

st. sekc. dr inż. Rafał WRÓBEL
Zakład Analiz Bezpieczeństwa Cywilnego
Wydział Inżynierii Bezpieczeństwa Cywilnego
Szkoła Główna Służby Pożarniczej

Koncepcja ochrony infrastruktury krytycznej na lata 2015-2017

The Concept of Critical Infrastructure Protection for the Years 2015-2017

Streszczenie

W artykule zaprezentowano koncepcję ochrony infrastruktury krytycznej na lata 2015-2017 wynikającą z aktualizacji Narodowego Programu Ochrony Infrastruktury Krytycznej, jak również zakres zmian prawnych mających bezpośredni wpływ na problematykę infrastruktury krytycznej. Prezentowana dyskusja stanowi pokłosie zmian w zakresie kierowania działami administracji rządowej mających kluczowe znaczenie z perspektywy zapewnienia bezpieczeństwa funkcjonowania infrastruktury krytycznej.

Słowa kluczowe: Narodowy Program Ochrony Infrastruktury Krytycznej, infrastruktura krytyczna koncepcja ochrony, aktualizacja, działy administracji rządowej, wizja Rady Ministrów

Summary

The article presents the concept of critical infrastructure protection for the years 2015-2017 resulting from the updating of the National Program for Critical Infrastructure Protection, as well as a range of legal solutions that have a direct impact on critical infrastructure. Discussed solutions are the aftermath of changes in the management of government administration of key importance from the perspective of ensuring the protection of the critical infrastructure.

Keywords: National Program for Critical Infrastructure Protection, critical infrastructure, concept of protection, update, departments of government, the vision of Council of Ministers

Wprowadzenie

Współczesna koncepcja ochrony infrastruktury krytycznej opiera się na założeniu, iż ta jest realizowana w ramach systemu zarządzania kryzysowego. Szczegółowe zadania z zakresu ochrony infrastruktury krytycznej określa ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym¹. Nadmieniony akt prawny, nazywany ustawą-matką w obszarze zarządzania kryzysowego, konstatuje, iż wizję Rady Ministrów w zakresie ochrony infrastruktury krytycznej (OIK) w Polsce określa Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK). Program ten przygotowuje Dyrektor Rządowego Centrum Bezpieczeństwa (Dyrektor RCB) we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy infrastruktury krytycznej (systemy IK) oraz z ministrami właściwymi w sprawach bezpieczeństwa narodowego. Wersja programu, przygotowana w 2011 roku, opatrzona została w całości klauzulą zastrzeżoną, toteż pierwsza powszechnie dostępna wersja ujrzała światło dzienne w 2013 roku. Narodowy Program Ochrony Infrastruktury Krytycznej na lata 2013-2015, w listopadzie 2015 r., zgodnie z dwuletnim czasem planowania, został zaktualizowany, Jego bieżąca wersja dotyczy prezentacji priorytetów, celów, wymagań i standardów na lata 2015-2017. Równocześnie listopad 2015 r. wydaje się być przełomowy dla koncepcji ochrony infrastruktury krytycznej z innych powodów. Zaprzysiężenie nowoutworzonego rządu oraz implementacja ustawy z 17 listopada 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw² wprowadza zmiany w zakresie odpowiedzialności wybranych ministrów odpowiedzialnych za systemy infrastruktury krytycznej. Prezentacja zmian zawartych w Narodowym Programie Ochrony Infrastruktury Krytycznej, jak również wskazanie kluczowych zmian wynikających ze zmianie ustawy o działach administracji rządowej, stanowią przedmiot zainteresowań poszczególnych części rozważań.

1. Podstawy prawne w zakresie ochrony infrastruktury krytycznej

Problematyka infrastruktury krytycznej i jej ochrony znalazła swoje odzwierciedlenie w zapisach ustawy z 26 kwietnia 2007 r.³ Precyzuje ona podstawowe definicje w zakresie ochrony infrastruktury krytycznej, cel tworzenia Narodowego Programu Ochrony Infrastruktury Krytycznej, zasady wyznaczania krajowej i europejskiej infrastruktury krytycznej, jak również zadania w zakresie ochrony infrastruktury krytycznej. Zadania te, obejmują:

¹ Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU z 2007 r., nr 89, poz. 590; z 2013 r. poz. 1166; z 2015 r. poz. 1485).

² Ustawa z 19 listopada 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (DzU z 2015 r., poz. 1960).

³ Ustawa z 26 kwietnia 2007 r. o zarządzaniu..., op. cit.

- gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej,
- opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej,
- odtwarzanie infrastruktury krytycznej,
- współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony⁴.

Poza wymienionymi elementami, ustawa sprecyzowała również obowiązki operatorów infrastruktury krytycznej polegające na ochronie infrastruktury poprzez przygotowanie i wdrożenie planów ochrony infrastruktury krytycznej, a także utrzymanie własnych systemów rezerwowych, które zapewniają bezpieczeństwo i podtrzymanie funkcjonowania infrastruktury do czasu jej pełnego odtworzenia. Równocześnie w ramach implementacji wymagań dyrektywy Rady Europy⁵, ustawa zobowiązała tychże operatorów infrastruktury krytycznej do wyznaczenia osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej.

Obowiązki w zakresie działań na rzecz infrastruktury krytycznej zdefiniowano również w odniesieniu do Dyrektora RCB oraz ministrów odpowiedzialnych za systemy infrastruktury krytycznej oraz właściwych w sprawach bezpieczeństwa narodowego.

Nadmieniona ustawa stwarza delegacje do rozwiązań szczegółowych dotyczących sposobu realizacji obowiązków i współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z operatorami infrastruktury krytycznej⁶, a także sposobu tworzenia, aktualizacji oraz struktury planów ochrony infrastruktury krytycznej opracowywanych przez operatorów tejże, warunków i trybu uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej⁷.

Poza wymienionymi elementami dotyczącymi infrastruktury krytycznej, ustawa o zarządzaniu kryzysowym, definiując strukturę planów zarządzania kryzysowego na poziomie krajowym, wojewódzkim, powiatowym oraz gminnym, wskazuje, iż zawierają one⁸:

⁴ Ibidem, art. 6.

⁵ Dyrektywa Rady Europy 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (DzU UE., L 345, 23/12/2008 P. 0075-0082).

⁶ Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (DzU 2010 nr 83 poz. 541).

⁷ Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (DzU 2010 r. nr 83 poz. 542).

⁸ R. Wróbel, M. Mytkowska, Ochrona infrastruktury krytycznej a obowiązek opracowania planów i programów wynikający z ustawy o zarządzaniu kryzysowym, *Zeszyty doktoranckie AON* 2012, nr 2.

- charakterystykę zagrożeń i ocenę ryzyka ich wystąpienia, w tym tych, które dotyczą infrastruktury krytycznej,
- procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną infrastruktury krytycznej,
- wykaz infrastruktury krytycznej zlokalizowanej na terenie województwa, powiatu, gminy, dla których przygotowywany jest plan zarządzania kryzysowego,
- priorytety w zakresie ochrony, a także odtwarzania infrastruktury krytycznej.

Poza wymienioną ustawą o zarządzaniu kryzysowym i wydanymi na jej podstawie rozporządzeniami z 30 kwietnia 2010 r., do aktów prawnych bezpośrednio traktujących o ochronie infrastruktury krytycznej zaliczyć należy:

- 1) Ustawę z 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw skarbu państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw płynnych⁹,
- 2) Rozporządzenie Prezesa Rady Ministrów z 14 lipca 2010 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej¹⁰,
- 3) Rozporządzenie Rady Ministrów z 3 grudnia 2015 r. w sprawie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej¹¹.

Pierwszy z przywołanych aktów prawnych stanowi prawny typ działań na rzecz zapewnienia bezpieczeństwa w systemie zaopatrzenia w energię, surowce energetyczne i paliwa. Rozporządzenie wykonawcze do diskutowanej ustawy określa szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej. Z kolei rozporządzenie w sprawie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej jest rozwiązaniem nowym, traktującym o wykonywaniu przez pełnomocnika wybranych uprawnień Skarbu Państwa w stosunku do operatora systemu elektroenergetycznego i operatora systemu przesyłowego gazu.

