Stan prawny na dzień 28.06.2022 r.

Zasady ochrony infrastruktury krytycznej

Czym jest infrastruktura krytyczna?

Aby mówić o zasadach ochrony infrastruktury krytycznej (IK), należałoby najpierw określić czym ona dokładniej jest. Głównym aktem prawnym, zajmującym się pojęciem infrastruktury krytycznej jest ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym[1]. Art. 3 pkt. 2 tejże ustawy definiuje powyższe pojęcie jako 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 Polsce, podobnie jak i w innych krajach, działająca sprawnie i w sposób niezakłócony infrastruktura krytyczna ma coraz większy wpływ na obywateli, struktury administracji i gospodarkę. Od dostaw usług dostarczanych przy wykorzystaniu infrastruktury krytycznej uzależniony jest każdy obywatel. Konieczne staje się uznanie ochrony jej systemów, jako procesu ukierunkowanego na ochronę ciągłości świadczenia określonej usługi oraz odtworzenia jej w razie potrzeby.

Ministrowie odpowiedzialni za poszczególne systemy Infrastruktury krytycznej

Ministrowie odpowiedzialni za systemy infrastruktury krytycznej pełnią istotną rolę w systemie ochrony infrastruktury krytycznej. Ich praca jest gwarancją zaangażowania najwyższych władz państwowych w proces budowy bezpieczeństwa państwa. Poniżej zostali wymienieni ministrowie odpowiedzialni za poszczególne systemy infrastruktury krytycznej.

[1] - Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590)

Wykaz tychże ministrów został zawarty w Narodowym Programie Ochrony Infrastruktury Krytycznej z 2020 roku[2] i są nimi:

Systemy infrastruktury krytycznej	Minister odpowiedzialny za system infrastruktury krytycznej
System zaopatrzenia w energię, surowce energetyczne i paliwa	minister właściwy do spraw aktywów państwowych minister właściwy do spraw energii minister właściwy do spraw gospodarki złożami kopalin
System łączności	minister właściwy do spraw informatyzacji minister właściwy do spraw łączności
System sieci teleinformatycznych	minister właściwy do spraw informatyzacji
System finansowy	minister właściwy do spraw budżetu minister właściwy do spraw finansów publicznych minister właściwy do spraw instytucji finansowych
System zaopatrzenia w żywność	minister właściwy do spraw rolnictwa minister właściwy do spraw rynków rolnych
System zaopatrzenia w wodę	minister właściwy do spraw gospodarki wodnej
System ochrony zdrowia	minister właściwy do spraw zdrowia
System transportowy	minister właściwy do spraw transportu minister właściwy do spraw gospodarki morskiej
System ratowniczy	minister właściwy do spraw wewnętrznych
System zapewniający ciągłość działania administracji publicznej	minister właściwy do spraw informatyzacji
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	minister właściwy do spraw klimatu

Tabela 1 – Wykaz ministrów odpowiedzialnych za poszczególne systemy infrastruktury krytycznej

[2] - Uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej.

Ochrona infrastruktury krytycznej

W myśl ustawy o zarządzaniu kryzysowym poprzez ochronę infrastruktury krytycznej należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie[3]. Innymi słowy jest to proces zapewniania jej bezpieczeństwa:

- uwzględniający dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie,
- obejmujący znaczną liczbę obszarów zadaniowych i kompetencji,
- angażujący wiele zainteresowanych stron,
- obejmujący wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej[4].

