2020

# Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity

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.



# Spis treści



[1] Podrozdział 2.6. „Ramy czasowe" usunięty został Uchwałą nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. *zmieniającą uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej*.

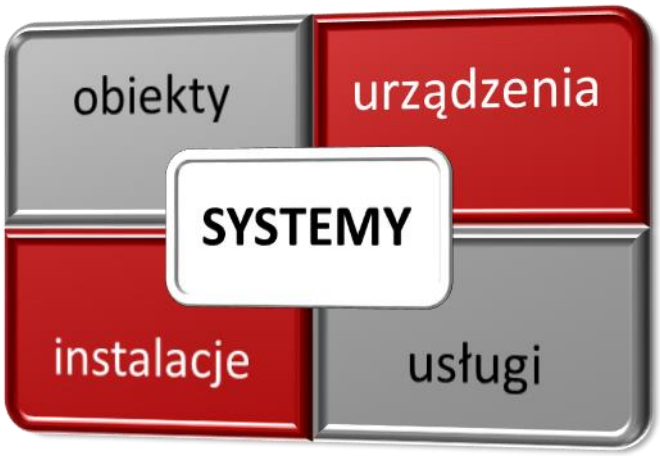
# Wprowadzenie

Niniejszy dokument stanowi aktualizację Narodowego Programu Ochrony Infrastruktury Krytycznej przyjętego uchwałą Rady Ministrów w dniu 26 marca 2013 roku.

Pierwsza edycja Programu ustanowiła ramy wielostronnej partnerskiej współpracy na rzecz nieprzerwanego dostępu do usług zapewniających utrzymanie określonego standardu życia oraz umożliwiających właściwe relacje między państwem a obywatelem.

Dostęp do tego rodzaju usług jest sprawą kluczową z punktu widzenia sprawnego funkcjonowania i rozwoju nowoczesnego państwa, społeczeństwa i gospodarki. Usługi te oraz dostarczająca je infrastruktura zostały określone mianem infrastruktury krytycznej.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r. poz. 1166 oraz z 2015 r. poz. 1485 – zwana dalej: „ustawą o zarządzaniu kryzysowym") definiuje infrastrukturę krytyczną 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.




*Rys. 1. Infrastruktura krytyczna.*

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.

Administracja i przedsiębiorcy stają się współzależni. Powstaje wspólna infrastruktura realizująca procesy na rzecz obydwu stron. Prowadzi to do uzależnienia się w takim stopniu, że dysfunkcja tej infrastruktury może prowadzić do skutków wykraczających poza granice władającej nią organizacji. Tym samym konieczne staje się uznanie ochrony IK jako procesu ukierunkowanego na ochronę ciągłości świadczenia określonej usługi oraz odtworzenia jej w razie potrzeby.

Dlatego, identyfikując te wyzwania, w bieżącej edycji Programu zostały zaadresowane zadania mające pomóc w ustaleniu skali współzależności i podjęciu skutecznych działań celem zredukowania ryzyka zakłócenia funkcjonowania IK.

# 1. Definicje i skróty użyte w dokumencie

## 1.1. Definicje

**koordynator systemu IK** – minister kierujący działem administracji rządowej odpowiedzialny za system infrastruktury krytycznej, koordynujący działania w zakresie ochrony IK wskazane w Narodowym Programie Ochrony Infrastruktury Krytycznej, ustawie o zarządzaniu kryzysowym oraz przepisach wykonawczych do niej. Koordynator systemu IK, do realizacji działań w zakresie ochrony IK, może wykorzystywać uprawnienia nadane mu na podstawie innych przepisów,

**ochrona IK** – zgodnie z art. 3 pkt 3 ustawy o zarządzaniu kryzysowym – 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,

**ochrona obowiązkowa** – ochrona obszarów, obiektów, urządzeń i transportów ważnych dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa prowadzona przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne, zgodnie z przepisami ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2014 r. poz. 1099 oraz z 2015 r. poz. 1505),

**ochrona szczególna** – ochrona obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa prowadzona przez specjalnie tworzone w tym celu, na podstawie odrębnych przepisów, jednostki zmilitaryzowane. Ochrona szczególna jest przygotowywana i prowadzona na podstawie przepisów ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2015 r. poz. 827, z późn. zm.) oraz rozporządzenia Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz. U. Nr 116, poz. 1090),

**operator IK** – zgodnie z § 1 rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. Nr 83, poz. 541) – właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej,

**sytuacja kryzysowa** – zgodnie z art. 3 pkt 1 ustawy o zarządzaniu kryzysowym – sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.

## 1.2. Wykaz skrótów

ABW – Agencja Bezpieczeństwa Wewnętrznego
IK – infrastruktura krytyczna
NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej
OIK – ochrona infrastruktury krytycznej
PSP – Państwowa Straż Pożarna
RCB – Rządowe Centrum Bezpieczeństwa
RP – Rzeczpospolita Polska
WCZK – Wojewódzkie Centrum Zarządzania Kryzysowego

# 2. Zakres, cele, priorytety i zasady Programu

## 2.1. Zakres Programu

Narodowy Program Ochrony Infrastruktury Krytycznej został opracowany na podstawie art. 5b ust. 1 ustawy o zarządzaniu kryzysowym.

Jest nim objęta IK umieszczona w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym.

NPOIK nie jest programem operacyjnym ani programem rozwoju w rozumieniu ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2014 poz. 1649, z późn. zm.) i jest komplementarny w stosunku do *Strategii rozwoju systemu bezpieczeństwa narodowego RP 2022* oraz *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*.

Mając na uwadze fakt członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego, Organizacji Bezpieczeństwa i Współpracy w Europie oraz innych organizacjach międzynarodowych, NPOIK uwzględnia również międzynarodowe porozumienia, których RP jest stroną.

## 2.2. Cele Programu

Celem Programu jest stworzenie warunków do poprawy bezpieczeństwa IK. Wraz z innymi dokumentami programowymi składa się on na cel nadrzędny – podniesienie bezpieczeństwa Rzeczypospolitej Polskiej.

Osiągnięcie tego celu wymaga osiągnięcia szeregu celów pośrednich:

- zdobycie określonego poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów i metod jej ochrony,
- wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń, w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach,
- wprowadzenie skoordynowanego i opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony IK,
- budowa partnerstwa między uczestnikami procesu ochrony IK,
- wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych między uczestnikami procesu ochrony IK.

## 2.3. Priorytety Programu

Na okres 2 lat od przyjęcia przez Radę Ministrów aktualizacji Programu określa się dla niego następujące priorytetowe działania:

1) pogłębienie współpracy między uczestnikami Programu w obszarze ochrony IK,
2) identyfikacja zależności pomiędzy systemami IK,
3) dokonanie oceny ryzyka zakłócenia funkcjonowania systemu IK.

## 2.4. Zasady Programu

W ustawie o zarządzaniu kryzysowym przyjęto bezsankcyjne podejście do ochrony infrastruktury krytycznej. Jego podstawą jest założenie, że zwiększenie skuteczności ochrony IK może nastąpić jedynie przez działania jej operatorów wspieranych przez możliwości i potencjał administracji publicznej. Operatorzy IK mają najlepszą wiedzę i narzędzia do ograniczenia zagrożeń dla ich działalności. Są również w stanie dokonać najwłaściwszego wyboru strategii minimalizacji skutków tych zagrożeń. Starając się zachować równowagę pomiędzy władczym oddziaływaniem państwa, a wydatkami niezbędnymi do poprawy bezpieczeństwa IK ustawa o zarządzaniu kryzysowym nie przewiduje sankcji za niedopełnienie obowiązków w niej określonych, jak również nie przewiduje wsparcia budżetowego operatorów IK.

Dlatego, aby osiągnąć cele Programu niezbędne jest przyjęcie zasad, którymi powinni się kierować jego uczestnicy. Filarami i najważniejszymi zasadami Programu są:

- **współodpowiedzialność – wiodąca zasada** przyjęta przy budowie systemu ochrony IK. 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 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.

Program kieruje się również zasadami:

- **proporcjonalności i działań opartych na ocenie ryzyka** – działania nakierowane na podniesienie poziomu ochrony IK powinny być adekwatne do poziomu ryzyka. Dotyczy to zarówno przyjętego modelu ochrony IK, jak i użytych sił i środków. Ocena ryzyka powinna być podstawą określenia standardów ochrony IK i do ustalenia priorytetów działań,
- **uznania różnic między systemami IK** – systemy IK cechuje wiele podobieństw, posiadają jednak pewne unikalne cechy, które w obszarze ochrony IK powinny zostać uwzględnione,
- **wiodącej roli ministra odpowiedzialnego za system IK** – inicjatywa zwiększenia poziomu ochrony infrastruktury kluczowej dla funkcjonowania społeczeństwa wyszła ze strony administracji, dlatego powinna ona mieć znaczący udział w działaniach na rzecz poprawy bezpieczeństwa IK. Tę rolę w budowie zaufania i skutecznej współpracy odgrywają ministrowie odpowiedzialni za system IK, niezależnie od obowiązku ochrony IK ciążącego na operatorze IK,
- **równości operatorów IK** – operatorami IK są zarówno podmioty prywatne, podmioty stanowiące własność państwa, jak i sama administracja. Program nie dokonuje rozróżnień i w jego rozumieniu wszyscy operatorzy są równi i zobowiązani do realizacji tego samego obowiązku – ochrony IK, którą władają,
- **komplementarności** – w użyciu pozostaje wiele rozwiązań, które skutecznie przyczyniają się do bezpiecznego funkcjonowania IK. Zapisy NPOIK mają charakter uzupełniający w stosunku do istniejących rozwiązań prawno-instytucjonalnych. Nie powielają rozwiązań i przyjętych praktyk wynikających z obowiązującego prawa.

Niezależnie od przyjętego podejścia:

- w przypadku negatywnej oceny skuteczności realizacji ustawy o zarządzaniu kryzysowym oraz Programu,
- jeśli zidentyfikowane istotne braki w systemach ochrony infrastruktury krytycznej nie zostaną usunięte przez operatorów IK,
- jeżeli ze względu na pojawienie się nowych zagrożeń, obecne przepisy prawne uznane zostaną za nieodpowiednie lub niemające zastosowania w odniesieniu do tych zagrożeń,
- w celu zoptymalizowania ochrony infrastruktury krytycznej,
- w celu redukcji niektórych rodzajów ryzyka,

dopuszcza się możliwość wprowadzenia szczegółowych uregulowań prawnych dotyczących realizacji Programu.

## 2.5. Adresaci Programu

Program adresowany jest w szczególności do administracji rządowej oraz operatorów IK. Postanowienia Programu mogą być jednak stosowane przez wszystkich, którzy uznają Program za pomocny w procesie zwiększania odporności na zakłócenia własnej infrastruktury, w tym organy samorządowe i podmioty prywatne, niebędące operatorami IK.

Program jest także adresowany do tych, którzy, kierując się zasadami Programu, chcieliby zaangażować się w proces osiągania jego celów.

### *2.5.1. Administracja rządowa*

Głównymi adresatami Programu w administracji rządowej są ministrowie odpowiedzialni za systemy IK oraz wojewodowie. Biorąc jednak pod uwagę rozległość i przekrojowość działań administracji, Program adresowany jest również do pozostałych organów, instytucji i podmiotów administracji. Jest on źródłem informacji o działaniach w ramach ochrony IK i otwiera możliwości zaangażowania się w jego realizację oraz nawiązania efektywnej współpracy z ministrami odpowiedzialnymi za systemy IK i operatorami IK.

### *2.5.2. Operatorzy IK*

Operatorzy IK, zgodnie z art. 6 ust. 5 ustawy o zarządzaniu kryzysowym, mają obowiązek jej ochrony. Program kierowany jest przede wszystkim do kierownictwa podmiotów będących operatorami IK. Adresatem Programu automatycznie staje się każdy operator nowo wyznaczonej IK.

### *2.5.3. Pozostałe podmioty gospodarcze i organizacje*

Nieustanny rozwój i postępujący poziom współzależności między różnymi sektorami gospodarki sprawiają, że zagrożenia charakterystyczne dla funkcjonowania IK mogą dotyczyć również innych obszarów. Zawarte w Programie rozwiązania i dobre praktyki ochrony IK mogą zostać wykorzystane w każdej organizacji, podnosząc w ten sposób jej odporność na zagrożenia.

### *2.5.4. Środowisko naukowe*

Program, bazując na trzech podstawowych zasadach, otwiera wiele nowych możliwości w zakresie badań naukowych i nastawionych na wdrożenia prac rozwojowych. Prezentacja działań podejmowanych przez administrację w celu podniesienia poziomu bezpieczeństwa IK służyć ma jako drogowskaz dla środowiska naukowego w celu opracowania narzędzi pomocnych w realizacji Programu.

