2013

Narodowy Program Ochrony Infrastruktury Krytycznej

Spis treści

Spis treści 2

Wprowadzenie 4

1. Zakres, cele, priorytety i zasady Programu 6

1.1. Zakres Programu 6

1.2. Cele Programu 6

1.3. Priorytety Programu 7

1.4. Zasady Programu 7

1.5. Adresaci Programu 9

1.5.1. Administracja publiczna 9
1.5.2. Operatorzy IK 9
1.5.3. Przedsiębiorcy 9
1.5.4. Środowisko naukowe 10
1.5.5. Społeczeństwo 10

1.6. Kontekst prawny 10

1.7. Ramy czasowe 10

2. Identyfikacja IK 11

3. Organy i podmioty uczestniczące w realizacji Programu, ich rola i odpowiedzialność 13

3.1. Rządowe Centrum Bezpieczeństwa 13

3.2. Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej 14

3.3. Ministrowie odpowiedzialni za systemy infrastruktury krytycznej 15

3.4. Inne organy administracji publicznej 19

3.4.1. Prezydent RP 19
3.4.2. Rada Ministrów 19
3.4.3. Ministrowie i kierownicy urzędów centralnych wykonujący zadania z zakresu zarządzania kryzysowego 19
3.4.4. Wojewodowie 20
3.4.5. Służby specjalne 21
3.4.6. Starostowie, wójtowie, burmistrzowie i prezydenci miast 21

3.5. Środowisko naukowe 22

4. Ochrona infrastruktury krytycznej 24

4.1. Ocena ryzyka 25

4.1.1. Identyfikacja zagrożeń i budowa scenariuszy 27
4.1.2. Określenie prawdopodobieństwa wystąpienia danego scenariusza 28
4.1.3. Określenie podatności IK oraz podatności środków ochrony 28

4.1.4. Określenie skutków wystąpienia danego scenariusza 29
4.1.5. Ocena ryzyka zakłócenia IK w danym scenariuszu 30

4.2. Rodzaje ochrony 31

4.3. Współpraca w ochronie infrastruktury krytycznej 33

4.3.1. Forum ochrony infrastruktury krytycznej 35
4.3.2. Mechanizm ochrony IK (bieżąca wymiana informacji) 37
4.3.3. Szkolenia, konferencje, doradztwo 40