Kolejnym, z ważniejszych dokumentów, zajmujących się pojęciem ochrony infrastruktury krytycznej jest wspomniany już wyżej Narodowy Program Ochrony Infrastruktury Krytycznej. Powstał w celu stworzenia warunków do poprawy bezpieczeństwa infrastruktury krytycznej, a co za tym idzie podniesienia bezpieczeństwa Polski. Określono w nim również trzy filary – najważniejsze zasady, niezbędne do osiągnięcia wyżej wymienionego celu:

- *współodpowiedzialność* – wiodąca zasada. Rozumiana jest jako wspólne (zbiorowe) dążenie do poprawy bezpieczeństwa IK wynikające ze świadomości jej znaczenia dla funkcjonowania zarówno organów administracji publicznej, jak i operatorów IK, społeczeństwa, gospodarki i państwa. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno jej operatorów, jak i odpowiedzialnej za funkcjonowanie państwa administracji,
- *współpraca* – drugi filar systemu ochrony IK. W kontekście Programu oznacza wykonywanie razem przez uczestników ochrony IK określonych, zbieżnych i wzajemnie

[3] - Art. 3 pkt. 3 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590)
[4] - Rozdział 5 Narodowego Programu Ochrony Infrastruktury Krytycznej z 2020 r.

uzupełniających się zadań dla osiągnięcia wspólnego celu, który wynika z zasady współodpowiedzialności. Współpraca jest niezbędna w przypadku chęci uniknięcia powielania działań i ponoszonych kosztów oraz efektywniejszego wykorzystania posiadanych sił i środków,

- *zaufanie* – trzeci filar systemu ochrony IK. W Programie rozumiane jako przekonanie, że motywacją działania uczestników ochrony IK (dotyczy to w szczególności administracji i operatorów IK) jest dążenie do wspólnego celu – poprawy bezpieczeństwa IK i RP. Osiągnięcie tego celu będzie zatem korzystne dla wszystkich zainteresowanych stron, w tym przede wszystkim społeczeństwa. Zaufanie jest niezbędne do osiągnięcia celów Programu[5].

Należy również pamiętać, że wszelkie działania podejmowane w celu zapewnienia ochrony infrastruktury krytycznej powinny być proporcjonalne do poziomu ryzyka zakłócenia jej funkcjonowania. Dotyczy to zarówno przyjętego modelu ochrony infrastruktury krytycznej, jej rodzajów, a także użytych sił i środków. Ponadto należy uwzględnić różnice między poszczególnymi systemami IK, ponieważ mimo wielu podobieństw, każdy z obszarów posiada swoje unikalne cechy.

Etapy ochrony infrastruktury krytycznej

Etapy ochrony infrastruktury krytycznej zostały również zawarte w Narodowym Programie Ochrony Infrastruktury Krytycznej w rozdziale 5. Wyróżnia się poszczególną kolejność działań w ramach realizacji powyższego procederu:

- wskazanie zakresu, celów do osiągnięcia w ramach ochrony IK oraz adresatów tych działań,
- identyfikacja krytycznych zasobów, funkcji oraz określenia sieci powiązań (zależności) z innymi systemami IK, w tym podmiotami i organami,
- określenie ról i odpowiedzialności uczestniczących w procesie ochrony IK,

[5] - Rozdział 2.4 Narodowego Programu Ochrony Infrastruktury Krytycznej z 2020 r.

- ocena ryzyka,
- wskazanie priorytetów działania i dokonania ich hierarchizacji w zależności od wyników oceny ryzyka,
- rozwój i wdrażanie systemu ochrony infrastruktury krytycznej, w tym opracowania i akceptacji planów ochrony i odtwarzania IK,
- testowanie (przez ćwiczenia) i przegląd (przez audyt i samoocenę) systemu ochrony IK oraz pomiar postępów na drodze do osiągnięcia celu,
- doskonalenie, rozumiane jako wprowadzanie modyfikacji i korekt w wyniku testów, przeglądów i pomiarów.

Można wyróżnić kilka rodzajów ochrony IK:

- *Ochrona fizyczna* - ochrona osób (zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej). Realizowana jest przez pracowników ochrony, którzy bronią dostępu do obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej.
- *Ochrona techniczna* - ogół przedsięwzięć związana z budową i eksploatacją obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, w tym również techniczne środki ochrony, minimalizujące zagrożenia IK.
- *Ochrona osobowa* - ma na celu minimalizację ryzyka będącego skutkiem działań pracowników oraz usługodawców, którzy mogą dopuścić do zakłóceń w funkcjonowaniu infrastruktury krytycznej.
- *Ochrona teleinformatyczna* - zespół przedsięwzięć i ich procedur, które mają na uwadze minimalizację zakłóceń w funkcjonowaniu IK związanych z wykorzystaniem do użytkowania tego typu infrastruktury systemów i sieci teleinformatycznych.
- *Ochrona prawna* - związana z kształtem współczesnej gospodarki rynkowej, w której dochodzi do zagrożeń ze strony innych podmiotów państwowych lub prywatnych[6].