### *2.5.5. Społeczeństwo*

Od dostaw usług dostarczanych przy wykorzystaniu IK uzależniony jest każdy obywatel. Wiedza w zakresie działań podejmowanych przez administrację w celu podniesienia poziomu bezpieczeństwa IK (a tym samym nas wszystkich) wymaga upowszechnienia. Program przedstawia rozwiązania i dobre praktyki z zakresu ochrony, umożliwia ich zastosowanie w życiu codziennym, co może być przydatne w podniesieniu indywidualnej odporności na zagrożenia.

# 3. Identyfikacja IK

Identyfikacja obiektów, urządzeń, instalacji lub usług, których zniszczenie lub zakłócenie funkcjonowania mogłoby spowodować sytuację kryzysową, jest kluczowym etapem procesu ochrony IK.

W celu maksymalnej obiektywizacji Rządowe Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych oraz przy wsparciu przedsiębiorców prywatnych, opracowało kryteria identyfikacji IK.

Kryteria podzielone są na dwie grupy:

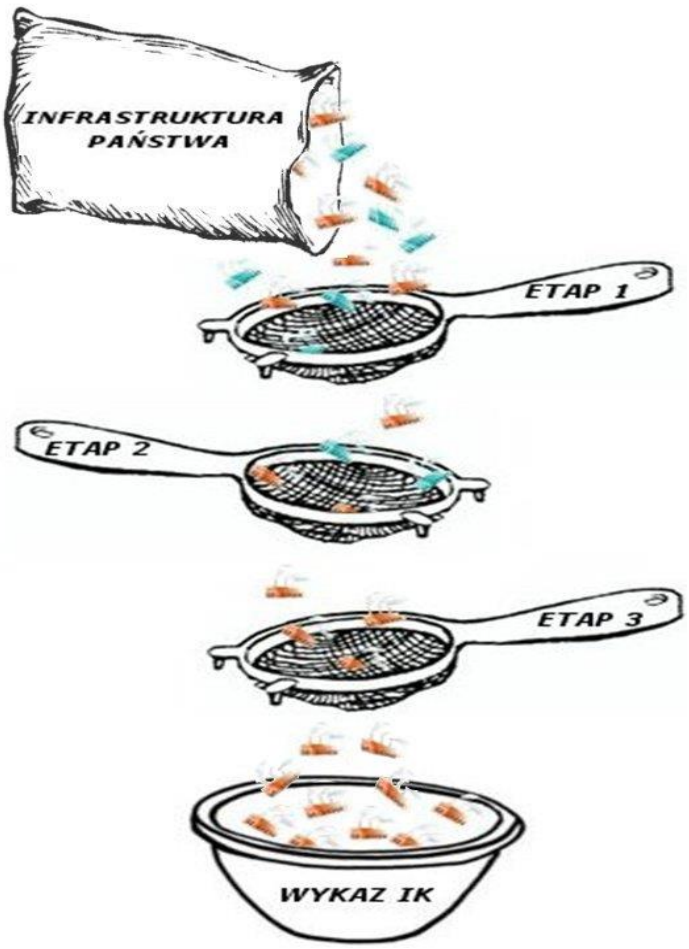
1) kryteria systemowe – charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów IK,
2) kryteria przekrojowe – opisujące parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria przekrojowe obejmują:
   - ofiary w ludziach,
   - skutki finansowe,
   - konieczność ewakuacji,
   - utratę usługi,
   - czas odbudowy,
   - efekt międzynarodowy,
   - unikatowość.

Kryteria określają wartości liczbowe, stosowane dla scharakteryzowania cechy, ze względu na którą dana infrastruktura klasyfikowana jest jako IK. W przypadku braku takiej możliwości opisano funkcje realizowane przez badaną infrastrukturę.

Identyfikacja IK została podzielona na trzy przedstawione poniżej etapy:

1) etap pierwszy – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK w danym systemie, do infrastruktury systemu należy zastosować kryteria systemowe, właściwe dla danego systemu IK,
2) etap drugi – w celu sprawdzenia, czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, do infrastruktury wyłonionej w etapie pierwszym należy zastosować definicję zawartą w art. 3 pkt 2 ustawy o zarządzaniu kryzysowym,

3) etap trzeci – w celu oceny potencjalnych skutków zniszczenia lub zaprzestania funkcjonowania potencjalnej IK, do infrastruktury wyłonionej w etapie pierwszym i drugim należy zastosować kryteria przekrojowe, przy czym potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe[2].




*Rys. 2. Identyfikacja infrastruktury krytycznej.*

Kryteria identyfikacji IK, podobnie jak sam Program, podlegają aktualizacji. Wraz ze wzrostem wiedzy na temat funkcjonowania systemów IK, mechanizm aktualizacji będzie wykorzystany do regulacji kryteriów tak, aby najlepiej odzwierciedlały potrzeby ochrony IK.

[2] Spośród kryteriów przekrojowych należy wybrać najlepiej odpowiadające charakterystyce danego systemu IK.

# 4. Organy i podmioty uczestniczące w realizacji Programu, ich rola i odpowiedzialność

Infrastruktura krytyczna służy zaspokojeniu potrzeb wszystkich obywateli. Dlatego nadrzędnym celem ochrony IK jest utrzymanie ciągłości świadczenia usług kluczowych dla państwa i nie może być ona traktowana jako wyłączna domena któregokolwiek z uczestników Programu. Wiedza oraz znajomość specyfiki systemu IK mają pomóc w osiągnięciu celów Programu.

Określenie podziału kompetencji uczestników Programu, zrozumienie roli i odpowiedzialności każdego z nich w systemie ochrony infrastruktury krytycznej RP stanowi podstawę skuteczności i trwałości podejmowanego w tym zakresie wysiłku i przyczyni się do osiągnięcia celów Programu.

Realizacja Programu wymaga zaangażowania wszystkich możliwych zainteresowanych stron, jednakże główny wysiłek spoczywa, zgodnie z posiadanymi kompetencjami, na Rządowym Centrum Bezpieczeństwa, ministrach odpowiedzialnych za systemy IK oraz operatorach infrastruktury krytycznej, wyszczególnionych w wykazie infrastruktury krytycznej.

Ustawa o zarządzaniu kryzysowym zdefiniowała podstawowe obowiązki podmiotów zaangażowanych w ochronę IK. Obowiązki organów wynikające z pozostałych przepisów ustawy, zwłaszcza w kontekście uwzględnienia zadań z zakresu ochrony IK w planach zarządzania kryzysowego, pozostają niezmienione.

## 4.1. Rządowe Centrum Bezpieczeństwa

W zakresie ochrony infrastruktury krytycznej Rządowe Centrum Bezpieczeństwa realizuje zadania określone w art. 11 ust. 2 pkt 11 ustawy o zarządzaniu kryzysowym oraz aktach wykonawczych do niej.

W ramach realizacji powyższych zadań Rządowe Centrum Bezpieczeństwa, pełniąc główną rolę w budowie systemu ochrony infrastruktury krytycznej, opartego na współodpowiedzialności, współpracy i zaufaniu, a także na pozostałych zasadach Programu, będzie realizować działania przewidziane w planie działań (rozdz. 6), a także m.in.:

- budować partnerstwo między wszystkimi zainteresowanymi stronami oraz wspierać i ułatwiać ten proces na niższych poziomach,
- budować, utrzymywać i rozwijać sieć wymiany informacji między uczestnikami Programu, podejmując działania opisane w rozdziale 5,

- wspierać ministrów i kierowników urzędów centralnych w dokonywaniu oceny ryzyka wystąpienia sytuacji kryzysowej, wywołanej zakłóceniem funkcjonowania systemu IK,
- opracowywać, rozpowszechniać i wdrażać wskazówki, rekomendacje i wytyczne dotyczące zarządzania ryzykiem zakłócenia IK,
- opracowywać mechanizmy wsparcia odtwarzania IK,
- wspierać tworzenie (jeżeli jest to uzasadnione) struktur w celu zwiększenia ścisłej współpracy między sektorem prywatnym i administracją publiczną na wszystkich szczeblach, aby podtrzymać skuteczność Programu,
- publikować informacje na temat dobrych praktyk w obszarze ochrony IK i ułatwiać ich wymianę,
- inicjować i wspierać związane z ochroną IK badania naukowe i prace rozwojowe,
- promować programy edukacyjne oraz działania mające na celu podnoszenie świadomości w obszarze ochrony IK,
- prowadzić szkolenia w obszarze ochrony IK i wspierać ich organizację,
- oceniać skuteczność Programu.

## 4.2. Operatorzy IK

Operatorzy IK mają najlepszą wiedzę i warunki do ograniczenia zagrożeń dla IK, zmniejszania jej podatności na te zagrożenia oraz wyboru najodpowiedniejszych strategii minimalizacji skutków tych zagrożeń. Zgodnie z ustawą o zarządzaniu kryzysowym to im powierzony został obowiązek ochrony obiektów, urządzeń, instalacji i usług infrastruktury krytycznej.

W związku z powyższym zobowiązani są oni 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 Programu.

Osoba (osoby) odpowiedzialna za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej powinna odbierać/przekazywać informacje o zagrożeniach dla danej IK i mieć techniczne możliwości realizacji tego

zadania w trybie 24-godzinnym. Powinna również posiadać możliwie największą wiedzę o infrastrukturze krytycznej operatora i jej funkcjonowaniu.

Operatorzy IK uczestniczą w działaniach na rzecz ochrony IK również przez:

- aktywną współpracę z administracją publiczną (na wszystkich poziomach) i innymi operatorami IK,
- wsparcie administracji publicznej (na wszystkich poziomach) wiedzą ekspercką dotyczącą funkcjonowania IK w procesie planowania na wypadek wystąpienia sytuacji kryzysowej,
- wymianę informacji na temat zagrożeń z innymi operatorami IK,
- poprawę umiejętności i zdolności do reagowania w sytuacjach kryzysowych, w tym przez właściwą edukację i organizację ćwiczeń personelu,
- dostarczanie administracji publicznej i innym operatorom IK wiedzy na temat zależności i współzależności między własną IK a IK funkcjonującą w innych sektorach gospodarki,
- identyfikację najlepszych praktyk i standardów mogących pomóc w ochronie IK,
- udział w promocji programów edukacyjnych i szkoleń z zakresu ochrony IK,
- udział w ćwiczeniach dotyczących zarządzania kryzysowego i ochrony IK.

## 4.3. Ministrowie odpowiedzialni za systemy infrastruktury krytycznej

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

Systemy IK wyróżniają: charakterystyka funkcjonowania, uwarunkowania prawne oraz użytkownicy. Biorąc pod uwagę przyjęty model ochrony IK, każdy z systemów IK potrzebuje koordynatora posiadającego najlepszą wiedzę o danym systemie IK, rozumiejącego jego budowę i potrzeby zaangażowanych podmiotów. Ministrowie właściwi w sprawach działów administracji rządowej lub obszarów zadaniowych porównywalnych z systemami IK są ze strony administracji najlepiej przygotowani do pełnienia tej roli.

Uznając różnice między systemami IK, zgodnie z wymogiem narzuconym ustawą o zarządzaniu kryzysowym, Program wskazuje ministrów odpowiedzialnych za te systemy.

WYKAZ MINISTRÓW ODPOWIEDZIALNYCH ZA POSZCZEGÓLNE SYSTEMY INFRASTRUKTURY KRYTYCZNEJ[3]

| Systemy infrastruktury krytycznej | Minister odpowiedzialny za system infrastruktury krytycznej |
|---|---|
| System zaopatrzenia w energię, surowce energetyczne i paliwa | minister właściwy do spraw aktywów państwowych<br>minister właściwy do spraw energii<br>minister właściwy do spraw gospodarki złożami kopalin |
| System łączności | minister właściwy do spraw informatyzacji<br>minister właściwy do spraw łączności |
| System sieci teleinformatycznych | minister właściwy do spraw informatyzacji |
| System finansowy | minister właściwy do spraw budżetu<br>minister właściwy do spraw finansów publicznych<br>minister właściwy do spraw instytucji finansowych |
| System zaopatrzenia w żywność | minister właściwy do spraw rolnictwa<br>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<br>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 |

[3] Wykaz zmieniony uchwałą Rady Ministrów nr 116/2020 z dnia 13 sierpnia 2020 r. *zmieniającą uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej*.