5. Wdrożenie Programu 44

5.1. Działania organizacyjno-prawne 44

5.2. Działania techniczne 44

5.3. Działania edukacyjne i szkoleniowe 45

5.4. Program strategiczny 45

5.5. Koordynacja wdrożenia Programu 46

5.6. Finansowanie Programu 46

6. Międzynarodowy aspekt ochrony infrastruktury krytycznej 47

6.1. Europejska infrastruktura krytyczna 47

6.2. Współpraca międzynarodowa w zakresie ochrony IK 49

7. Ocena skuteczności Programu 50

7.1. Przewidywane efekty programu 50

7.2. Wprowadzenie kontroli poziomu ochrony IK 51

7.3. Audyt stanu ochrony IK 51

7.4. Ćwiczenia z udziałem służb ratowniczych i ochronnych 51

7.5. Wdrożenie procesu analitycznego w zakresie efektów stosowania programu i opracowanie dokumentów ewaluacyjnych 51

8. Definicje i skróty użyte w dokumencie 52

8.1. Definicje 52

8.2. Wykaz skrótów 53

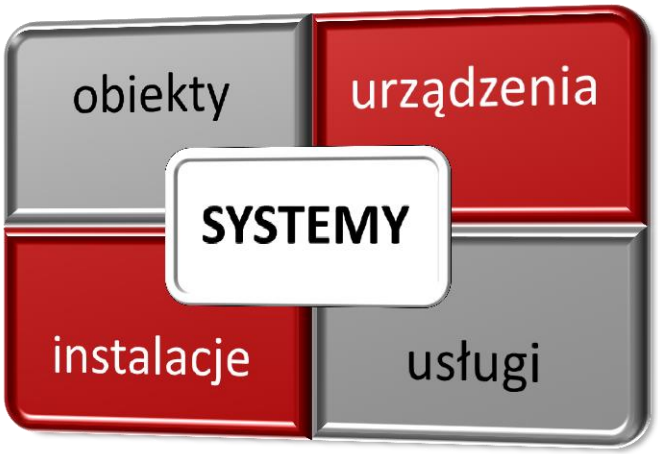
Wprowadzenie

Społeczeństwo polskie, po okresie deficytu dóbr i usług, weszło na drogę intensywnego rozwoju – zarówno gospodarczego, jak i społecznego. Polska dołączyła do grupy państw wysoko uprzemysłowionych. Wiąże się to z dostępem do usług zapewniających utrzymanie określonego standardu życia oraz umożliwiających właściwe relacje między państwem a obywatelem.

Dostęp do tego rodzaju usług staje się 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.

W wyniku zdarzeń spowodowanych siłami natury lub działaniami człowieka infrastruktura krytyczna może ulec zniszczeniu lub uszkodzeniu. Konsekwencją może być zagrożenie ciągłości świadczenia kluczowych usług, a tym samym mienia, zdrowia lub nawet życia obywateli. Biorąc pod uwagę również fakt, że incydenty tego typu negatywnie wpływają na rozwój gospodarczy państwa, należy stwierdzić, że infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli, a jej ochrona jest jednym z priorytetów stojących przed państwem polskim.

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

Infrastruktura krytyczna obejmuje systemy:

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

Ochrona infrastruktury krytycznej to proces obejmujący znaczną liczbę obszarów zadaniowych i kompetencji oraz angażujący wiele zainteresowanych stron. Proces ten obejmuje wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej, zakłada również stopniowe dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie. Zadania w tym zakresie obejmują zapobieganie zagrożeniom i ograniczanie ich skutków, zmniejszanie podatności infrastruktury krytycznej na zagrożenia oraz szybkie przywrócenie jej prawidłowego funkcjonowania na wypadek wszelkich zdarzeń mogących je zakłócić.

Niniejszy dokument w sposób syntetyczny i kompleksowy określa wizję i cele ochrony infrastruktury krytycznej, model współpracy w realizacji zadań, role uczestników i dobre praktyki ochrony IK.

1. Zakres, cele, priorytety i zasady Programu

1.1. Zakres Programu

Narodowy Program Ochrony Infrastruktury Krytycznej dotyczy zidentyfikowanej IK, umieszczonej 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.

Operatorami znacznej części IK są prywatni przedsiębiorcy niepowiązani z administracją publiczną. Program ustanawia ramy, w których administracja publiczna i operatorzy IK współpracują w celu zapewnienia ciągłości działania IK, chroniąc tym samym gospodarcze i społeczne fundamenty naszego kraju. Program zakreśla mechanizmy rozwoju partnerskich relacji między administracją publiczną i operatorami IK w zakresie ochrony IK.

Program ilustruje nowatorskie w naszym kraju (bezsankcyjne) podejście do ochrony kluczowych składników infrastruktury państwa. Jest ono oparte na zasadzie współodpowiedzialności zainteresowanych stron, rozbudowanej współpracy i wzajemnym zaufaniu. Do wdrożenia Programu niezbędne jest wykorzystanie wiedzy i doświadczeń jednostek naukowych oraz opracowanie metodyki oceny ryzyka zakłócenia funkcjonowania IK, opartej o możliwie szeroki wachlarz zagrożeń. Wszystkie te składniki Programu umożliwią podjęcie i utrzymanie skoordynowanych wysiłków na rzecz ochrony IK.

Narodowy Program Ochrony Infrastruktury Krytycznej wynika z art. 5b ust. 1 ustawy o zarządzaniu kryzysowym i nie jest programem operacyjnym ani programem rozwoju w rozumieniu ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2009 r. Nr 84, poz. 712, z późn. zm.).