[6] - Narkowicz J., *Infrastruktura krytyczna*, https://mfiles.pl/pl/index.php/Infrastruktura_krytyczna [dostęp 28.05.2022 r.]

Działania organów i podmiotów na rzecz ochrony infrastruktury krytycznej

Ustawa o zarządzaniu kryzysowym oraz Narodowy Program Ochrony Infrastruktury Krytycznej wyróżniają podstawowe obowiązki organów i podmiotów zaangażowanych w ochronę IK. Głównymi podmiotami utrzymującymi ciągłość świadczenia usług kluczowych w Polsce są: Rządowe Centrum Bezpieczeństwa; operatorzy IK oraz ministrowie odpowiedzialni za systemy IK. Pierwszy z nich pełni główną rolę w budowie systemu infrastruktury krytycznej, opartego na zasadach Narodowego Programu Ochrony Infrastruktury Krytycznej. Do jego zadań w myśl ustawy o zarządzaniu kryzysowym należy m. in.: planowanie cywilne; 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; zapewnienie koordynacji polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej; 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; 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 Traktatu Północnoatlantyckiego oraz ich krajami członkowskimi w zakresie ochrony infrastruktury krytycznej[7].

[7] - Art. 11 ust. 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590)

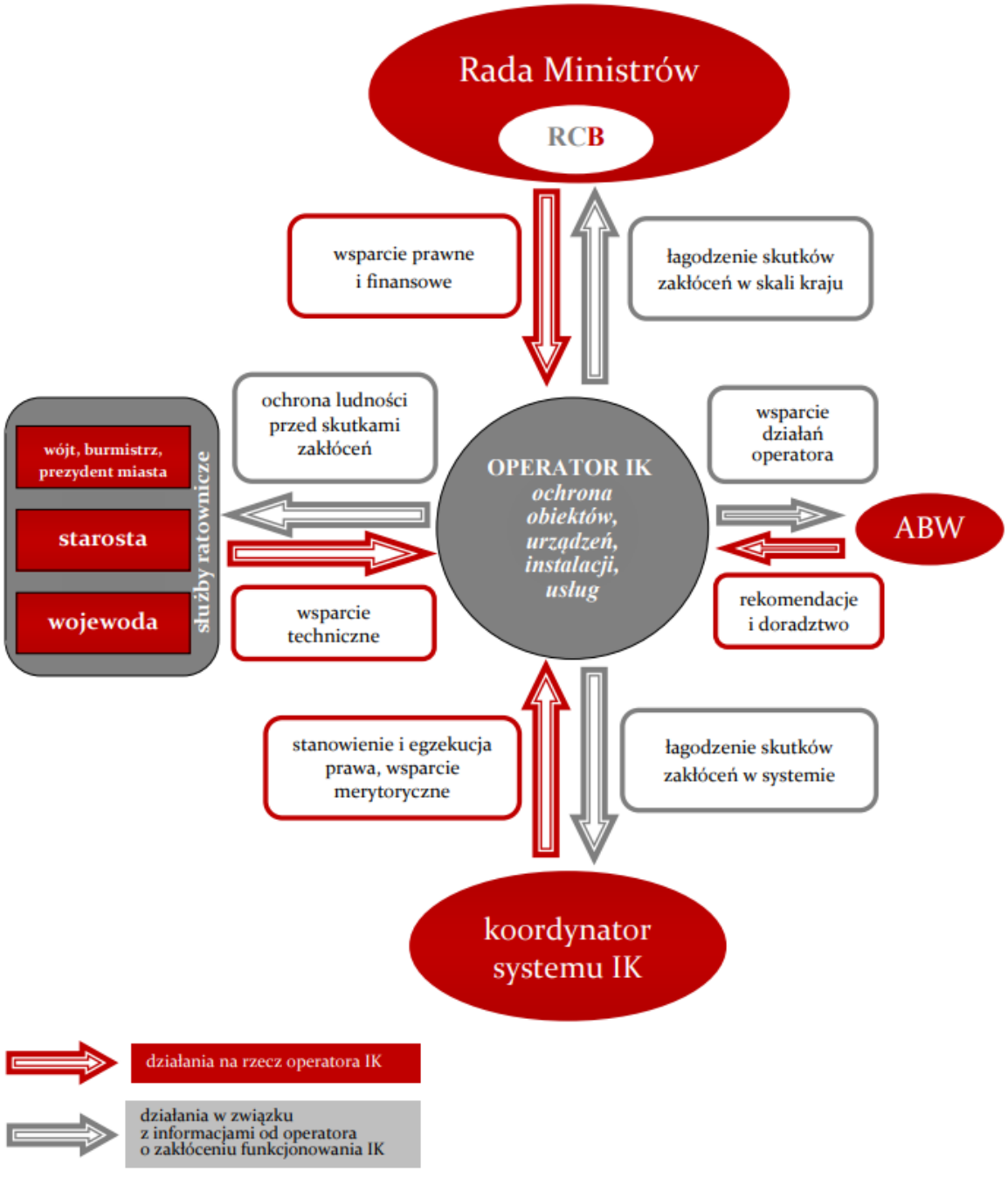
Operatorzy infrastruktury krytycznej mają natomiast obowiązek ochrony obiektów, urządzeń, instalacji i usług IK, w związku z tym są oni zobowiązani do:

- przygotowania i wdrażania, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia,
- wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej,
- niezwłoczne przekazywanie Szefowi Agencji Bezpieczeństwa Wewnętrznego, informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej,
- współpracy w tworzeniu i realizacji Narodowego Programu Ochrony Infrastruktury Krytycznej[8].

Z kolei ministrowie odpowiedzialni za systemy IK również pełnią istotną rolę w systemie ochrony infrastruktury krytycznej. Ich praca jest gwarancją zaangażowania najwyższych władz państwowych w proces budowy bezpieczeństwa państwa. Do ich zadań należy między innymi: wsparcie RCB w budowie systemu ochrony IK; współpraca z RCB i wsparcie w identyfikacji IK oraz wdrażaniu i aktualizacji NPOIK; inicjowanie zmian aktów prawnych w celu ułatwienia i wsparcia wykonywania zadań z zakresu ochrony IK; dokonywanie oceny ryzyka zakłócenia funkcjonowania systemu IK, wywołanego zniszczeniem lub zakłóceniem funkcjonowania IK; współpraca z organami, w kompetencji których znajdują się sprawy dotyczące części składowych systemu IK, nie będących bezpośrednio we właściwości koordynatora; współpraca z innymi koordynatorami systemów IK w zakresie zależności między systemami IK; współpraca z operatorami infrastruktury krytycznej w zakresie jej ochrony, animowanie tej współpracy i jej podtrzymywanie; wsparcie organizacji ćwiczeń systemowych oceniających sprawność ochrony IK; wsparcie działań zmierzających do odtworzenia IK; dokonywanie okresowych analiz i ocen skuteczności ochrony infrastruktury krytycznej we właściwym systemie; organizowanie szkoleń, konferencji i sympozjów naukowo-badawczych,

[8] - Rozdział 4.2 Narodowego Programu Ochrony Infrastruktury Krytycznej z 2020 r.

doskonalących organizacyjne, technicznie i formalno-prawne środki przeciwdziałania zakłóceniom funkcjonowania infrastruktury krytyczne; pobudzanie do aktywności podmiotów zaangażowanych w proces ochrony IK w ramach systemu; doradztwo i pomoc dla operatorów IK oraz administracji publicznej; uzgadnianie planów ochrony IK, ujętej w wykazie IK w ramach danego systemu[9].