W rozumieniu Programu odpowiedzialność za system IK polega w szczególności na *(w nawiasie przykładowe konkretne działania związane z zadaniem)*:

- wsparciu RCB w budowie systemu ochrony infrastruktury krytycznej, opartego na współodpowiedzialności, współpracy i zaufaniu, a także innych zasadach Programu *(propagowanie zasad Programu w dostępnych im kanałach informacyjnych, popieranie Programu na zewnątrz, pomoc merytoryczna lub pomoc w znalezieniu kompetentnych ekspertów mogących rozwiązać szczegółowe problemy pojawiające się w fazie realizacji Programu)*;
- współpracy z RCB i wsparciu w identyfikacji IK oraz wdrażaniu i aktualizacji NPOIK *(pomoc merytoryczna lub pomoc w znalezieniu kompetentnych ekspertów w kwestii budowy kryteriów, sposobów wykorzystania kryteriów, metod obliczeniowych mogących mieć zastosowanie w identyfikacji IK, zgłaszanie problemów zidentyfikowanych podczas wdrażania Programu, składanie propozycji rozwiązań problemów oraz propozycji udoskonalenia systemu ochrony IK)*;
- inicjowaniu zmian aktów prawnych w celu ułatwienia i wsparcia wykonywania zadań z zakresu ochrony IK *(inicjacja i prowadzenie procesu legislacyjnego aktów prawnych mających poprawić funkcjonowanie systemu ochrony IK w zakresie koordynowanego systemu)*;
- dokonywaniu oceny ryzyka zakłócenia funkcjonowania systemu IK, wywołanego zniszczeniem lub zakłóceniem funkcjonowania IK *(gromadzenie informacji niezbędnych do identyfikacji zagrożeń, określenia skutków zakłócenia IK oraz określenia podatności systemu IK)*;
- współpracy z organami, w kompetencji których znajdują się sprawy dotyczące części składowych (elementów) systemu IK, nie będących bezpośrednio we właściwości koordynatora *(podejmowanie – jeśli jest taka konieczność – współpracy z innymi organami, które na mocy ustaw mają np. władcze kompetencje w danym fragmencie systemu IK, informowanie tych organów o działaniach w kwestii ochrony IK pozostających w ich kompetencji)*;
- współpracy z innymi koordynatorami systemów IK w zakresie zależności między systemami IK *(identyfikacja zależności i współzależności między systemami IK, praca z ekspertami z innych systemów nad modelowaniem tych zależności, informowanie o potencjalnych zagrożeniach będących skutkiem zakłóceń w innych systemach)*;
- współpracy z operatorami infrastruktury krytycznej w zakresie jej ochrony, animowanie tej współpracy i jej podtrzymywanie *(inicjowanie i utrzymywanie kontaktów z operatorami IK, zapraszanie na konferencje, sympozja itp. w których poruszane są sprawy związane z ochroną IK, oceną ryzyka, metodami zarządzania w sytuacjach awaryjnych itp., wizyty w obiektach IK)*;

- organizacji i obsłudze systemowego forum ochrony IK i udziale w mechanizmie ochrony IK w zakresie opisanym w Programie *(przygotowanie dwa razy do roku spotkania z operatorami IK, przygotowanie dyskusji o problemach związanych z ochroną IK, zidentyfikowanych słabościach systemu ochrony IK, potrzebach operatorów i administracji w zakresie wymiany informacji itp., aktywne uczestnictwo ekspertów ministra w wymianie informacji na platformie internetowej)*;
- wsparciu organizacji ćwiczeń systemowych oceniających sprawność ochrony IK *(pomoc w budowie scenariusza ćwiczenia, pomoc w określeniu wprowadzeń do scenariusza, pełnienie ewentualnej roli rozjemców, obserwatorów ćwiczenia, pomoc w ocenie wyników ćwiczenia, pomoc w przekazywaniu informacji w trakcie ćwiczenia i po ćwiczeniu)*;
- wsparciu działań zmierzających do odtworzenia IK *(utrzymywanie kontaktów z operatorami IK w zakresie ich potrzeb, ewentualne przekazywanie informacji w tym zakresie RCB, innym koordynatorom systemów, Radzie Ministrów, pomoc merytoryczna dla operatora IK lub pomoc w znalezieniu kompetentnych ekspertów)*;
- dokonywaniu okresowych analiz i ocen skuteczności ochrony infrastruktury krytycznej we właściwym systemie *(bazując na współpracy z operatorami IK oraz w oparciu o wizyty, ankiety, wywiady próba ilościowego i jakościowego opisu mającego służyć jako materiał statystyczny i wyjściowy np. propozycji na forum systemowym)*;
- inspirowaniu wdrażania nowoczesnych technik ochrony IK w systemie *(zbieranie we własnym zakresie oraz we współpracy z innymi uczestnikami Programu informacji o nowoczesnych technikach ochrony, dzielenie się tymi informacjami z operatorami IK, pomoc wizerunkowa dla podjętych przez operatorów działań np. ustanowienie certyfikatu „firmy odpowiedzialnej społecznie" itp.)*;
- organizowaniu szkoleń, konferencji i sympozjów naukowo-badawczych, doskonalących organizacyjne, technicznie i formalno-prawne środki przeciwdziałania zakłóceniom funkcjonowania infrastruktury krytycznej *(zbieranie informacji o tego typu inicjatywach i przekazywanie ich do operatorów IK, wsparcie logistyczne tego typu przedsięwzięć)*;
- pobudzaniu do aktywności podmiotów zaangażowanych w proces ochrony IK w ramach systemu *(korespondencja, ankiety i wywiady dotyczące identyfikacji luk w systemie ochrony IK oraz potrzeb operatorów IK, wizyty, zbieranie tematów do rozmów w ramach forum systemowego, przekazywanie materiałów w zakresie ochrony z prośbą o zajęcie stanowiska, namawianie do poszukiwania własnych rozwiązań dotyczących ochrony IK i oferowanie ich przedstawienia na wyższym szczeblu lub w ramach systemu IK)*;

- doradztwie i pomocy dla operatorów IK oraz administracji publicznej *(pomoc merytoryczna lub pomoc w znalezieniu kompetentnych ekspertów)*;
- wspieraniu systemowych inicjatyw zmierzających do poprawy bezpieczeństwa funkcjonowania IK *(zbieranie informacji o inicjatywach operatorów IK w zakresie poprawy jej bezpieczeństwa, użyczanie logotypu ministerstwa, wsparcie logistyczne, pomoc w kontaktach z osobami, które mogą wzmocnić inicjatywę itp.)*;
- uzgadnianiu planów ochrony IK, ujętej w wykazie IK w ramach danego systemu *(obowiązek wynika z §4 ust. 1 pkt 2 rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej – Dz. U. nr 83, poz. 542)*

Ponadto, kierując się zasadami Programu, ministrowie odpowiedzialni za system IK:

- współuczestniczą w przygotowaniu i promocji przygotowanych na poziomie centralnym strategii mających na celu zachęcenie sektora prywatnego do udziału w Programie,
- przygotowują strategie mające na celu zachęcenie sektora prywatnego do udziału w Programie,
- budują partnerstwo między zainteresowanymi stronami w ramach systemu IK,
- promują na poziomie systemu IK programy edukacyjne w zakresie ochrony IK,
- organizują w ramach systemu IK szkolenia z zakresu ochrony IK dla samorządów i partnerów z sektora prywatnego,
- promują działania mające na celu podnoszenie świadomości w obszarze ochrony IK,
- wdrażają system zarządzania ciągłością działania obsługujących ich urzędów,
- dbają, aby zadania z zakresu ochrony IK uwzględniano w działalności podległych lub podporządkowanych im organów.

Kreując politykę w ramach systemu IK, ministrowie odpowiedzialni za systemy ściśle współpracują z podmiotami właściwymi w danym obszarze.

W przypadku, gdy odpowiedzialność za system została podzielona między więcej niż jednego ministra, każdy z koordynatorów będzie realizować wymienione wyżej zadania w stosunku do tych obiektów, które zostały uzgodnione z pozostałymi współkoordynatorami.

## 4.4. Inne organy administracji publicznej

### *4.4.1. Prezydent RP*

Prezydent RP, chociaż nie jest bezpośrednio zaangażowany w zadania na rzecz ochrony IK, ze względu na swoje kompetencje w obszarze bezpieczeństwa państwa jest ważnym elementem systemu ochrony IK. Jest gwarantem zaangażowania najwyższych władz państwowych w proces poprawy poziomu bezpieczeństwa IK i tym samym państwa.

Prezydent RP bierze udział w Programie w zakresie swoich konstytucyjnych kompetencji obejmujących bezpieczeństwo narodowe i obronność. Wspiera administrację rządową i samorządową w działaniach na rzecz ochrony IK oraz zmierzających do osiągnięcia celów Programu.

### *4.4.2. Rada Ministrów*

Rada Ministrów sprawuje władzę wykonawczą i kieruje administracją rządową. Zadania Rady Ministrów dotyczą wszystkich dziedzin życia politycznego, gospodarczego, społecznego oraz kulturalnego państwa, w tym zapewnienia bezpieczeństwa wewnętrznego i zewnętrznego państwa oraz porządku publicznego.

Rada Ministrów, przyjmując w drodze uchwały Narodowy Program Ochrony Infrastruktury Krytycznej, nadaje impuls działaniom zmierzającym do osiągnięcia jego celów realizowanych przez podległe jej organy i podmioty, a także poprzez funkcjonowanie Rządowego Zespołu Zarządzania Kryzysowego:

- czuwa nad przestrzeganiem zasad Programu i wypełnieniem jego postanowień,
- wskazuje kierunki działań innym podmiotom zaangażowanym w osiągnięcie celów Programu,
- wspiera i promuje działania na rzecz osiągnięcia celów Programu,
- umożliwia uzyskiwanie środków finansowych na ochronę IK, uwzględniając te zadania w budżecie państwa.

### *4.4.3. Ministrowie i kierownicy urzędów centralnych wykonujący zadania z zakresu zarządzania kryzysowego*

Rola pozostałych ministrów i kierowników urzędów centralnych, którzy nie są odpowiedzialni za systemy IK, polega na:

- wsparciu wiedzą działań zaangażowanych stron na rzecz osiągnięcia celów Programu,
- udziale w procesie oceny ryzyka wystąpienia sytuacji kryzysowej w państwie, wywołanej zakłóceniem funkcjonowania systemu IK,

- współpracy z podmiotami właściwymi w sprawach ochrony IK w zakresie wymiany informacji, dobrych praktyk, programów badań naukowych i prac rozwojowych i innych,
- wykonywaniu zadań określonych w ustawie o zarządzaniu kryzysowym.

### 4.4.4. Wojewodowie

Wojewodowie pełnią ważną rolę w systemie ochrony infrastruktury krytycznej i zarządzania kryzysowego. Zgodnie z obowiązującymi aktami prawnymi zadaniem wojewodów oraz komórek organizacyjnych właściwych w sprawach zarządzania kryzysowego w urzędzie wojewódzkim jest:

- organizowanie wykonania zadań z zakresu ochrony infrastruktury krytycznej, wynikających z faktu jej lokalizacji na terytorium województwa, w tym ujęcie tych zadań w wojewódzkich planach zarządzania kryzysowego,
- gromadzenie i przetwarzanie informacji dotyczących infrastruktury krytycznej zlokalizowanej na terenie województwa,
- przekazywanie, jeżeli istnieje potrzeba wynikająca z wojewódzkiego planu zarządzania kryzysowego, niezbędnej informacji o infrastrukturze krytycznej na terenie województwa właściwemu organowi administracji publicznej działającemu na tym terenie,
- uzgadnianie planów ochrony infrastruktury krytycznej operatorów IK.

Poziom wojewódzki stanowi punkt przejścia między systemowym i terytorialnym ujęciem zadań w zakresie ochrony infrastruktury krytycznej, a służby, straże i inspekcje podległe wojewodom są istotnym elementem planowania na wypadek zakłócenia funkcjonowania IK zlokalizowanej na terytorium województwa. W związku z powyższym wojewodowie, dążąc do osiągnięcia celów Programu, m.in.:

- organizują i obsługują regionalne forum ochrony IK i biorą udział w mechanizmie ochrony IK w zakresie opisanym w Programie,
- biorą udział w procesie oceny ryzyka wystąpienia sytuacji kryzysowej w państwie, wywołanej zniszczeniem lub zakłóceniem funkcjonowania IK zlokalizowanej na terytorium województwa, przez sporządzanie i aktualizowanie „Raportu cząstkowego o zagrożeniach bezpieczeństwa narodowego”,
- współpracują z samorządem wojewódzkim, powiatowym i gminnym w realizacji zadań z zakresu zarządzania kryzysowego i planowania cywilnego, wynikających z kompetencji samorządu województwa,
- współpracują z operatorami IK i podmiotami właściwymi w sprawach ochrony IK oraz wspierają działania zmierzające do osiągnięcia celów Programu.

### 4.4.5. Służby specjalne

Służby specjalne pełnią specyficzną rolę w ochronie IK. Posiadają w swojej dyspozycji rozwinięte siły i środki służące do identyfikacji zagrożeń intencjonalną działalnością człowieka. Wymiana informacji o tych zagrożeniach z operatorami IK i innymi podmiotami właściwymi w sprawach ochrony IK w sposób określony przepisami prawa i wewnętrznymi procedurami, w zakresie dopuszczonym przepisami o ochronie informacji niejawnych, jest kluczowa w procesie planowania ochrony IK.