1.2. Cele Programu

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

Osiągnięcie tego celu wymaga osiągnięcia szeregu celów pośrednich (operacyjnych):

- podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów jej ochrony,

- określenie ról i zakresu odpowiedzialności podmiotów publicznych i prywatnych uczestniczących w działaniach na rzecz ochrony IK,
- 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,
- przygotowanie strategicznego programu podniesienia bezpieczeństwa IK oraz wsparcia wybranych programów badawczych i rozwojowych, edukacyjnych i szkoleniowych ukierunkowanych na podnoszenie odporności infrastruktury.

1.3. Priorytety Programu

Decydujące znaczenie dla osiągnięcia celów Programu mają:

1) podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów jej ochrony,
2) zainicjowanie skutecznej współpracy między uczestnikami Programu w obszarze ochrony IK.

Działania te traktowane są jako priorytety w pierwszym cyklu funkcjonowania Programu.

1.4. Zasady Programu

W ochronie kluczowych elementów infrastruktury państwa powszechnie stosuje się podejście regulacyjne – określające szczegółowo obowiązki oraz przewidujące sankcje za ich niedopełnienie. Jego skuteczność okazuje się jednak niezadowalająca. Represyjny charakter takiego podejścia przynosi skutki uboczne – głęboką niechęć wykonawców do narzuconych zadań i w konsekwencji próby uchylania się od realizacji narzuconych obowiązków bądź wykonywanie ich minimalnym kosztem.

Aby osiągnąć cele Programu, 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. Podejście to nie przewiduje sankcji za niedopełnienie obowiązków określonych w ustawie.

Niezależnie od przyjętego podejścia, w przypadku negatywnej oceny skuteczności Programu bądź działań uczestników procesu ochrony IK lub w celu redukcji niektórych rodzajów ryzyka, dopuszcza się możliwość wprowadzenia szczegółowych uregulowań prawnych dotyczących realizacji Programu.

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 w konsekwencji 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. We wzajemnej współpracy administracji publicznej i sektora prywatnego tkwi potencjał, który z powodzeniem można wykorzystać. Warunkiem skutecznej współpracy są jej autentyczność, wzajemność i dążenie do wspólnej korzyści,
- **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. 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, dlatego działania w obszarze ochrony IK powinny uwzględniać charakterystykę poszczególnych systemów,
- **wiodącej roli ministra odpowiedzialnego za system IK** – inicjatywa zwiększenia poziomu ochrony infrastruktury kluczowej dla funkcjonowania

społeczeństwa wyszła ze strony administracji. Istotną 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 będą miały charakter uzupełniający w stosunku do istniejących rozwiązań prawno-instytucjonalnych. Nie będą powielały rozwiązań i przyjętych praktyk wynikających z obowiązującego prawa.

1.5. Adresaci Programu

Program adresowany jest przede wszystkim do administracji publicznej 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.

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

1.5.1. Administracja publiczna

Głównymi adresatami Programu w administracji publicznej są gospodarze systemów IK. 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 gospodarzami systemów IK i operatorami IK.

1.5.2. Operatorzy IK

Operatorzy IK, zgodnie z art. 6 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 nowy operator IK.

1.5.3. Przedsiębiorcy

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.

1.5.4. 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.

1.5.5. 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.

1.6. Kontekst prawny

NPOIK został opracowany na podstawie art. 5b ustawy o zarządzaniu kryzysowym. NPOIK jest zgodny z obowiązującymi aktami prawnymi i nie narusza postanowień żadnego z nich. 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.

1.7. Ramy czasowe

Ochrona infrastruktury krytycznej jako proces zakłada stopniowe dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie. Nie jest to stan ani tym bardziej produkt końcowy. Sam Program nie jest przez to ograniczony żadną datą końcową. Tym niemniej zakłada się, że zawarte w Programie cele powinny zostać osiągnięte w ciągu 6 lat.