Prezentowane rozwiązania prawne należałoby uzupełnić o akty prawne, w których użyto bezpośredniego odniesienia do infrastruktury krytycznej¹², jak również formalno-prawnych rozwiązań branżowych, które znajdują zastosowanie w odniesieniu do obiektów, urządzeń, instalacji i usług uznanych za infrastrukturę krytyczną. Zakres podejmowanej dyskusji określonej tytułem artykułu

⁹ Ustawa z 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw skarbu państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw płynnych (DzU z 2010 r. nr 65, poz. 404).

¹⁰ Rozporządzenie Prezesa Rady Ministrów z 14 lipca 2010 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej (DzU z 2010 r. nr 135, poz. 906).

¹¹ Rozporządzenie Rady Ministrów z 3 grudnia 2015 r. w sprawie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej (DzU z 2015 r., poz. 2116).

¹² Przykładem może być tu między innymi Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z 28 lipca 2015 r. w sprawie ogłoszenia jednolitego tekstu ustawy o rezerwach strategicznych (DzU z 2015 r., poz. 1229), art. 3, 4, 8 (pkt 9), 18.

pozwała jednak rozważania na temat rozwiązań branżowych w poszczególnych systemach infrastruktury krytycznej pozostawić jako treść odrębnego materiału.

2. Wizja Rady Ministrów w zakresie zapewnienia bezpieczeństwa funkcjonowania infrastruktury krytycznej

Koncepcja Rady Ministrów dotycząca zapewnienia bezpieczeństwa funkcjonowania infrastruktury krytycznej została zaprezentowana w kolejnych wersjach Narodowego Programu Ochrony Infrastruktury Krytycznej¹³. Dyskutowany dokument określa zakres, cele, priorytety, zasady programu, jego adresatów, jak również zasady identyfikacji infrastruktury krytycznej, zakres odpowiedzialności poszczególnych uczestników programu, podejmowane działania na rzecz ochrony infrastruktury krytycznej oraz ponadnarodowy wymiar. Składa się on z kilku części, obejmujących część główną oraz załączniki. Charakterystyki części Narodowego Programu Ochrony Infrastruktury Krytycznej wydanego w 2013 r. oraz jego zaktualizowanej wersji z 2015 r. dokonano w tabeli 1.

Tabela 1. Charakterystyka części Narodowego Programu Ochrony Infrastruktury Krytycznej

Dokument	NPOIK 2013	NPOIK 2015
Dokument główny	Narodowy Program Ochrony Infrastruktury Krytycznej – dokument główny (na lata 2013-2015)	Narodowy Program Ochrony Infrastruktury Krytycznej – dokument główny (na lata 2015-2017)
Załącznik nr 1	Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 1 – Charakterystyka systemów infrastruktury krytycznej	Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 1 – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje
Załącznik nr 2	Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 2 – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje	Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 2 – Kryteria pozwalające wyodrębnić instalacje i usługi wchodzące w skład systemów infrastruktury krytycznej*
Załącznik nr 3	Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 3 – Kryteria pozwalające wyodrębnić instalacje i usługi wchodzące w skład systemów infrastruktury krytycznej**	Nie dotyczy

*Dokument chroniony w oparciu o przepisy ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (DzU z 2010 r. nr 182, poz. 1228).

**Ibidem.

Źródło: opracowanie własne na podstawie [4] oraz [7].

¹³ RCB, *Narodowy Program Ochrony Infrastruktury 2013 oraz Narodowy Program Ochrony Infrastruktury Krytycznej 2015*.

Co do zasady, NPOIK ma stwarzać warunki do poprawy bezpieczeństwa infrastruktury krytycznej w Polsce dotyczące zwłaszcza:

- zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej,
- przygotowania na sytuacje, które mogą niekorzystnie wpłynąć na infrastrukturę krytyczną,
- reagowania w przypadku dysfunkcji funkcjonowania infrastruktury krytycznej (zniszczenia lub zakłócenia),
- odtwarzania infrastruktury krytycznej¹⁴.

Priorytetami programu są działania na rzecz pogłębiania współpracy w relacji publiczno-prywatnej pomiędzy uczestnikami programu¹⁵, identyfikacja zależności, jak również dokonanie oceny ryzyka zakłócenia funkcjonowania systemu przez operatorów infrastruktury krytycznej we współpracy z organami dokonującymi identyfikacji zagrożeń na poszczególnych poziomach administracji publicznej w terenie oraz służbami specjalnymi, w tym przede wszystkim z szefem Agencji Bezpieczeństwa Wewnętrznego.

Wśród wielu zasad programu niezmiennie najważniejsze pozostają trzy, odnoszące się do: współodpowiedzialności¹⁶, współpracy¹⁷ oraz zaufania¹⁸.

Zaktualizowany w 2015 r. NPOIK zawiera listę adresatów programu, którymi w szczególności są administracja rządowa, reprezentowana przez ministrów odpowiedzialnych za systemy infrastruktury krytycznej i wojewodów, a także operatorzy infrastruktury krytycznej. Listę potencjalnie zainteresowanych uczestników programu uzupełniają pozostałe podmioty gospodarcze i organizacje¹⁹, środowisko naukowe i społeczeństwo.

Wykaz obiektów infrastruktury krytycznej w oparciu o przyjęte kryteria systemowe oraz przekrojowe sporządza Dyrektor RCB. Kryteria, o których mowa, także podlegają aktualizacji, co stanowi jeden z powodów zmieniającej się liczby elementów w poszczególnych systemach infrastruktury krytycznej. Liczbę elementów infrastruktury krytycznej²⁰ w latach 2012-2015, z podziałem na systemy, zaprezentowano w tabeli 2.

¹⁴ Por. Ustawa z 26 kwietnia 2007 r. o zarządzaniu..., op. cit., art. 5b.

¹⁵ R. Wróbel, Infrastruktura krytyczna i jej powszechny charakter [w:] Paradygmaty Badań nad bezpieczeństwem. Zarządzanie w sytuacjach kryzysowych w teorii i w praktyce, Wyd. Wyższej Szkoły Bezpieczeństwa, Poznań 2013, s. 686-697.

¹⁶ Podział odpowiedzialności wynikający z funkcji spełnianej przez infrastrukturę krytyczną – z jednej strony służebny charakter administracji, z drugiej zaś działalność komercyjna sektora prywatnego.

¹⁷ Zbieżne, wzajemne, skoordynowane działania na rzecz osiągnięcia określonego celu, pozwalające unikać dublowania działań.

¹⁸ Przekonanie, że powodem podejmowanych działań, jest dążenie do realizacji wspólnie zdefiniowanego przez administrację publiczną i operatorów infrastruktury krytycznej celu polegającego na poprawie bezpieczeństwa infrastruktury krytycznej.

¹⁹ W poprzedniej wersji NPOIK z 2013 r. przedsiębiorcy.

²⁰ Elementy infrastruktury krytycznej w rozumieniu artykułu oznaczają obiekty, urządzenia, instalacje i usługi uznane za infrastrukturę krytyczną w oparciu o przyjęte kryteria identyfikacji IK.

Tabela 2. Liczba elementów infrastruktury krytycznej w latach 2012-2015 z podziałem na systemy

	1*	2	3	4	5	6	7	8	9	10	11	Razem
2012	186	230	60	58	1	5	2	73	20	47	0	682
2013	188	225	56	84	1	69	3	64	20	47	3	760
2014	188	162	54	85	1	67	3	63	20	44	2	689
2015	191	162	53	85	1	67	3	63	20	28	2	675

*gdzie: 1,2, (...) oznacza system, o którym mowa w art. 3, pkt 2 ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Źródło: opracowanie własne na podstawie [3], [14] oraz [15].

Najwięcej obiektów, urządzeń, instalacji i usług zaliczonych w poczet infrastruktur krytycznych na przestrzeni omawianych lat zidentyfikowano w systemie zaopatrzenia w energię, surowce energetyczne i paliwa, zaś najmniej w systemie zaopatrzenia w żywność. Ten ostatni, obok systemu ratowniczego, są systemami, w których na przestrzeni lat 2012-2015 liczba elementów infrastruktury krytycznej nie uległa zmianie.

Poza przypisaniem konkretnej liczby elementów infrastruktury krytycznej do poszczególnych systemów istnieje jeszcze inne kryterium etykietowania IK. Jej lokalizacja determinuje podział elementów infrastruktury krytycznej na województwa. Przykładowy rejestr, w oparciu o nadmienione kryterium, obejmujący lata 2013-2014, zaprezentowano w tabeli 3.