Szczególna rola została przypisana Agencji Bezpieczeństwa Wewnętrznego. Zgodnie z art. 12a ustawy o zarządzaniu kryzysowym szef ABW, w przypadku podjęcia 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. Szef ABW informuje o powyższych działaniach dyrektora RCB oraz wspiera organy administracji publicznej w działaniach związanych z zapobieganiem, przeciwdziałaniem i usuwaniem skutków zdarzeń o charakterze terrorystycznym.

Organy administracji publicznej zobowiązane są do niezwłocznego przekazywania Szefowi Agencji Bezpieczeństwa Wewnętrznego będących w ich posiadaniu informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej.

### 4.4.6. Starostowie, wójtowie, burmistrzowie i prezydenci miast

Infrastruktura krytyczna jest fizycznie zlokalizowana na terenie gmin, miast i powiatów. W związku z tym starostowie, wójtowie, burmistrzowie i prezydenci miast oraz służby im podległe odgrywają istotną rolę w zakresie ochrony ludności narażonej na potencjalne skutki zakłócenia funkcjonowania IK oraz w zakresie ochrony IK, umożliwiając bezpośrednie i najszybsze wsparcie jej operatorów.

W zakresie ochrony infrastruktury krytycznej, zadaniem starostów, wójtów, burmistrzów i prezydentów miast jest organizowanie wykonania zadań z zakresu ochrony infrastruktury krytycznej, w szczególności:

- ujęcie zadań z zakresu ochrony infrastruktury krytycznej zlokalizowanej w obszarze właściwości w planach zarządzania kryzysowego,
- określanie procedur reagowania na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej w obszarze właściwości organu,
- ochrona ludności przed skutkami zakłócenia funkcjonowania IK z wykorzystaniem zasobów własnych oraz operatora IK,

- wsparcie operatorów IK technicznymi i ludzkimi zasobami pozostającymi w dyspozycji własnej oraz podległych lub nadzorowanych służb, inspekcji i straży,
- współpraca i wsparcie operatorów IK w zakresie jej ochrony i współdziałanie w przypadku wystąpienia sytuacji kryzysowej w obszarze właściwości organu,
- zapobieganie zagrożeniom życia i zdrowia obywateli powstałym na skutek zakłócenia funkcjonowania IK z wykorzystaniem rezerwy celowej tworzonej na podstawie art. 26 ust. 4 ustawy o zarządzaniu kryzysowym.

## 4.5. Środowisko naukowe

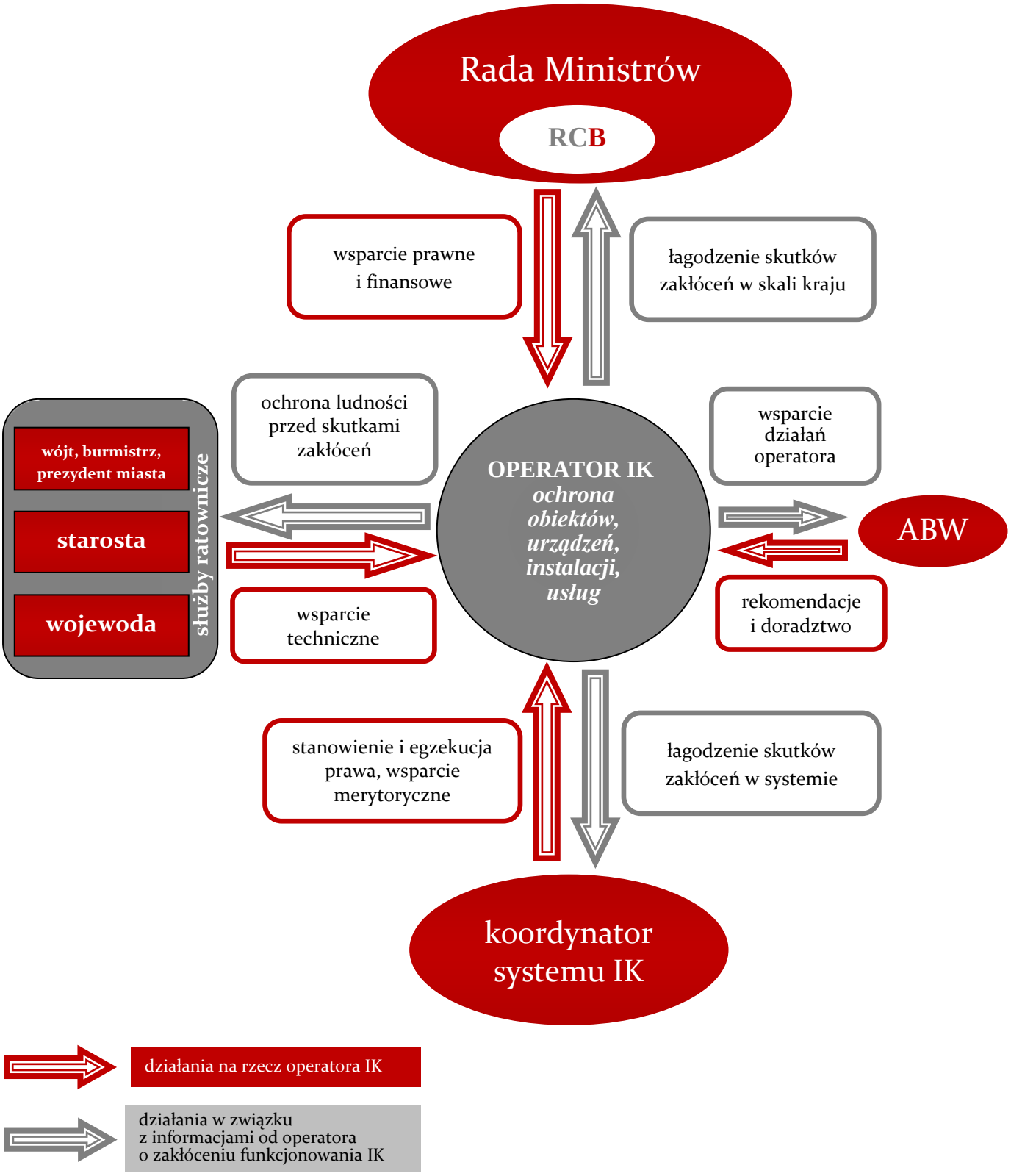
Dla realizacji Programu niezbędne jest opracowanie narzędzi pozwalających na efektywniejsze działanie wszystkich zainteresowanych stron. Jednostki i środowisko naukowe są źródłem wiedzy w tym zakresie oraz stanowią wsparcie eksperckie dla uczestników Programu.

Wsparcie obejmuje:

- zapewnienie niezależnej analizy i ekspertyz w zakresie ochrony IK,
- prowadzenie badań naukowych i prac rozwojowych w celu określenia nowych technologii i metod analitycznych, które mogą być stosowane przez uczestników Programu np. w zakresie oceny ryzyka zniszczenia lub zaprzestania funkcjonowania IK, oceny podatności IK na zagrożenia, oceny współzależności między systemami IK,
- testowanie, ocenę i wdrażanie technologii ochrony IK,
- przygotowanie wytycznych oraz opisy najlepszych praktyk w zakresie ochrony IK,
- działania promocyjne na rzecz osiągnięcia celów Programu.

Powyższe zadania mogą być realizowane w formie:

- projektów edukacyjnych i szkoleniowych,
- badań własnych uczelni,
- projektów badawczo-rozwojowych.




*Rys. 3. Główne podmioty uczestniczące w procesie ochrony IK i ich role.*

# 5. Ochrona infrastruktury krytycznej

Ochronę infrastruktury krytycznej należy pojmować jako proces zapewnienia 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.

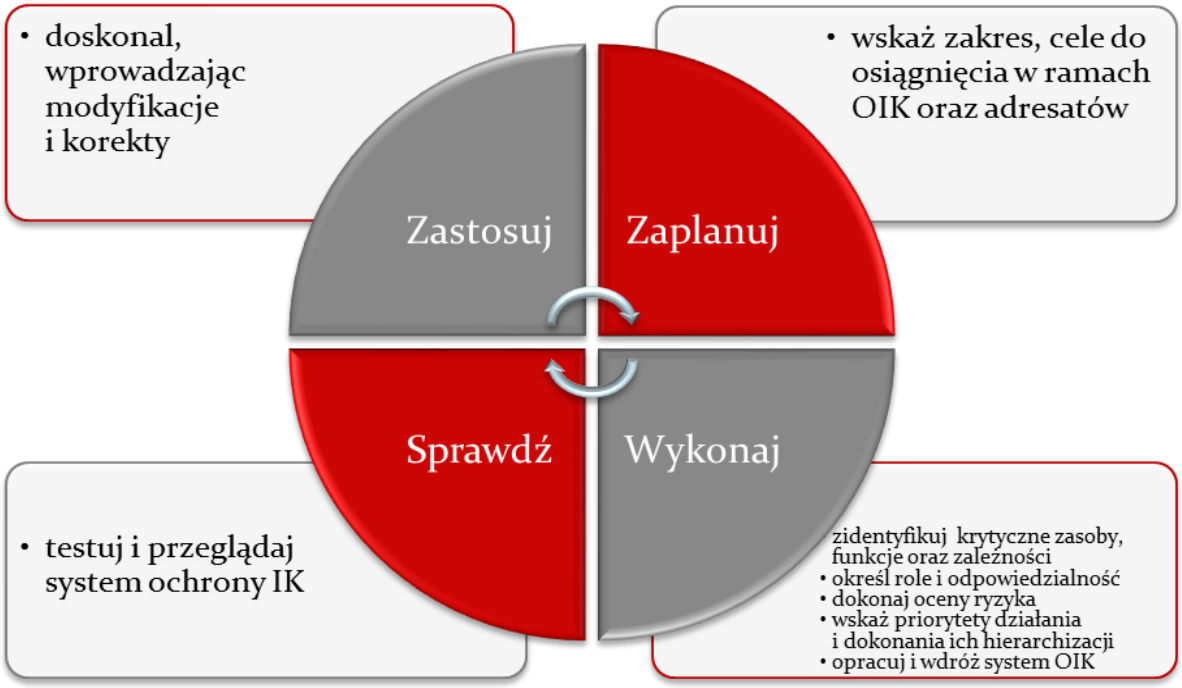
Tak rozumiany proces ochrony infrastruktury krytycznej składa się z następujących etapów:

1) wskazanie zakresu, celów do osiągnięcia w ramach ochrony IK oraz adresatów tych działań,
2) identyfikacja krytycznych zasobów, funkcji oraz określenia sieci powiązań (zależności) z innymi systemami IK, w tym podmiotami i organami,
3) określenie ról i odpowiedzialności uczestniczących w procesie ochrony IK,
4) ocena ryzyka,
5) wskazanie priorytetów działania i dokonania ich hierarchizacji w zależności od wyników oceny ryzyka,
6) rozwój i wdrażanie systemu ochrony infrastruktury krytycznej, w tym opracowania i akceptacji planów ochrony i odtwarzania IK,
7) testowanie (przez ćwiczenia) i przegląd (przez audyt i samoocenę) systemu ochrony IK oraz pomiar postępów na drodze do osiągnięcia celu,
8) doskonalenie, rozumiane jako wprowadzanie modyfikacji i korekt w wyniku testów, przeglądów i pomiarów.

Konieczność nieustannego doskonalenia pozwala na ujęcie procesu ochrony IK w cykl Deminga[4]. Ujęcie procesu ochrony IK w cykl pozwala, po dokonaniu pomiarów efektów, na podjęcie działań doskonalących lub korygujących na etapie, na którym stwierdzono odchylenie od oczekiwanych rezultatów. Możliwe jest również ponowne zdefiniowanie celów. Kolejne powtórzenia cyklu powinny przybliżać do ich osiągnięcia.

Cykl Deminga ma zastosowanie na każdym z poziomów, na którym odbywa się ochrona IK i powinien być powtarzany w ustalonych odstępach czasu.

[4] Znany także jako cykl ZWSZ (Zaplanuj-Wykonaj-Sprawdź-Zastosuj) z ang. *PDCA (Plan-Do-Check-Act)*.