Rysunek 1 - Główne podmioty uczestniczące w procesie ochrony IK i ich role
Źródło: Rozdział 4.5 Narodowego Programu Ochrony Infrastruktury Krytycznej z 2020 r.

[9] - Rozdział 4.3 Narodowego Programu Ochrony Infrastruktury Krytycznej z 2020 r.

Ponadto w ochronę IK zaangażowani są także Prezydent RP, Rada Ministrów, ministrowie i kierownicy urzędów centralnych wykonujący zadania z zakresu zarządzania kryzysowego, wojewodowie, służby specjalne, starostowie, wójtowie, burmistrzowie i prezydenci miast.

Działania podejmowane na rzecz zapewnienia bezpieczeństwa

- *zapewnienie bezpieczeństwa fizycznego* – zespół działań mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
- *zapewnienie bezpieczeństwa technicznego* – zespół działań mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
- *zapewnienie bezpieczeństwa osobowego* – zespół działań mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;.
- *zapewnienie bezpieczeństwa teleinformatycznego* – zespół działań mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
- *zapewnienie bezpieczeństwa prawnego* – zespół działań mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
- *plany ciągłości działania i odtwarzania*, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK[10].

[10] - Rozdział 5.1 Narodowego Programu Ochrony Infrastruktury Krytycznej z 2020 r.

Rodzaje obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa i ich kategorie

Rodzajami obiektów, które Rada Ministrów uznaje za szczególnie ważne dla bezpieczeństwa lub obronności państwa, są:

1) obiekty, w których produkuje się, remontuje i magazynuje uzbrojenie, sprzęt wojskowy oraz środki bojowe, a także obiekty, w których są prowadzone prace naukowo-badawcze lub konstruktorskie w zakresie produkcji na potrzeby bezpieczeństwa lub obronności państwa;

2) magazyny, w których są przechowywane rezerwy strategiczne; magazyny ropy naftowej i paliw o pojemności powyżej 100 tys. m3, w których są przechowywane zapasy interwencyjne; magazyny, w których są przechowywane zapasy obowiązkowe gazu ziemnego; kluczowe elementy infrastruktury przesyłowej ropy naftowej, paliw i gazu ziemnego oraz instalacje skroplonego gazu ziemnego, a także dyspozycje mocy, stacje elektroenergetyczne o strategicznym znaczeniu dla krajowego systemu elektroenergetycznego;

3) obiekty stanowiące siedzibę urzędu obsługującego Ministra Obrony Narodowej oraz obiekty jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

4) mosty, wiadukty i tunele, które znajdują się w ciągu dróg o znaczeniu obronnym oraz które znajdują się w ciągu linii kolejowych o znaczeniu obronnym;

5) centrum zarządzania ruchem lotniczym oraz obiekty niezbędne do realizacji zadań w zakresie zapewniania służb żeglugi powietrznej, a także lotniska wyznaczone do startów i lądowań statków powietrznych w ruchu międzynarodowym;

6) porty morskie o znaczeniu obronnym i śródlądowe przeprawy wodne o znaczeniu obronnym;

7) obiekty infrastruktury łączności, w tym obiekty operatorów pocztowych i przedsiębiorców telekomunikacyjnych, przeznaczone do realizacji zadań na rzecz bezpieczeństwa lub obronności państwa;

8) centralny ośrodek dokumentacji geodezyjnej i kartograficznej;

9) zapory wodne i inne urządzenia hydrotechniczne, których awaria może spowodować zatopienie terenów o powierzchni powyżej 500 km2 albo obszaru o mniejszej powierzchni, na którym znajdują się obiekty uznane za szczególnie ważne dla bezpieczeństwa lub obronności państwa;

10) obiekty jednostek organizacyjnych Agencji Wywiadu, Narodowego Banku Polskiego oraz Banku Gospodarstwa Krajowego; Polskiej Wytwórni Papierów Wartościowych S.A. oraz Mennicy Polskiej S.A.;