Tabela 3. Liczba elementów infrastruktury krytycznej w latach 2013-2014 z podziałem na województwa

	dolnośląskie	kujawsko-pom.	lubelskie	lubuskie	łódzkie	małopolskie	mazowieckie	opolskie	podkarpackie	podlaskie	pomorskie	śląskie	świętokrzyskie	warm.-maz.	wielkopolskie	zachodniopom.	Razem
2013	50	33	31	12	28	40	242	14	36	18	46	76	17	15	59	40	757*
2014	45	31	28	11	24	38	221	14	34	17	41	68	15	16	47	36	686**

*W zestawieniu nie uwzględniono trzech obiektów zlokalizowanych poza granicami RP.

**Ibidem.

Źródło: opracowanie własne na podstawie [15].

Dyskusja dotycząca infrastruktury krytycznej byłaby niepełna bez informacji, że liczba elementów infrastruktury krytycznej w systemach/województwach może się zmieniać z różnych powodów, wśród których za najważniejsze należy uznać:

- odwoływanie się operatorów IK od decyzji o uznaniu (bądź też nie) administrowanego przez niego elementu za infrastrukturę krytyczną,

- aktualizację kryteriów identyfikacji,
- zmiany prawne (np. związane ze zmianą ministra zarządzającego danym działem administracji rządowej, w ramach którego rozpoznano elementy IK).

Zaprezentowane w tabeli 3 zestawienie wskazuje, iż jedynie w województwie opolskim liczba elementów infrastruktury krytycznej w 2014 r. nie uległa zmianie względem roku poprzedniego.

Narodowy Program Ochrony Infrastruktury Krytycznej definiuje ministrów kierujących działami administracji rządowej odpowiedzialnych za systemy infrastruktury krytycznej. W NPOIK na lata 2013-2015 ministrów tych określono gospodarzami/współgospodarzami systemów infrastruktury krytycznej, niemniej jednak NPOIK na lata 2015-2017 nie używa tego określenia w odniesieniu do nadmienionych podmiotów. Z uwagi na zakres podejmowanych przez nich inicjatyw, zostali oni nazwani koordynatorami/współkoordynatorami systemów IK²¹. Ministrów odpowiedzialnych za systemy infrastruktury krytycznej wraz z liczbą elementów IK w latach 2013-2014 zaprezentowano w tabeli 4.

Tabela 4. Ministrowie odpowiedzialni za systemy infrastruktury krytycznej wraz z liczbą elementów IK w latach 2013-2014

Minister	Minister Gospodarki, Minister Skarbu Państwa	Minister Administracji i Cyfryzacji	Minister Finansów	Minister Rolnictwa i Rozwoju Wsi	Minister Środowiska	Minister Zdrowia	Minister Infrastruktury i Rozwoju	Minister Spraw Wewnętrznych	Razem
2013	188	392	84	1	8	3	64	20	760
2014	188	322	85	1	7	3	63	20	689

Źródło: opracowanie własne na podstawie [15].

Liczbowa klasyfikacja elementów IK nadzorowanych przez ministrów odpowiedzialnych za systemy infrastruktury krytycznej dokonana w tabeli 4, wskazuje, że – poza jednym przypadkiem – liczba elementów IK nadzorowanych przez danego ministra zmienia się. Spadek znacznej liczby elementów IK pozostających w zakresie zainteresowań Ministra Administracji i Cyfryzacji w 2014 r. wiązał się w głównej mierze z aktualizacją kryteriów stosowanych w odniesieniu do systemu łączności oraz spadkiem ogólnej liczby elementów uznanych za IK w ramach tego systemu aż o 63 pozycje.

Operatorami infrastruktury krytycznej są właściciele oraz posiadacze samostni lub zależni obiektów, instalacji, urządzeń i usług infrastruktury krytycznej. Mogą oni zarządzać więcej niż jedną infrastrukturą krytyczną. Dla zobrazowania

²¹ Zobacz NPOIK 2015, s. 6, 17, 19, 20, 21, 26, 37, 42, 43, 46.

zróźnicowania powiazan wlasnosciowych na przykladzie lat 2013-2014, w tabeli 5 przedstawiono liczbe operatorow infrastruktury krytycznej w jej poszczegolnych systemach.

Tabela 5. Liczba operatorow infrastruktury krytycznej w poszczegolnych systemach w latach 2013-2014

	1*	2	3	4	5	6	7	8	9	10	11	Razem
2013	27	31	5	7	1	38	3	9	19	26	3	169
2014	28	27	6	7	1	37	3	8	19	24	2	162

*gdzie: 1,2, (...) oznacza system, o ktorym mowa w art. 3, pkt 2 ustawy z 26 kwietnia 2007 r. o zarzadaniu kryzysowym.

Źrodo: opracowanie wlasne na podstawie [15].

Dokonane w tabelach 2 i 5 zestawienia wskazuja, i w systemach zawierajacych dua liczbe IK, najwiksze zróźnicowanie wlasnosciowe wystepuje w systemie ratowniczym (20 elementow IK, 19 operatorow IK). Dla porownania w 2014 roku na jednego operatora przypadao rednio:

- w ramach systemu zapewniajacego ciagosc dziaania – 2 (ok. 1,8) elementy IK (44 elementy IK, 24 operatorow IK),
- w ramach systemu zaopatrzenia w wode – 2 (ok. 1,8) elementy IK (67 elementow IK, 37 operatorow IK),
- w ramach systemu acznosci – 6 elementow IK (162 elementy IK, 27 operatorow IK),
- w ramach systemu zaopatrzenia w energe, surowce energetyczne i paliwa – bez maa 7 (ok. 6,7) elementow IK (188 elementow IK, 28 operatorow IK),
- w ramach systemu transportowego – 8 (ok. 7,9) elementow IK (63 elementy IK, 8 operatorow IK),
- w ramach systemu sieci teleinformatycznych – 9 elementow IK (54 elementy IK, 6 operatorow IK),
- w ramach systemu finansowego – 12 (ok. 12,1) elementow IK (85 elementow IK, 7 operatorow IK).

Dziaania ministrow odpowiedzialnych za systemy IK – koordynatorow/wspokoordynatorow systemow IK, podzielone zostay na kilka grup tj. dziaania inicjujace, wykonawcze, wspierajace, konsultacyjne oraz promujace²².

Wród dziaan inicjujacych znajduja sie te, ktore zwiazane sa z:

- inicjowaniem i prowadzeniem procesu legislacyjnego aktow prawnych majacych poprawic funkcjonowanie systemu ochrony IK w zakresie koordynowanego systemu,
- inicjowaniem i utrzymywaniem kontaktow z operatorami IK,
- wdrazaniem nowoczesnych technik ochrony infrastruktury krytycznej,
- pobudzaniem do aktywnosci uczestnikow programu,

²² Por. NPOIK 2015, s. 19-21.

- przygotowaniem strategii zachęcających sektor prywatny do udziału w programie.

Działania wykonawcze sprowadzają się do:

- dokonywania oceny ryzyka zakłócenia funkcjonowania IK w wyniku dysfunkcji,
- dokonywania regularnych analiz i ocen skuteczności ochrony infrastruktury krytycznej w danym systemie IK,
- organizacji i obsługi forum IK na poziomie systemowym,
- uczestnictwa w mechanizmie ochrony IK,
- organizacji w ramach systemu IK szkoleń z zakresu ochrony infrastruktury krytycznej dla samorządów i sektora prywatnego,
- wdrażania systemu zarządzania ciągłością działania,
- zapewniania dbałości o uwzględnienie zadań z zakresu ochrony infrastruktury krytycznej w działalności podległych lub podporządkowanych organów,
- współpracy z innymi koordynatorami w zakresie rozpoznania współzależności pomiędzy systemami IK,
- udzielania pomocy RCB w zakresie identyfikacji IK oraz wdrażaniu i aktualizacji NPOIK,
- współpracy z organami, nadzorującymi element IK, jeśli ten nie znajduje się bezpośrednio we właściwości danego ministra,

Poza działaniami o charakterze pobudzającym oraz stricte wykonawczymi, ministrowie odpowiedzialni za systemy infrastruktury krytycznej służą wsparciem dla innych podmiotów zajmujących się problematyką infrastruktury krytycznej. Przybiera ono postać:

- wspierania RCB w budowie systemu ochrony infrastruktury krytycznej,
- wspierania w organizacji ćwiczeń na poziomie systemu służących ocenie sprawności ochrony IK,
- wspierania działań zmierzających do odtworzenia IK.