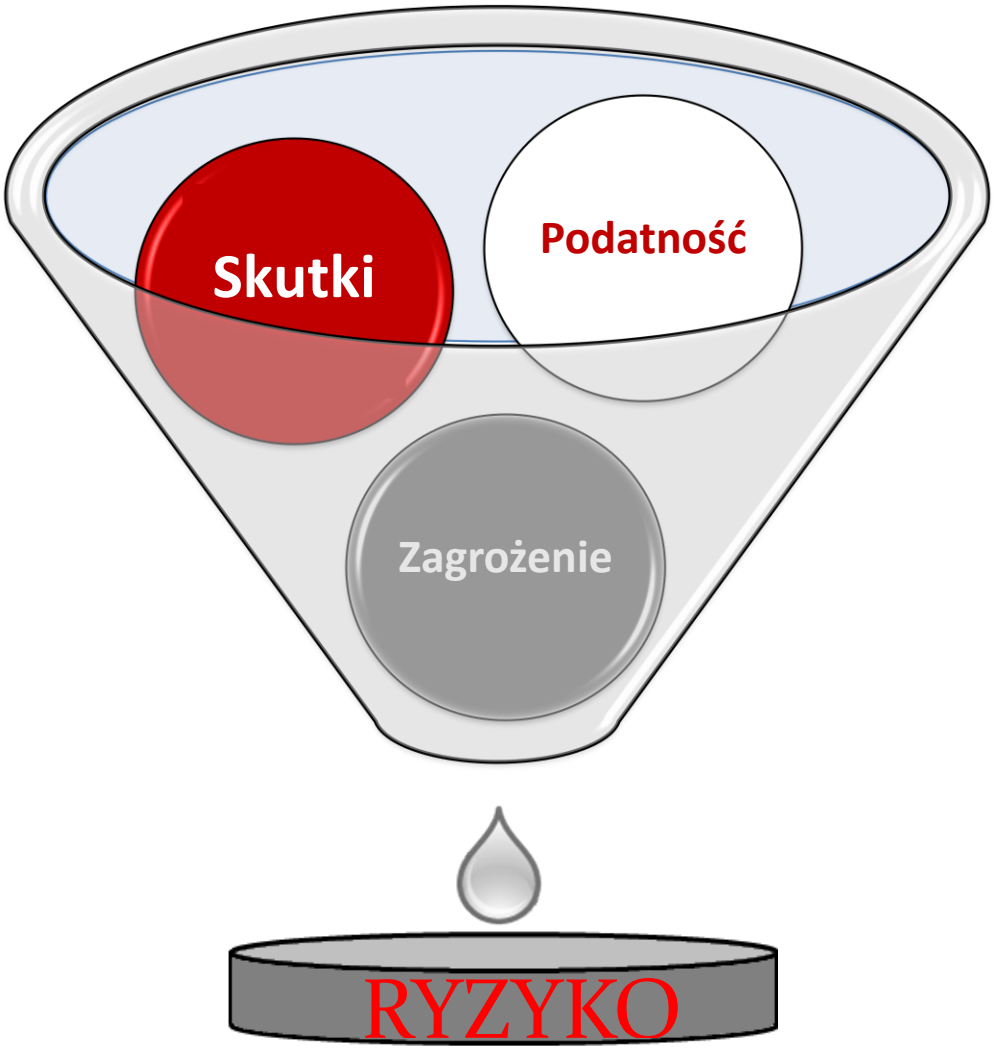



*Rys. 4. Proces ochrony IK w cyklu Deminga.*

Wszelkie działania podejmowane w celu zapewnienia ochrony IK powinny być proporcjonalne do poziomu ryzyka zakłócenia jej funkcjonowania. Dotyczy to zarówno przyjętego modelu ochrony IK, jej rodzajów, a także użytych sił i środków.

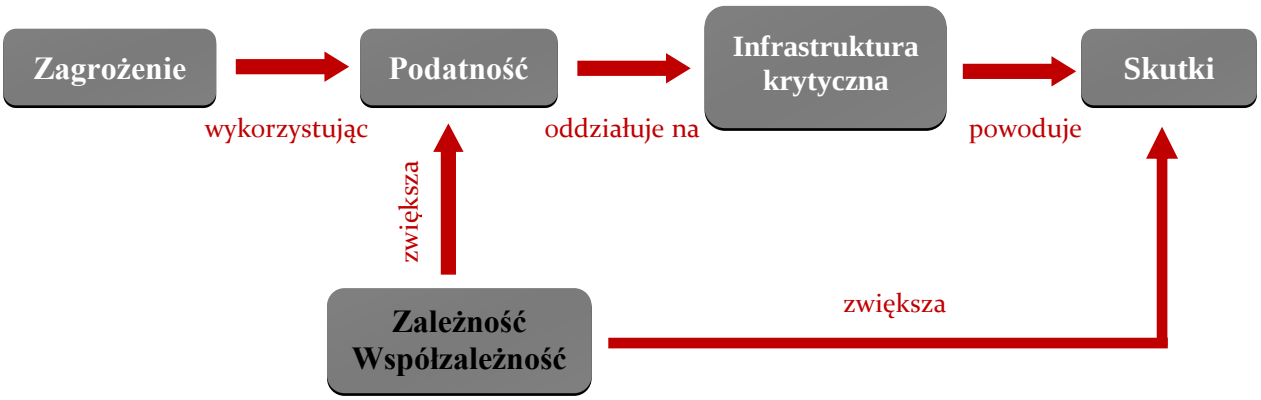
Z punktu widzenia Programu jest to element kluczowy, determinujący i uzasadniający działania podejmowane w celu obniżenia ryzyka zakłócenia funkcjonowania IK do poziomu akceptowalnego. Ocena ryzyka powinna być podstawą określenia standardów ochrony IK i ustalenia priorytetów działań.

W kontekście Programu ryzyko należy rozumieć jako funkcję zagrożenia, podatności oraz skutków, co ilustruje rysunek 5.




*Rys. 5. Ryzyko jako funkcja zagrożenia, podatności i skutków.*

Ocena ryzyka zakłócenia funkcjonowania IK wymaga dobrego zrozumienia związku między zagrożeniem, podatnością i skutkami. Związek ten przedstawia się następująco:




*Rys. 6. Związek między zagrożeniem, podatnością i skutkami.*

Ryzyko powinno zostać zaakceptowane przez jego właściciela. Decyzja o akceptacji ryzyka powinna uwzględniać najgorszy możliwy scenariusz.

Przeprowadzanie okresowej oceny ryzyka zakłócenia funkcjonowania infrastruktury krytycznej powinno się odbywać:

- wraz z identyfikacją nowych zagrożeń, które wpływają lub mogą wpłynąć na poprawne funkcjonowanie infrastruktury krytycznej,
- wraz z przeglądem (aktualizacją) planu ochrony infrastruktury krytycznej,
- w celu zapewnienia zgodności ze wszystkimi dokumentami rządowymi.

## 5.1. Zapewnienie bezpieczeństwa IK

System ochrony IK powinien mieć zastosowanie do wszystkich typów zidentyfikowanych zagrożeń, tak naturalnych, jak i intencjonalnych oraz technicznych, a także być przygotowany do możliwie szybkiego przywrócenia funkcji realizowanych przez daną IK. Ponadto powinna cechować go kompleksowość i elastyczność oraz, co nie mniej ważne, łatwość zastosowania i zrozumienia przez odpowiedzialnych za ochronę IK.

Działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia IK przez:

- zmniejszenie prawdopodobieństwa wystąpienia zagrożenia,
- zmniejszanie podatności,
- minimalizowanie skutków wystąpienia zagrożenia.

Na te działania składają się:

1) zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych 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;
2) zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
4) zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka

zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;

5) zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;

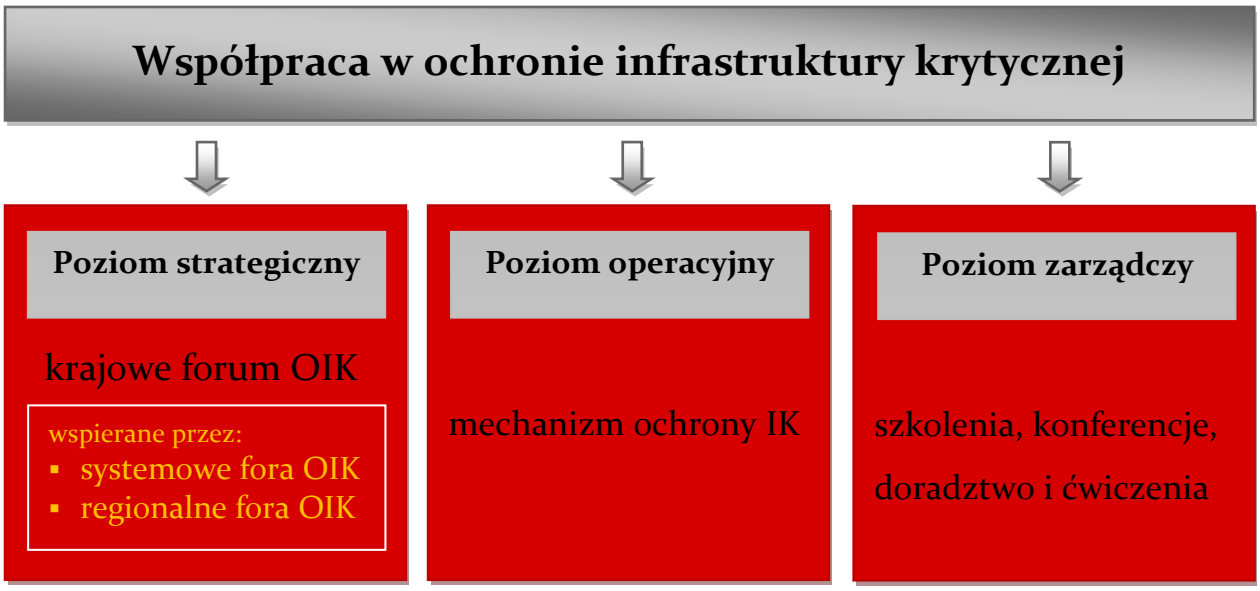
6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

Zastosowanie konkretnych środków zapewnienia bezpieczeństwa powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK.

## 5.2. Współpraca w ochronie infrastruktury krytycznej

Współpraca, jako jedna z najważniejszych zasad Programu, jest kluczowym elementem zapewniającym spójność podejmowanych decyzji i skuteczność realizowanych działań zarówno w toku bieżącej pracy, jak i w sytuacjach wystąpienia zagrożeń. Aby była efektywna, powinna być prowadzona na poziomie krajowym, systemowym, regionalnym i lokalnym, a także angażować operatorów infrastruktury krytycznej, bez względu na ich formę własności. Wymaga również ustanowienia mechanizmów w celu jej ułatwienia. Warunkiem skutecznej współpracy są jej autentyczność, wzajemność i dążenie do wspólnej korzyści.

Przez współpracę w obszarze IK rozumie się wymianę wszelkich informacji mogących mieć wpływ na osiągnięcie celów Programu i utrzymywanie stałych kontaktów między uczestnikami procesu ochrony IK.




*Rys. 7. Model współpracy w ochronie IK.*

Funkcjonalnie skonfigurowana wymiana informacji w zakresie ochrony infrastruktury krytycznej będzie odbywać się w trzech obszarach:

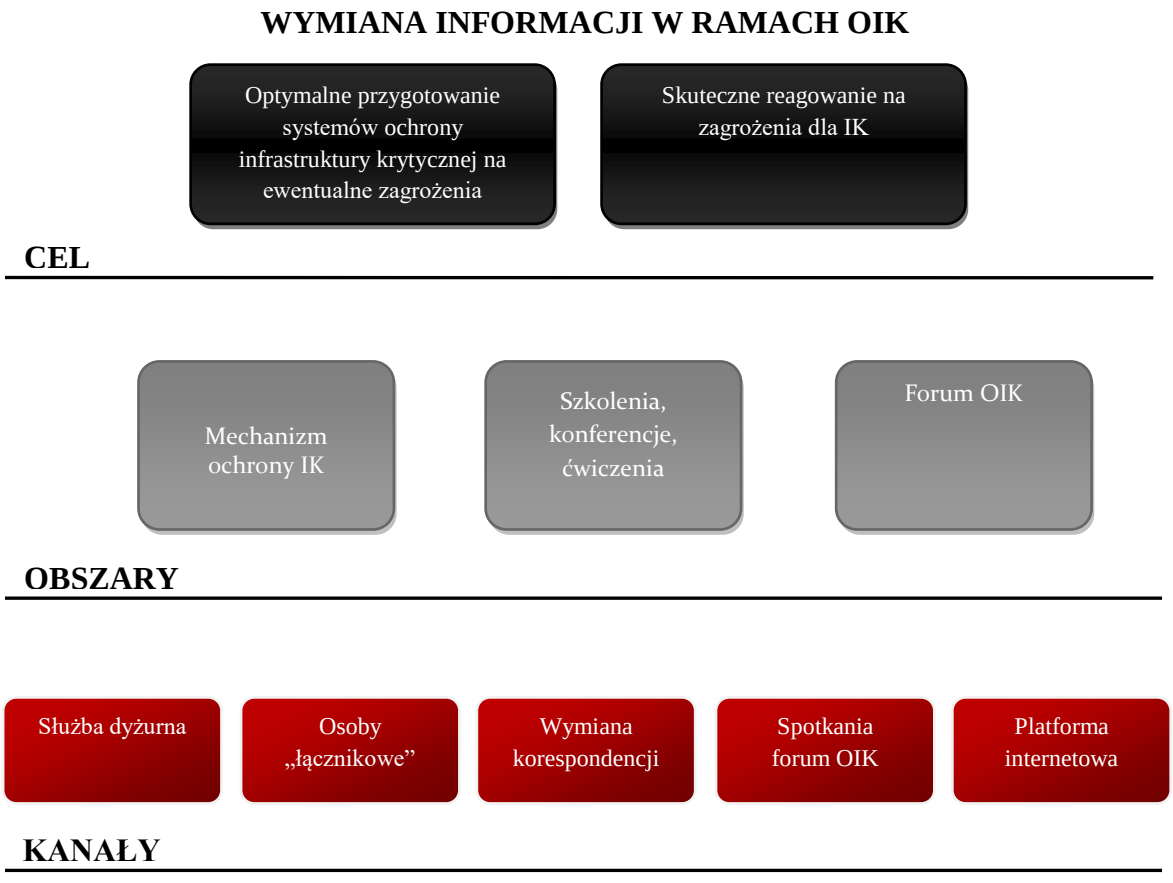
1) forum ochrony infrastruktury krytycznej,
2) bieżąca wymiana informacji przez bezpośrednie kontakty stron (mechanizm ochrony IK),
3) wspólne szkolenia, konferencje, doradztwo i organizacja ćwiczeń.

