferze edukacji, komunikacji społecznej, gospodarki narodowej, bezpieczeństwa powszechnego itp., jak i kooperacji negatywnej. Ta ostatnia aktywność może przybierać postać:

- cyberinwigilacji (obostrzonej kontroli społeczeństwa za pośrednictwem narzędzi teleinformatycznych w państwach autorytarnych i totalitarnych),
- cyberprzestępczości (wykorzystania cyberprzestrzeni do celów kryminalnych, w szczególności w ramach przestępczości zorganizowanej i przestępczości o charakterze ekonomicznym),
- cyberterroryzmu (wykorzystania cyberprzestrzeni w działaniach terrorystycznych),
- cyberwojny (użycia cyberprzestrzeni jako czwartego, obok ziemi, morza i powietrza, wymiaru prowadzenia działań wojennych)[13].

Mówiąc o cyberterroryzmie napotykamy na kluczowy problem, jakim jest brak jednoznacznej i uznanej przez społeczność międzynarodową definicji tego pojęcia. Wielu badaczy uważa, że definicja cyberterroryzmu powinna być poprzedzona definicją pojęcia terroryzm. Jest to trudny problem, mimo prowadzonych dyskusji i prezentowaniu stanowisk, społeczność międzynarodowa nie wypracowała dotychczas uniwersalnej definicji terroryzmu, co odnosi się także do definicji cyberterroryzmu. Należy przyjąć, że podstawową przeszkodą są względy polityczne. Jak mówi stara, wciąż żywa maksyma: człowiek będący dla jednych terrorystą dla innych jest bojownikiem o wolność – w podobnym duchu wypowiadał się Jaser Arafat, nieżyjący lider Autonomii Palestyńskiej[14].

W związku z powyższym warto przedstawić pojęcie cyberterroryzmu według autorów zajmujących się tym złożonym zjawiskiem – zob. tabela 95.

Tabela 95. Definicje cyberterroryzmu

Źródło	Definicja
Centrum Ochrony Infrastruktury Krytycznej w Stanach Zjednoczonych utworzone Prezydencką Dyrektywą Wykonawczą 63 w 1998 roku	Cyberterroryzm to czyn kryminalny popełniony z wykorzystaniem komputerów, powodujący przemoc, śmierć i/lub zniszczenia i tworzący poczucie zagrożenia w celu zmuszenia rządu do zmiany jego polityki. Aby w tym ujęciu mówić o cyberterroryzmie, musimy wypełniać kryteria politycznej motywacji, niszczycielskiego efektu oraz wykorzystania technologii komputerowej.

[12] P. Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni*, [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Warszawa 2009.

[13] Ibidem.

[14] J. Arafat, *Przemówienie na forum Zgromadzenia Ogólnego ONZ 13 listopada 1974 roku*, cyt. za: B. Hoffman, *Oblicza terroryzmu*, Warszawa 1999, s. 24.

B. Collin za: R. Białoskórski, *Wyzwania i zagrożenia bezpieczeństwa XXI wieku*, Warszawa 2010, s. 59	Cyberterroryzm to działalność terrorystyczna przy użyciu technologii informatycznych w cyberprzestrzeni.
J.A. Lewis, *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, Center for Strategic and International Studies 2002 – http://www.csis.org/tech/0211_lewis.pdf [pobrano12.09.2011]	Cyberterroryzm to wykorzystanie sieci komputerowych jako narzędzi do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe) bądź do zastraszania czy wymuszania na rządzie lub populacji określonych działań.
M. Pollit, *Cyberterrorism – Fact or Fancy*? – http:/www.cs.georgetwon.edu/-denning/infosec/pollitt.html [pobrano 12.09.2011]	Cyberterroryzm to przemyślany, politycznie umotywowany atak, skierowany przeciw informacjom, systemom komputerowym, programom i danym, który prowadzi do oddziaływania na niemilitarne cele, przeprowadzony przez grupy narodowościowe lub przez tajnych agentów.
K.C. White, *Cyber Terrorism: Modem Mache*, Carlisle 1998	Cyberterroryzm to świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji.
D.E. Denning, *Cyberterrorism, Global Dialogue*, August 24, 2000 – http://www.cs georgetwon.edu/-denning/infosec/cyberterror-GD.doc [pobrano 14.09.2011]	Cyberterroryzm to połączenie pojęcia cyberprzestrzeni i terroryzmu. To groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych dążeń (politycznych).
R. Stark, *Cyber Terrorism: Rethinking New Technology* – http://www.infowar.com/MIL_C41/stark/Cyber_Terrorism-Rethinking_New_Technology1.doc.	Cyberterroryzm to zdeterminowane i świadome użycie środków walki informacyjnej przez aktorów niepaństwowych lub grupy sponsorowane przez państwa, motywowane politycznie, społecznie, ekonomicznie lub religijnie w celu zastraszenia, wzbudzenia niepokoju i paniki wśród atakowanej ludności oraz doprowadzenia do zniszczenia wojskowych i cywilnych celów.
R. Kośla, Cyberterroryzm – definicje, zjawiska i zagrożenia dla Polski, wystąpienie na konferencji w Bemowie 29 listopada 2002 roku – http://www.abw.gov.pl [pobrano 14.09.2011]	Cyberterroryzm działania blokujące, niszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy.
D. Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, Warszawa 2004	Cyberterroryzm – polityczne umotywowana, przemyślana działalność grup narodowościowych lub innych wrogich sił, wymierzona przeciw informacji, systemom komputerowym, programom i danym, która powoduje straty cywilne.
K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 36	Cyberterroryzm to politycznie umotywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia czy wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów w szerszym rozumieniu tego słowa.
W.M. Stankiewicz, *Cyberterroryzm jako zagrożenie asymetryczne współczesnego świata*, [w:] *Zagrożenia asymetryczne współczesnego świata*, red. R. Wojciechowski, R. Fiedler, Poznań 2009, s. 258	W wąskim znaczeniu cyberterroryzm to działalność terrorystyczna w systemach teleinformatycznych, ukierunkowana na zniszczenie lub modyfikację danych, skutkująca ofiarami śmiertelnymi lub zniszczeniem mienia w znacznych rozmiarach. W szerszym znaczeniu pojęcie to oznacza zaś wszelką działalność terrorystyczną związaną z cyberprzestrzenią (systemami informatycznymi), włączając fizyczne ataki na systemy oraz aktywność propagandową.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 125	Cyberterroryzm to działania blokujące, niszczące lub zniekształcające informację, która jest przetwarzana, przechowywana i przekazywana w systemach teleinformatycznych.
Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Warszawa 2010	Cyberterroryzm to cyberprzestępstwo o charakterze terrorystycznym.
http://www.abw.gov.pl/palm/pl/88/306/Cyberterroryzm.html [pobrano 13.9.2011]	Cyberterroryzm to wykorzystywanie zdobyczy technologii informacyjnej w celu wyrządzenia szkody.

Źródło: Opracowanie własne na podstawie dostępnej literatury

Dla określenia działalności terrorystycznej w cyberprzestrzeni używane jest określenie cyberterroryzm, terroryzm informacyjny lub hi-tech terroryzm. Np. infoterroryzm to celowe nadużycie cyfrowego systemu informacyjnego, sieci lub ich składników w celu wsparcia bądź ułatwienia przeprowadzenia kampanii lub akcji terrorystycznej. W takim przypadku nadużycie systemu niekoniecznie wiąże się z bezpośrednią przemocą przeciwko ludziom, jednak wciąż może powodować poczucie zagrożenia[15].

W środowisku specjalistów zajmujących się cyberterroryzmem panuje pogląd, iż jest to jedno z najpoważniejszych wyzwań XXI wieku, przed jakim stoją nie tylko pojedyncze państwa, ale cała społeczność międzynarodowa. Specjaliści przyjmują sześć powodów, dla których terroryści są zainteresowani wykorzystaniem cyberprzestrzeni dla swoich celów – zob. tabela 96.

Tabela 96. Powody zainteresowania terrorystów cyberprzestrzenią

Dlaczego cyberterroryzm?	Jaki to ma wpływ na bezpieczeństwo?
niskie koszty	każdy może zostać cyberterrorystą, wystarczy mieć komputer, modem i trochę umiejętności
działania ponad granicami państwa	nie wiadomo skąd pochodzi atak, kto atakuje i kto za tym stoi
postrzeganie zagrożenia	nie wiadomo, które zagrożenie jest realne, a które wirtualne
wykrycie cyberataków	nie wiadomo, jakie są zdolności i intencje atakującego
cel ataku	nie wiadomo, co będzie celem ataku, ani w jaki sposób zostanie on dokonany
budowa koalicji	nie wiadomo, kto jest swój, a kto obcy

Źródło: Za A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 88

Biorąc pod uwagę wskazane powody zainteresowania terrorystów cyberprzestrzenią należy wyjaśnić, że:

- niskie koszty takiej działalności, zwłaszcza w porównaniu z kosztami regularnych działań zbrojnych, do ataku cybernetycznego wystarczy przeciętny sprzęt, dostęp do Internetu i trochę umiejętności,
- zanikanie wszelkich granic – państwa tracą część swojej suwerenności, nie ma sensu dzielić cyberterroryzmu na międzynarodowy czy narodowy, ataku

[15] B. Bolechów, *Terroryzm w świecie podwubiegunowy. Przewartościowania i kontynuacje*, Toruń 2003, s. 498.

można dokonać z każdego miejsca na ziemi, w którym jest dostęp do sieci, zacierają się granice między tym, co prywatne a państwowe, wojskowe a komercyjne itd., konsekwencją zanikania wszelkiego rodzaju barier jest prawdopodobieństwo, że zaatakowane państwo nie będzie sobie z tego zdawało sprawy (zacieranie się granicy między wojną a pokojem); w Stanach Zjednoczonych w publikacjach sprzed 11 września 2001 roku podkreślano, że terytorium USA przestaje być oazą bezpieczeństwa od wszelkiego rodzaju uderzeń,

- możliwość dokonywania nagłych i nieprzewidywalnych akcji – ofiary są całkowicie nieświadome i nieprzygotowane do ich odparcia,
- całkowita anonimowość – daje możliwość manipulowania informacją, utrudnia państwom odparcie ataku i budowanie koalicji,
- minimalne ryzyko wykrycia przygotowanego ataku,
- zamiast uderzać w niewinnych ludzi, można sparaliżować system wrogiego państwa,
- większy efekt propagandowy i uznanie opinii publicznej[16].

Inne powody zainteresowania terrorystów cyberprzestrzenią:

– po pierwsze, konwencjonalne metody działalności terrorystycznej są niebezpieczne dla samych terrorystów; w cyberprzestrzeni mogą oni dokonać ataków nie narażając się na niebezpieczeństwo,
– po drugie, nie trzeba posiadać wielkich umiejętności, przeprowadzając swoją akcję; można wynająć choćby hakerów (crackerów), którzy za wynagrodzenie są w stanie przeprowadzić atak terrorystyczny dla zabawy, łamiąc zabezpieczenia i nie zdając sobie nawet sprawy ze skutków swojego działania,
– po trzecie, walka z cyberterroryzmem wymaga o wiele większej koordynacji niż w przypadku innych działań; w połączeniu z bardzo szybko rozwijająca się techniką i nowymi metodami szyfrowania danych, stenografii itd. powstaje komfort bezpiecznego działania,
– po czwarte, zmienia się postrzeganie zagrożenia; na dobrą sprawę nie wiadomo, która groźba jest realna, a która pozostaje tylko wirtualna,
– po piąte, państwa dysponują bardzo małymi możliwościami zastosowania sankcji wobec cyberterrorystów,
– po szóste, umasowienie dostępu do komputerów sprawia, że stają się one coraz prostsze w obsłudze. [...] W Internecie można znaleźć bardzo wiele programów umożliwiających odszyfrowanie kodu dostępu do komputera lub bazy danych czy włamanie się do systemu; wraz ze zmniejszaniem się potrzebnych umiejętności do przeprowadzenia cyberataku, zwiększa się skuteczność i jakość programów mających to ułatwić; w konsekwencji każdy może zostać cyberterorystą[17].

Należy podkreślić, że cyberterroryzm obok cyberprzestępczości stanowi największe zagrożenie dla społeczności międzynarodowej. Istotne jest to, że cyber-

[16] G. Buchan, *Information Warfare and the Air Force: Wave of Future? Current Fad?,* Washington 1996, s. 8.

[17] B.C. Collin, *Cyber Terrorism. From Virtual Darkness: New Weapons in a Timeless Battle*, San Luis Obispo 1998, http://www..nici.org.

ataki mają miejsce w niematerialnej cyberprzestrzeni. Przestrzeń wirtualna jest na tyle nieuchwytna dla laika, że najczęściej lekceważy zagrożenia generowane brakiem kontroli nad zachodzącymi tam procesami. Ponadto specjaliści posiadający odpowiednią wiedzę i dostęp do informacji bardzo często stają się sprawcami potencjalnych ataków.

> Cyberterroryzm stanowi przecież zjawisko z pogranicza kilku sfer: informatyki, bezpieczeństwa informacyjnego, technologii, bezpieczeństwa międzynarodowego i narodowego, ochrony danych, regulacji prawnych itd. Może stanowić zagrożenie interesów: jednostek, państw, wspólnot międzynarodowych. [...] cyberataków nie monopolizują ugrupowania terrorystyczne, które zaadaptowały nowe narzędzia wywierania nacisków. Sprawcami ataków mogą być również: jednostki (hakerzy, crackerzy), ruchy narodowo-wyzwoleńcze, ruchy powstańcze, służby specjalne (wywiad i kontrwywiad), a także inne podmioty wykorzystujące sieć, na przykład dla celów zarobkowych[18].

Bezpieczeństwo systemów informacyjnych i systemów informatycznych ma kluczowe znaczenie dla właściwego funkcjonowania nie tylko państw, ale i pojedynczego człowieka. Dlatego zwalczanie cyberprzestępczości obok cyberterroryzmu jest tak ważne.

Analogicznie jak przy braku definicji terroryzmu czy cyberterroryzmu brak jest ogólnie obowiązującej definicji cyberprzestępczości. Termin ten jest używany zamiennie z takimi pojęciami, jak przestępczość komputerowa, przestępczość związana z komputerami czy przestępczość przy użyciu zaawansowanych technologii.

Według komunikatu Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22 maja 2007 roku w sprawie kierunku ogólnej strategii zwalczania cyberprzestępczości, pod pojęciem cyberprzestępczości rozumie się czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom.

W praktyce terminu cyberprzestępczość używa się w odniesieniu do trzech rodzajów przestępstw:

- pierwszy obejmuje tradycyjne formy przestępstw, takie jak oszustwo czy fałszerstwo, jednak w kontekście cyberprzestępczości odnoszą się one konkretnie do przestępstw popełnionych przy użyciu elektronicznych sieci informatycznych i systemów informatycznych (zwanych dalej sieciami łączności elektronicznej),
- drugi rodzaj stanowi publikacja nielegalnych treści w mediach elektronicznych (np. materiałów związanych z seksualnym wykorzystywaniem dzieci czy też nawoływaniem do nienawiści rasowej),
- trzeci rodzaj obejmuje przestępstwa typowe dla sieci łączności elektronicznej, tj. ataki przeciwko systemom informatycznym, ataki typu *denial of service* oraz hakerstwo.

[18] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 39.

Tego rodzaju ataki mogą być również skierowane przeciwko najważniejszym infrastrukturom krytycznym w Europie i uszkodzić istniejące systemy szybkiego reagowania w wielu obszarach, co może spowodować dramatyczne konsekwencje dla całego społeczeństwa. Wszystkie te rodzaje przestępstwa łączy jedna cecha – mogą być popełnianie na masową skalę, a odległość geograficzna między miejscem popełnienia przestępstwa a jego skutkami może być znaczna.

Powszechny dostęp do cyberprzestrzeni, trudności w jej monitorowaniu, brak wiarygodnych informacji, a także ciągły rozwój przestępczości sprawiają, że trudno jest uzyskać dokładny obraz, co do skali i dynamiki cyberprzestępczości. Można jednak stwierdzić kilka ogólnych trendów:

- liczba przestępstw informatycznych stale rośnie, działania przestępcze stają się też coraz bardziej wyrafinowane i wykraczają poza granice państwowe,
- wyraźne przesłanki wskazują na rosnący udział w cyberprzestępczości zorganizowanych grup przestępczych,
- nie wzrasta jednak liczba aktów oskarżenia na podstawie transgranicznej współpracy oddziałów ścigania w Europie.