Dbałość o właściwą adaptację wdrożonych rozwiązań sprawia, że Program będzie aktualizowany nie rzadziej niż co 2 lata, z uwzględnieniem zmian otoczenia i uwarunkowań ochrony IK.

2. 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 identyfikacji IK Rządowe Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych oraz przy wsparciu przedsiębiorców prywatnych, opracowało kryteria identyfikacji IK. Określono 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.

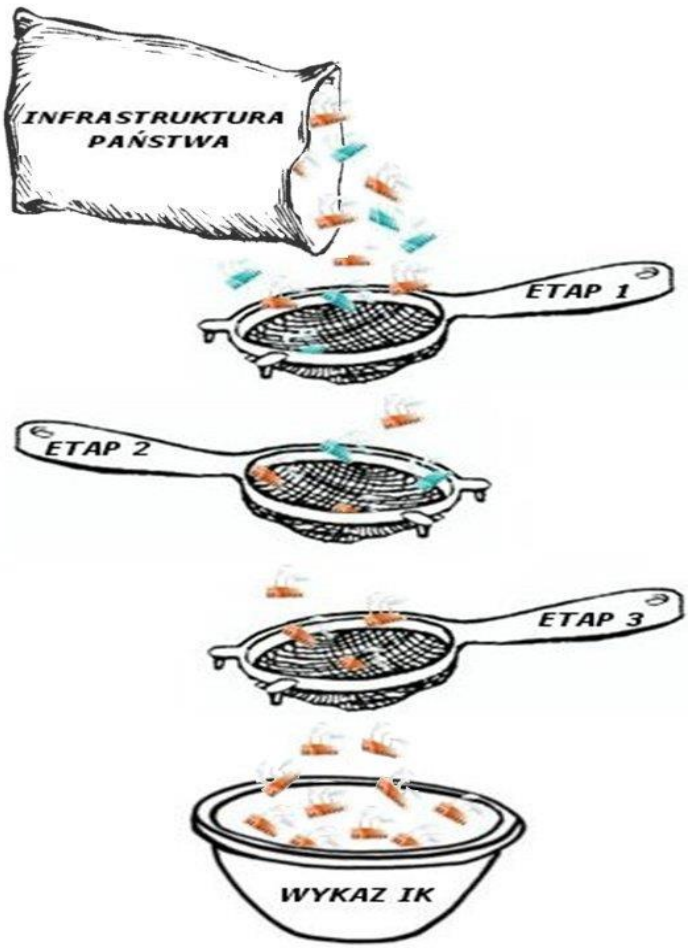
Kryteria podzielone są na dwie grupy:

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.

Identyfikacja IK, zgodnie z przyjętą metodyką, 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[1], przy czym potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe.



Rys. 2. Identyfikacja infrastruktury krytycznej.

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

Zakłada się, że wraz z opracowaniem narzędzi, pozwalających w miarodajny sposób ocenić skutki zniszczenia lub zaprzestania funkcjonowania IK, możliwa będzie rezygnacja z kryteriów systemowych. W efekcie kryteria przekrojowe stosowane byłyby do dowolnie wybranej infrastruktury systemu lub do jakiejkolwiek infrastruktury państwa.

[1] Spośród kryteriów przekrojowych wymienionych na str. 11 należy wybrać najlepiej odpowiadające charakterystyce systemu IK.

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

Infrastruktura krytyczna służy zaspokojeniu potrzeb wszystkich obywateli. Jej ochrona nie może być zatem 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 i kierownikach urzędów centralnych 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.

3.1. 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 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 4,
- opracowywać i wdrażać metodykę oceny ryzyka zakłócenia funkcjonowania IK,
- przeprowadzać, po wdrożeniu metodyki i we współpracy z ministrami i kierownikami urzędów centralnych, ocenę 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.