Stronami w ramach omawianej wymiany informacji będą operatorzy IK oraz administracja publiczna. Do współpracy mogą być zapraszani eksperci reprezentujący

różne dziedziny nauki oraz praktycy, których wiedza może stanowić wartość dodaną w ramach realizacji zadań związanych z OIK.

Wymiana informacji prowadzona będzie wielotorowo, przez:

- działające całodobowo centra zarządzania kryzysowego oraz służby dyżurne, w ramach systemu zarządzania kryzysowego,
- bieżące, bezpośrednie kontakty przedstawicieli stron,
- wymianę korespondencji jawnej i niejawnej w tradycyjny sposób i z wykorzystaniem elektronicznych systemów wymiany informacji jawnych i niejawnych,
- cykliczne, wspólne spotkania w ramach forów ochrony infrastruktury krytycznej,
- wspólną platformę internetową stworzoną specjalnie dla celów wymiany informacji, prezentowania doświadczeń i wiedzy z zakresu OIK, współpracy w ramach forum, organizacji spotkań, szkoleń itp.




*Rys. 8. Wymiana informacji w ramach ochrony IK – ujęcie funkcjonalne.*

Współpraca w ramach wymienionych obszarów ma na celu:

- zwiększenie poziomu bezpieczeństwa i niezawodności infrastruktury krytycznej przez:
  - uzyskanie efektu synergii w działaniach operatorów IK i administracji publicznej,
  - efektywne wykorzystanie sił i środków przeznaczanych na ochronę infrastruktury krytycznej,
  - zapewnienie wymiany informacji między operatorami IK i administracją publiczną;
- zwiększenie zaufania do operatorów jako firm odpowiedzialnych społecznie przez udział w przedsięwzięciu mającym na celu poprawę bezpieczeństwa systemów istotnych dla funkcjonowania społeczeństwa w ujęciu ogólnopolskim i lokalnym;
- wypromowanie idei partnerstwa publiczno-prywatnego przez:
  - ukazanie praktycznych zalet współpracy między sektorem publicznym i prywatnym,
  - identyfikację i realizację wspólnych interesów sektora publicznego i prywatnego.

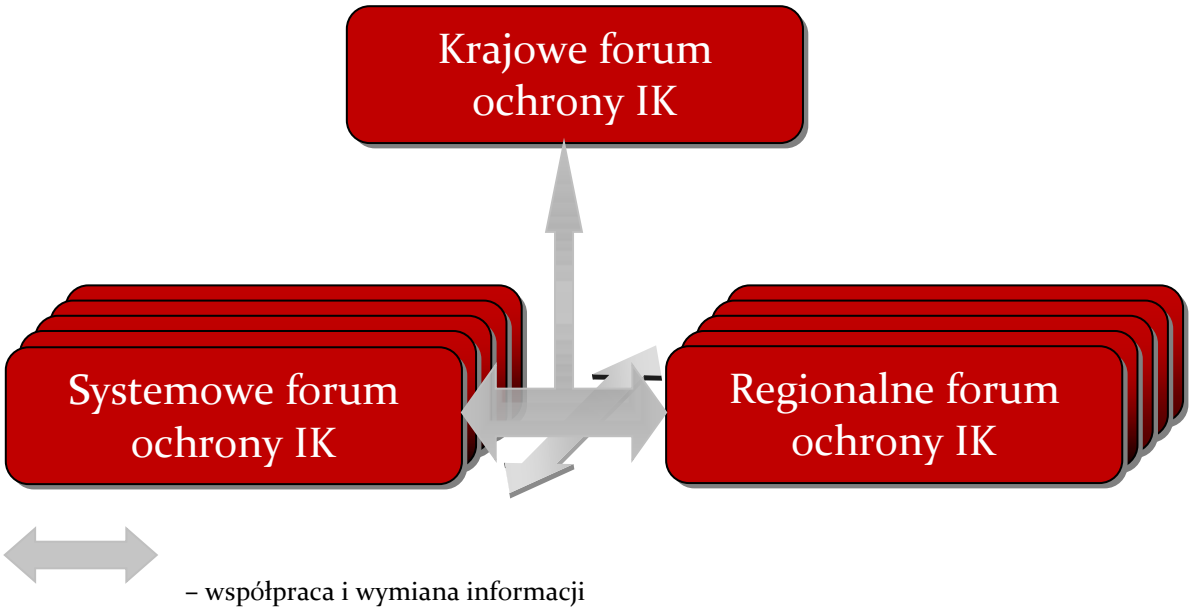
### *5.2.1. Forum ochrony infrastruktury krytycznej*

Administracja ma możliwość gromadzenia uczestników ochrony IK w niezależnym od uwarunkowań biznesowych środowisku, pozwalającym na dyskusję o współzależnościach systemów IK, międzysystemowych podatnościach i kwestiach będących we właściwości wielu uczestników ochrony IK.

W związku z tym przewiduje się utworzenie na trzech poziomach forów ochrony IK:

- forum krajowego,
- forów systemowych – dla każdego systemu IK,
- forów regionalnych (wojewódzkich) – mających charakter międzysystemowy.

Fora będą budowane w możliwie jak najszerszym zakresie na bazie istniejących form koordynacji i konsultacji. Program, uznając różnice między systemami i ich specyfikę, nie określa struktury forum. Sieć forów systemowych odzwierciedla model partnerstwa, które umożliwi administracji i operatorom infrastruktury krytycznej podjęcie szeregu działań (np. oceny ryzyka, ćwiczeń) w sposób uwzględniający charakterystykę każdego z systemów. Celem forum jest identyfikacja kluczowych problemów z zakresu ochrony infrastruktury krytycznej oraz inicjowanie prac mających na celu wypracowywanie propozycji rozwiązań.




*Rys. 9. Schemat funkcjonowania forów ochrony IK.*

#### 5.2.1.1. Organizacja forum

Uczestnikami forum są przedstawiciele operatorów infrastruktury krytycznej i administracji publicznej. Do prac forum mogą być zapraszani przedstawiciele świata nauki i mediów, organizacji branżowych itp. Obsługę krajowego forum zapewnia Rządowe Centrum Bezpieczeństwa (w przypadku forów systemowych – minister odpowiedzialny za dany system, w przypadku forum regionalnego właściwy terytorialnie wojewoda). Przewodniczącym krajowego forum jest dyrektor RCB (odpowiednio: przewodniczącym forum systemowego jest minister lub kierownik urzędu centralnego odpowiedzialny za dany system, regionalnego właściwy terytorialnie wojewoda). Fora zbierają się:

- krajowe, raz w roku lub częściej, zależnie od okoliczności,
- systemowe, dwa razy w roku lub częściej, zależnie od okoliczności,
- wojewódzkie, trzy razy w roku lub częściej, zależnie od okoliczności – forum wojewódzkie zbiera się w pełnym składzie przynajmniej raz w roku. Pozostałe posiedzenia mogą mieć charakter branżowy lub tematyczny.

#### 5.2.1.2. Funkcjonowanie forum

Forum jest miejscem dyskusji na tematy mające strategiczne znaczenie dla ochrony infrastruktury krytycznej tj.:

1) określenie rodzaju i szczegółowości informacji przekazywanych między operatorami i administracją publiczną,
2) określenie zakresu możliwego wsparcia udzielanego przez służby państwowe na rzecz operatorów w przypadku zwiększenia poziomu zagrożeń dla IK,
3) udział w pracach nad Narodowym Programem Ochrony Infrastruktury Krytycznej,
4) identyfikacja zależności i współzależności występujących w ochronie infrastruktury krytycznej, w tym między organami administracji publicznej,
5) udział w opracowaniu strategii partnerstwa publiczno-prywatnego w zakresie OIK realizowanego na poziomie centralnym, systemowym, regionalnym (wojewódzkim) i lokalnym (powiatowym i gminnym),
6) określenie działań koniecznych do podjęcia przez administrację publiczną w celu zwiększenia poziomu ochrony infrastruktury krytycznej (m.in. przez działania legislacyjne i administracyjne),
7) wypracowanie opinii dotyczących strategicznych działań Rządu mogących mieć wpływ na bezpieczeństwo funkcjonowania infrastruktury krytycznej,
8) określenie priorytetów i celów badań naukowych z zakresu ochrony infrastruktury krytycznej finansowanych ze środków publicznych (forum krajowe),
9) wypracowanie form współpracy i wsparcia w odtwarzaniu IK.

Prace zainicjowane podczas obrad forum są kontynuowane poza jego posiedzeniami.

### *5.2.2. Mechanizm ochrony IK (bieżąca wymiana informacji)*

Bieżąca wymiana informacji obejmuje:

a) przekazywanie operatorom informacji dotyczących zagrożeń infrastruktury krytycznej,
b) przekazywanie przez właścicieli oraz posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej informacji o zidentyfikowanych zagrożeniach zarządzanej przez nich infrastruktury,
c) przekazywanie informacji o spodziewanym lub zaobserwowanym zwiększeniu zapotrzebowania na usługi lub produkty dostarczane przez operatorów,
d) funkcjonowanie platformy internetowej.

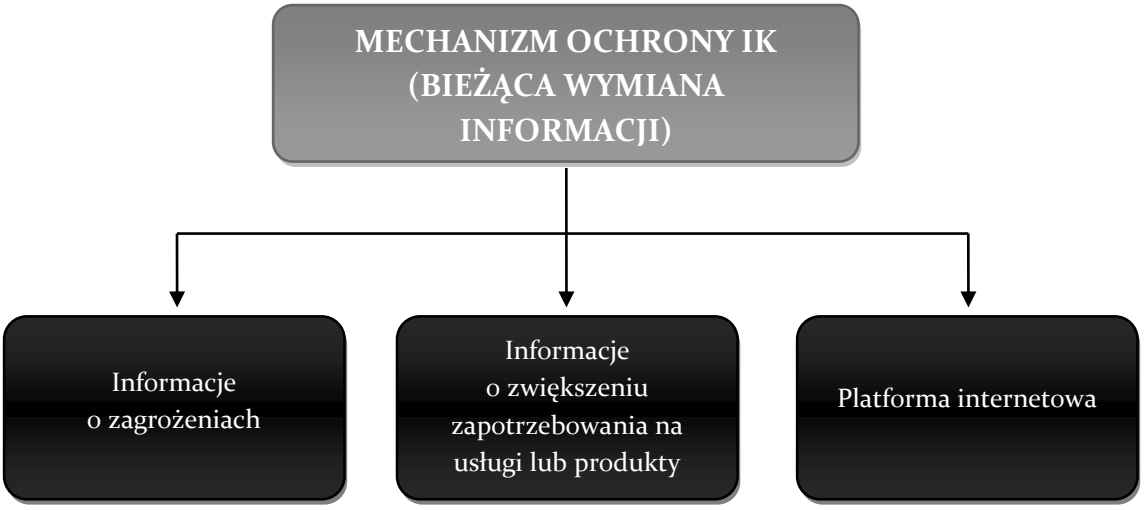
Platforma internetowa funkcjonuje jako platforma wymiany informacji na temat zagrożeń i podatności, a także jako platforma opracowania wytycznych do strategii i rozwiązań zmniejszających ryzyko zakłócenia funkcjonowania IK, które mogą być

później przedstawiane podczas obrad forów ochrony IK. Członkami platformy są operatorzy infrastruktury krytycznej, przedstawiciele organów administracji publicznej, agencji rządowych, a także inne zaangażowane podmioty.