Równocześnie koordynatorzy systemów IK uzgadniają plany ochrony infrastruktury krytycznej elementów pozostających w ich właściwości, doradzają i udzielają pomocy merytorycznej i pomocy w zakresie znalezienia ekspertów operatorom IK oraz podejmują działania promujące. Te ostatnie dotyczą promowania na poziomie systemu IK programów edukacyjnych w zakresie ochrony IK oraz działań mających na celu podnosić świadomość w obszarze ochrony IK. Zadania pozostałych uczestników programu zostały zdefiniowane stanowią przedmiot osobnych rozważań.

Dokonane w zaktualizowanej wersji NPOIK 2015 zmiany objęły swoim zakresem również część zatytułowaną ochrona infrastruktury krytycznej. Ochrona tejże niezmiennie jest traktowana w ujęciu procesowym jako działalność realizowana w powtarzanym cyklu Zaplanuj-Wykonaj-Sprawdź-Zastosuj²³, niemniej

²³ Cykl ten znany jest również jako cykl ZWSZ, cykl PDCA (ang. Plan-Do-Check-Act) i jest popularnie znany jako cykl Deminga.

jednak w stosunku do programu z 2013 r., w bieżącej wersji dokumentu zrezygnowano z rekomendacji metody scenariuszowej wykorzystywanej do oceny ryzyka. NPOIK na lata 2015-2017 w tej części programu powtarza jedynie powszechnie znane stwierdzenie, iż ryzyko jest funkcją zagrożenia i podatności, a działania dotyczące wyboru modelu ochrony, rodzajów stosowanej ochrony oraz sił i środków powinny być oparte na zasadzie proporcjonalności – wartości poziomu ryzyka. Ocena ryzyka zakłócenia funkcjonowania infrastruktury krytycznej dokonywana jest każdorazowo w przypadku identyfikacji nowych zagrożeń wpływających lub mogących mieć wpływ na IK, wraz z aktualizacją planu ochrony infrastruktury krytycznej, a także wówczas, gdy niezbędne jest zapewnienie zgodności z dokumentami rządowymi.

Zaktualizowany program zawiera nowe ujęcie w obszarze podejmowanych działań na rzecz ochrony infrastruktury krytycznej. Nie sprowadzają się one, jak to miało miejsce w poprzedniej wersji do przedsięwzięć i procedur ochrony fizycznej, technicznej, osobowej, teleinformatycznej, prawnej, planów odtwarzania, ale do zespołów działań organizacyjnych i technicznych mających na celu zapewnienie bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego elementom infrastruktury krytycznej oraz prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK. Zmianę w podejściu sposobu definiowania działań na rzecz ochrony infrastruktury krytycznej, w oparciu o analizę Narodowego Programu Ochrony Infrastruktury Krytycznej z 2013 i 2015 r., zaprezentowano w tabeli 6.

Tabela 6. Sposób definiowania działań na rzecz ochrony infrastruktury krytycznej

NPOIK 2013	NPOIK 2013
Działania ochronne	Działania na rzecz zapewnienia bezpieczeństwa
Ochrona fizyczna	Zapewnienie bezpieczeństwa fizycznego
Ochrona techniczna	Zapewnienie bezpieczeństwa technicznego
Ochrona osobowa	Zapewnienie bezpieczeństwa osobowego
Ochrona teleinformatyczna	Zapewnienie bezpieczeństwa teleinformatycznego
Ochrona prawna	Zapewnienie bezpieczeństwa prawnego
Plany odtwarzania	Plany ciągłości działania i odtwarzania

Źródło: opracowanie własne.

Jednym z filarów budowanego systemu ochrony infrastruktury krytycznej jest współpraca stron zainteresowanych osiągnięciem wspólnego celu. Jest ona realizowana przez wymianę wszystkich informacji, które mogą oddziaływać na osiągnięcie zamierzonego celu, jak również utrzymanie regularnych kontaktów pomiędzy podmiotami zaangażowanymi w proces ochrony infrastruktury krytycznej. Przyjmuje się, iż model współpracy w ochronie infrastruktury krytycznej współtworzą:

- poziom strategiczny,
- poziom operacyjny,

- poziom zarządczy²⁴.

Skuteczność współpracy determinuje jej występowanie na wszystkich poziomach systemu ochrony infrastruktury krytycznej, toteż wymiana informacji stanowiąca sedno definiowanej współpracy realizowana jest w postaciach:

- forum ochrony infrastruktury krytycznej,
- bieżącej wymiany informacji,
- organizacji szkoleń, konferencji, ćwiczeń oraz udzielania doradztwa²⁵.

Wymiana informacji w ramach forum odbywa się z wykorzystaniem forum krajowego, systemowego oraz regionalnego. To ostatnie ma charakter międzysystemowy i zbiera się przynajmniej trzy razy w roku lub częściej, jeśli wystąpi taka potrzeba²⁶. Prace rozpoczęte w trakcie posiedzenia forum są kontynuowane także po jego zakończeniu.

Bieżąca wymiana informacji odbywa się w ramach mechanizmu ochrony infrastruktury krytycznej, którego funkcjonowanie opiera się na wymianie informacji o zagrożeniach, zwiększonym zapotrzebowaniu na usługi lub produkty oraz w ramach platformy internetowej²⁷.

W wyniku dokonanej aktualizacji programu do procesu wymiany informacji o zagrożeniach włączono RCB jako pierwszy punkt kontaktowy w wymianie informacji pomiędzy operatorami IK, wojewodami, koordynatorami systemów IK oraz innymi podmiotami. Szczególny przypadek stanowi jedynie casus art. 12a ustawy o zarządzaniu kryzysowym, obejmujący wymianę informacji na rzecz przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym.

Zmiany dokonane w zakresie organizacji szkoleń, konferencji, ćwiczeń objęły zniesienie obowiązków organizatora ćwiczeń (przygotowanie planów ćwiczeń i ich uzgadnianie, określenie celu i efektu ćwiczeń, zapewnienie właściwych warunków do realizacji ćwiczeń, przygotowanie dokumentacji ćwiczeń, zapewnienie środków finansowych, przekazanie Dyrektorowi RCB zatwierdzonego sprawozdania z ćwiczeń) oraz założeń określających między innymi cele i efekty, zakres ćwiczeń, formę/rodzaj/zasięg, miejsce przeprowadzenia, harmonogram, termin, zakres dokumentacji²⁸.

²⁴ Poprzednia wersja programu zawierała dwa poziomy: strategiczny oraz operacyjny.

²⁵ Por. R. Wróbel, I. Kulik, Gra decyzyjna w przygotowaniu podmiotów ochrony infrastruktury krytycznej [w:] Piątek Z., Truchan J. (red.), *Technologie w ochronie infrastruktury krytycznej – zewnętrzne państwa Unii Europejskiej*, Wyd. Stowarzyszenia Ruch Wspólnot Obronnych, Szczelno 2013, s. 199-210.

²⁶ Przynajmniej raz w roku forum wojewódzkie musi zebrać się w pełnym składzie – w pozostałych przypadkach spotkania mogą mieć charakter tematyczny lub branżowy.

²⁷ Nadmieniona platforma z jednej strony spełnia funkcję platformy wymiany informacji o zagrożeniach i podatności, z drugiej zaś platformy opracowania wytycznych do strategii i rozwiązań zmniejszających ryzyko zakłócenia funkcjonowania IK.

²⁸ Por. R. Wróbel, *Multimedialny Trening Decyzyjny w kontroli przygotowania podmiotów ochrony infrastruktury krytycznej w Polsce* [w:] J. Stawnicka, M. Woszczyński, M. Walancik (red.), *Współczesne wyzwania dla bezpieczeństwa narodowego*, Wyd. Naukowe Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015.

Zaktualizowany program przedstawia również plan działań na lata 2015-2017 o charakterze organizacyjno-prawnym, technicznym oraz edukacyjnym i szkoleniowym. Plan ten zaprezentowano w tabeli 7.