Pojęcie cyberprzestępczości, zwanej również przestępczością internetową, jako określenie zabronionych prawem działań dokonywanych za pomocą komputera w sieci internetowej lub przy jej wykorzystaniu, godzących m.in. w bezpieczeństwo wykorzystania technologii informatycznych, znalazło już swoje miejsce zarówno w doktrynie nauk prawnych, jak i wśród ekspertów zajmujących się bezpieczeństwem teleinformatycznym[19].

Można przyjąć, że cyberprzestępczość obejmuje trzy kategorie przestępstw:

– tradycyjne przestępstwa popełniane z wykorzystaniem sieci i systemów informatycznych,
– publikację nielegalnych treści w mediach elektronicznych,
– inne przestępstwa typowe dla sieci łączności elektronicznej.

W komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 roku zatytułowanym *W kierunku ogólnej strategii zwalczania cyberprzestępczości*[20] jako cyberprzestępstwa wymienione zostały:

- przestępstwa przeciwko poufności, integralności i dostępności danych (tzw. przestępstwa CIA); zaliczane są do nich głównie nielegalny dostęp do systemów poprzez hacking, podsłuch i oszukiwanie uprawnionych pracowników, szpiegostwa komputerowe, sabotaż oraz wymuszenia komputerowe (wirusy, ataki DoS, DDoS, spam),
- przestępstwa tradycyjne powiązane z komputerami, takie jak oszustwa (od klasycznych oszustw manipulacji fakturami lub kontami firmowymi, do ma-

[19] M. Czyżak, *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary Automatyka Kontrola" 2009, nr 7.

[20] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 roku *w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego* (Dz. U. L 178, 17.7.2000, s. 1).

nipulacji online – oszukańczych aukcji czy nielegalnego używania kart kredytowych); obejmują również komputerowe podróbki, molestowanie dzieci, aż do ataków na życie ludzkie (np. przez manipulowanie systemami szpitalnymi lub kontroli ruchu powietrznego),

- przestępstwa „contentowe" (dotyczące zawartości); ta kategoria obejmuje np. dziecięcą pornografię, dostarczanie instrukcji przestępczych, oferty popełniania przestępstw, molestowanie i lobbing poprzez sieć, rozpowszechnianie fałszywych informacji (czarny PR, schematy *pump-and-dump*), internetowy hazard,
- przestępstwa powiązane z naruszeniem prawa autorskiego i praw pokrewnych, takie jak nieautoryzowane kopiowanie i rozpowszechnianie programów komputerowych, nieautoryzowane użycie baz danych.

W komunikacie zwrócono także uwagę na narastającą tendencję popełniania klasycznych przestępstw, których ślady pozostają w systemach komputerowych – kradzieży, korupcji, oszustw, defraudacji.

W podręczniku Interpolu[21] z 2007 roku zwraca się szczególną uwagę na cztery obszary, na których koncentruje się aktualnie cyberprzestępczość: hacking, oprogramowanie złośliwe (włącznie z botnetami), piractwo intelektualne, nielegalna zawartość cyfrowych nośników danych.

Specyfika cyberprzestępczości została bardzo trafnie ujęta w raporcie Europolu[22] za 2007 rok. Cyberprzestępstwa są w nim wykazane w dwóch ujęciach – wertykalnym i horyzontalnym. Ujęcie wertykalne dotyczy przestępstw, które są specyficzne dla cyberprzestrzeni i poza nią nie mogą być dokonane. Wśród nich wyróżniono: hacking (ataki DDoS, botnety, zombies itp.), crimeware (wirusy, robaki, konie trojańskie), spamming. W ujęciu horyzontalnym znalazły się przestępstwa, w których wypadku wykorzystanie technik komputerowych i informatycznych uprościło znacznie ich dokonanie. Jako największe zagrożenia uznano: pornografię dziecięcą, nieuprawnione wykorzystanie kart płatniczych, kradzież tożsamości (phishing), piractwo intelektualne, pranie brudnych pieniędzy za pośrednictwem Internetu (cyberlaundering), cyberterroryzm.

Nowoczesne technologie, ze szczególnym wskazaniem na teleinformatykę, z uwagi na powszechny dostęp i edukację, a także adaptację praktycznie do wszystkich obszarów życia człowieka stanowią poważne wyzwanie dla współczesności.

Z punktu widzenia bezpieczeństwa państwa czwarty wymiar, jakim jest cyberprzestrzeń, to konieczność wypracowania polityki jej bezpieczeństwa zarówno w wymiarze cywilnym, jak i wojskowym.

[21] *IT Crime Manual of the Interpol Working Party on Information Technology Crime – Europe 2007*.

[22] *High Tech Crimes within EU. Threat Assessment 2007*, Europol, Hague 2007.

11.2. Podstawy prawne ochrony cyberprzestrzeni

Procesowi transformacji środowiska międzynarodowego towarzyszą dynamicznie rozwijająca się globalizacja i społeczeństwo informacyjne. Należy podkreślić, że rozwój ten przebiega w sposób chaotyczny i jest pełen anarchii. Wszechobecna anarchia dominuje nie tylko w przestrzeni tradycyjnej, ale stopniowo zaznacza swoją obecność w przestrzeni wirtualnej, która stanowi źródło szans i zagrożeń, a przy tym jest nieprzewidywalna. Przed państwami staje nowe zadanie, by zapanować nad anarchią, której generatorem jest digitalizacja życia, ujarzmić rosnący na gruncie postępu technicznego chaos [23].

Warto mieć na uwadze rozwijające się społeczeństwo informacyjne i powszechną internatyzację naszego życia.

> Społeczeństwo informacyjne generuje zarówno szanse, jak i zagrożenia bezpieczeństwa, wśród których zdecydowanie najprężniejszy jest cyberterroryzm i cyberprzestępstwa, wymagające odgórnej ochrony kluczowych działów gospodarki, którą może zapewnić tylko państwo. W sytuacjach kryzysowych, związanych z atakiem na infrastrukturę krytyczną państwa (w tym krytyczną infrastrukturę teleinformatyczną[24]), tylko państwo może spowodować akcje retorsyjne, wykorzystując klasyczne środki prewencji i odwetu: wojsko i policję [służby specjalne – przyp. autora]. Wyłączną kompetencją władz państwowych jest zwalczanie przestępstw cybernetycznych i ochrona ładu wewnętrznego poprzez nowelizację prawa i poszerzenie działania wymiaru sprawiedliwości[25].

W cyberprzestrzeni granice między pokojem a wojną stają się coraz bardziej umowne. Wynika stąd potrzeba zagwarantowania odpowiednich form komunikacji pomiędzy częścią wojskową (niejawną w rozumieniu tejże ustawy) a częścią cywilną (w części jawną w rozumieniu tejże ustawy *o ochronie informacji niejawnych*). Obiektami cyberwojny są tak wojskowe, jak i cywilne elementy krytycznej infrastruktury teleinformatycznej. Funkcjonowanie infrastruktury wojskowej nawet w 90% zależy od sprawności infrastruktury cywilnej, w związku z tym jej ochrona wymaga wypracowania rozwiązań prawnych (m.in. przyjęcie sankcji karnych) i organizacyjnych, wskazania podmiotów właściwych w sferze jej bezpieczeństwa, określenia zasad współpracy z podmiotami krajowymi i międzynarodowymi.

Z uwagi na wzrost zagrożeń ze strony sieci publicznej, od których całkowita separacja jest niemożliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, niezbędne jest skoordynowanie działań w zakresie

[23] A. Bógdał-Brzezińska, M.F. Gawrycki, op. cit., s. 11.

[24] Krytyczna infrastruktura teleinformatyczna to infrastruktura krytyczna wyodrębniona w systemie łączności i sieciach teleinformatycznych i ujawniona w wykazie Infrastruktury Krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.).

[25] A. Bógdał-Brzezińska, M.F. Gawrycki, op. cit., s. 11.

zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni, które umożliwiają szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom, sieciom teleinformatycznym i oferowanym przez nie usługom[26]. W państwach członkowskich Unii Europejskiej problematyka związana z ochroną teleinformatycznej infrastruktury krytycznej jest regulowana zarówno przez prawo międzynarodowe (w tym unijne), jak i prawo krajowe. Polska jest stroną konwencji międzynarodowych, które mają znaczenie dla bezpieczeństwa teleinformatycznego. Natomiast prawo krajowe w przedmiotowej sprawie ma przede wszystkim charakter branżowy. Obowiązujące regulacje prawne nie stanowią zamkniętego katalogu, co oznacza, że będzie on w uzasadnionych przypadkach uzupełniany o nowe przepisy.

Obowiązujące w Polsce przepisy prawa dotyczące bezpieczeństwa teleinformatycznego:

Prawo międzynarodowe

1) Konwencja Narodów Zjednoczonych *o zwalczaniu finansowania terroryzmu*, przyjęta przez Zgromadzenie Ogólne NZ rezolucją Nr 54/109 z 9 grudnia 1999 roku (Dz. U. z 2004 r. Nr 263, poz. 2620),
2) Konwencja Narodów Zjednoczonych *przeciwko międzynarodowej przestępczości zorganizowanej*, przyjęta przez Zgromadzenie Ogólne NZ 15 listopada 2000 roku (Dz. U. z 2005 r. Nr 18, poz. 158),
3) Rezolucja 1267 (1999 r.) Rady Bezpieczeństwa ONZ *w sprawie sankcji wobec Al-Kaidy i Talibów*, 1373 (2001 r.) zobowiązująca państwa członkowskie do pociągania do odpowiedzialności karnej osobę lub organizację finansującą terroryzm,
4) *Globalna Strategia Zwalczania Terroryzmu* z załączonym Planem Działania, przyjęta w dniu 8 września 2006 roku przez Organizację Narodów Zjednoczonych,
5) Konwencja Rady Europy z dnia 27 stycznia 1977 roku *o zwalczaniu terroryzmu* (Dz. U. z 1996 r. Nr 117, poz. 557), do Konwencji sporządzony został protokół zmieniający w dniu 15 maja 2003 roku (CETS No. 190),
6) Konwencja Rady Europy z dnia 23 listopada 2001 roku *o zwalczaniu cyberprzestępczości* (ETS No. 185), Konwencja weszła w życie w dniu 18 marca 2004 roku, sporządzony został do niej protokół dodatkowy o kryminalizacji aktów rasizmu i ksenofobii popełnianych z wykorzystaniem systemów komputerowych (ETS No. 189),
7) Konwencja Rady Europy z dnia 16 maja 2005 roku *o zapobieganiu terroryzmowi* (Dz. U. z 2008 r. Nr 161, poz. 998),
8) Konwencja Rady Europy z dnia 16 maja 2005 roku *o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz finansowania terroryzmu* (Dz. U. z 2008 r. Nr 165, poz. 1028),
9) Program Sztokholmski – *Otwarta i bezpieczna Europa dla dobra i ochrony obywateli* z 2010 roku (Dz. Urz. UE C 115/1 z 4 maja 2010 roku),

[26] *Rządowy Program Ochrony Cyberprzestrzeni…*, s. 5.

10) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 20 kwietnia 2010 roku *w sprawie Planu działań służących realizacji programu sztokholmskiego* KOM(2010) 171,
11) *Strategia Unii Europejskiej w sprawie walki z terroryzmem* z dnia 2 grudnia 2005 roku, przyjęta przez Radę Unii Europejskiej,
12) *Plan działania Unii Europejskiej w zakresie zwalczania terroryzmu* z dnia 13 lutego 2006 roku, przyjęty przez Radę Unii Europejskiej,
13) Strategia Bezpieczeństwa Wewnętrznego Unii Europejskiej, przyjęta przez Radę Europejską w dniach 25–26 marca 2010 roku,
14) Dyrektywa Rady Europy 2008/114/WE z dnia 8 grudnia 2008 roku *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony* (Dz. Urz. UE L 345/75 z 23 grudnia 2008 roku),
15) Decyzja Rady Ministerialnej OBWE Nr 3/04 z dnia 7 grudnia 2004 roku i Nr 7/06 z dnia 5 grudnia 2006 roku *w sprawie działań związanych ze zwalczaniem wykorzystywania Internetu do celów terrorystycznych*,
16) Decyzja Rady Ministerialnej OBWE Nr 5/07 z dnia 30 listopada 2007 roku *związana z partnerstwem publiczno-prywatnym w zwalczaniu terroryzmu*,
17) Rozporządzenie Parlamentu Europejskiego i Rady Europy Nr 460/2004 z dnia 10 marca 2004 roku *w sprawie powołania Europejskiej Agencji Bezpieczeństwa Sieci i Informacji* oraz wcześniejsza Dyrektywa Parlamentu Europejskiego i Rady Europy Nr 2002/21/EC z dnia 7 marca 2002 roku *w sprawie ramowych uregulowań dla sieci komunikacji elektronicznej i usług*,
18) *Plan działania partnerstwa przeciw terroryzmowi*, przyjęty na szczycie NATO w dniu 22 listopada 2002 roku w Pradze,
19) *Militarna koncepcja obrony przed terroryzmem*, przyjęta na szczycie NATO w dniu 22 listopada 2002 roku w Pradze.

Prawo krajowe

1) *Konstytucja Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 roku (Dz. U. z !997 r. Nr 78, poz. 483 z późn. zm.),
2) Ustawa z dnia 6 czerwca 1997 roku *Kodeks karny* (Dz. U. z 1997 r. Nr 88, poz. 53 z późn. zm.),
3) Ustawa z dnia 29 sierpnia 1997 roku *Prawo bankowe* (Dz. U. z 1997 r. Nr 140, poz. 939 z późn. zm.),
4) Ustawa z dnia 29 sierpnia 1997 roku *o ochronie danych osobowych* (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
5) Ustawa z dnia 27 lipca 2001 roku *o ochronie baz danych* (Dz. U. z 2001 r. Nr 128, poz. 1402 z późn. zm.),
6) Ustawa z dnia 24 maja 2002 roku *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.),
7) Ustawa z dnia 16 lipca 2004 roku *Prawo telekomunikacyjne* (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.),

8) Ustawa z dnia 17 lutego 2005 roku *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.),
9) Ustawa z dnia 6 czerwca 2006 roku *o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego* (Dz. U. z 2006 r. Nr 104, poz. 709 i Nr 218, poz. 1592, z 2007 r. Nr 25, poz. 162, z 2009 r. Nr 85, poz. 716),
10) Ustawa z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* (Dz. U. z 2007 r. Nr 89, poz. 590 z późn. zm.),
11) Ustawa z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych* (Dz. U. z 2010 r. Nr 182, poz. 1228),
12) Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego* (Dz. U. z 2010 r. nr 83, poz. 540),
13) Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej* (Dz. U. z 2010 r. nr 83, poz. 541),
14) Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku *w sprawie planów ochrony infrastruktury krytycznej* (Dz. U. z 2010 r. nr 83, poz. 542),
15) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku *w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego* (Dz. U. z 2011 r., Nr 156, poz. 926),
16) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego* (Dz. U. z 2011 r., Nr 159, poz. 948),
17) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 roku *w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego* (Dz. U. z 2011 r., Nr 159, poz. 949),
18) Decyzja Ministra Obrony Narodowej Nr 357/MON z dnia 29 lipca 2008 roku *w sprawie organizacji systemów reagowania na incydenty komputerowe w resorcie obrony narodowej*,
19) *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, Warszawa 2010.

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016 wpisuje się w przyjęty przez Komisję Europejska dokument pod nazwą *Europejska Agenda Cyfrowa Rady Europejskiej* (KOM(2010)245), której celem jest uzyskanie trwałych korzyści ekonomicznych i społecznych z jednolitego rynku cyfrowego w oparciu o szybki Internet i interoperacyjne aplikacje.