11) obiekty, w których wytwarza się, przetwarza, stosuje lub przechowuje materiały jądrowe oraz średnio aktywne lub wysokoaktywne odpady lub źródła promieniotwórcze;

12) obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych;

13) obiekty jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego, oraz podległych Ministrowi Sprawiedliwości lub przez niego nadzorowanych;

14) obiekty mające bezpośredni związek z wydobywaniem: gazu ziemnego, ropy naftowej, węgla brunatnego i kamiennego, rud metali z wyjątkiem darniowych rud żelaza, rud pierwiastków rzadkich oraz pierwiastków promieniotwórczych, piasków formierskich i szklarskich oraz ziemi krzemionkowej;

15) obiekty, w których wytwarza się, przetwarza, stosuje lub przechowuje materiały stwarzające szczególne zagrożenie wybuchowe lub pożarowe, w których prowadzi się działalność z wykorzystaniem toksycznych związków chemicznych i ich prekursorów, a także środków biologicznych, mikrobiologicznych, mikroorganizmów, toksyn i innych substancji wywołujących choroby u ludzi lub zwierząt - zlokalizowane w miejscowościach powyżej 20 tys. mieszkańców;

16) elektrownie i elektrociepłownie zawodowe, z wyjątkiem elektrowni jądrowych, których produkcja energii jest przekazywana do wspólnej sieci elektroenergetycznej lub stacje elektroenergetyczne należące do operatorów systemów dystrybucyjnych;

17) inne obiekty, których zniszczenie lub uszkodzenie może stanowić zagrożenie w znacznych rozmiarach dla życia i zdrowia ludzi, dziedzictwa narodowego, środowiska albo spowodować poważne straty materialne lub zakłócić funkcjonowanie państwa[11];

Obiekty wymienione po numerze 11 są obiektami kategorii II, natomiast pozostałe – kategorii I.

Organy wykazane w art. 614 ustawy o obronie Ojczyzny[12] t.j. Prezes Rady Ministrów, ministrowie i przewodniczący komitetów wchodzących w skład Rady Ministrów; organy administracji rządowej nadzorowane przez Prezesa Rady Ministrów; Prezes Narodowego Banku Polskiego; Prezes Zarządu Banku Gospodarstwa Krajowego; wojewodowie, wykonując zadania w zakresie szczególnej ochrony wyżej wymienionych obiektów:

- organizują szczególną ochronę obiektów, w stosunku do których wystąpiły z wnioskiem o uznanie za szczególnie ważne dla bezpieczeństwa lub obronności państwa, w tym określają:
  - zakres prac związanych z przygotowaniem tej ochrony,
  - osoby odpowiedzialne za jej realizację,
  - terminy wykonywania prac;
- formują jednostki przewidziane do militaryzacji w celu prowadzenia ochrony obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa;
- po sformowaniu jednostek, mogą wystąpić odpowiednio do:
  - Ministra Obrony Narodowej - z wnioskiem o wsparcie Sił Zbrojnych Rzeczypospolitej Polskiej w szczególnej ochronie obiektów kategorii I,
  - ministra właściwego do spraw wewnętrznych - z wnioskiem o wsparcie Policji oraz Państwowej Straży Pożarnej w szczególnej ochronie obiektów kategorii II – wskazując na okoliczności uzasadniające konieczność ich zaangażowania;
- ujmują problematykę szczególnej ochrony obiektów, w stosunku do których wystąpiły z wnioskiem o uznanie za szczególnie ważne dla bezpieczeństwa lub obronności

[11] - § 2 Rozporządzenia Rady Ministrów z dnia 21 kwietnia 2022 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa oraz ich szczególnej obrony (Dz.U.2022.880)
[12] - ustawa z dnia 11 marca 2022 r. o obronie ojczyzny (Dz.U. 2022 poz. 655)

państwa, w dokumentach dotyczących przygotowań obronnych Rzeczypospolitej Polskiej;