Tabela 7. Rola wybranych podmiotów w planie działań na lata 2015-2017

Rodzaj działań	Zadanie	Rola podmiotu			
		RCB	Koordynatorzy systemów IK	Operatorzy IK	Wojewoda
Działania organizacyjno-prawne	Opracowanie procedur prowadzenia kontroli i audytów wewnętrznych	Wiodący	Wspierający	Wspierający	Nie dotyczy
	Opracowanie metodyki oceny ryzyka zakłócenia funkcjonowania IK i identyfikacji zależności między systemami IK	Wiodący	Wspierający	Wspierający	Nie dotyczy
	Opracowanie procedury komunikacji w przypadku wystąpienia zagrożeń dla IK	Wiodący	Wspierający	Wspierający	Nie dotyczy
Działania techniczne	Uruchomienie grup roboczych do opracowania minimalnych standardów w zakresie zapewnienia bezpieczeństwa IK	Wiodący	Nie dotyczy	Wspierający	Nie dotyczy
	Weryfikacja skuteczności metodyki identyfikacji obiektów IK	Wiodący	Wspierający	Wspierający	Nie dotyczy
	Uruchomienie bazy danych o incydentach w obiektach IK	Wiodący	Nie dotyczy	Wspierający	Wspierający
	Uruchomienie platformy szkoleniowej dla operatorów IK i administracji publicznej	Wiodący	Nie dotyczy	Nie dotyczy	Nie dotyczy
Działania edukacyjne i szkoleniowe	Opracowanie programu szkolenia podstawowego z zakresu ochrony IK oraz przygotowanie materiałów dydaktycznych do samokształcenia dla operatorów IK i administracji publicznej	Wiodący	Wspierający	Wspierający	Nie dotyczy
	Opracowanie i wydawanie broszur informacyjnych oraz poradników z zakresu ochrony IK dla operatorów IK i administracji publicznej	Wiodący Wspierający Wspierający n/d	Wspierający	Wspierający	Nie dotyczy
	Przeprowadzenie pilotażowych ćwiczeń z zakresu ochrony IK w jednym z obiektów IK	Wiodący	Wspierający	Wspierający	Nie dotyczy

Źródło: opracowanie własne na podstawie [7].

Program dokonuje również niewielkich korekt w zakresie zakresu działań ochronnych infrastruktury krytycznej wykonywanych w ramach Europejskiego Programu Ochrony Infrastruktury Krytycznej. Niezmiennie najważniejszym elementem pozostaje dyrektywa w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, instrumenty finansujące działania z zakresu ochrony infrastruktury krytycz-

nej²⁹ oraz koncepcja współpracy z państwami trzecimi. Zadania w zakresie ochrony IK, zakładające współpracę z innymi krajami i organizacjami międzynarodowymi, posiadają Rządowe Centrum Bezpieczeństwa, Ministerstwo Spraw Zagranicznych, koordynatorzy systemów IK oraz organy administracji lokalnej.

Za koordynację wdrożenia programu odpowiada Dyrektor RCB, który w cyklu corocznym przedstawia Radzie Ministrów ocenę skuteczności programu, uwzględniając przy tym informacje otrzymane od ministrów odpowiedzialnych za systemy IK oraz wojewodów. Nadmieniona ocena skuteczności programu obejmuje takie mierniki, jak:

- 1) zatwierdzone plany ochrony IK,
- 2) audyty stanu ochrony IK,
- 3) zmiany strukturalne i budżetowe,
- 4) ćwiczenia z udziałem służb ratowniczych i ochronnych³⁰.

Dyskusja nad zakresem zmian w Narodowym Programie Ochrony Infrastruktury Krytycznej nie byłaby kompletna bez komentarza dotyczącego załączników do dokumentu głównego. Jak wynika z analizy treści zawartych w tabeli 1, dotychczasowy załącznik nr 1 – Charakterystyka systemów infrastruktury krytycznej został wycofany, a w jego miejsce przesunięto zaktualizowaną wersję dotychczasowego załącznika nr 2 – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje. Zmiany, które wprowadzono, poszerzają znacznie zakres praktyk i rekomendacji o:

- najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa wszystkich typów,
- elementy systemu zarządzania ciągłością działania w części poświęconej planom ciągłości działania i odbudowy,
- szacowanie ryzyka.

Szczególne znaczenie, w aspekcie zapewnienia bezpieczeństwa infrastruktury krytycznej, mają plany ciągłości działania składające się z planów zarządzania kryzysowego, planów/procedur awaryjnych zogniskowanych na przywróceniu/wznowieniu działania procesów i zasobów po wystąpieniu awarii oraz planów/procedur odtworzenia utraconych zasobów. Plan odtwarzania tych ostatnich, mając na uwadze różne przyczyny zniszczenia zasobów, powinien uwzględniać też różne warianty ich obudowy, niezależnie, czy dotyczy to ludzi, lokalizacji, technologii, informacji czy łańcuchach dostaw.

Ocena ryzyka służy określeniu standardów ochrony IK i ustaleniu priorytetów działań dlatego też powinna zostać wykonana w sposób staranny. Podejście procesowe w ochronie infrastruktury krytycznej wymaga w pierwszej kolejności

²⁹ Program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa” – CIPS w latach 2007–2013 oraz instrument „Fundusz Bezpieczeństwa Wewnętrznego” – ISF w latach 2014–2020.

³⁰ NPOIK 2015, s. 47.

przeprowadzenia analizy wpływu zdarzenia na biznes (analiza BIA³¹). Jej przeprowadzenie przyczynia się do szacowania ryzyka w sposób rzetelny, które może obejmować elementy metodyki zaprezentowanej w normie ISO 31000³². Przeprowadzenie analizy BIA oraz szacowania ryzyka należy wykonywać, realizując kolejno takie kroki, jak:

- 1) identyfikacja procesów zachodzących w organizacji,
- 2) identyfikacja procesów krytycznych,
- 3) określenie zasobów,
- 4) identyfikacja zagrożeń oraz podatności,
- 5) analiza ryzyka,
- 6) ewaluacja ryzyka³³.

Zaprezentowane podejście w przygotowywaniu działań sprzyja niezakłóconej realizacji procesów krytycznych organizacji.

3. Zakres zmian w nadzorze wybranych systemów infrastruktury krytycznej

Kluczową rolę w budowie systemu ochrony infrastruktury krytycznej w Polsce odgrywają ministrowie odpowiedzialni za systemy IK. Zakres ich działań w poszczególnych obszarach szczegółowo definiuje NPOIK. Przywołany dokument, zarówno w wersji z 2013, jak i 2015 roku dookreślił z nazwy ministrów koordynatorów/współkoordynatorów systemów IK, niemniej jednak nowe ustalenia w zakresie zarządzania działami administracji rządowej wprowadzają nieco zmian. Ustawa z 17 listopada 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw³⁴ zmienia w kilku przypadkach ministra zarządzającego danym działem administracji rządowej. Mając powyższe na uwadze, dla uporządkowania dyskutowanej kwestii w pierwszej kolejności, w tabeli 8 zaprezentowano ministrów rządu odgrywających kluczową rolę w ochronie elementów infrastruktury krytycznej, zarządzane przez nich działy administracji publicznej oraz prawne podstawy działania.

Analizując zestawienie dokonane w tabeli 8, należy zauważyć, iż w nowoutworzonym rządzie powołano Ministra Gospodarki Morskiej i Żeglugi Śródlądowej, któremu powierzona zarządzanie działami gospodarka morska, rybołówstwo oraz żegluga śródlądowa, a także Ministra Energii. Ten ostatni zarządza działami energii i gospodarki złożami kopalin.

³¹ BIA – ang. Business Impact Analysis.

³² Norma PN-ISO 31000:2012 opracowana przez Komitet Techniczny (KT) nr 6 do spraw Systemów Zarządzania i zatwierdzona przez Prezesa PKN 27 lutego 2012 r. jest dosłownym tłumaczeniem Normy Międzynarodowej 31000:2009. Norma PN-ISO 31000:2012 jest dedykowana organizacjom podejmującym działania wiążące się z ryzykiem, zmuszonym do zarządzania nim.

³³ NPOIK 2015, s. 126.

³⁴ Ustawa z 19 listopada 2015 r. o zmianie ustawy o działach..., op. cit.