Wzmocnienie zwalczania cyberprzestępczości należy do priorytetów Unii Europejskiej. W Programie Sztokholmskim Rada Europejska apeluje do państw członkowskich m.in. o udzielenie pełnego poparcia krajowym platformom powiadamiania odpowiedzialnym za walkę z cyberprzestępczością i podkreśla, że konieczna jest współpraca z krajami spoza Unii Europejskiej, a także wzywa państwa członkowskie do poprawy współpracy sądowej w sprawach dotyczących cyberprzestępczości. Program Sztokholmski odwołuje się także do wzmocnienia/

usprawnienia partnerstw publiczno-prywatnych (zadanie dla KE) oraz do zintensyfikowania analizy strategicznej w zakresie cyberprzestępczości (zadanie dla Europolu). Ponadto dokument wskazuje na możliwość podjęcia działań na rzecz utworzenia europejskiej platformy identyfikowania cyberprzestępczości przy wykorzystaniu możliwości oferowanych przez Europol.

Cyberprzestępczość stanowi globalne techniczne, transgraniczne i anonimowe zagrożenie naszych systemów informacyjnych, dlatego stwarza wiele dodatkowych problemów służbom ochrony porządku publicznego. Zagrożeniem o globalnym zasięgu i katastrofalnych skutkach jest także terroryzm. W *Strategii bezpieczeństwa wewnętrznego Unii Europejskiej* sformułowano 10 wytycznych, pozwalających zagwarantować w nadchodzących latach bezpieczeństwo wewnętrzne UE. Są to m.in. prewencja i profilaktyka oparta na danych wywiadowczych, opracowanie kompleksowego modelu wymiany informacji, współpraca operacyjna, współpraca organów wymiaru sprawiedliwości w sprawach karnych, zewnętrzny wymiar bezpieczeństwa wewnętrznego, współpraca z państwami trzecimi.

Instrumenty legislacyjne ujęte w aktualnym *Planie działania partnerstwa przeciwko terroryzmowi*, a wynikające z Deklaracji z 25 marca 2004 *roku w sprawie zwalczania terroryzmu* zostały zaimplementowane do prawa polskiego, to m.in.: Decyzja Ramowa Rady 2002/465/WSiSW z 13 czerwca 2002 roku *w sprawie powołania wspólnych zespołów dochodzeniowo-śledczych*, Decyzja Ramowa Rady 2002/475/WSiSW z 13 czerwca 2002 roku *w sprawie zwalczania terroryzmu*, Decyzja Ramowa 2001/500/WSiSW z 26 czerwca 2001 roku *w sprawie prania pieniędzy oraz identyfikacji, wykrywania, zamrożenia, zajęcia i konfiskaty narzędzi oraz zysków pozyskanych z przestępstwa*, Decyzja Ramowa 2003/577/WSiSW z 22 lipca 2003 roku *w sprawie konfiskaty korzyści pochodzących z przestępstwa*, Decyzja Ramowa 2005/222/JHA z 24 lutego 2005 roku *przeciwko atakom na system informacyjny*.

W Unii Europejskiej przyjęte zostały także inne akty prawne regulujące zwalczanie cyberprzestępczości. Niektóre dotyczą konkretnego aspektu cyberprzestępczości, np. Decyzja Ramowa 2005/222/WSiSW *w sprawie ataków na systemy informatyczne*[27]. Decyzja nakazuje penalizację umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego (art. 2), umyślnego, bezprawnego, poważnego naruszenia lub przerwania funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych (art. 3) oraz umyślnego, bezprawnego usunięcia, uszkodzenia, pogorszenia, zmiany, zatajania lub uczynienia niedostępnymi danych komputerowych w systemie informatycznym (art. 4), które nie są przypadkami mniejszej wagi. Decyzja wymaga karania także osób kierujących popełnieniem przestępstwa, pomagających w jego popełnieniu lub nakłaniających do jego popełnienia (podżeganie) oraz zakłada karalność usiłowania popełnienia przestępstwa (co jest bardzo często spotykanym przypadkiem w cyberprzestępczości).

[27] Dz. Urz. L 69 z dnia 16 marca 2005.

Akty prawne, dotyczące konkretnego problemu przestępczości, zawierają również zapisy dotyczące bezprawnego wykorzystywania Internetu. Decyzja Ramowa 2004/68/WSiSW *dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej*[28], która określa przedsięwzięcia w zakresie ochrony dzieci, zwłaszcza związanych ze zwalczaniem wszystkich materiałów związanych z seksualnym wykorzystywaniem dzieci nielegalnie publikowanych przy użyciu systemów informatycznych. Decyzja Ramowa 2001/413/WSiSW z dnia 28 maja 2001 roku *w sprawie walki z oszustwami i fałszerstwami dotyczącymi bezgotówkowych środków płatności* (dotycząca m.in. kradzieży tożsamości). Dyrektywa 2002/58/WE *o prywatności i łączności elektronicznej* nakłada na dostawców ogólnodostępnych usług komunikacji elektronicznej obowiązek zadbania o bezpieczeństwo ich usług, zawarte są w niej również przepisy o ochronie przed spamem i oprogramowaniem szpiegującym. Również stworzenie w 2004 roku Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) uświadomiło państwom członkowskim i obywatelom europejskim konieczność współpracy nad zapewnieniem bezpieczeństwa systemów informatycznych i wypracowaniem na poziomie europejskim podstaw wspólnych praktyk w zakresie zabezpieczania systemów informatycznych. Zagadnienie to zostało również poruszone w siódmym ramowym programie badawczym UE.

Należy zwrócić uwagę na aktywne działania związane ze zwalczaniem cyberprzestępczości prowadzone przez Prezydencję Francuską, która w lipcu 2008 roku przedstawiła *Globalny plan w sprawie zwalczania cyberprzestępczości*. W planie podkreślono, że Internet stanowi skuteczny środek komunikowania się i werbowania stosowany przez terrorystów na całej kuli ziemskiej. Umożliwia również upowszechnianie nielegalnych treści zawierających pochwałę przemocy i terroryzmu i zachęcających do nienawiści rasowej. Pokazuje obrazy przemocy seksualnej wobec dzieci. Ułatwia przestępcom używającym fałszywej tożsamości wyszukiwanie przyszłych ofiar. Internet i gospodarka cyfrowa same mogą stać się ofiarą ataków przestępczych. Zagrożone może być bezpieczeństwo systemów niezbędnych dla zapewnienia bezpieczeństwa ludności, suwerenności państw i życia gospodarczego. Jako przykład z niedalekiej przeszłości przedstawiono internetowy atak na Estonię w 2007 roku[29].

Wynikiem prac Prezydencji Francuskiej jest Strategia Komisji Europejskiej nt. *zwalczania cyberprzestępczości* z 28 listopada 2008, w której założono: lepszą współpracę operacyjną organów ścigania, lepszą współpracę i koordynację polityczną miedzy państwami członkowskimi Unii Europejskiej, współpracę polityczną i prawną z państwami trzecimi, podnoszenie świadomości, szkolenia, badania, ściślejszy dialog z sektorem przemysłu, działania legislacyjne[30]. Ponadto Strategia

[28] Dz. Urz. L 13 z dnia 20 stycznia 2004.

[29] J. Kosiński, S. Kmiotek, *Międzynarodowa współpraca w zwalczaniu cyberprzestępczości*, http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberrteroryzm/kosinski_kmiotek.pdf [pobrano 7.01.2012].

[30] R. Chinalski, *Międzynarodowe instrumenty wspierające zwalczanie cyberprzestępczości. Organizacja zwalczania cyberprzestępczości w polskiej Policji,* [w:] *Praktyczne elementy zwalczania przestępczości*

zaleca podjęcie serii środków operacyjnych, takich jak powołanie do życia tzw. cyberpatroli, wspólnych zespołów dochodzeniowo-śledczych, wprowadzenie zdalnego przeszukiwania w Internecie oraz osobnych jednostek badawczych, które zostałyby zaangażowane do walki z cyberprzestępczością w następnych pięciu latach. Strategia Komisji Europejskiej wprowadza również konkretne rozwiązania dotyczące współpracy i wymiany informacji pomiędzy organami wymiaru sprawiedliwości a jednostkami sektora prywatnego (partnerstwo publiczno-prywatne).

Parlament Europejski w zaleceniach z dnia 26 marca 2009 roku dla Rady w sprawie utrwalenia bezpieczeństwa i podstawowych wolności w Internecie[31] zalecił dbałość o pełny i bezpieczny dostęp do Internetu dla wszystkich, ciągłą czujność w odniesieniu do bezwzględnej ochrony i intensywnego promowania podstawowych swobód w Internecie, ale jednocześnie jednoznacznie zobowiązał do zwalczania przestępczości w cyberprzestrzeni. Tworząc ten dokument Parlament wziął pod uwagę Decyzję Ramową Rady 2008/919/WSiSW z dnia 28 listopada 2008 roku zmieniającą Ramową Decyzję 2002/475/WSiSW *w sprawie zwalczania terroryzmu oraz niemiecką inicjatywę na rzecz wykrywania ciężkiej przestępczości i terroryzmu.* Zwrócił także uwagę, że dzięki wolności, jaką gwarantuje Internet, wykorzystuje się go również jako miejsce rozpowszechniania przesłań charakteryzujących się przemocą, takich jak nawoływanie do ataków terrorystycznych, jak również tworzenie stron internetowych, które mogą wyraźnie prowokować do opartych na nienawiści działań przestępczych.

Do ważnych krajowych przepisów regulujących kwestie związane z bezpieczeństwem cyberprzestrzeni należy zaliczyć:

- *Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z dnia 13 listopada 2007 roku,
- *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2009–2011*[32],
- *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*[33].

W Polsce w celu skutecznego przeciwdziałania zagrożeniom cyberterrorystycznym, a także zapewnienia odpowiedniego poziomu bezpieczeństwa teleinformatycznego państwa w podrozdziale dotyczącym Bezpieczeństwa Informacyjnego i Telekomunikacyjnego (pkt. 3.8.) *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2007 roku uwzględnione zostały problemy dotyczące walki z cyberterroryzmem oraz zagrożeniami płynącymi z cyberprzestrzeni:

zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 160.

31 *Strengthening security and fundamental freedoms on the Internet* 2008/2160 (INI).

32 http://e-prawnik.pl/wiadomosci/informacje/zalozenia-do-rzadowego-programu-ochrony-cyberprzestrzeni-rp-na-lata-2009-2011 [pobrano 1.02.2012].

33 http://www.locos.pl/publikacje/6111-rządowy-program-ochrony-cyberprzestrzeni-rp-na-lata-2011-2016 [pobrano 1.02.2012].

- skuteczne zapobieganie próbom destrukcyjnego oddziaływania na infrastrukturę telekomunikacyjną państwa poprzez redukowanie jej podatności na to oddziaływanie, minimalizowanie skutków ewentualnych ataków oraz przywrócenie w krótkim czasie stanu pełnej jej funkcjonalności,
- tworzenie i rozwijanie długofalowych planów ochrony kluczowych systemów teleinformatycznych przed uzyskiwaniem dostępu do danych przez podmioty do tego niepowołane, zakłócaniem normalnego ich funkcjonowania, kradzieżą tożsamości i sabotażem; ocenianie możliwości wtargnięcia do systemów teleinformatycznych, przygotowanie możliwych form odpowiedzi na ataki oraz rozwijanie metody ewaluacji poniesionych strat informacyjnych; priorytetem państwa będzie wspieranie narodowych programów i technologii informacyjnych,
- zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych w celu przeciwdziałania przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjną, w tym zapobieganie atakom na elementy tej infrastruktury; szczególne znaczenie ma ochrona informacji niejawnych przechowywanych lub przekazywanych w postaci elektronicznej; opracowanie i wdrożenie przejrzystych zasad dostępu uprawnionych organów państwa do treści przesyłanych drogą elektroniczną, co wymaga ciągłego dostosowywania przepisów prawa telekomunikacyjnego do szybko zmieniających się dzięki postępowi technologicznemu realiów, uwzględniając bezpieczeństwo Polski,
- zapewnienie należytego poziomu bezpieczeństwa telekomunikacyjnego, co wymaga rozwoju środków zapobiegania zakłóceniom, jakie mogą wystąpić w tej sferze, a także zwiększania zdolności do koordynacji procesów dochodzeniowych w ramach instytucji posiadających elementy rządowej infrastruktury telekomunikacyjnej; wyznaczone służby będą podejmować odpowiednie działania samodzielnie lub wspólnie z analogicznymi strukturami w innych państwach, zwłaszcza krajach członkowskich NATO i UE, a także z producentami i dostawcami urządzeń informatycznych oraz oprogramowania, krajowymi operatorami telekomunikacyjnymi, dostawcami usług internetowych, ośrodkami badawczymi i szkoleniowymi; zapewnienie bezawaryjnego funkcjonowania infrastruktury informatycznej systemu bankowego; uczestnictwo w pracach NATO nad przeciwdziałaniem próbom destrukcji infrastruktury informacyjnej państwa,
- niezbędne dla bezpieczeństwa państwa zapewnienie systemu łączności dla administracji rządowej, sił zbrojnych i innych kluczowych instytucji państwowych, opartego na najnowocześniejszych technologiach telekomunikacyjnych i najwyższych standardach bezpieczeństwa; możliwie szybkie stworzenie własnego systemu łączności satelitarnej przy wykorzystaniu przyznanych geostacjonarnych pozycji orbitalnych[34].

[34] *Strategia Bezpieczeństwa Narodowego RP 2007*, http://www.bbn.gov.pl [pobrano 2.02.2012].

11.3. Organy właściwe w sferze bezpieczeństwa cyberprzestrzeni[35]

W Polsce problematyka ochrony cyberprzestrzeni została uregulowana w *Rządowym programie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, który został przygotowany przez Ministerstwo Spraw Wewnętrznych i Administracji w 2010 roku. *Program* zawiera przedsięwzięcia prawne, organizacyjne, techniczne i edukacyjne, które mają na celu zwiększenie zdolności państwa do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. Należy zaznaczyć, że *Program* nie dotyczy bezpieczeństwa niejawnych sieci i systemów teleinformatycznych. Ten obszar jest regulowany ustawą z dnia 5 sierpnia 2010 roku *o ochronie informacji niejawnych*[36] wraz z aktami wykonawczymi.

Systemy i sieci teleinformatyczne eksploatowane przez administrację rządową, organy władzy ustawodawczej, władzy sądowniczej, samorządu terytorialnego, a także strategicznych z punktu widzenia bezpieczeństwa państwa przedsiębiorców (np. podmioty działające w obszarze telekomunikacji, energii, gazu, bankowości, a także podmioty o szczególnym znaczeniu dla obronności i bezpieczeństwa państwa, podmioty działające w obszarze ochrony zdrowia), jak również przedsiębiorcy oraz użytkownicy indywidualni cyberprzestrzeni są objęci niniejszym *Programem* i traktowani jako użytkownicy cyberprzestrzeni[37]. Teleinformatyczna infrastruktura krytyczna (TIK) jest częścią cyberprzestrzeni o krytycznym znaczeniu dla jej funkcjonowania.

Celem strategicznym *Programu* jest zapewnienie bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, co ze strony uprawnionych podmiotów wymaga stworzenia ram prawnych i organizacyjnych, systemu koordynacji i wymiany informacji pomiędzy administracją publiczną a innymi podmiotami i użytkownikami cyberprzestrzeni Rzeczypospolitej Polskiej, w tym z przedsiębiorcami.

Do celów szczegółowych *Programu* zalicza się:

- zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej, w tym teleinformatycznej infrastruktury krytycznej państwa,
- zmniejszenie skutków naruszeń bezpieczeństwa cyberprzestrzeni,
- zdefiniowanie kompetencji podmiotów odpowiedzialnych za ochronę cyberprzestrzeni,
- stworzenie i realizację spójnego dla wszystkich podmiotów administracji publicznej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych,
- stworzenie stałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni oraz przedsiębiorcami dostarczającymi usługi w cyberprzestrzeni i operatorami teleinformatycznymi infrastruktury krytycznej,

[35] Podrozdział opracowano na podstawie *Rządowego programu ochrony cyberprzestrzeni na lata 2011–2016*.

[36] Dz. U. z 2010 r. Nr 182, poz. 1228.

[37] *Rządowy program ochrony cyberprzestrzeni…*, s. 5.

- zwiększanie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni[38].