- koordynują i nadzorują prace związane z przygotowaniem szczególnej ochrony obiektów oraz zapewniają warunki do realizacji tych prac;
- opracowują i aktualizują plany szczególnej ochrony obiektów, zgodnie z zasadami określonymi odpowiednio w wytycznych;
- uzgadniają plany, odpowiednio z Ministrem Obrony Narodowej w przypadku obiektu kategorii I lub ministrem właściwym do spraw wewnętrznych w przypadku obiektu kategorii II;
- realizują zadania związane z uzyskaniem limitów osobowych, środków finansowych oraz innych zasobów niezbędnych do prowadzenia szczególnej ochrony obiektów, a także dysponują przydzielonymi limitami i środkami przeznaczonymi na tę ochronę;
- zapewniają ciągłość i terminowość prowadzenia szczególnej ochrony obiektów[13].

Do zadań Ministra Obrony Narodowej należy dodatkowo:

- opracowanie dla obiektów kategorii I wytycznych w sprawie przygotowania i prowadzenia szczególnej ochrony;
- wyrażanie zgody na wsparcie Sił Zbrojnych Rzeczypospolitej Polskiej w szczególnej ochronie obiektów kategorii I;
- informowanie ministra właściwego do spraw wewnętrznych o zmianach dokonywanych w wykazie w zakresie dotyczącym obiektów kategorii II[14].

Natomiast do zadań ministra właściwego do spraw wewnętrznych, poza zadaniami określonymi powyżej, należy dodatkowo:

- opracowanie dla obiektów kategorii II wytycznych w sprawie przygotowania i prowadzenia szczególnej ochrony;

[13] - § 8 pkt. 1 Rozporządzenia Rady Ministrów z dnia 21 kwietnia 2022 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa oraz ich szczególnej obrony (Dz.U.2022.880)
[14] - tamże § 8 pkt. 2

- wyrażanie zgody na wsparcie Policji oraz Państwowej Straży Pożarnej w szczególnej ochronie obiektów kategorii II.[15]

Podsumowanie

Dzisiejsze czasy pokazują jak ważną rolę odgrywa infrastruktura krytyczna w kontekście bezpieczeństwa wewnętrznego. Na co dzień temat ten jest mało poruszany w mediach i przestrzeni publicznej przez co społeczeństwo zapomina o tym aspekcie. Ostatnie miesiące oraz agresywna polityka Rosji pokazała, że ważnym jest nie tylko tworzenie elementów infrastruktury krytycznej, lecz także ich udoskonalanie i polepszanie. Dzięki niej możemy spokojnie żyć nie martwiąc się o jedzenie, wodę, paliwa, zdrowie, czy pieniądze. Ich rynkowe ceny w zależności od sytuacji politycznej mogą wzrastać, lecz dzięki tym buforowym elementom możemy względnie sprawnie funkcjonować w codziennym życiu. W szczególności w obecnym czasie ważne jest, by wszelkie systemy i obiekty niezbędne do minimalnego funkcjonowania gospodarki działały – dla naszego wspólnego dobra. Każde zaburzenie efektywności pracy tych elementów może doprowadzić do rozkładu polskiej gospodarki, a w ostateczności upadku państwa. Infrastruktura krytyczna to wg ustawy o zarządzaniu kryzysowym kluczowe obiekty i systemy w rozumieniu bezpieczeństwa państwa i jego obywateli. Należy więc wszelkimi siłami dbać o zapewnienie bezpieczeństwa funkcjonowania tak ważnych dla nas elementów życia codziennego.

[15] - tamże § 8 pkt. 3

Źródła:

1. Ustawa z dnia 11 marca 2022 r. o obronie ojczyzny (Dz.U. 2022 poz. 655)
2. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590)
3. Rozporządzenie Rady Ministrów z dnia 21 kwietnia 2022 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa oraz ich szczególnej obrony (Dz.U.2022.880)
4. Narodowy Program Ochrony Infrastruktury Krytycznej – Uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej
5. Narkowicz J., *Infrastruktura krytyczna*, https://mfiles.pl/pl/index.php/Infrastruktura_krytyczna [dostęp 28.05.2022 r.]