Tabela 8. Ministrowie odgrywający kluczową rolę w ochronie elementów infrastruktury krytycznej, zarządzane przez nich działy oraz prawne podstawy działania

Minister	Zarządzany dział	Podstawa prawna
Minister Skarbu Państwa	Skarb Państwa	<ol style="list-style-type: none"> 1) Rozporządzenie RM z 3 listopada 1999 r. w sprawie utworzenia Ministerstwa Skarbu Państwa (DzU z 1999 r., nr 91, poz. 1023). 2) Rozporządzenia Prezesa Rady Ministrów z 17 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Skarbu Państwa (DzU z 2015 r., poz. 1902). 3) Zarządzenie nr 70 Prezesa Rady Ministrów z 20 września 2013 r. w sprawie nadania statutu Ministerstwu Skarbu Państwa (M.P. z 2013 r., poz. 761).
Minister Energii	<ul style="list-style-type: none"> – Energia – Gospodarka złożami kopalnin 	<ol style="list-style-type: none"> 1) Rozporządzenia Rady Ministrów z 7 grudnia 2015 r. w sprawie utworzenia Ministerstwa Energii (DzU z 2015 r., poz. 2075). 2) Rozporządzenie Prezesa Rady Ministrów z 9 grudnia 2015 r. w sprawie szczegółowego zakresu działania Ministra Energii (DzU z 2015 r., poz. 2087).
Minister Cyfryzacji	Informatyzacja ¹⁾	<ol style="list-style-type: none"> 1) Rozporządzenie Prezesa Rady Ministrów z 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (DzU z 2015 r., poz. 1910). 2) Rozporządzenie Prezesa Rady Ministrów z 9 grudnia 2015 r. zmieniające rozporządzenie w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (DzU z 2015 r., poz. 2090). 3) Rozporządzenia Rady Ministrów z 7 grudnia 2015 r. w sprawie utworzenia Ministerstwa Cyfryzacji (DzU z 2015 r., poz. 2077).
Minister Finansów	<ul style="list-style-type: none"> – Budżet – Finanse publiczne – Instytucje finansowe 	<ol style="list-style-type: none"> 1) Rozporządzenia Rady Ministrów z 3 grudnia 2015 r. w sprawie utworzenia Ministerstwa Finansów (DzU z 2015 r., nr 91, poz. 1021).
Minister Rolnictwa i Rozwoju Wsi	<ul style="list-style-type: none"> – Rolnictwo – Rozwój wsi – Rynki rolne 	<ol style="list-style-type: none"> 1) Rozporządzenie Prezesa Rady Ministrów z 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Rolnictwa i Rozwoju Wsi (DzU z 2015 r., poz. 1906). 2) Rozporządzenia Rady Ministrów z 20 listopada 2015 r. w sprawie przekształcenia Minister Rolnictwa i Rozwoju Wsi²⁾ (DzU z 2015 r., poz. 1945).
Minister Środowiska	<ul style="list-style-type: none"> – Gospodarka wodna – Środowisko 	<ol style="list-style-type: none"> 1) Rozporządzenie Prezesa Rady Ministrów z 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Środowiska (DzU z 2015 r., poz. 1904). 2) Rozporządzenie Prezesa Rady Ministrów z 9 grudnia 2015 r. zmieniające rozporządzenie w sprawie szczegółowego zakresu działania Ministra Środowiska (DzU z 2015 r., poz. 2095).
Minister Zdrowia	– Zdrowie	<ol style="list-style-type: none"> 1) Rozporządzenia Rady Ministrów z 26 października 1999 r. w sprawie utworzenia Ministerstwa Zdrowia (Dz. U. z 1999 r., Dz. U. nr 91, poz. 1018). 2) Rozporządzenie Prezesa Rady Ministrów z 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Zdrowia (DzU z 2015 r., poz. 1908).
Minister Infrastruktury i Budownictwa	– Budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo ³⁾	<ol style="list-style-type: none"> 1) Rozporządzenie Prezesa Rady Ministrów z 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Infrastruktury i Budownictwa (Dz. U. 2015, poz. 1907)

Minister	Zarządzany dział	Podstawa prawna
	<ul style="list-style-type: none"> – Łączność⁴⁾ – Transport 	<ul style="list-style-type: none"> 2) Rozporządzenia Rady Ministrów z 7 grudnia 2015 r. w sprawie utworzenia Ministerstwa Infrastruktury i Budownictwa (DzU z 2015 r., poz. 2080). 3) Rozporządzenia Rady Ministrów z 9 grudnia 2015 r. zmieniające rozporządzenie w sprawie utworzenia Ministerstwa Infrastruktury i Budownictwa (DzU z 2015 r., poz. 2094). 4) Zarządzenie nr 151 Prezesa Rady Ministrów z 28 grudnia 2015 r. w sprawie nadania statutu Ministerstwu Infrastruktury i Budownictwa (M.P. poz. 1303).
Minister Spraw Wewnętrznych i Administracji	<ul style="list-style-type: none"> – Administracja publiczna⁵⁾ – Sprawy wewnętrzne – Wyznania religijne oraz mniejszości narodowe i etniczne 	<ul style="list-style-type: none"> 1) Rozporządzenia Rady Ministrów z 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (DzU z 2015 r., poz. 1897). 2) Rozporządzenia Rady Ministrów z 20 listopada 2015 r. w sprawie utworzenia Ministerstwa Spraw Wewnętrznych i Administracji (DzU z 2015 r., poz. 1946). 3) Rozporządzenia Rady Ministrów z 7 grudnia 2015 r. w sprawie przekształcenia Ministerstwa Spraw Wewnętrznych i Administracji (DzU z 2015 r., poz. 2079). 4) Rozporządzenia Rady Ministrów z 9 grudnia 2015 r. zmieniające rozporządzenie w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (DzU z 2015 r., poz. 2088). 5) Zarządzenie nr 152 Prezesa Rady Ministrów z 28 grudnia 2015 r. w sprawie nadania statutu Ministerstwu Spraw Wewnętrznych i Administracji (DzU z 2015 r., poz. 1294). 6) Zarządzenie nr 11 Prezesa Rady Ministrów z 26 stycznia 2016 r. zmieniające zarządzenie w sprawie nadania statutu Ministerstwu Spraw Wewnętrznych i Administracji (DzU z 2016 r., poz. 91).
Minister Gospodarki Morskiej i Żeglugi Śródlądowej	<ul style="list-style-type: none"> – Gospodarka morską⁶⁾ – Rybołówstwo⁷⁾ – Żegluga śródlądowa 	<ul style="list-style-type: none"> 1) Rozporządzenia Rady Ministrów z 7 grudnia 2015 r. w sprawie utworzenia Ministerstwa Minister Gospodarki Morskiej i Żeglugi Śródlądowej (DzU z 2015 r., poz. 2078). 2) Rozporządzenie Prezesa Rady Ministrów z 9 grudnia 2015 r. zmieniające rozporządzenie w sprawie szczegółowego zakresu działania Ministra Gospodarki Morskiej i Żeglugi Śródlądowej (DzU z 2015 r., poz. 2091).

¹⁾ Informatyzacja obejmuje także sprawy komunikacji. Ministerstwo Cyfryzacji będzie zarządzało najważniejszymi rejestrami, za które dotychczas odpowiadało Ministerstwo Administracji i Cyfryzacji.

²⁾ Przekształcenie, o którym mowa w ust. 1, polega na wyłączeniu z Ministerstwa Rolnictwa i Rozwoju Wsi, obsługującego dotychczas sprawy działów rolnictwo, rozwój wsi, rynki rolne i rybołówstwo, komórek organizacyjnych obsługujących sprawy działu rybołówstwo oraz pracowników obsługujących ten dział.

³⁾ Przejęte od dotychczasowego Ministerstwa Infrastruktury i Rozwoju.

⁴⁾ Łączność przeniesiono z doczasowego MAiC. Łączność obejmuje tylko sprawy poczty.

⁵⁾ Poza sprawami działu administracja publiczna w zakresie geodezji i kartografii, które „przekazano” do Ministerstwa Infrastruktury i Budownictwa.

⁶⁾ Gospodarka morską i żegluga śródlądowa przejęte od dotychczasowego Ministerstwa Infrastruktury i Rozwoju.

⁷⁾ Dotychczas w Ministerstwie Rolnictwa i Rozwoju Wsi.

Źródło: opracowanie własne.