Powyższe cele będą realizowane poprzez stworzenie systemu koordynacji przeciwdziałania i reagowania na zagrożenia: i ataki na cyberprzestrzeń, w tym ataki o charakterze cyberterrorystycznym, powszechne wdrożenie wśród jednostek administracji publicznej, a także podmiotów niepublicznych mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń dla bezpieczeństwa cyberprzestrzeni oraz właściwemu postępowaniu w przypadku stwierdzonych incydentów, powszechną edukację społeczną oraz specjalistyczną edukację w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej[39].

Program skierowany jest do wszystkich użytkowników cyberprzestrzeni znajdujących się w granicach państwa i w miejscach poza jego terytorium, gdzie znajdują się polskie przedstawicielstwa (placówki dyplomatyczne, placówki konsularne, kontyngenty wojskowe, kontyngenty Policji czy Żandarmerii Wojskowej). Cyberprzestrzeń państwa w przypadku Polski nazywana jest Cyberprzestrzenią Rzeczypospolitej Polskiej (CRP).

Adresatów *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* przedstawiono w tabeli 97.

Tabela 97. Adresaci *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*

Adresaci	
Organy władzy publicznej	
Administracja rządowa	naczelne organy administracji rządowej: Prezes Rady Ministrów, Rada Ministrów, ministrowie i przewodniczący określonych w ustawach komitetów centralne organy administracji rządowej: organy inne niż wymienione w pkt. 1 lit. a), tj. organy podporządkowane Prezesowi Rady Ministrów bądź poszczególnym ministrom terenowe organy administracji rządowej: wojewoda, organy administracji zespolonej i niezespolonej
Administracja samorządowa (szczebel gminny, powiatowy i wojewódzki)	organy stanowiące (sejmik wojewódzki, rada powiatu, rada gminy) organy wykonawcze (marszałek i zarząd województwa, starosta i zarząd powiatu, wójt/burmistrz, prezydent miasta) a także inne podległe im jednostki organizacyjne lub przez nie nadzorowane
Administracja państwowa (jednostki nie należące do administracji rządowej i samorządowej)	Prezydent Rzeczypospolitej Polskiej Krajowa Rada Radiofonii i Telewizji Rzecznik Praw Obywatelskich Rzecznik Praw Dziecka Krajowa Rada Sądownicza organy kontroli państwowej i ochrony prawa Narodowy Bank Polski Komisja Nadzoru Finansowego

[38] Ibidem, s. 7.

[39] Ibidem.

	centralne organy administracji podległe Sejmowi i Senatowi Rzeczypospolitej Polskiej, niewymienione wyżej państwowe osoby prawne i inne niż wymienione powyżej państwowe jednostki organizacyjne
Operatorzy infrastruktury krytycznej, których działalność jest zależna i niezależna od prawidłowego funkcjonowania cyberprzestrzeni	
Przedsiębiorcy oraz użytkownicy indywidualni cyberprzestrzeni	
Inne instytucje będące użytkownikami cyberprzestrzeni	

Źródło: Opracowano na podstawie *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, Warszawa 2010, s. 7 i 8

Za ochronę Cyberprzestrzeni Rzeczypospolitej Polskiej odpowiedzialny jest Prezes Rady Ministrów, który zadania w tym zakresie wykonuje poprzez: Ministra Spraw Wewnętrznych i Administracji[40], Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Służby Kontrwywiadu Wojskowego[41]. Wymienione podmioty zajmują kluczową pozycję w realizacji *Programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* i są odpowiedzialne za bezpieczeństwo wewnętrzne państwa, każdy w zakresie swojej właściwości. Natomiast Rządowe Centrum Bezpieczeństwa (RCB) odpowiedzialne jest za koordynację działań w zakresie ochrony teleinformatycznej infrastruktury krytycznej.

Z uwagi na cel *Programu,* wykonawstwo zadań wymaga stworzenia podstaw udziału i współpracy podmiotów pozostających poza administracją publiczną, ze wskazaniem na przedsiębiorców. Część infrastruktury teleinformatycznej jest własnością państwa, natomiast jej większość stanowi własność prywatną, dlatego w realizacji *Programu* wymagany jest udział przedsiębiorców będących właścicielami zasobów stanowiących infrastrukturę państwa. Zgodnie z posiadanymi kompetencjami udział w realizacji *Programu* biorą podmioty wskazane w tabeli 98.

Tabela 98. Podmioty biorące udział w realizacji *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*

Podmioty	
Odpowiedzialne za realizację Programu ochrony CRP	Zaangażowane w działania na rzecz ochrony CRP
Prezes Rady Ministrów	Kancelaria Prezes Rady Ministrów
Minister Edukacji Narodowej	Minister Spraw Wewnętrznych
Minister Nauki i Szkolnictwa Wyższego	Minister Obrony Narodowej
Minister Obrony Narodowej	Minister Edukacji Narodowej
Minister Spraw Wewnętrznych	Minister Infrastruktury
Minister Administracji i Cyfryzacji	Minister Administracji i Cyfryzacji
Szef Agencji Bezpieczeństwa Wewnętrznego	Minister Nauki i Szkolnictwa Wyższego

[40] W dniu 21 listopada 2011 roku na bazie Ministerstwa Spraw Wewnętrznych i Administracji utworzone zostało Ministerstwo Spraw Wewnętrznych (Dz. U. z 2011 r. Nr 250, poz. 1502) i Ministerstwo Administracji i Cyfryzacji (Dz. U. z 2011 r. Nr 250, poz. 1501).

[41] *Rządowy program ochrony cyberprzestrzeni…*, s. 8.

Szef Służby Kontrwywiadu Wojskowego	Rządowe Centrum Bezpieczeństwa
Dyrektor Rządowego Centrum Bezpieczeństwa	Agencja Bezpieczeństwa Wewnętrznego
Komendant Główny Policji	Służba Kontrwywiadu Wojskowego
Komendant Główny Straży Granicznej	Komenda Główna Policji
Komendant Główny Państwowej Straży Pożarnej	Komenda Główna Straży Granicznej
Inne organy administracji publicznej	Komenda Główna Państwowej Straży Pożarnej
Przedsiębiorcy – właściciele zasobów stanowiących infrastrukturę krytyczną państwa	Naukowa i Akademicka Sieć Komputerowa – Zespół CERT Polska
	Przedsiębiorcy telekomunikacyjni posiadający własną infrastrukturę telekomunikacyjną

* Rozporządzenie Rady Ministrów z dnia 21 listopada 2011 roku *w sprawie utworzenia Ministerstwa Spraw Wewnętrznych* (Dz. U. z 2011 r. Nr 250, poz. 1502).

** Rozporządzenie Rady Ministrów z dnia 21 listopada 2011 roku *w sprawie utworzenia Ministerstwa Administracji i Cyfryzacji* (Dz. U. z 2011 r. Nr 250, poz. 1501).

Źródło: Opracowanie własne na podstawie *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, Warszawa 2010, s. 8 i 12

W ramach systemu ochrony cyberprzestrzeni zostanie powołany Międzyresortowy Zespół Koordynujący ds. Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, w skład którego wejdą jednostki administracji rządowej: Kancelaria Prezes Rady Ministrów, Minister Spraw Wewnętrznych, Minister Obrony Narodowej, Minister Administracji i Cyfryzacji, Minister Edukacji Narodowej, Minister Infrastruktury, Minister Nauki i Szkolnictwa Wyższego, Rządowe Centrum Bezpieczeństwa, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Komenda Główna Policji, Komenda Główna Straży Granicznej, Komenda Główna Państwowej Straży Pożarnej. Podstawowym zadaniem Zespołu będzie: nadzorowanie i kompleksowa koordynacja wszelkich działań w ramach *programów* szczegółowych oraz dalsze działania, które są rekomendowane i wdrażane na podstawie tych programów, określenie wzajemnych relacji, zadań oraz zasad współpracy wszystkich zaangażowanych podmiotów, nadzorowanie stanu realizacji programów szczegółowych przez instytucje realizujące zadania wynikające z programów, organizowanie cyklicznych spotkań i szkoleń dotyczących bezpieczeństwa cyberprzestrzeni, rekomendowanie do realizacji rozwiązań przedstawionych przez użytkowników cyberprzestrzeni z zakresu bezpieczeństwa[42].

Użytkownicy, przedsiębiorcy i inne instytucje biorące udział w realizacji *Programu* będą informowali uprawnione podmioty o realizacji jego poszczególnych etapów na podstawie analiz prowadzonych przez operatorów, dostawców usług. Wyznacznikiem wdrażania *Programu* będą statystyki incydentów obsługiwanych przez zespoły ds. naruszeń w sieci.

Docelowym rozwiązaniem uwzględnianym przez *Program* jest utworzenie jednostki technicznej wykonującej zadania dotyczące zarządzania i koordynacji przedsięwzięć w zakresie ochrony Cyberprzestrzeni Rzeczypospolitej Pol-

[42] Ibidem, s. 24.

skiej, która przejęłaby zadania Międzyresortowego Zespołu Koordynującego ds. Ochrony Cyberprzestrzeni RP. Ponieważ zespoły typu CERT posiadają doświadczenie dotyczące bezpieczeństwa teleinformatycznego, uznano, że powinny stanowić ważny element systemu ochrony cyberprzestrzeni. Dlatego przyjęty *Program* będzie promował działania na rzecz powstawania nowych zespołów typu CERT oraz doprowadzania do powstawania funkcjonalności, związanej w szczególności ze zdolnością do reagowania na incydenty sieciowe, a także działania na rzecz wypracowywania, upowszechniania i wdrażania standardów i najlepszych praktyk związanych z funkcjonowaniem zespołów typu CERT poprzez realizację następujących szczegółowych celów:

- w dziedzinie tworzenia zespołów reagujących typu CERT:
  - wspólne działania istniejących zespołów prowadzące do tworzenia lub wspierania tworzenia nowych zespołów,
  - przystępowanie istniejących i powstających zespołów do inicjatywy ABUSE FORUM,
  - bezpośrednie działania przedstawicieli ABUSE FORUM oraz odpowiedzialnych za realizację RPOC wobec ISPs i ICPs, które nie posiadają zdolności do reagowania na incydenty, w celu utworzenia takiej zdolności (preferowane powstanie zespołów typu CERT); działania te będą miały charakter dobrowolny w oparciu o najlepsze praktyki w tej dziedzinie,
- w dziedzinie wypracowywania, upowszechniania i wdrażania standardów i najlepszych praktyk działania związane z funkcjonowaniem zespołów typu CERT:
  - stworzenie zestawu standardów i dobrych praktyk, np. opracowanie oczekiwanego poziomu świadczenia usług z zakresu usług świadczonych przez CERT, a w szczególności poziomu obsługi incydentów bezpieczeństwa oraz priorytetów obsługi incydentów bezpieczeństwa,
  - organizację wspólnych ćwiczeń zespołów reagujących sektora prywatnego i publicznego, prowadzących do wypracowania sposobów reagowania i koordynacji działań, w przypadku wystąpienia szczególnie groźnych przypadków ataków z cyberprzestrzeni, w szczególności skierowanych na infrastrukturę krytyczną[43].

W ramach współdziałania jednostek organizacyjnych w zakresie ochrony cyberprzestrzeni zostaną utworzone sektorowe (resortowe) punkty kontaktowe (SPK). Tym samym sektorowe punkty kontaktowe staną się elementami systemu komunikacji instytucji związanych z ochroną cyberprzestrzeni. Według autorów *Programu* sektorowy punkt kontaktowy ma być odpowiedzialny za organizację współpracy, wymianę informacji o zagrożeniach, trendach w formie raportów, biuletynów itp. Pozwoli to abonentom, dostawcom usług, zespołom CERT itp. na realizację procedur operacyjnych potrzebnych do obsługi incydentu oraz prowadzenia działań zgodnie z uprawnieniami ustawowymi tak, aby nie musieli oni zwracać się do kilku właściwych podmiotów w ramach jednej organizacji w celu

[43] Ibidem, Załącznik nr 16.

zebrania wszelkich potrzebnych informacji. Dotyczy to pełnego cyklu obsługi incydentu oraz innych ustaleń objętych zawartymi porozumieniami. Wyłączeniu podlegają informacje dotyczące zagrożeń, procedur dochodzeniowo-śledczych, odwoławczych o charakterze sądowym lub administracyjnym oraz dokumenty kierowane do kierownictwa resortu/firmy.

Współpraca Międzyresortowego Zespołu Koordynującego ds. Ochrony Cyberprzestrzeni RP z punktami sektorowymi obejmuje:

- organizację współpracy pomiędzy użytkownikami tego samego obszaru CRP oraz wymianę informacji pomiędzy obszarami administracyjnym, wojskowym i cywilnym,
- usprawnienie wymiany informacji o podatnościach, zagrożeniach, trendach w bezpieczeństwie cyberprzestrzeni,
- opracowanie struktury wymiany informacji i współpracy pomiędzy jednostkami w danym sektorze oraz jednostkami a właściwymi organami państwa,
- formalne przyporządkowanie i zatwierdzenie odpowiedzialności za obszary cyberprzestrzeni: CERT.GOV.PL – administracyjny, CERT Polska – cywilny, MIL CERT – wojskowy,
- przygotowanie wytycznych dla sektorowych punktów (tworzonych w zależności od potrzeb) właściwych dla poszczególnych działów administracji rządowej: wskazanie jednostek odpowiedzialnych na prowadzenie SPK w jednostkach podległych, opracowanie zakresów obszarowych każdego z punktów sektorowych, opracowanie zakresu raportowanych danych, opracowanie wzoru sprawozdań.

W realizacji *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej w latach 2011–2016* istotna jest współpraca z podmiotami krajowymi i międzynarodowymi odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz odpowiedzialnymi za zwalczanie przestępczości komputerowej o charakterze kryminalnym. W ramach tej współpracy wypracowane formy będą miały zarówno postać roboczą, w celu zminimalizowania opóźnień reakcji na incydenty komputerowe, jak i sformalizowaną służącą eliminowaniu problemów kompetencyjnych.

Współpraca krajowa

Kluczową rolę w realizacji *Programu* odgrywają Ministerstwo Spraw Wewnętrznych, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego (ABW), Ministerstwo Obrony Narodowej oraz Służba Kontrwywiadu Wojskowego (w zakresie systemów leżących w gestii Ministerstwa Obrony Narodowej), jako podmioty wykonujące zadania w sferze bezpieczeństwa wewnętrznego państwa (każdy w zakresie swojej właściwości), a także Rządowe Centrum Bezpieczeństwa odpowiedzialne za koordynację działań w zakresie ochrony teleinformatycznej infrastruktury krytycznej.

Szczególną pozycję w systemie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej z uwagi na posiadane kompetencje zajmuje Szef Agencji Bezpieczeń-

stwa Wewnętrznego. Agencja Bezpieczeństwa Wewnętrznego współpracuje z podmiotami odpowiedzialnymi za bezpieczeństwo Rzeczypospolitej Polskiej (Ministerstwem Obrony Narodowej, Ministerstwem Spraw Wewnętrznych, Ministerstwem Administracji i Cyfryzacji, Służbą Kontrwywiadu Wojskowego) oraz odpowiedzialnymi za zwalczanie przestępczości w cyberprzestrzeni (Policją, Żandarmerią Wojskową). Jednocześnie poprzez zespół CERT.GOV.PL koordynuje działania krajowych zespołów reagowania (Projekt Działanie Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL).

Ważną pozycję w zakresie reagowania na incydenty bezpieczeństwa komputerowego dla jednostek administracji publicznej Rzeczypospolitej Polskiej zajmuje Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL). Jednocześnie jest on właściwy dla koordynacji działań pomiędzy poszczególnymi instytucjami w kraju oraz innymi zespołami CERT w zakresie rozpoznawania, zapobiegania i przeciwdziałania cyberzagrożeniom. Zespół CERT.GOV.PL pełni rolę wiodącą w stosunku do innych zespołów reagowania w kraju. Program zakłada, że docelowa struktura CERT.GOV.PL składać się będzie z pięciu zespołów: Analitycznego, Informatyki Śledczej, Monitorującego, Grupy Szybkiego Reagowania, Zespołu Eksperckiego (nieetatowego, o dynamicznym składzie).

Dla skutecznej ochrony cyberprzestrzeni ważne są bezpośrednie robocze kontakty krajowych zespołów reagowania na incydenty komputerowe[44], m.in. takich jak: Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, System Reagowania na Incydenty Komputerowe resortu obrony narodowej CERT Polska, CERT-y powołane przez przedsiębiorców telekomunikacyjnych, inne zespoły ds. naruszeń w sieci, a w szczególności członkowie ABUSE Forum.