O tym, jakie informacje są wymieniane w ramach internetowej platformy, decydują sami jej członkowie. Wymiana informacji o zagrożeniach czy zidentyfikowanych podatnościach może korzystnie wpływać na wizerunek wszystkich podmiotów systemu IK, oznaczając dojrzałość w podejściu do prowadzenia działalności gospodarczej i zwiększając zaufanie klientów do wszystkich podmiotów.

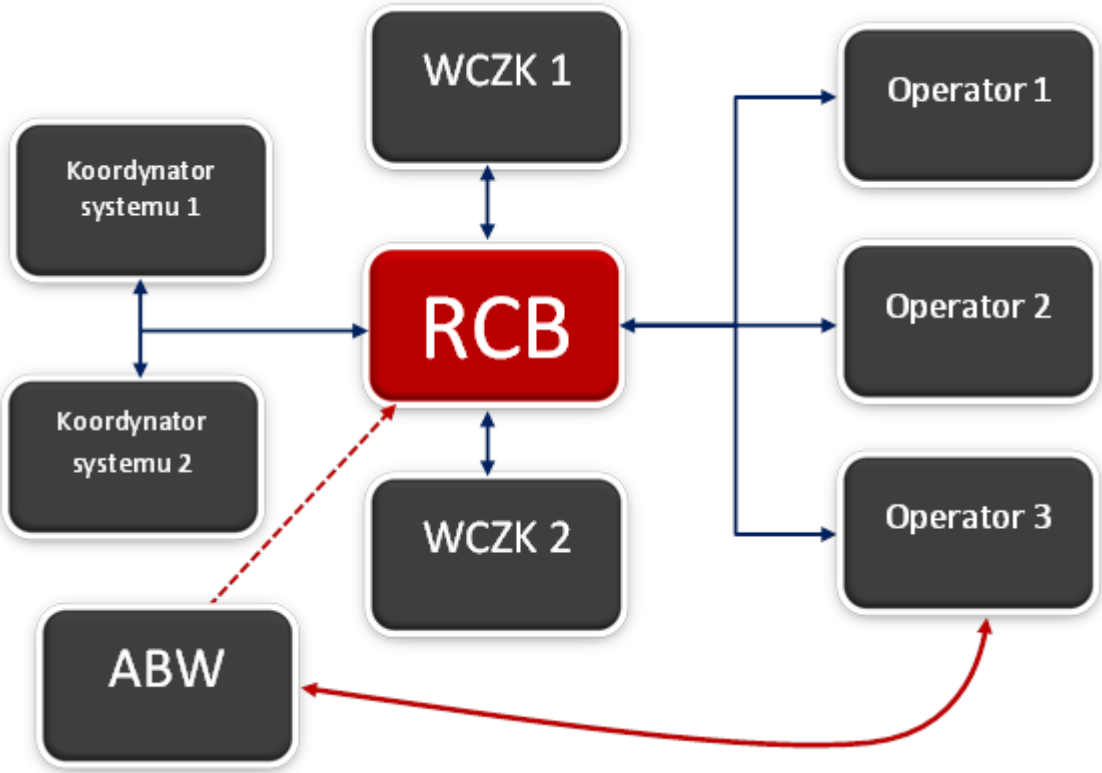
Duże znaczenie ma bezpieczeństwo informacji wymienianych w ramach platformy. Administracja publiczna podejmie wszelkie działania zmierzające do zapewnienia odpowiedniego poziomu ochrony i zaufania w zakresie dostępu osób postronnych i ochrony tajemnicy przedsiębiorstwa.

W ramach mechanizmu w jednostkach administracji publicznej powołane zostaną punkty kontaktowe (osoby mające za zadanie utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej i operatorami IK), podobnie jak ma to miejsce w stosunku do operatorów IK. Punkty kontaktowe są elementem systemu komunikacji instytucji związanych z ochroną IK.




*Rys. 10. Funkcjonowanie mechanizmu współpracy w OIK.*

Aktualna informacja o zagrożeniach dla obiektów IK oraz zagrożeniach dla bezpieczeństwa państwa i obywateli będących skutkiem zakłócenia funkcjonowania IK ma decydujące znaczenie dla właściwej reakcji na te zagrożenia. Dlatego RCB stanowi pierwszy punkt komunikacji pomiędzy operatorami IK, wojewodami, koordynatorami systemów IK oraz innymi podmiotami - rolę tę pełni centrum operacyjne RCB. Uczestnicy Programu oraz podmioty zaangażowane w mechanizm ochrony IK wymieniają informacje o zagrożeniach wg poniższego schematu:




informacje o zagrożeniach terrorystycznych (na podst. art. 12a ustawy o zarządzaniu kryzysowym)

informacje o pozostałych zagrożeniach

*Rys. 11.* Schemat komunikacji

### 5.2.3. *Szkolenia, konferencje, doradztwo*

W celu zapewnienia sprawnej i rzetelnej wymiany informacji między uczestnikami mechanizmu ochrony IK, konieczne jest wsparcie działań podejmowanych w ramach forów ochrony IK działaniami o charakterze szkoleniowym. Działania te obejmują:

a) udzielanie wzajemnego wsparcia merytorycznego (na zasadzie doradztwa oraz szkoleń) przez podmioty administracji publicznej oraz operatorów IK,
b) udział operatorów IK i podmiotów administracji w ćwiczeniach z zakresu ochrony infrastruktury krytycznej,
c) udział operatorów IK i podmiotów administracji w konferencjach z zakresu ochrony infrastruktury krytycznej,
d) integrację środowisk odpowiedzialnych za ochronę infrastruktury krytycznej.

#### 5.2.3.1. Ćwiczenia z zakresu ochrony infrastruktury krytycznej

Ćwiczenia są najskuteczniejszą formą szkolenia. Umożliwiają kompleksowe opanowanie i utrzymanie wysokiego poziomu wiedzy i praktycznych umiejętności szkolonych. Mają na celu wyrabianie, utrwalanie i doskonalenie nawyków niezbędnych w procesie kierowania realizacją zadań przez osoby funkcyjne i zespoły ludzkie wszystkich szczebli. Stwarzają warunki do trafnego wyboru skutecznych form i metod działania w różnorodnych sytuacjach, głównie przy podejmowaniu i realizacji określonych decyzji oraz kierowaniu podległymi ogniwami. Prowadzone będą na wszystkich szczeblach administracji publicznej i w sektorze prywatnym.

Ćwiczenia mają na celu:

1) praktyczne sprawdzenie poprawności działania systemu ochrony IK,
2) przygotowanie osób, którym powierzono wykonywanie zadań w ramach ochrony infrastruktury krytycznej, a także osób uczestniczących w wykonywaniu tych zadań,
3) kształtowanie umiejętności współdziałania organów i jednostek organizacyjnych zapewniających bezpieczeństwo IK z odpowiednimi służbami, instytucjami i organami administracji rządowej,
4) kształtowanie świadomości na temat zagrożeń i adekwatnych sposobów reagowania u osób podlegających ćwiczeniom.

Ćwiczenia z zakresu ochrony IK mogą przyjąć formę:

1) testów gotowości (sprawdzenie czasu reakcji),
2) testów standardowych procedur operacyjnych (np. procedur wymiany informacji),
3) ćwiczeń sztabowych *(table-top)*,
4) ćwiczeń praktycznych,
5) gier decyzyjnych.

W ćwiczeniach uczestniczą:

1) osoby zajmujące kierownicze stanowiska w administracji publicznej, w szczególności:
   a) ministrowie (sekretarze stanu lub podsekretarze stanu), osoby będące centralnymi organami administracji rządowej lub ich zastępcy, kierownicy państwowych jednostek organizacyjnych lub ich zastępcy, a także wojewodowie lub ich zastępcy,
   b) marszałkowie województw, prezydenci miast, burmistrzowie, starostowie i wójtowie (lub zastępcy wcześniej wymienionych) oraz podległe im lub nadzorowane służby, inspekcje i straże,
   c) dyrektorzy generalni lub ich zastępcy, dyrektorzy departamentów lub ich zastępcy, kierownicy biur w urzędach obsługujących ministrów, urzędach centralnych i innych państwowych jednostkach organizacyjnych

wykonujących zadania z zakresu ochrony infrastruktury krytycznej, a także dyrektorzy wydziałów w urzędach wojewódzkich lub ich zastępcy,

2) pracownicy komórek organizacyjnych kierowanych przez osoby zajmujące stanowiska, o których mowa w pkt 1 lit. c, zatrudnieni na stanowiskach związanych z ochroną infrastruktury krytycznej,
3) właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej, a także wyznaczeni przez nich pracownicy.

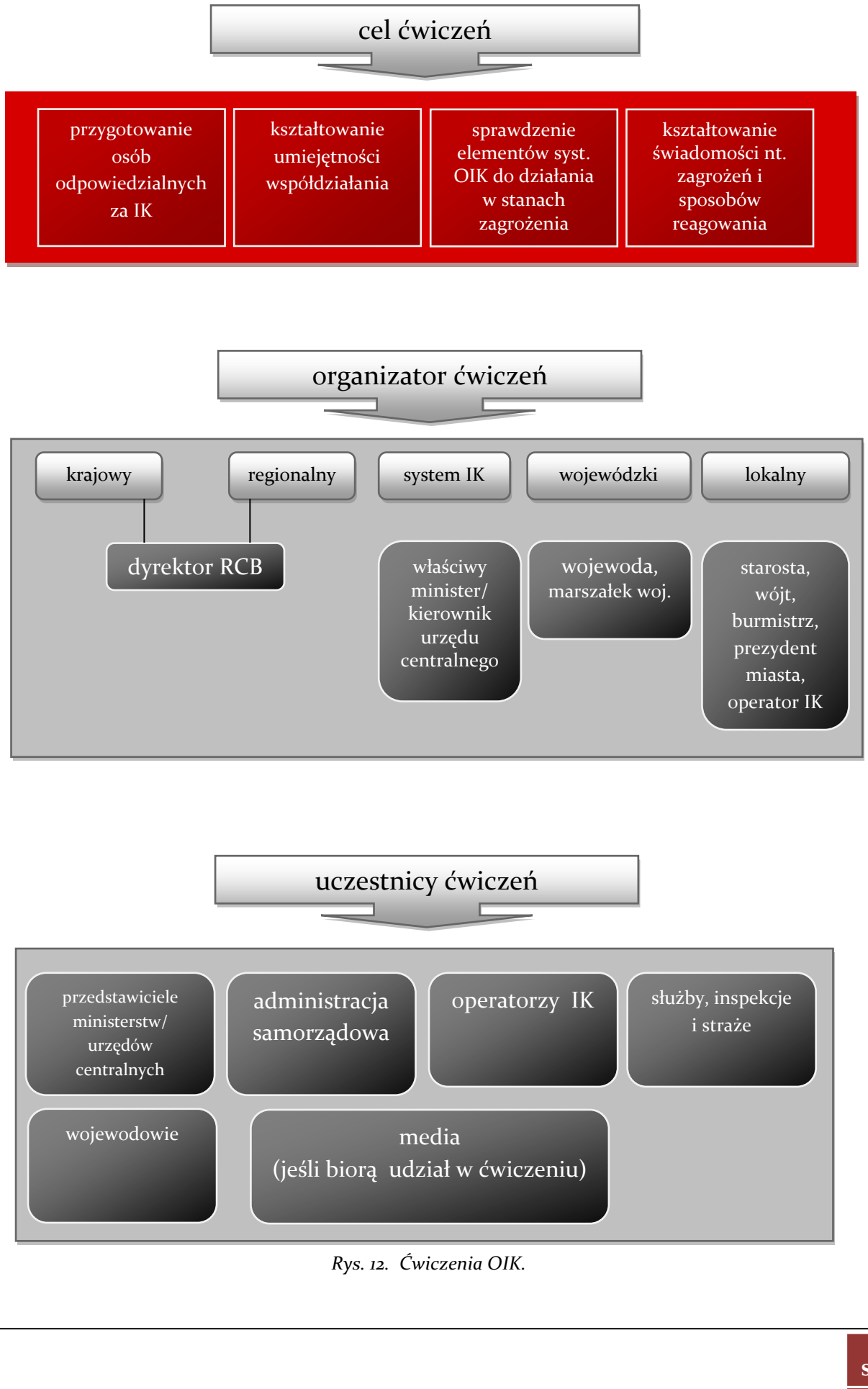
Ćwiczenia są również dostępne dla:

1) przedstawicieli świata nauki oraz stowarzyszeń i związków branżowych – jeżeli ćwiczenie przewiduje ich udział,
2) przedstawicieli mediów – jeżeli ćwiczenie przewiduje ich udział,
3) innych osób niewymienionych w pkt. 1.