Równocześnie istotne zmiany wprowadzono w zakresie działania ministrów: Spraw Wewnętrznych i Administracji, Cyfryzacji, Infrastruktury i Budownictwa. Temu pierwszemu, po czteroletniej przerwie ponownie oddano sprawy administracji publicznej z wyłączeniem spraw geodezji i kartografii, które od

7 grudnia 2015 r. leżą w gestii Ministra Infrastruktury i Budownictwa, a także dział wyznania religijne oraz mniejszości narodowe i etniczne. Minister Cyfryzacji zarządza od 9 grudnia 2015 r. jedynie działem informatyzacja, mimo iż pierwsza wersja rozporządzenia w sprawie szczegółowego zakresu działania Ministra Cyfryzacji z 17 listopada 2015 r. ministrowi temu powierzała także kierowanie działem łączność. Ostatecznie działem tym zarządza Minister Infrastruktury i Budownictwa, przy czym dział łączność obejmuje wyłącznie sprawy poczty (a nie jak do 17 listopada 2015 r. sprawy poczty i telekomunikacji). Uwzględniając klasyfikację odpowiedzialności zdefiniowaną w Narodowym Programie Ochrony Infrastruktury Krytycznej z 2013 i 2015 r., jak również nową koncepcję Rady Ministrów w zakresie odpowiedzialności za poszczególne działy administracji publicznej, w tabeli 9 dokonano zestawienia ministrów odpowiedzialnych za systemy infrastruktury krytycznej wraz z propozycją zmian, które powinny być naturalną konsekwencją przyjęcia ustawy o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw.

Tabela 9. Ministrowie odpowiedzialni za systemy infrastruktury krytycznej w dokumentach i przepisach prawa

Minister odpowiedzialny za system infrastruktury krytycznej			
Minister wg NPOIK 2013	Minister wg NPOIK 2015	Minister w świetle przepisów prawa	Rekomendowana zmiana
– Minister Gospodarki – Minister Skarbu Państwa	– Minister Gospodarki – Minister Skarbu Państwa	– Minister właściwy ds. energii – Minister właściwy ds. skarbu państwa	– Minister Energii – Minister Skarbu Państwa
Minister Administracji i Cyfryzacji	Minister Administracji i Cyfryzacji	Minister właściwy ds. łączności	Minister Infrastruktury i Budownictwa
Minister Administracji i Cyfryzacji	Minister Administracji i Cyfryzacji	Minister właściwy ds. informatyzacji	Minister Cyfryzacji
Minister Finansów	Minister Finansów	Minister właściwy ds. finansów	Minister Finansów
Minister Rolnictwa i Rozwoju Wsi	Minister Rolnictwa i Rozwoju Wsi	Minister właściwy ds. rolnictwa	Minister Rolnictwa i Rozwoju Wsi
– Minister Środowiska – Minister Administracji i Cyfryzacji	– Minister Środowiska – Minister Administracji i Cyfryzacji	– Minister właściwy ds. środowiska – Minister właściwy ds. administracji publicznej	– Minister Środowiska – Minister Spraw Wewnętrznych i Administracji
Minister Zdrowia	Minister Zdrowia	Minister właściwy ds. zdrowia	Minister Zdrowia
Minister Transportu, Budownictwa i Gospodarki Morskiej	Minister Infrastruktury i Rozwoju	– Minister właściwy ds. transportu – Minister właściwy ds. gospodarki morskiej i żeglugi śródlądowej	– Minister Infrastruktury i Budownictwa – Minister Gospodarki Morskiej i Żeglugi Śródlądowej
Minister Spraw Wewnętrznych	Minister Spraw Wewnętrznych	Minister właściwy ds. spraw wewnętrznych	Minister Spraw Wewnętrznych i Administracji

Minister odpowiedzialny za system infrastruktury krytycznej			
Minister wg NPOIK 2013	Minister wg NPOIK 2015	Minister w świetle przepisów prawa	Rekomendowana zmiana
Minister Administracji i Cyfryzacji	Minister Administracji i Cyfryzacji	– Minister właściwy ds. administracji publicznej – Minister właściwy ds. informatyzacji	– Minister Spraw Wewnętrznych i Administracji – Minister Cyfryzacji ¹⁾
Minister Środowiska	Minister Środowiska	Minister właściwy ds. środowiska	Minister Środowiska

¹⁾Wydaje się, że z uwagi na charakter systemu zapewniającego ciągłość działania administracji publicznej ministrem odpowiedzialnym za system powinien być Minister Spraw Wewnętrznych i Administracji. Autor jest jednak zdania, iż należałoby się zastanowić, czy współodpowiedzialnym za system nie należy uczynić Ministra Cyfryzacji – wszak do tego ministra należą sprawy informatyzacji administracji publicznej oraz systemów i sieci teleinformatycznych administracji publicznej.

Źródło: opracowanie własne³⁵.

Wśród rekomendowanych zmian, będących efektem przeprowadzonej analizy, jest:

- zmiana współgospodarza systemu zaopatrzenia w energię, surowce energetyczne i paliwa – z Ministra Gospodarki na Ministra Energii,
- zmiana gospodarza systemu łączności – z Ministra Administracji i Cyfryzacji na Ministra Infrastruktury i Budownictwa,
- zmiana nazwy gospodarza systemu sieci teleinformatycznych – z Ministra Administracji i Cyfryzacji na Ministra Cyfryzacji,
- zmiana współgospodarza systemu zaopatrzenia w wodę – z Ministra Administracji i Cyfryzacji na Ministra Spraw Wewnętrznych i Administracji,
- zmiana nazwy gospodarza systemu transportowego – z Ministra Infrastruktury i Rozwoju na Ministra Infrastruktury i Budownictwa oraz dodanie jako współgospodarza Ministra Gospodarki Morskiej i Żeglugi Śródlądowej,
- zmiana nazwy gospodarza systemu ratowniczego – z Ministra Spraw Wewnętrznych na Ministra Spraw Wewnętrznych i Administracji,
- zmiana nazwy gospodarza systemu zapewniającego ciągłość działania administracji publicznej – z Ministra Administracji i Cyfryzacji na Ministra Spraw Wewnętrznych i Administracji oraz przedyskutowanie kwestii dodania jako współgospodarza Ministra Cyfryzacji.

Poza zakresem prezentowanych zmian w zarządzaniu działami administracji publicznej ustawa o zmianie ustawy o działach administracji publicznej i niektórych innych ustaw, w związku z art. 12a ustawy Prawo energetyczne³⁶, wprowadza jeszcze jeden ważny aspekt służący ochronie elementów infrastruktury krytycznej. Jest nim powołanie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej. Zakres jego uprawnień reguluje rozporządzenie

³⁵ Por. R. Wróbel, I. Kulik, Rola administracji publicznej w ochronie infrastruktury krytycznej państwa [w:] Z. Piątek, S. Olearczyk, Przygotowanie obronne w działach administracji rządowej, Wyd. Stowarzyszenia Ruch Wspólnot Obronnych, Warszawa 2012, s. 164-172.

³⁶ Ustawa z 10 kwietnia 1997 r. Prawo energetyczne (DzU z 2012 r., poz. 392, DzU z 2015 r., poz. 1064).

Rady Ministrów z 3 grudnia 2015 r. w sprawie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej³⁷. Funkcję nadmienionego pełnomocnika pełni sekretarz stanu w Kancelarii Prezesa Rady Ministrów. Wykonuje on między innymi zadania wynikające z praw majątkowych Skarbu Państwa w zakresie praw z akcji i udziałów należących do Skarbu Państwa, łącznie z wynikającymi z nich prawami osobistymi oraz uprawnienia określone w art. 5a i art. 18 ust. 1 ustawy o zasadach wykonywania uprawnień przysługujących Skarbowi Państwa w stosunku do operatora systemu przesyłowego elektroenergetycznego i operatora systemu przesyłowego gazowego³⁸. Równocześnie posiada kompetencję do przedstawiania Radzie Ministrów do rozpatrzenia projektów aktów prawnych i dokumentów wynikających z zakresu jego działania, może powoływać zespoły eksperckie, doradcze oraz zlecać przeprowadzenie badań i ekspertyz w zakresie realizowanych przez niego zadań. Corocznie przedstawia Radzie Ministrów analizy, oceny i wnioski, a także sprawozdania ze swojej działalności.