> Realizacja *Programu* poprzez wzajemne porozumienia pomiędzy zespołami pozwoli na utworzenie więzi i bezpośrednich relacji współdziałania pomiędzy zespołami, do tej pory realizującymi zadania samodzielnie. Pozwoli na zespołowe wykonywanie zadań oraz wspólne rozwiązywanie problemów. Rozwiązanie w zakresie bezpośredniej komunikacji elektronicznej zapewni skrócenie czasu reakcji na zaistniałe zagrożenie. Istotną zaletą jest rozwijanie idei ABUSE Forum w zakresie kontaktów osobistych pozwalające na uwierzytelnienie uczestnika procesu reagowania z wykorzystaniem zdefiniowanych kanałów komunikacyjnych[45].

W sferze współpracy podstawowym celem *Programu* jest:

- wypracowanie mechanizmów i zasad współpracy pomiędzy zespołami,
- analiza wzajemnych relacji, określenie wzajemnych interesów,
- zdefiniowanie jasnych obszarów działania dla poszczególnych sektorów,
- budowanie wizerunku zespołów pozwalających na właściwe postrzeganie drugiej strony,
- opracowanie wspólnej klasyfikacji incydentów sieciowych na potrzeby wymiany informacji, obserwacji trendów oraz ustalania działań profilaktycznych prowadzących do ograniczenia liczby zagrożeń w sieci,

[44] Ibidem, s. 27.

[45] Ibidem, Załącznik nr 20.

- wypracowanie metod komunikacji i działania pomiędzy zespołami typu CERT w przypadku zaistnienia sytuacji krytycznych z punktu widzenia bezpieczeństwa cyberprzestrzeni,
- zwiększenie efektywności działania podmiotów publicznych oraz komercyjnych w zakresie systemu reagowania na incydenty bezpieczeństwa,
- opracowanie i wdrożenie wytycznych do współpracy wszystkich podmiotów publicznych oraz komercyjnych w zakresie ochrony systemów i sieci teleinformatycznych,
- budowanie jednolitej bazy wiedzy w zakresie systemów ochrony systemów teleinformatycznych,
- możliwość budowania zespołów eksperckich i zadaniowych w odpowiedzi na zidentyfikowane zagrożenie[46].

Kolejnymi podmiotami zaangażowanymi w proces ochrony cyberprzestrzeni są producenci urządzeń i systemów teleinformatycznych.

> W celu podniesienia poziomu bezpieczeństwa teleinformatycznego użytkowników CRP, a także systemów teleinformatycznych, prowadzone będą działania polegające na współpracy z komercyjnymi partnerami będącymi producentami oprogramowania i sprzętu teleinformatycznego. Główny nacisk położony zostanie na wprowadzenie na rynek urządzeń i oprogramowania standardowo zawierającego skonfigurowane rozwiązania pozwalające na zapewnienie minimalnego poziomu bezpieczeństwa. Rozwój współpracy z tymi partnerami, w tym wymiana doświadczeń i oczekiwań, stanowić będzie jeden z ważniejszych czynników mających duży wpływ na system edukacji społecznej i specjalistycznej, jak i na jakość tworzonych systemów. Istotne znaczenie dla rozszerzenia spektrum dostępnych narzędzi ma współpraca podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne z producentami systemów zabezpieczeń. Należy dążyć do udostępniania pojedynczym, jak i instytucjonalnym użytkownikom jak największego wachlarza rozwiązań służących szeroko rozumianemu bezpieczeństwu teleinformatycznemu oraz ochronie informacji[47].

W procesie ochrony cyberprzestrzeni ważną rolę odgrywają przedsiębiorcy telekomunikacyjni. Ze względu na globalny charakter zagrożeń w cyberprzestrzeni wymagana jest ścisła skoordynowana współpraca pomiędzy Urzędem Komunikacji Elektronicznej (UKE), przedsiębiorcami telekomunikacyjnymi i użytkownikami cyberprzestrzeni. W celu utrzymania zakładanego poziomu bezpieczeństwa istnieje potrzeba wypracowania zachowań i komunikacji użytkowników cyberprzestrzeni na wypadek wystąpienia incydentów bezpieczeństwa, cyberprzestępstw i cyberterroryzmu[48]. Dla zachowania minimalnego poziomu bezpieczeństwa podłączonego sprzętu przygotowane zostaną propozycje zapisów do umów związanych z dostępem do cyberprzestrzeni regulujące standard zachowania i reagowania w przypadku zagrożenia czy incydentu.

[46] Ibidem.

[47] Ibidem, s. 27 i Załącznik nr 21.

[48] Ibidem, s. 27.

W ramach projektu zostaną też wypracowane metody reagowania i usprawniona komunikacja pomiędzy organami odpowiedzialnymi za ochronę CRP a przedsiębiorcami telekomunikacyjnymi. W tym obszarze współpraca obejmuje:

- wypracowanie standardów reagowania i komunikacji z przedsiębiorcami telekomunikacyjnymi dotyczących informowania o zagrożeniach, incydentach, skutecznych metodach przeciwdziałania incydentom oraz cyberprzestępstwom i cyberterroryzmowi,
- wypracowanie propozycji zapisów dotyczących bezpieczeństwa cyberprzestrzeni do umów podpisywanych pomiędzy przedsiębiorcami telekomunikacyjnymi a użytkownikiem końcowym cyberprzestrzeni,
- wypracowanie metod informowania użytkowników końcowych cyberprzestrzeni przez przedsiębiorców telekomunikacyjnych o zagrożeniach i występujących incydentach w cyberprzestrzeni[49].

Współpraca międzynarodowa

Mając na uwadze globalny charakter ochrony cyberprzestrzeni, ważnym elementem dla jej skuteczności jest utrzymanie i rozwijanie współpracy międzynarodowej w tym obszarze. Rząd Rzeczypospolitej Polskiej deklaruje, poprzez swoich przedstawicieli, organy rządowe, instytucje państwowe oraz współpracę z instytucjami pozarządowymi, aktywne działania zmierzające do zwiększenia bezpieczeństwa Cyberprzestrzeni Rzeczypospolitej Polskiej oraz międzynarodowej[50].

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016 ma za zadanie stymulować współpracę krajowych struktur odpowiedzialnych za bezpieczeństwo cyberprzestrzeni z inicjatywami istniejącymi na poziomie europejskim. W Europie została powołana do życia Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA), która zajmuje się tym obszarem zagadnień. ENISA dokonuje wielu ważnych analiz, publikuje raporty, opracowania, najlepsze praktyki w konkretnych obszarach NIS (Network and Information Security). Współpracuje także z rządami krajów członkowskich Unii Europejskiej w dziedzinie między innymi propagowania wspólnych standardów bezpieczeństwa, wspólnych ćwiczeń w odniesieniu do odporności sieci teleinformatycznych na rozmaite zagrożenia. ENISA kładzie również duży nacisk na zwiększanie świadomości bezpieczeństwa ze strony użytkowników Internetu. Niniejszy projekt szczegółowy zakłada ciągłą współpracę przedstawicieli Polski w ENISA (członek Rady Zarządzającej, Zastępca oraz Krajowy Oficer Łącznikowy) z Międzyresortowym Zespołem Koordynującym ds. Ochrony Cyberprzestrzeni RP w celu jak najpełniejszego wykorzystania doświadczeń agencji dla osiągania realizacji celów *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*[51].

Projekt szczegółowy będzie realizowany poprzez przedstawicieli Polski w agencji ENISA. Mają oni za zadanie obustronne przedkładanie analiz możliwo-

[49] Ibidem, Załącznik nr 22.

[50] Ibidem, s. 28.

[51] Ibidem, Załącznik nr 23.

ści wykorzystania wytypowanych wyników prac pomiędzy ENISA a MZKOC. Stała grupa ekspertów powołana przez Międzyresortowy Zespół Koordynujący ds. Ochrony Cyberprzestrzeni RP będzie analizowała celowość i możliwości wykorzystania osiągnięć agencji ENISA w realizacji *Programu*. Grupa ekspertów powinna być wybierana spośród wszystkich uczestników obszaru cyberprzestrzeni (administracja państwowa, operatorzy, dostawcy rozwiązań, organizacje zajmujące się bezpieczeństwem systemów i sieci komputerowych itd.). Stała grupa ekspertów wraz z przedstawicielami Polski w agencji ENISA proponuje odpowiednie działania w celu wykorzystania efektów prac Europejskiej Agencji Bezpieczeństwa Sieci i Informacji w Polsce. Propozycje te są przedstawiane Międzyresortowemu Zespołowi Koordynującemu ds. Cyberprzestrzeni. Celem powyższych przedsięwzięć jest wykorzystanie raportów, analiz, dobrych praktyk opracowywanych przez ENISA dla realizacji celów stawianych w *Programie*, możliwość wystąpienia do agencji ENISA o wsparcie eksperckie w dziedzinie bezpieczeństwa cyberprzestrzeni, monitorowanie innych inicjatyw w Europie (a także na świecie) dotyczących ochrony cyberprzestrzeni, w szczególności programów przygotowywanych przez Komisję Europejską[52]. W zakresie współpracy z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA) Polskę reprezentują przedstawiciele: członek Rady Zarządzającej, zastępca członka Rady Zarządzającej oraz krajowy oficer łącznikowy[53]. Ponadto Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL współpracuje z Forum of Incident Response and Security Teams (FIRST) oraz innymi międzynarodowymi organizacjami zrzeszającymi zespoły CERT, występując jako polski CERT typu rządowego. Realizacja zadania poprawi efektywność reakcji pomiędzy wystąpieniem zagrożenia w światowej cyberprzestrzeni a rozpoczęciem działań w obszarze CRP. Dodatkowo współpraca z FIRST pozwoli na wymianę doświadczeń w zakresie bezpieczeństwa oraz dobrych praktyk z innymi zespołami reagowania na całym świecie.

Szef Agencji Bezpieczeństwa Wewnętrznego wraz z kadrowym zapleczem technicznym stanowi Krajowy Punkt Centralny (Focal Point) w ramach polityki ochrony cyberprzestrzeni NATO. Podmiotami odpowiedzialnymi w sferze rządowej za koordynację reagowania na incydenty w sieciach i systemach komputerowych są: Rządowy Zespół Reagowania na Incydenty Komputerowe w odniesieniu do cyberprzestrzeni Rzeczypospolitej Polskiej oraz Wojskowy Zespół Reagowania na Incydenty Komputerowe Ministerstwa Obrony Narodowej w odniesieniu do sieci i systemów komputerowych leżących w gestii tego ministerstwa[54]. Minister Obrony Narodowej i Szef Agencji Bezpieczeństwa Wewnętrznego przy współpracy z ministrem właściwym do spraw wewnętrznych występują jako bezpośredni partnerzy NATO Cyber Defence Management Authority (CDMA).

[52] Ibidem.

[53] Ibidem, s. 28.

[54] Ibidem.

Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej zakłada, że sprawny system koordynacji zapewni wymianę informacji pozyskanych w ramach współpracy międzynarodowej bez ponoszenia dodatkowych kosztów pomiędzy zespołami rządowymi, wojskowymi i cywilnymi, zgodnie z obowiązującymi przepisami prawa, a w szczególności zgodnie z ustawą o ochronie danych osobowych oraz o ochronie informacji niejawnych.

Zarządzanie ryzykiem

W procesie realizacji *Programu* szczególną uwagę zwraca się na zarządzanie ryzykiem, które stanowi podstawowy element procesu ochrony cyberprzestrzeni. Szczególną pozycję w tym względzie zajmują Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego, które w celu zunifikowania podejścia przedstawiają podmiotom administracji publicznej katalogi zawierające specyfikację zagrożeń oraz możliwych podatności. Ponadto zapewnieniu spójności polityki bezpieczeństwa informacji jednostek organizacyjnych służyć mają przygotowane przez Ministerstwo Spraw Wewnętrznych, Ministerstwo Administracji i Cyfryzacji w porozumieniu z Ministerstwem Obrony Narodowej, Agencją Bezpieczeństwa Wewnętrznego i Służbą Kontrwywiadu Wojskowego wytyczne dotyczące systemów zarządzania bezpieczeństwem informacji. Wytyczne uwzględniają ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów stwierdzonych w każdym z sektorów, które stanowią oddzielny dokument oznaczony właściwą klauzulą niejawności, ponadto określają wzory sprawozdań.

Podmioty zaangażowane w ochronę cyberprzestrzeni każdego roku w przedmiotowej sprawie przekazują do Ministerstwa Spraw Wewnętrznych sprawozdania. Na ich podstawie MSW i instytucje zaangażowane oceniają, czy należy na poziomie współpracy rozważyć dalsze środki ochrony. Działania te podejmowane są w połączeniu z przeglądem *Programu*.

W ramach programu MSW we współpracy z zaangażowanymi instytucjami opracuje wspólne wytyczne w sprawie metod przeprowadzania oceny ryzyka w odniesieniu do teleinformatycznej infrastruktury krytycznej. Wdrażanie przyjętych wytycznych będzie obligatoryjne dla zaangażowanych instytucji, ponadto zostanie określona forma i okres sporządzania raportów, a także wprowadzona zostanie dla wszystkich użytkowników Cyberprzestrzeni Rzeczypospolitej Polskiej jednolita metodyka szacowania ryzyka[55].

Do innych przedsięwzięć realizowanych w ramach zarządzania ryzykiem, należy:

- identyfikacja zasobów, podsystemów, funkcji i zależności od innych systemów istotnych z punktu widzenia funkcjonowania CRP,
- zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej, w tym krytycznej infrastruktury teleinformatycznej państwa, w sposób adekwatny do prawdopodobieństwa wystąpienia zagrożeń,

[55] Ibidem, Załącznik nr 1.

- identyfikacja zagrożeń i ocena ryzyka,
- ujednolicenie oceny ryzyka we wszystkich jednostkach,
- zidentyfikowanie zagrożeń i ich specyfikacji oraz przedstawienie podmiotom administracji,
- ujednolicenie szablonów sprawozdań dotyczących rodzajów ryzyka, zagrożeń i słabych punktów stwierdzonych w każdym z sektorów,
- stworzenie i uruchomienie podmiotowych i sektorowych punktów kontaktowych[56].

Za nadzór i realizację programu odpowiada Międzyresortowy Zespół Koordynujący ds. Ochrony Cyberprzestrzeni, który koordynuje ocenę ryzyka w ramach ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej.

W celu skutecznego zarządzania bezpieczeństwem teleinformatycznej infrastruktury krytycznej każdy podmiot realizujący zadania publiczne powinien ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i doskonalić System Zarządzania Bezpieczeństwem Informacji (SZBI). Wprowadzenie tego systemu powinno być decyzją strategiczną kierownictwa podmiotu umocowaną w akcie prawa miejscowego. Na projektowanie i wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji powinny mieć wpływ potrzeby i cele działania podmiotu, wymagania bezpieczeństwa, realizowane procesy oraz wielkość i struktura podmiotu. Działania tego charakteru mają na celu zapoznanie kierownictwa podmiotów publicznych z istotą systemu zarządzania bezpieczeństwem informacji, opracowanie wytycznych do wdrożenia systemu zarządzania bezpieczeństwem informacji dla typowych klas podmiotów publicznych, wprowadzanie SZBI w podmiotach publicznych, określenie zasad współpracy z istniejącymi już składnikami SZBI, powołanymi na mocy odrębnych regulacji (ochrona danych osobowych, zarządzanie ciągłością działania, ochrona informacji niejawnych)[57]. Przy opracowywaniu polityki bezpieczeństwa podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji, a w szczególności grupy norm serii PN ISO/IEC 27000 i innych norm z nią powiązanych.

W ramach systemu zarządzania ochroną cyberprzestrzeni w jednostce organizacyjnej korzystającej z Cyberprzestrzeni Rzeczypospolitej Polskiej ma być powołany Pełnomocnik ds. ochrony cyberprzestrzeni, do którego zadań należy:

- realizacja obowiązków wynikających z przepisów, aktów prawnych właściwych dla ochrony cyberprzestrzeni,
- ustalanie i wdrożenie procedur w organizacji w zakresie reagowania na incydenty komputerowe,
- identyfikowanie i prowadzenie cyklicznej analizy zagrożeń,
- przygotowanie planów awaryjnych,
- komunikacja z organami odpowiedzialnymi za ochronę CRP,

[56] Ibidem.