Organizatorami ćwiczenia są:

1) dyrektor Rządowego Centrum Bezpieczeństwa – w odniesieniu do ćwiczenia prowadzonego w formie:
   a) ćwiczeń o zasięgu krajowym,
   b) ćwiczeń regionalnych, obejmujących obszar dwóch lub więcej województw,
2) minister odpowiedzialny za system IK – w odniesieniu do ćwiczeń organizowanych w ramach kierowanego przez siebie systemu IK,
3) wojewoda – w odniesieniu do ćwiczenia organizowanego w województwie, prowadzonego w formie ćwiczeń wojewódzkich, obejmujących dwa lub więcej powiatów na obszarze województwa,
4) prezydent miasta, burmistrz, starosta i wójt – w odniesieniu do ćwiczenia w samorządzie terytorialnym, odpowiednio województwa, powiatowym i gminnym, prowadzonego w formie ćwiczeń terenowych lub wojewódzkich,
5) operatorzy IK – w odniesieniu do ćwiczeń organizowanych w posiadanych obiektach, instalacjach lub urządzeniach infrastruktury krytycznej.

Ćwiczenia zawierające elementy ochrony infrastruktury krytycznej powinny być organizowane przynajmniej raz na 2 lata. Wnioski i rekomendacje z ćwiczeń stanowią przedmiot obrad forów ochrony IK na właściwym poziomie.




*Rys. 12. Ćwiczenia OIK.*

# 6. Plan działań w 2-letnim okresie po przyjęciu przez Radę Ministrów aktualizacji NPOIK

W ujęciu przedmiotowym plan działań obejmuje:

a) działania organizacyjno-prawne,
b) działania techniczne,
c) działania edukacyjne i szkoleniowe.

## 6.1. Działania organizacyjno-prawne

Działania organizacyjno-prawne obejmują:

1) opracowanie procedur prowadzenia kontroli i audytów wewnętrznych (wiodący: RCB, wspierający: koordynatorzy systemów IK + operatorzy IK);
2) opracowanie metodyki oceny ryzyka zakłócenia funkcjonowania IK i identyfikacji zależności między systemami IK (wiodący: RCB, wspierający: koordynatorzy systemów IK + operatorzy IK);
3) opracowanie procedury komunikacji w przypadku wystąpienia zagrożeń dla IK (wiodący: RCB, wspierający: koordynatorzy systemów IK + operatorzy IK).

## 6.2. Działania techniczne

Działania techniczne obejmują:

1) uruchomienie grup roboczych do opracowania minimalnych standardów w zakresie zapewnienia bezpieczeństwa IK (wiodący: RCB, wspierający: operatorzy IK);
2) weryfikacja skuteczności metodyki identyfikacji obiektów IK (wiodący: RCB, wspierający: koordynatorzy systemów IK + operatorzy IK);
3) uruchomienie bazy danych o incydentach w obiektach IK (wiodący: RCB, wspierający: wojewodowie + operatorzy IK);
4) uruchomienie platformy szkoleniowej dla operatorów IK i administracji publicznej (wiodący: RCB).

## 6.3. Działania edukacyjne i szkoleniowe

Działania edukacyjne i szkoleniowe obejmują:

1) opracowanie programu szkolenia podstawowego z zakresu ochrony IK oraz przygotowanie materiałów dydaktycznych do samokształcenia dla operatorów IK i administracji publicznej (wiodący: RCB, wspierający: koordynatorzy systemów IK + operatorzy IK);
2) opracowanie i wydawanie broszur informacyjnych oraz poradników z zakresu ochrony IK dla operatorów IK i administracji publicznej (wiodący: RCB + koordynatorzy systemów IK, wspierający: operatorzy IK);
3) przeprowadzenie pilotażowych ćwiczeń z zakresu ochrony IK w jednym z obiektów IK (wiodący: RCB, wspierający: koordynator wybranego systemu IK + operatorzy IK).

## 6.4. Koordynacja wdrożenia Programu

Koordynatorem wdrożenia Narodowego Programu Ochrony Infrastruktury Krytycznej jest dyrektor Rządowego Centrum Bezpieczeństwa.

We współpracy ze wszystkimi zainteresowanymi stronami, kierując się zasadami Programu, RCB wprowadzać będzie w życie postanowienia Programu. Dyrektor RCB, z uwzględnieniem informacji otrzymanych od ministrów odpowiedzialnych za systemy IK oraz wojewodów, przedstawia corocznie ocenę skuteczności Programu na posiedzeniu Rady Ministrów.

Ponadto, biorąc pod uwagę fakt, że Rządowe Centrum Bezpieczeństwa jest krajowym punktem kontaktowym dla instytucji Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz ich krajów członkowskich w zakresie ochrony infrastruktury krytycznej oraz europejskiej infrastruktury krytycznej, będzie ono koordynować w kraju regulacje, postanowienia i podjęte zobowiązania RP dotyczące ochrony IK.

## 6.5. Finansowanie działań z zakresu ochrony IK

Działania z zakresu ochrony IK są finansowane ze środków własnych uczestników Programu i planowane w ich budżetach:

- w przypadku administracji na podstawie art. 26 ust. 1 i 2 ustawy o zarządzaniu kryzysowym,
- w przypadku operatorów IK na podstawie art. 6 ust. 5 ustawy o zarządzaniu kryzysowym.

# 7. Międzynarodowy aspekt ochrony infrastruktury krytycznej

## 7.1. Europejska infrastruktura krytyczna

Działania z zakresu ochrony infrastruktury krytycznej prowadzone na szczeblu krajowym wpisują się w szerszy kontekst europejski, czego przejawem jest wdrażany na forum Unii Europejskiej Europejski Program Ochrony Infrastruktury Krytycznej (EPOIK).

Na działania w ramach Europejskiego Programu Ochrony Infrastruktury Krytycznej składają się:

- dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony,
- instrumenty finansujące działania z zakresu ochrony infrastruktury krytycznej – w latach 2007–2013: program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa" – CIPS, w latach 2014-2020 instrument „Fundusz Bezpieczeństwa Wewnętrznego" – ISF,
- działania wspomagające państwa członkowskie w implementacji dyrektywy (m.in. system wymiany informacji – CIWIN),
- wymiar zewnętrzny – koncepcja współpracy z państwami trzecimi, na których terytorium zlokalizowana jest infrastruktura, która w przypadku wystąpienia zakłóceń lub zniszczenia może mieć wpływ na infrastrukturę państw członkowskich (konkluzje Rady w sprawie rozwoju zewnętrznego wymiaru Europejskiego Programu Ochrony Infrastruktury Krytycznej),
- możliwa pomoc państwom członkowskim w pracach nad rozwiązaniami krajowymi z zakresu IK,

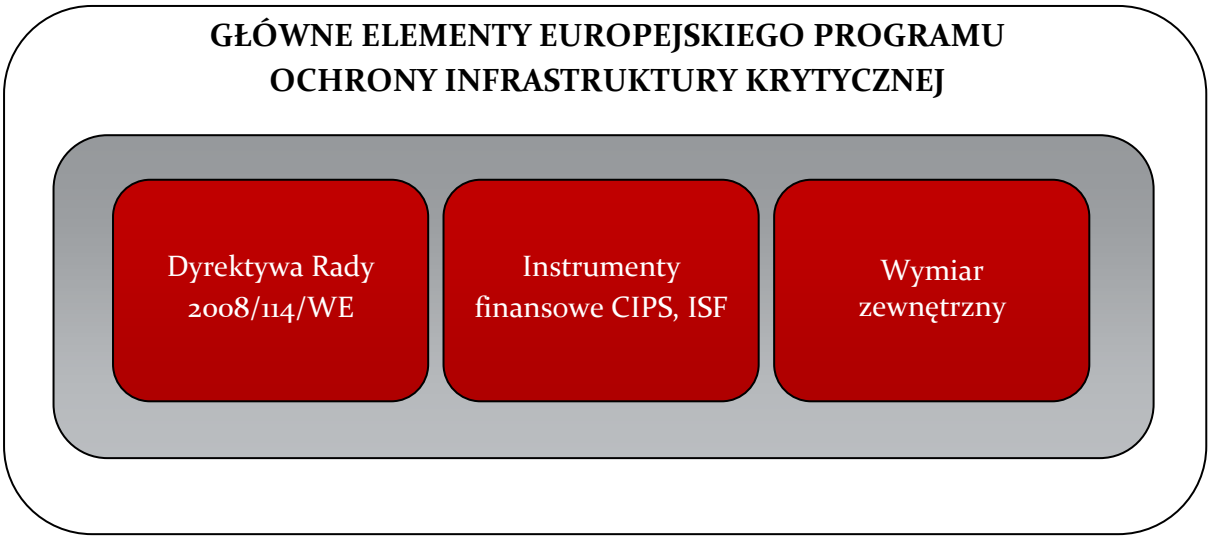
Najważniejszym elementem EPOIK jest wymieniona powyżej dyrektywa, która wyznacza proces rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej. Jednocześnie zapewnia ona wspólne podejście do oceny potrzeb poprawy ochrony tej infrastruktury.

Dyrektywa w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony określa europejską infrastrukturę krytyczną jako infrastrukturę 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.

Europejska infrastruktura krytyczna wyznaczana jest w dwóch sektorach – sektorze energii i sektorze transportu.

W 2013 roku, po dokonaniu przeglądu dyrektywy i EPOIK Komisja przyjęła „Dokument Roboczy Komisji w sprawie nowego podejścia do Europejskiego Programu Ochrony Infrastruktury Krytycznej" (SWD(2013) 318) uszczegóławiający kierunki prac uczestników programu w kolejnych latach.

Polska aktywnie uczestniczy w przedsięwzięciach realizowanych w ramach EPOIK. Rolę koordynatora tych działań, jako krajowy punkt kontaktowy, pełni Rządowe Centrum Bezpieczeństwa.




*Rys. 13. Elementy Europejskiego Programu Ochrony Infrastruktury Krytycznej.*

## 7.2. Współpraca międzynarodowa w zakresie ochrony IK

Rządowe Centrum Bezpieczeństwa, Ministerstwo Spraw Zagranicznych, koordynatorzy systemów IK oraz lokalne władze współpracują z innymi krajami oraz organizacjami międzynarodowymi w zakresie ochrony IK.

O efektach tej współpracy podmioty prowadzące będą informować się wzajemnie, a także uczestników forów i mechanizmu ochrony IK.

# 8. Ocena skuteczności Programu

Biorąc pod uwagę fakt, że pomiar bezpieczeństwa IK jest zadaniem niezwykle złożonym oraz brak wiarygodnych wzorców takiej oceny, do pomiaru realizacji celów NPOIK przyjmuje się następujące mierniki:

1) zatwierdzony plan ochrony IK – plan ochrony IK jest podstawowym dokumentem potwierdzającym spełnienie przez operatora obowiązku ochrony IK, o którym mowa w art. 6 ust. 5 ustawy o zarządzaniu kryzysowym. Plan jest ilustracją nakładu pracy włożonej w przygotowanie i wdrożenie ochrony IK. Poprawnie przeprowadzony proces planowania podnosi zdolność organizacji do identyfikacji i zmniejszania podatności, przeciwdziałania zagrożeniom, reakcji na nie oraz minimalizacji skutków ich wystąpienia.
2) audyt stanu ochrony IK – sprawdzenie skuteczności systemu ochrony IK będzie realizowane przez jej operatorów, przy wsparciu merytorycznym administracji publicznej, w formie audytu wewnętrznego. Raporty z przeprowadzonych audytów będą przekazywane do wiadomości ministra odpowiedzialnego za system IK oraz do dyrektora RCB.
3) zmiany strukturalne i budżetowe – realizacja zadań z zakresu ochrony IK wymaga zaangażowania zarówno potencjału ludzkiego, jak i finansowego uczestników Programu. Zapewnienie spójnego z oceną ryzyka dla danej organizacji poziomu finansowania ochrony IK (w tym inwestycji w kompetencje ludzkie oraz sprzęt) oraz obsady kluczowych dla tego procesu stanowisk potwierdza dojrzałość organizacji do realizacji zadań z zakresu ochrony IK.
4) ćwiczenia z udziałem służb ratowniczych i ochronnych – sprawdzenie funkcjonowania współpracy między uczestnikami ochrony IK będzie realizowane w formie ćwiczeń z udziałem służb ratowniczych i ochronnych (Policja, PSP, pogotowie ratunkowe). Wnioski z ćwiczeń będą przekazywane do wiadomości ministra odpowiedzialnego za system IK oraz do dyrektora RCB.

Informacja o skuteczności Programu sporządzana będzie na podstawie ankiet bezpieczeństwa obiektów, urządzeń, instalacji lub usług IK, raportów z audytów wewnętrznych przekazywanych przez operatorów IK i wniosków z ćwiczeń przekazywanych przez podmioty ćwiczące.

# 9. Wykaz załączników

Załącznik nr 1 – „Załącznik nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje”,
Załącznik nr 2 – ZASTRZEŻONY – „Załącznik nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej – Kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej – tekst jednolity”.