Podsumowanie

Wizja Rady Ministrów w zakresie ochrony obiektów, urządzeń, instalacji i usług uznanych za infrastrukturę krytyczną prezentowana jest w Narodowym Programie Ochrony Infrastruktury Krytycznej. Jego pierwsza dostępna szerokiemu gronu odbiorców wersja z 2013 r. zakładała, iż osiągnięcie zamierzonego celu programu powinno zostać osiągnięte w perspektywie 6 lat, przy czym dbałość o adaptację rozwiązań zakłada aktualizację nie rzadziej, niż co dwa lata. Aktualizowany dokument powinien uwzględniać zmiany otoczenia a także uwarunkowania ochrony. Aktualizacja NPOIK dokonana w 2015 r. owocująca wersją programu na lata 2015-2017, poszerza zakres realizacji zadań przewidzianych dla ministrów odpowiedzialnych za systemy infrastruktury krytycznej, nazywanych już nie gospodarzami/współgospodarzami a koordynatorami/współkoordynatorami. Równocześnie zmiany dostrzegalne są w dokonywaniu oceny ryzyka, pozostającej w ścisłej korelacji z system ciągłości działania. Obecne dotychczas rodzaje ochrony infrastruktury krytycznej zastąpiono działaniami na rzecz zapewnienia bezpieczeństwa. Model współpracy w ochronie infrastruktury krytycznej przeorganizowano z dwóch na trzy poziomy, wprowadzając dodatkowo schemat komunikacji w ramach mechanizmu ochrony IK i dokonując kosmetycznych korekt w dotychczas zarysowanych schematach. Z programu usunięto obowiązki organizatorów ćwiczeń z zakresu ochrony infrastruktury krytycznej oraz założenia do nich. Zredefiniowano plan działań na dwa po zatwierdzeniu aktualizacji NPOIK przez Radę Ministrów³⁹, zakres elementów działań w ramach Europejskiego Programu Ochrony Infrastruktury Krytycznej

³⁷ Rozporządzenie Rady Ministrów z 3 grudnia 2015 r. w sprawie Pełnomocnika Rządu..., op. cit.

³⁸ Ustawa z 8 sierpnia 1996 r. o zasadach wykonywania uprawnień przysługujących Skarbowi Państwa (DzU z 2015 r. poz. 978, 1223 i 1322).

³⁹ Uchwała Rady Ministrów nr 210/2015, <http://rcb.gov.pl/?p=5744> (dostęp: 01.02.2016 r.).

oraz mierniki skuteczności programu. Za najważniejsze zmiany w dotychczasowych załącznikach do programu należy uznać rezygnację z załącznika poświęconego charakterystyce systemów infrastruktury krytycznej oraz rozbudowę części poświęconej dobrym praktykom i rekomendacjom, zwłaszcza w zakresie działań na rzecz zapewnienia bezpieczeństwa teleinformatycznego, planów ciągłości działania i odbudowy oraz szacowania ryzyka.

Zmiana koncepcji przydziału zarządzania działami administracji rządowej w listopadzie 2015 r. wywołuje bezpośredni wpływ na niektóre systemy infrastruktury krytycznej oraz nadzór nad nimi. Tym samym katalog ministrów odpowiedzialnych z systemu infrastruktury krytycznej przedstawiony w NPOIK w 2015 r. należałoby uaktualnić. Zakres rekomendowanych zmian zaprezentowano w artykule. Wywołująca zmiany przywołana ustawa o zmianie ustawy o działach administracji rządowej i niektórych innych ustaw równocześnie stwarza delegację do powołania Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej. Rozwiązanie to potwierdza priorytet ochrony systemu zaopatrzenia w energię, surowce energetyczne i paliwa⁴⁰.

Literatura

- [1] Dyrektywa Rady Europy 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. U. UE., L 345, 23/12/2008 P. 0075-0082).
- [2] Krajowy Plan Zarządzania Kryzysowego 2013/2015, Rządowe Centrum Bezpieczeństwa, Warszawa 2015.
- [3] Kulik I., Bezpieczeństwo obiektów europejskiej infrastruktury krytycznej na obszarach morskich [w:] Kustra W. (red.), Współpraca Sił Zbrojnych z administracją publiczną na obszarach morskich, Wyd. SRWO, Warszawa 2012.
- [4] Narodowy Program Ochrony Infrastruktury Krytycznej – dokument główny, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.
- [5] Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 1. Charakterystyka systemów infrastruktury krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.
- [6] Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 2. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.
- [7] Narodowy Program Ochrony Infrastruktury Krytycznej – dokument główny, Rządowe Centrum Bezpieczeństwa, Warszawa 2015.
- [8] Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik nr 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, Warszawa 2015.
- [9] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z 28 lipca 2015 r. w sprawie ogłoszenia jednolitego tekstu ustawy o rezerwach strategicznych (DzU z 2015 r., poz. 1229).

⁴⁰ RCB, Krajowy Plan Zarządzania Kryzysowego 2013/2015, Warszawa 2015, s. 620-622.

- [10] Rozporządzenie Prezesa Rady Ministrów z 14 lipca 2010 r. w sprawie pełnomocnika do spraw ochrony infrastruktury krytycznej (DzU z 2010 r. nr 135, poz. 906).
- [11] Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (DzU 2010 nr 83 poz. 541).
- [12] Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (DzU 2010 nr 83 poz. 542).
- [13] Rozporządzenie Rady Ministrów z 3 grudnia 2015 r. w sprawie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej (DzU z 2015 r., poz. 2116).
- [14] Skomra W., Materiały z wystąpienia nt. „Współpraca administracji z sektorem prywatnym w obszarze ciągłości działania”, I Ogólnopolski Kongres Zarządzania Ciągłością Działania, Jachranka (26-27 marca 2015).
- [15] Szewczyk T., Materiały z wystąpienia nt. „Narodowy Program Ochrony Infrastruktury Krytycznej – dotychczasowe doświadczenia”, Konferencja „Zapewnienie ciągłości funkcjonowania organów państwa w obliczu dzisiejszych zagrożeń”, Szczytno (23-24 września 2014).
- [16] Wróbel R., Kulik I., Rola administracji publicznej w ochronie infrastruktury krytycznej państwa [w:] Z. Piątek, S. Olearczyk, Przygotowanie obronne w działach administracji rządowej, Wyd. Stowarzyszenia Ruch Wspólnot Obronnych, Warszawa 2012.
- [17] Wróbel R., Kulik I., Gra decyzyjna w przygotowaniu podmiotów ochrony infrastruktury krytycznej [w:] Piątek Z., Truchan J. (red.), Technologie w ochronie infrastruktury krytycznej – zewnętrznego państwa Unii Europejskiej, Wyd. Stowarzyszenia Ruch Wspólnot Obronnych, Szczytno 2013.
- [18] Wróbel R., Infrastruktura krytyczna i jej powszechny charakter [w:] Paradymaty Badań nad bezpieczeństwem. Zarządzanie w sytuacjach kryzysowych w teorii i w praktyce, Wyd. Wyższej Szkoły Bezpieczeństwa, Poznań 2013.
- [19] Wróbel R., Multimedialny Trening Decyzyjny w kontroli przygotowania podmiotów ochrony infrastruktury krytycznej w Polsce [w:] Stawnicka J., Woszczyński M., Walancik M. (red.), Współczesne wyzwania dla bezpieczeństwa narodowego, Wyd. Naukowe Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015.
- [20] Wróbel R., Mytkowska M., Ochrona infrastruktury krytycznej a obowiązek opracowania planów i programów wynikający z ustawy o zarządzaniu kryzysowym, *Zeszyty doktorskie AON* 2012, nr 2.
- [21] Ustawa z 10 kwietnia 1997 r. Prawo energetyczne (DzU z 2012 r., poz. 392, DzU z 2015 r., poz. 1064).
- [22] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU z 2007 r., Nr 89, poz. 590; z 2013 r. poz. 1166; z 2015 r. poz. 1485).
- [23] Ustawa z 8 sierpnia 1996 r. o zasadach wykonywania uprawnień przysługujących Skarbowi Państwa (DzU z 2015 r. poz. 978, 1223 i 1322).
- [24] Ustawa z 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw skarbu państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw płynnych (DzU z 2010 r. nr 65, poz. 404).
- [25] Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (DzU z 2010 r. nr 182, poz. 1228).
- [26] Ustawa z 19 listopada 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (DzU z 2015 r., poz. 1960).