[57] Ibidem, Załącznik nr 5.

- szkolenie pracowników w podległej jednostce z zasad postępowania i bezpiecznego korzystania z cyberprzestrzeni oraz zasad reagowania na zagrożenia, incydenty, cyberprzestępstwa, cyberterroryzm,
- informowanie o zagrożeniach i incydentach użytkowników cyberprzestrzeni w podległej jednostce,
- prowadzenie postępowania w podległej jednostce organizacyjnej w przypadku wykrycia incydentu bezpieczeństwa,
- rekomendowanie zabezpieczeń adekwatnych do zagrożeń – na podstawie prowadzonej analizy ryzyka i zaistniałych incydentów bezpieczeństwa,
- niezwłoczne informowanie właściwych zespołów CERT o wystąpieniu incydentów komputerowych czy zmianie lokalizacji jednostki organizacyjnej[58].

Powyższe przedsięwzięcia mają na celu podniesienie bezpieczeństwa cyberprzestrzeni, zasobów teleinformatycznych oraz ich użytkowników. W ramach pełnionej funkcji nadzorowałby i koordynował bezpieczeństwo zasobów informatycznych firmy, która jest podłączona do cyberprzestrzeni, oraz utrzymywał kontakty z jednostkami odpowiedzialnymi za ochronę cyberprzestrzeni. Osoba pełniąca funkcję Pełnomocnika miałaby też za zadanie upowszechnianie wiedzy poprzez szkolenie użytkowników w podległej jednostce w zakresie bezpiecznego korzystania z zasobów cyberprzestrzeni, zagrożeń w cyberprzestrzeni, sposobów zabezpieczenia, odpowiedzialności, miejsc i sposobów zgłaszania incydentów, ataków, przypadków naruszenia prawa. Szkolenia kończyć się będą wydaniem certyfikatu. Szczególny nacisk położony ma zostać na specjalistyczne szkolenie z zakresu reagowania na incydenty związane z bezpieczeństwem informacji. Szkolenia takie będą organizowane przez zespoły reagowania na incydenty (CERT), Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego lub firmy komercyjne. Szkolenia w zakresie podstaw bezpieczeństwa eksploatacji systemów i sieci teleinformatycznych prowadzone będą przez ośrodki kształcenia autoryzowane przez producentów sprzętu komputerowego lub oprogramowania sieciowego.

Obok szkolenia Pełnomocników ds. ochrony cyberprzestrzeni *Rządowy programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* uwzględnia:

- uruchomienie kształcenia na uczelniach wyższych w zakresie bezpieczeństwa teleinformatycznego. Zagadnienia związane z bezpieczeństwem cyberprzestrzeni powinny stać się elementem każdego programu nauczania. Dotyczy to uczelni technicznych kształcących informatyków. Działania te mają na celu stworzenie wykwalifikowanych kadr w sektorze publicznym i prywatnym odpowiadających za utrzymanie systemów i sieci teleinformatycznych, ze szczególnym uwzględnieniem zasobów kluczowych dla bezpieczeństwa państwa;
- prowadzenie akcji edukacyjnej dla pracowników administracji publicznej w zakresie zagadnień dotyczących bezpieczeństwa w cyberprzestrzeni. Zakres tematyczny będzie przygotowany tak, aby oprócz podstawowych zagad-

[58] Ibidem, s. 17.

nień uwzględniał również tematykę odpowiednią dla zajmowanego stanowiska oraz konsekwencje wynikające z naruszenia bezpieczeństwa teleinformatycznego. Znajomość problematyki dotyczącej bezpieczeństwa teleinformatycznego jest dodatkowym kryterium obsady stanowisk w administracji publicznej;

- prowadzenie kampanii wśród społeczeństwa o charakterze edukacyjno-prewencyjnym, która skierowana jest do każdego użytkownika komputera, ze szczególnym wskazaniem na dzieci i młodzież, rodziców i nauczycieli;
- programy badawcze, które dotyczą przygotowania i uruchomienia krajowych programów badawczych w zakresie bezpieczeństwa teleinformatycznego. Koordynatorem w tym zakresie jest Ministerstwo Nauki i Szkolnictwa Wyższego.

Zakres szkolenia pracowników administracji publicznej obejmować powinien zagadnienia dotyczące:

- zachowania w sytuacjach kryzysowych,
- bezpieczeństwa informacji w praktyce codziennego funkcjonowania organizacji,
- polityki bezpieczeństwa oraz polityki zachowania ciągłości działania,
- procedur ochrony informacji i zasobów oraz osób (w tym bezpieczeństwa fizycznego i środowiskowego),
- zagrożeń występujących w cyberprzestrzeni,
- procedur postępowania w przypadku naruszenia bezpieczeństwa, w wyniku cyberataku na zasoby instytucji, państwa itd.,
- roli jednostki w bezpieczeństwie instytucji i cyberprzestrzeni,
- przełamania zabezpieczeń przez cyberprzestępców,
- procedur zgłaszania wykrytych prób naruszenia bezpieczeństwa teleinformatycznego,
- zakresu odpowiedzialności, jaką ponosi urzędnik w przypadku nienależytego korzystania z zasobów cyberprzestrzeni,
- metod bezpiecznego korzystania z zasobów cyberprzestrzeni,
- funkcji i zadań realizowanych przez jednostki odpowiedzialne za ochronę CRP,
- punktów i sposobów zgłaszania oraz reagowania na incydenty bezpieczeństwa poza godzinami pracy,
- metod i miejsca poszukiwania informacji dotyczących bezpieczeństwa teleinformatycznego,
- metod przywracania pracy organizacji do stanu normalnego po wystąpieniu sytuacji kryzysowej[59].

Skuteczne zarządzanie bezpieczeństwem teleinformatycznym wymaga systemu wczesnego ostrzegania, który pozwoli na niedopuszczenie do ataku lub zminimalizowanie jego negatywnych następstw.

[59] Ibidem.

W ramach *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* kontynuowane są inicjatywy realizowane na podstawie wniosków zawartych w Sprawozdaniu z prac Zespołu ds. Krytycznej Infrastruktury Teleinformatycznej, zatwierdzonym w maju 2005 roku przez Kolegium ds. Służb Specjalnych. Departament ABW wraz z zespołem CERT Polska działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK) dokonał wdrożenia systemu wczesnego ostrzegania przed zagrożeniami z sieci Internet – ARAKIS–GOV. Rozbudowa systemu jest realizowana zgodnie z programem szczegółowym. Prace prowadzone są we współpracy zarówno z krajowymi jednostkami naukowo-badawczymi, jak i z uwzględnieniem rozwiązań wewnętrznych Agencji Bezpieczeństwa Wewnętrznego[60].

Przedsięwzięcia realizowane w ramach ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej muszą być traktowane jako proces, a nie jako działanie jednorazowe, okazjonalne, w tym celu przyjęta została zasada skoordynowania *Planów ciągłości działania* z uwzględnieniem wszystkich użytkowników.

Zgodnie z Polską Normą PN-ISO/IEC 17799: 2007 zaleca się wprowadzenie procesu zarządzania ciągłością działania tak, aby zminimalizować wpływ utraty i odtwarzania aktywów informacyjnych na podmiot publiczny (co może wynikać z katastrof naturalnych, wypadków, awarii urządzeń oraz celowego działania) do akceptowalnego poziomu poprzez kombinację zabezpieczeń prewencyjnych i służących do odtwarzania. W związku z tym:

- zaleca się aby proces ten określał krytyczne procesy biznesowe i integrował wymagania bezpieczeństwa informacji odnoszące się do ciągłości działania z wymaganiami ciągłości działania związanymi z takimi aspektami, jak eksploatacja, personel, materiały, transport i urządzenia,
- zaleca się, aby analiza wpływu biznesowego uwzględniała konsekwencje wynikające z katastrof, awarii zabezpieczeń, utraty usług oraz ich dostępności,
- zaleca się opracowanie i wdrożenie planów awaryjnych, aby zapewnić możliwość przywrócenia procesów biznesowych w wymaganym czasie,
- zaleca się, aby bezpieczeństwo informacji było integralną częścią całościowego procesu zapewnienia ciągłości działania oraz wszystkich innych procesów zarządzania w podmiocie publicznym,
- zaleca się, aby zarządzanie ciągłości działania obejmowało: środki umożliwiające identyfikowanie i ograniczanie ryzyk, traktowane jako rozszerzenie ogólnego procesu szacowania ryzyka, ograniczanie skutków niszczących incydentów oraz zapewnienie, że wymagane dla procesów biznesowych informacje będą z łatwością dostępne[61].

Tworzenie planów ciągłości działania będzie opierało się także na normie BS-25999 oraz zaleceniach DRII (Disaster Recovery Institute International).

Wypracowanie i przyjęcie planów ciągłości działania ma na celu: zapoznanie kierownictwa podmiotów publicznych z istotą tego typu planowania, opracowanie wytycznych do planowania ciągłości działania dla typowych klas podmiotów

[60] Ibidem, Załączniki nr 14 i s. 22.

[61] Ibidem, Załącznik nr 17 i s. 23.

publicznych, wprowadzanie planów ciągłości działania w podmiotach publicznych, testy planów ciągłości działania[62].

Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016 jest poddawany ocenie co do jego skuteczności. Jej miarą jest ocena przyjętych regulacji prawnych, ocena działalności instytucji, współpraca w realizacji zadań w sferze ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. W związku z tym w ramach *Programu* zostanie:

- opracowany zestaw wytycznych do pomiaru skuteczności poszczególnych działań organizacyjno-proceduralnych, technicznych i edukacyjnych w zakresie bezpieczeństwa Cyberprzestrzeni RP,
- opracowany przez Międzyresortowy Zespół Koordynujący ds. Ochrony Cyberprzestrzeni RP zestaw formularzy do oceny skuteczności *Programu*, które zostaną przekazane do wszystkich użytkowników w obszarze administracji publicznej oraz innych użytkowników, którzy wyrażą chęć udziału w ocenie jego skuteczności,
- opracowany system przekazywania, analizowania i wyciągania wniosków w zakresie bezpieczeństwa Cyberprzestrzeni RP,
- wskazana jednostka organizacyjna odpowiedzialna za zbieranie, analizowanie i wyciąganie wniosków oraz sporządzanie raportów dla Pełnomocnika ds. ochrony cyberprzestrzeni[63].

Przewiduje się następujące długofalowe efekty skutecznego wdrożenia *Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*:

- wyższy poziom bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa oraz odporności państwa na ataki cybernetyczne,
- spójną dla wszystkich zaangażowanych podmiotów administracji publicznej i innych współstanowiących krytyczną infrastrukturę teleinformatyczną państwa politykę dotyczącą bezpieczeństwa cyberprzestrzeni,
- mniejszą skuteczność ataków cyberterrorystycznych i mniejsze koszty usuwania ich następstw,
- funkcjonujący skuteczny system koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnienie bezpieczeństwa cyberprzestrzeni oraz władającymi zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa,
- większą kompetencję odnośnie bezpieczeństwa cyberprzestrzeni podmiotów zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej państwa,
- większe zaufanie obywateli do właściwego zabezpieczenia usług państwa świadczonych drogą elektroniczną, upowszechnianie elektronicznej drogi korzystania z tych usług,
- większą świadomość obywateli na temat metod bezpiecznego użytkowania systemów dostępności elektronicznej i sieci teleinformatycznych[64].

[62] Ibidem, Załącznik nr 17.

[63] Ibidem, Załącznik nr 26.

[64] Ibidem, s. 31 i 32.

Zakończenie

Dynamika i skala zmian w środowisku międzynarodowym ma istotny wpływ na poziom bezpieczeństwa wewnętrznego i zewnętrznego poszczególnych państw. Współczesne uwarunkowania polityczno-wojskowe i społeczno-gospodarcze przy całej złożoności stanowią nie tylko szanse, ale i zagrożenia dla bezpieczeństwa państwa. Zagrożenia mogą powstać na tle uwarunkowań wewnętrznych i/lub zewnętrznych, a także militarnych i/lub pozamilitarnych. Każde z nich może wystąpić w dowolnej konfiguracji, a ich źródeł należy upatrywać zarówno w otoczeniu zewnętrznym państwa (bliższym i/lub dalszym), jak i wewnętrznym. Przy całej złożoności i turbulencji zjawisk występujących w środowisku międzynarodowym ma miejsce wzajemne przenikanie się przyczyn i uwarunkowań zagrożeń dla bezpieczeństwa państwa.

Asymetryczne środowisko międzynarodowe i narodowe generuje całe spektrum zagrożeń, które wzajemnie się przenikają i utrudniają podejmowanie działań mających na celu niedopuszczenie do ich powstania lub też zminimalizowania ich negatywnych skutków. Poszkodowana najczęściej jest ludność cywilna, która w obliczu zagrożeń pozostaje bezradna. Takim przykładem są współczesne konflikty zbrojne o zróżnicowanym podłożu, którym obok zniszczeń towarzyszą prześladowania, cierpienie, głód i masowe migracje.

Zagrożenia przełomu wieków spowodowane są m.in. skalą i dynamiką zmian cywilizacyjnych oraz globalizacją wraz z jej następstwami. Istniejące zróżnicowanie co do rozwoju poszczególnych państw (regionów), gdzie widoczny jest pogłębiający się dystans między Bogatą Północą i Biednym Południem, jest źródłem postępującej pauperyzacji społeczeństwa, które w poszukiwaniu lepszych warunków do życia masowo przemieszcza się. Procesom tym towarzyszy wspomniany głód i bieda, a także baza werbunkowa dla grup przestępczych, w tym o charakterze międzynarodowym. Narkomania, prostytucja, handel żywym towarem (dziećmi i kobietami), handel organami i tkankami ludzkimi, alkoholizm, choroby (np. HIV, AIDS), to przykłady współczesnych środowisk ludzi dotkniętych m.in. przemianami cywilizacyjnym. Kolejna kwestia to mniejszości narodowe, problem, z którym praktycznie boryka się większość państw. Na problemy grup etnicznych i narodowościowych, różniących się religią, kulturą, językiem i stanem posiadania, nakładają się kwestie masowych migracji z powodów wojen domowych, suszy, głodu i innych kataklizmów. W określonych warunkach

mniejszości narodowe lub etniczne mogą stanowić kartę przetargową w rozmowach między państwami, gdzie ma miejsce ekspansja gospodarcza, kulturowa i polityczna. Ponadto mogą stanowić zagrożenie spowodowane rozruchami na tle niezadowolenia z prowadzonej polityki przez państwo pobytu.

Do innych zjawisk mogących destabilizować sytuację wewnętrzną państwa należy zaliczyć poczucie ze strony społeczeństwa (grup zawodowych czy środowiskowych) zagrożenia związanego z obawą niemożliwości zaspokojenia potrzeb egzystencjalnych. Sprzyjają temu trwające przemiany systemowe, gdzie często słyszy się o państwie prawa czy demokracji.

> Przy czym ci przywódcy, którzy o tym najczęściej mówią, zazwyczaj najmniej tego pragną. Nie wiadomo, czy chcą ustanowić pewien rodzaj despotyzmu, czy dążą do tego, by ktoś zrobił za nich to, co sami zrobić powinni. Może to prowadzić do destabilizacji sytuacji wewnętrznej (i zewnętrznej)[1].

Ponadto wykorzystywanie niezadowolenia społeczeństwa może doprowadzić do konfliktu nie tylko wewnętrznego, ale i zewnętrznego z innymi państwami.

> Zjawiska destrukcyjne i ich objawy występują z różnym nasileniem, są bowiem funkcją impulsów sprawczych, najczęściej wywoływanych niepopularnymi decyzjami władzy lub brakiem skutecznych decyzji. W pierwszym przypadku społeczeństwo odnosi wrażenie, iż jest traktowane instrumentalnie, w drugim irytują je przejawy niemocy i postępującego bezprawia (anarchizacji)[2].

Przyjmuje się, że groźba konfliktu zbrojnego w skali globalnej nie grozi ludzkości, jednak wydarzenia na arenie międzynarodowej zaprzeczają takim tezom. Postępujący wyścig zbrojeń, w tym dostępu do broni masowego rażenia przez podmioty państwowe, jak i pozapaństwowe, któremu towarzyszy niekiedy agresywna polityka zagraniczna, stanowi groźbę wybuchu konfliktu zbrojnego z użyciem broni masowej zagłady. To wynik m.in. erozji systemu międzynarodowej kontroli proliferacji tego rodzaju broni, który przyczynia się do militaryzacji niektórych państw.

Należy również mieć na uwadze zagrożenia związane z rozwojem nacjonalizmu, szowinizmu i fundamentalizmu religijnego, a także terroryzmu międzynarodowego. Społeczność międzynarodowa żyje w permanentnym zagrożeniu ze strony wspomnianego terroryzmu, który jest nieprzewidywalny co do czasu i miejsca ataku, form, metod i środków. Rozwój techniki teleinformatycznej i Internetu stworzył dla gryp terrorystycznych i przestępczych, a także państw nowe środowisko walki, jakim jest tzw. cyberprzestrzeń, wrażliwa zarówno na ataki wewnętrzne, jak i zewnętrzne, gdzie atakujący najczęściej jest nieznany. Do innych zagrożeń mających destrukcyjny wpływ na bezpieczeństwo państwa należy zaliczyć zagrożenia naturalne (powodzie, silne wiatry, susze, anomalie pogodowe, trzęsienia ziemi, epidemie, plagi zwierzęce), techniczne (pożary, awarie

[1] S. Dworecki, *Od konfliktu do wojny*, Warszawa 1996, op. cit., s. 31.

[2] Ibidem, s. 33.

chemiczne i radiacyjne, katastrofy komunikacyjne, górnicze i budowlane, awarie urządzeń technicznych), zbiorowe akty zakłócania porządku publicznego, kosmiczne, konflikty zbrojne w państwach ościennych i inne. Wymienione zjawiska w określonych warunkach mogą przyczynić się do powstania stanu miedzy pokojem i wojną, który w literaturze nazywany jest kryzysem. Oznacza to sytuację powstałą w wyniku załamania się stabilnego dotąd procesu rozwoju, grążącą utratą inicjatywy i koniecznością godzenia się na przyjmowanie niekorzystnych warunków wymagających podjęcia zdecydowanych i wszechstronnych kroków zaradczych[3].

Państwo w celu niedopuszczenia do powstania kryzysu lub zminimalizowania jego negatywnych następstw wprowadza rozwiązania systemowe przy uwzględnieniu elementów organizacyjnych i prawnych. Należy do nich system zarządzania kryzysowego, który stanowi element systemu bezpieczeństwa państwa. W Polsce problematyka ta jest uregulowana ustawą z dnia 26 kwietnia 2007 roku *o zarządzaniu kryzysowym* wraz z aktami wykonawczymi.

Mówiąc o zarządzaniu kryzysowym w Polsce, należy mieć na uwadze istniejący dualizm władzy wykonawczej z Prezydentem Rzeczypospolitej Polskiej i Radą Ministrów. Ustawodawca wspomnianą ustawą *o zarządzaniu kryzysowym* kierowanie w tej sferze powierzył Radzie Ministrów. Natomiast Prezydent RP może delegować swojego przedstawiciela do pracy Rządowego Zespołu Zarządzania Kryzysowego. Udział prezydenta jest również widoczny w czasie wprowadzania i znoszenia stanów nadzwyczajnych. W Polsce brak jest na poziomie państwa podmiotu zajmującego się kierowaniem bezpieczeństwem państwa w sytuacji zagrożenia jego bezpieczeństwa wewnętrznego i zewnętrznego (w tym i zarządzania kryzysowego), w którego skład wchodziłby zarówno Prezydent RP jak i Rada Ministrów z wyraźnie określonymi zadaniami, kompetencjami i zasadami współpracy w drodze ustawy. Pamiętać przy tym należy, że struktury organizacyjne tego podmiotu nie powinny odbiegać od struktur czasu pokoju (z niezbędnymi korektami), dotyczy to również dowodzenia siłami zbrojnymi. Przyjęcie takiego rozwiązania pozwoliłoby na usprawnienie procesu informacyjnego, decyzyjnego, a także sprawne kierowanie. Kolejna kwestia to konieczność uproszczenia dowodzenia siłami zbrojnymi bez konieczności rozbudowy organów dowodzenia, co również ma wpływ na skuteczne zarządzanie kryzysowe z wykorzystaniem specjalistycznych oddziałów i pododdziałów sił zbrojnych.

Zarządzanie kryzysowe na poziomach krajowym, wojewódzkim, powiatowym i gminnym wymaga dla swojej skuteczności właściwego finansowania z budżetu państwa, a także wsparcia finansowego w sytuacjach nagłych. System zarządzania kryzysowego jest dynamiczny i zależny od sytuacji, w której funkcjonuje. Bazuje on na doświadczeniach, ma ścisły związek z teraźniejszością i powinien zabezpieczać przyszłość. Jego poszczególne elementy (podsystemy) są budowane na podstawie przewidywań, hipotez przebiegu określonych zjawisk i wydarzeń. W związku z tym istotne jest monitorowanie zarówno otocze-

[3] *Słownik z zakresu terminów bezpieczeństwa narodowego*, Warszawa 2009, s. 61.

nia wewnętrznego, jak i zewnętrznego państwa, ze szczególnym wskazaniem na miejsca o podwyższonym ryzyku. Skuteczne zarządzanie kryzysowe to również konieczność podnoszenie świadomości społeczeństwa o konieczności przygotowania sprawnego systemu ochrony ludności. Zarządzanie kryzysowe powinno być gwarantem zachowania standardów życia społeczeństwa w obliczu różnych zagrożeń.

Bibliografia

I. Akty prawne

Wykaz podstaw prawnych zarządzania kryzysowego w Rzeczypospolitej Polskiej – zob. rozdział IV s. 93, s. 95–98

II. Literatura zwarta

Amstrong M., *Jak być dobrym menadżerem*, Warszawa 1997

Arafat J., *Przemówienie na forum Zgromadzenia Ogólnego ONZ 13 listopada 1974 roku* [za:] Hoffman B., *Oblicza terroryzmu*, Warszawa 1999

Balcerowicz B., *Pokój i nie-pokój na progu XXI wieku*, Warszawa 2002

Balcerowicz B., *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010

Balcerowicz B., *Sojusz a obrona narodowa*, Warszawa 1999

Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych*, Siedlce 2002

Bauman Z., *Globalizacja*, Warszawa 2000

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa Polskiego*, Toruń 2006

Berliński T., *Różnorodność postrzegania zagrożeń*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Kraków 2000

Białoskórski R., *Wyzwania i zagrożenia bezpieczeństwa XXI wieku*, Warszawa 2010

Bolechów B., *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Toruń 2003

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003

Brydak L.B., *Grypa, pandemia grypy – mit czy realne zagrożenie*?, Warszawa 2008

Buchan G., *Information Warfare and the Air Force: Wave of Future? Current Fad*?, Washington 1996

Budyn K., *Funkcjonowanie systemu wykrywania skażeń w Siłach Zbrojnych RP. Systemy wykrywania skażeń w wybranych państwach Sojuszu Północnoatlantyckiego oraz w państwach sąsiadujących z Polską*, [w:] *Kurs podstawowy dla specjalistów Krajowego Systemu Wykrywania Skażeń*, praca zbiorowa, Warszawa 2005

Chinalski R., *Międzynarodowe instrumenty wspierające zwalczanie cyberprzestępczości. Organizacja zwalczania cyberprzestępczości w polskiej Policji,* [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009

Ciesielski M., Szudrowicz A., *Ekonomia transportu*, Poznań 2000

Cieślarczyk M., Kuriata R., *Kryzysy i sposoby radzenia sobie z nimi*, Łódź 2005

Clarke M., *Charakterystyka zachowania się w kryzysie*, Bruksela 1995 (maszynopis)

Dąbrowski M., *Działania Policji podczas niebezpiecznego zbiorowego naruszenia porządku publicznego*, Szczytno 2004

Dąbrowski M., Gampf J., *Wybrane zagadnienia pracy sztabowej w Policji*, Szczytno 2004

Denczew S., *Podstawy gospodarki komunalnej. Współczesne zagadnienia sektorów inżynieryjnych*, Białystok 2004

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002

Dictionary of Military and Associated Terms, Department of Defense, US Government Printing Office, Washington 1989

Dworecki S., *Od konfliktu do wojny*, Warszawa 1996

Dworecki S., *Zagrożenia bezpieczeństwa państwa*, Warszawa 1994

Elementarne pojęcia pedagogiki społecznej i pracy socjalnej, red. D. Ladek, T. Pilch, Warszawa 1999

Encyklopedia biznesu, red. W. Pomykało, t. II, Warszawa 1995

Encyklopedia organizacji i zarządzania, red. L. Pasieczny, Warszawa 1981

Ficoń K., *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007

Flakiewicz W., *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje*, Warszawa 2002

Gąsiorek K., Kitler W., *Wojskowe wsparcie władz cywilnych i społeczeństwa*, Warszawa 2005

Gibson W., *Neuromancer*, Warszawa 2009

Gołębiewski J., *Zarządzanie kryzysowe metodą rozwiązywania problemów bezpieczeństwa*, [w:] *Zarządzanie kryzysowe w transporcie lądowym na Pomorzu. Materiały konferencyjne*, Szczecin 2003

Gould J.W., Kolb W.L., *A dictionary of the Social Science*, London 1964

Grewlich K.W., *Conflict and Good Governance in Cyberspace*, [w:] *Global Networks and Local Value. A Comparative Look at German and the United States,* New York 2002

Griffin R.W., *Podstawy zarządzania organizacjami*, Warszawa 1996

Gryz J., Kitler W., *System reagowania kryzysowego*, Toruń 2007

Gryz J., *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, Toruń 2009

Grzywacz W., *Infrastruktura transportu*, Warszawa 1982

Haber L.H., *Management. Zarys zarządzania małą firmą,* Kraków 1998

Handbuch zur Ökonomie der Verteidigungspolitik, Regensburg 1986

Ingalls J., *Human Energy*, Menlo Park 1976

Iwanek T., *Kryzys i jego odmiany*, Wrocław 2004

Jakubczak R., *Obrona narodowa w tworzeniu bezpieczeństwa III RP*, Warszawa 2004

Jemioło T., Dawidczyk A., *Wprowadzenie do metodologii badań bezpieczeństwa*, Warszawa 2007

Jendraszczak E., Kozłowski W., *Zarządzanie w sytuacjach kryzysowych* – opracowanie na podstawie podręcznika *Generic Crisis Management Handbook (GCMH)* wydanego przy Radzie ds. Operacji i Komitecie ds. ćwiczeń NATO (17.05.1997 r.), MON – DSO, Warszawa 1997

Kaliński M., *Miejsce gotowości cywilnej i zarządzania kryzysowego we współpracy cywilno-wojskowej*, Warszawa 1999

Karleszko S., *Zarządzanie kryzysowe i logistyka humanitarna jako rola i zadania rządowe i samorządu terytorialnego – wybrane zagadnienia,* [w:] *Logistyka humanitarna i zarządzanie kryzysowe – wybrane problemy*, red. T. Pokusa, M. Dumezal, Opole 2009

Karpiniuk M., *Bezpieczeństwo narodowe a bezpieczeństwo międzynarodowe,* [w:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej w świetle prawa wewnętrznego i międzynarodowego,* red. R. Szynowski, M. Karpiuk, Warszawa 2011

Kast F.E., Rosenzweig J.E., *Organization and Management*, New York 1979

Kieżun W., *Sprawne zarządzanie organizacją*, Warszawa 1997

Kisielnicki J., *Informatyczna infrastruktura zarządzania*, Warszawa 1992

Kisielnicki J., *Systemy informatyczne zarządzania*, Warszawa 2008

Kocik J., *Kryteria idealnego środka broni biologicznej*, [w:] *Bioterroryzm. Zasady postępowania lekarskiego*, red. K. Chomiczewski, J. Kocik, M.T. Szkoda, Warszawa 2002

Kolińska M., *Prawnoorganizacyjne uwarunkowania funkcjonowania Rządowego Centrum Bezpieczeństwa*, Warszawa 2010

Koncepcja Strategii Sojuszu Północnoatlantyckiego z 23–24 kwietnia 1999 roku

Konieczny J., *Zarządzanie w sytuacjach kryzysowych. Rola i zadania administracji publicznej*, Inowrocław 2000

Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Warszawa 2000

Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1988

Korycki S., *System bezpieczeństwa Polski*, Warszawa 1994

Korzecki K., *Typologia zagrożeń kryzysowych*, Warszawa 1998

Kosowski B., *Sprawne i elastyczne zarządzanie w kryzysie*, Warszawa 2008

Kostera M., *Współczesne koncepcje zarządzania*, Warszawa 2008

Kotarbiński T., *Traktat o dobrej robocie*, Wrocław 1969

Koźmiński A.K., *Zarządzanie tu i teraz*, Warszawa 1996

Kroenke D., *Management Information Systems*, New York 1989

Krzyżanowski L., *Podstawy nauk o organizacji i zarządzaniu*, Warszawa 1998

Kunikowski J., *Słownik terminów z zakresu wiedzy i edukacji dla bezpieczeństwa*, [w:] *Bezpieczeństwo człowieka i zbiorowości społecznych*, red. W.J. Maliszewski, Bydgoszcz 2005

Kwećka R., *Procesy informacyjne w ramach systemu reagowania kryzysowego Unii Europejskiej*, [w:] *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, red. J. Gryz, Toruń 2009

Kwiatkowski S., *Zarządzanie bezpieczeństwem w sytuacjach kryzysowych*, Pułtusk 2011

Lach Z., Łaszczuk S.A., *Geografia bezpieczeństwa*, Warszawa 2004

Leksykon wiedzy wojskowej, red. S. Torecki i in., Warszawa 1979

Leksykon zarządzania, red. M. Romanowska, Warszawa 2004

Lidawa W., Krzeszowski W., Więcek W., *Zarządzanie w sytuacjach kryzysowych*, Warszawa 2010

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008

Lipski S., *Zarządzanie bezpieczeństwem – wybrane kwestie terminologiczne*, [w:] *Próba identyfikacji współczesnych zagrożeń dal bezpieczeństwa i porządku publicznego w Polsce*, red. K. Rajchel, Warszawa 2006

Lisiecki M., *Zarządzanie bezpieczeństwem publicznym*, Warszawa 2011

Marczak J., Pawłowski J., *O obronie militarnej Polski przełomu XX–XXI wieku*, Warszawa 1995

Mądrzejewski W., *Przestępczość zorganizowana. System zwalczania,* Warszawa 2008

Mierzejewski D.J., *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*, Toruń 2011

Mikuła B., *Organizacje oparte na wiedzy*, Kraków 2006

Moore P., *Tajemnicze choroby współczesnego świata. Nowe zagrożenia – wirusy, bakterie, zarazki*, Warszawa 2009

Narski Z., *O dyktaturze kapitału globalnego*, Toruń 2004

Naumann K., *Die Bundeswehr in einer Welt im Umbruch*, Berlin 1994

Nowacki G., *Rozpoznanie satelitarne USA i Federacji Rosyjskiej*, Warszawa 2002

Nowak E., *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, Warszawa 2007

Nowak E., *Zarządzanie logistyczne w sytuacjach kryzysowych*, Warszawa 2008

Nowakowski Z., Ciepielewski S., *Wymiar społeczny bezpieczeństwa państwa*, [w:] *Bezpieczeństwo osobiste obywatela w RP*, red. K. Rajchel, Warszawa 2007

Oldcorn R., *Management,* Londyn 1989

Penc J., *Leksykon biznesu*, Warszawa 1997

Penc J., *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Kraków 1998

Poskrobko B., *Zarządzanie środowiskiem*, Warszawa 2007

Program Państwowego Monitoringu Środowiska na lata 2010–2012, Warszawa 2009

Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Wrocław 1978

Ratajczak Z., *Oblicza ludzkiej zaradności*, [w:] *Człowiek w sytuacji zagrożenia. Kryzysy, katastrofy, kataklizmy*, red. K. Popiołek, Poznań 2001

Rattray G.J., *Wojna strategiczna w cyberprzestrzeni*, Warszawa 2004

Rotfeld A.D., *Europejski system bezpieczeństwa in statu nascendi*, Warszawa 1990

Rozwadowska B., *Public relations w sytuacjach kryzysowych*, Wrocław 2002

Rozwój infrastruktury transportu, red. K. Wojewódzka-Król, Gdańsk 1999

Rutkowski C., Kasprzewski A., *Wojskowe aspekty sytuacji kryzysowej. Zadania obronne Polski*, Warszawa 1996

Rydlewski G., *Rządowy system decyzyjny w Polsce,* Warszawa 2002

Shrode W.A., Voich D., *Organization and Management: Basic systems concepts*, Illinois 1974

Sienkiewicz P., Błażejczyk W., Lichocki E., Jóźwiak M., Świeboda H., *Analiza systemowa cyberterroryzmu zagrożenie dla bezpieczeństwa państwa. Analiza systemowa zagrożeń informatycznych w środowisku bezpieczeństwa państwa,* Warszawa 2006

Sienkiewicz P., *Teoria efektywności systemów kierowania*, t. I: *Wstęp do systematologii*, Warszawa 1979

Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni*, [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, red. T. Jemioła, J. Kisielnicki, K. Rajchel, Warszawa 2009

Sienkiewicz-Małyjurek K., Krynojewski F.R., *Zarządzanie kryzysowe w administracji publicznej*, Warszawa 2010

Sjöstrand S.E., *Företagsledning (Zarządzanie),* [in:] B. Czarniawska, *Organisationsteori på svenska (Teoria organizacji po szwedzku),* Malmö 1998

Skomra W., *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wrocław 2010

Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Kraków 2002

Słownik ekonomiczny dla przedsiębiorcy w warunkach rynku, red. Z. Dowgiałło, Szczecin 1994

Słownik języka polskiego PWN, t. VIII, Warszawa 1996

Słownik podstawowych terminów dotyczących bezpieczeństwa, Warszawa 1994

Słownik terminów i definicji NATO, Warszawa 1998

*Słownik terminów z zakresu bezpieczeństwa narodow*ego, Warszawa 2009

Słownik terminów z zakresu dowodzenia i zarządzania, Warszawa 2000

Słownik wyrazów obcych PWN, Warszawa 1980

Šmid W., *Leksykon menedżera*, Kraków 2000

Sobolewski G., *Organizacja i funkcjonowanie centrum zarządzania kryzysowego*, Warszawa 2011

Sobolewski G., *Reagowanie kryzysowe w środowisku miejskim. Aspekt militarny*, Warszawa 2009

Solarz J.K., *Narodowe style zarządzania. Mity czy fakty*, Wrocław 1984

Stankiewicz W.M., *Cyberterroryzm jako zagrożenie asymetryczne współczesnego świata*, [w:] *Zagrożenia asymetryczne współczesnego świata*, red. R. Wojciechowski, R. Fiedler, Poznań 2009

Stanton W.J., Etzel M.J., Walker B.J., *Fundamentals of marketing*, New York 1994

Stefanowicz J., *Bezpieczeństwo współczesnego państwa*, Warszawa 1984

Stoner J.A.F., Freeman R.E., Gilbert D.R., *Kierowanie*, Warszawa 1999

Sułek M., *Potencjał gospodarczo-obronny – pojęcie, pomiar, decyzje*, Warszawa 1993

Sypion N., *Współczesne zagrożenia bezpieczeństwa zbiorowego,* [w:] *Wybrane zagadnienia: propozycje metodyczne*, Toruń 2003

Szlachcic B., *Bezpieczeństwo wewnętrzne państwa. Administracja rządowa i samorządowa w zarządzaniu reagowaniem kryzysowym*, [w:] *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, red. K. Liedel, J. Prońko, B. Wiśniewski, Bielsko-Biała, Warszawa 2007

Szmidka T., *Charakterystyka zagrożeń mogących powodować zaistnienie sytuacji kryzysowych (zagrożenia niemilitarne),* [w:] *Łączność w sytuacjach kryzysowych o charakterze niemilitarnym na obszarze kraju. Materiały z konferencji Zakładu Systemów Łączności i Informatyki AON*, Warszawa 2004

Świniarski J., *Filozofia bezpieczeństwa personalnego i strukturalnego próbą kompleksowego ujęcia wyzwań współczesności*, [w:] *Filozofia bezpieczeństwa personalnego i strukturalnego*, red. R. Rosa, Warszawa 1993

Teoria organizacji i zarządzania, red. J. Kurnal, Warszawa 1979

Twórcy naukowych podstaw organizacji, red. J. Kurnal, Warszawa 1972

Verton D., *Black Ice. Niewidzialna groźba cyberterroryzmu*, Warszawa 2004

Wasilewski G., *Żandarmeria Wojskowa w niemilitarnych sytuacjach kryzysowych*, [w:] *Wojsko w niemilitarnych sytuacjach kryzysowych*, red. W.S. Krzeszowski, Warszawa 2008

Wawrzyniak W., *Odnawianie przedsiębiorstwa. Od kryzysu do sukcesu*, Warszawa 1999

White K.C., *Cyber Terrorism:* Carlisle 1998

Wielka encyklopedia powszechna PWN, t. 5, Warszawa 1965

Wiśniewski B., *Obrona Cywilna w krajowym porządku prawnym. Zbiór dokumentów,* Bielsko-Biała 2008

Wojnarowski J., *System obronności państwa,* Warszawa 2005

Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, Warszawa 2005

Wróblewski R., *Państwo w kryzysie*, Warszawa 2001

Wróblewski R., *Podstawowe pojęcia z dziedziny polityki bezpieczeństwa, strategii i sztuki wojennej,* Warszawa 1993

Wróblewski R., *Wprowadzenie do strategii wojskowej*, Warszawa 1998

Wróblewski R., *Zagrożenia kryzysowe i wojenne Polski w kontekście jej członkostwa w NATO*, Warszawa 1998

Wróblewski R., *Zarys teorii kryzysu. Zagadnienia prewencji i zarządzania kryzysami*, Warszawa 1996

Wrzosek M., *Identyfikacja zagrożeń organizacji zhierarchizowanej*, Warszawa 2010

Współczesny wymiar funkcjonowania Policji, red. B. Wiśniewski, Z. Piątek, Warszawa 2009

Zagrożenia kryzysowe, red. G. Sobolewski, Warszawa 2011

Zając J., *Bezpieczeństwo państwa*, [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009

Zalewski S., *Służby specjalne w państwie demokratycznym,* Warszawa 2005

Zarządzanie kryzysowe a media i granice państw w erze globalizacji, red. M. Koziński, Słupsk 2010

Zawadzki P.W., *Bezpieczeństwo społeczne*, [w:] *Bezpieczeństwo państwa*, red. K.A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa 2009

Zawiślak A., *Pułapy i pułapki zarządzania*, Warszawa 1982

Zbiegień-Maciąg L., Pawnik W., *Zarządzania organizacją. Aspekt socjologiczny*, Kraków 1998

Zeidler K., *Zadania Biura Ochrony Rządu wobec zagrożeń przestępczością zorganizowaną i terroryzmem*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu. Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009

Zelek A., *Zarządzanie kryzysowe w przedsiębiorstwie – perspektywa strategiczna*, Warszawa 2003

Ziarko J., *Orientowanie się i funkcjonowanie jednostki w sytuacji zagrożenia. Aspekty psychologiczno-dydaktyczne,* [w:] *Administracja, zarządzanie i handel zagraniczny w warunkach integracji. Materiały konferencyjne – zarządzanie bezpieczeństwem,* red. K. Budzowski, Kraków 2002

Ziarko J., Walas-Trębacz J., *Podstawy zarządzania kryzysowego*, Kraków 2010

Zieleniewski J., *Organizacja zespołów ludzkich. Wstęp do teorii organizacji i kierowania*, Warszawa 1976

Zieliński K., *Bezpieczeństwo obywateli podczas kryzysów niemilitarnych oraz reagowanie w razie katastrof i klęsk żywiołowych*, Warszawa 2004

Żebrowski A., *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej (Wywiad i kontrwywiad w latach 1989–2003)*, Kraków 2005

III. Artykuły

Czyżak M., *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary Automatyka Kontrola" 2009, nr 7

Ferenc B., *O bezpieczeństwie w Europie*, „Myśl Wojskowa" 1996, nr 2

Gołębiewski J., *Bezpieczeństwo narodowe RP*, „Towarzystwo Wiedzy Obronnej" 1999, nr 1

Gołębiewski J., *Zarządzanie kryzysowe*, „Wiedza Obronna" 2001, nr 1

Jałoszyński K., *O współczesnym terroryzmie i roli państwa w walce z nim,* „Policyjny Biuletyn Szkoleniowy" 1998, nr 1–2

Kamiński S., *Bezpieczeństwo Polski: problemy i wyzwania*, „Biuletyn Towarzystwa Wiedzy Obronnej", [b.r.wyd.]

Kitler W., *Podstawowa terminologia zarządzania kryzysowego,* [w:] *Zarządzanie kryzysowe w sytuacji klęski żywiołowej*, red. E. Nowak, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 2006, nr 1

Kozłowska K., *Etymologia, pojęcia i typologia kryzysów*, „Myśl Wojskowa" 2001, nr 2

Kral Z., Zabłocka-Kluczka A., *Sposób postrzegania kryzysów w polskich przedsiębiorstwach*, „Ekonomika i Organizacja Przedsiębiorstw" 2004, nr 11

Lichocki E., Kasperska K., *Krytyczna infrastruktura teleinformatyczna w Polsce*, „Terroryzm" 2001, nr 1

Marczyński D., *Dokąd zmierza Państwowa Straż Pożarna,* „Przegląd Pożarniczy" 2008, nr 1

Michalski Z.C., *Dostosowanie regulacji prawno-organizacyjnych w ochronie tajemnicy państwowej i wojskowej do standardów NATO*, „Zeszyt Problemowy Towarzystwa Wiedzy Obronnej" 1999, nr 3

Michnowski L., *Sieć informatyczna jako warunek intensywnego rozwoju organizacji gospodarczej*, „Przegląd Organizacji" 1981, nr 9

Sienkiewicz P., Górny P., *Analiza systemowa sytuacji kryzysowej,* „Zeszyty Naukowe AON" 2005, nr 4

Socha Z., *Krajowy system ratowniczo-gaśniczy w przyszłym powszechnym systemie ratowniczym,* „Towarzystwo Wiedzy Obronnej" 1999, nr 1

Stankiewicz W., *Konflikt i bezpieczeństwo – kilka uwag teoretycznych*, „Zeszyty Naukowe AON" 1991, nr 3/4

Wawrzyniak B., *Przedsiębiorczość – klucz do przyszłości*, „Przegląd Organizacji" 1988, nr 7

Wilson L.R., *The New Frontier. Cyberspace and the Telecoms*, „Vital Speech of the Day" LXIV, 1998, nr 6

Wróblewski R., *Wybrane problemy diagnozy bezpieczeństwa narodowego*, „Zeszyty Naukowe AON" 1991, nr 3/4

IV. Inne źródła

Brzozowska K., Łatuszyńska M., *Infrastruktura informacyjna jako element infrastruktury publicznej*, http://mikro.uiv.szczecin.pl/bp/pdf/46/17.pdf [pobrano 9.09.2012]

Collin B. C., *Cyber Terrorism. From Virtual Darkness: New Weapons in a Timeless Battle*, San Luis Obispo 1998, http://www.nici.org.

Cyberprzestrzeń – definicje (http://www.techsty.art.pl/hipertekst/cyberprzestrzen/cybe_696.htm [pobrano 13.09.2011]

Denning D.E., *Cyberterrorism, Global Dialogue*, August 24, 2000 – http://www.cs georgetwon.edu/-denning/infosec/cyberterror-GD.doc [pobrano 14.09.2011]

Dobosz M., *Zarządzanie kryzysowe. Kryzys – Termin*, www.obronacywilna.pl [pobrano 19.04.2012]

Górczyński J., *Procesy informacyjne zarządzania*, http://www.wszimsochaczew.edu.pl/www/download%5CProcesyInformacyjne%5CArchiwum%5CProcesyInformacyjneZjazd_8.pdf [pobrano 3.03.2012]

http://e-prawnik.pl/wiadomosci/informacje/zalozenia-do-rzadowego-programu-ochrony-cyberprzestrzeni-rp-na-lata-2009-2011.html [pobrano 1.02.2012]

http://www.locos.pl/publikacje/6111-rzadowy-program-ochrony-cyberprzestrzeni-rp-na-lata-2011-2016 [pobrano 1.02.2012]

Kosiński J., Kmiotek S., *Międzynarodowa współpraca w zwalczaniu cyberprzestępczości*, http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/Cyberrteroryzm/kosinski_kmiotek.pdf [pobrano 7.01.2012]

Kośla R., *Cyberterroryzm – definicje, zjawiska i zagrożenia dla Polski*, wystąpienie na konferencji w Bemowie 29 listopada 2002 roku, http://www.abw.gov.pl [pobrano 14.09.2011]

Lewis J.A., *Assessing The risk of cyber terrorism, cyber war and other cyber threats*, Center for Strategic and International Stidiies 2002, http://www.csis.org/tech/0211_lewis.pdf [pobrano 12.09.2011]

Pollit M., *Cyberterrorism – Fact or Fancy*? – http:/www.cs.georgetwon.edu/-denning/infosec/pollitt.html [pobrano 12.09.2011]

Stark R., *Cyber Terrorism: Rethinking New Technology* – http://www.infowar.com/MIL_C41/stark/Cyber_Terrorism-Rethinking_New_Technology1.doc.

Strategia Bezpieczeństwa Narodowego RP 2007, http://www.bbn.gov.pl – [pobrano 2.02.2012]

Tokarski H., *Dowodzenie jednostkami Policji w sytuacjach kryzysowych*, http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/BEZPIECZENSTWO/Tokarskic.pdf [pobrano 27.02.2012]

Wiatr K., *Migracje na świecie*, http://www.psz.pl/tekst-27340/migracje-na-świecie [pobrano 27.02.2012]

Zwoliński J., *Koncepcja wykrywania zagrożeń, ostrzegania i alarmowania* – ock.gov.pl [pobrano 10.03.2012]

Skorowidz terminów i instytucji

Spis tabel

Spis treści

Andrzej Żebrowski, prof. nadzw. dr hab. inż. nauk humanistycznych w zakresie nauki o polityce, kierownik Katedry Prawa i Nauki o Administracji Instytutu Politologii Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie, autor licznych publikacji z zakresu bezpieczeństwa państwa, służb specjalnych, walki informacyjnej, zarządzania bezpieczeństwem informacji. Ostatnie publikacje: *Wywiad i kontrwywiad XXI wieku* (Lublin 2010), *Zwalczanie przestępczości zorganizowanej w Unii Europejskiej. Zagadnienia politologiczno-prawne* (Lublin 2011).

Z recenzji

Autor wszechstronnie omówił aktualne problemy związane z bezpieczeństwem państwa, podkreślając wpływ takich zjawisk jak globalizacja i rozwój techniki na występujące zagrożenia i sposoby ich likwidowania. Celnie wypunktował najważniejsze źródła konfliktów i zagrożeń, ponadto słusznie zauważył, że współczesny świat daleki jest od idei wzajemnego zrozumienia i partnerskiej współpracy. Zarządzanie kryzysowe staje się w tym kontekście jednym z podstawowych i najważniejszych sposobów stawiania czoła kryzysom.

Prof. zw. dr hab. Janusz Szreniawski

Autor podjął się opracowania bardzo ważnego, aktualnego i jednocześnie trudnego problemu. Zarządzanie kryzysowe w dobie przeobrażeń cywilizacyjnych, skutkujących między innymi negatywnymi zjawiskami o charakterze militarnym i pozamilitarnym, jest konieczne dla zapewnienia bezpieczeństwa ludności i państwa.
Monografia stanowi nie tylko kompendium wiedzy niezbędnej dla osób zajmujących się zawodowo tym obszarem działania państwa, ale również zainteresuje szerokie grono czytelników.

Prof. zw. dr hab. Eugeniusz Zieliński

Uniwersytet Pedagogiczny
im. Komisji Edukacji Narodowej
w Krakowie
Prace Monograficzne nr 627

ISSN 0239-6025
ISBN 978-83-7271-746-7