3.2. Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej

Właściciele oraz posiadacze samoistni i zależni 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.

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 właściwymi organami administracji publicznej i 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.

3.3. 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 posiadają właściwą sobie charakterystykę funkcjonowania, uwarunkowania prawne oraz użytkowników. Biorąc pod uwagę przyjęty model ochrony IK, każdy z systemów IK potrzebuje gospodarza 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.

W rozumieniu Programu odpowiedzialność za system IK polega w szczególności na:

- wsparciu RCB w budowie systemu ochrony infrastruktury krytycznej, opartego na współodpowiedzialności, współpracy i zaufaniu, a także innych zasadach Programu,
- współpracy z RCB i wsparciu w identyfikacji IK oraz wdrażaniu i aktualizacji NPOIK,
- inicjowaniu zmian aktów prawnych w celu ułatwienia i wsparcia wykonywania zadań z zakresu ochrony IK,
- dokonywaniu oceny ryzyka zakłócenia funkcjonowania systemu IK, wywołanego zniszczeniem lub zakłóceniem funkcjonowania IK,
- współpracy z organami, w których kompetencji znajdują się sprawy dotyczące części składowych (elementów) systemu IK, niebędących bezpośrednio we właściwości gospodarza,
- współpracy z innymi gospodarzami systemów IK w zakresie zależności między systemami IK,
- współpracy z operatorami infrastruktury krytycznej w zakresie jej ochrony, animowaniu tej współpracy i jej podtrzymywaniu,
- organizacji i obsłudze systemowego forum ochrony IK i udziale w mechanizmie ochrony IK w zakresie opisanym w Programie,
- wsparciu organizacji ćwiczeń systemowych oceniających sprawność ochrony IK,
- wsparciu działań zmierzających do odtworzenia IK,
- dokonywaniu okresowych analiz i ocen skuteczności ochrony infrastruktury krytycznej we właściwym systemie,
- inspirowaniu wdrażania nowoczesnych technik ochrony IK w systemie,
- organizowaniu szkoleń, konferencji i sympozjów naukowo-badawczych, doskonalących organizacyjne, technicznie i formalnoprawne środki przeciwdziałania zakłóceniom funkcjonowania infrastruktury krytycznej,
- pobudzaniu do aktywności podmiotów zaangażowanych w proces ochrony IK w ramach systemu,
- doradztwie i pomocy dla operatorów IK oraz administracji publicznej,

- wspieraniu systemowych inicjatyw zmierzających do poprawy bezpieczeństwa funkcjonowania IK,
- uzgadnianiu planów ochrony IK, ujętej w wykazie IK w ramach danego systemu.

Systemy infrastruktury krytycznej	Minister odpowiedzialny za system infrastruktury krytycznej
System zaopatrzenia w energię, surowce energetyczne i paliwa	Minister Gospodarki Minister Skarbu Państwa
System łączności	Minister Administracji i Cyfryzacji
System sieci teleinformatycznych	Minister Administracji i Cyfryzacji
System finansowy	Minister Finansów
System zaopatrzenia w żywność	Minister Rolnictwa i Rozwoju Wsi
System zaopatrzenia w wodę	Minister Środowiska Minister Administracji i Cyfryzacji
System ochrony zdrowia	Minister Zdrowia
System transportowy	Minister Transportu, Budownictwa i Gospodarki Morskiej
System ratowniczy	Minister Spraw Wewnętrznych
System zapewniający ciągłość działania administracji publicznej	Minister Administracji i Cyfryzacji
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	Minister Środowiska

Rys. 3. Ministrowie odpowiedzialni za systemy IK.

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,
- 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 ze współgospodarzy będzie realizować wymienione wyżej zadania w stosunku do tych obiektów, które zostały uzgodnione z pozostałymi współgospodarzami.

3.4. Inne organy administracji publicznej

3.4.1. 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.

3.4.2. 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:

- 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,
- dba, aby zadania z zakresu ochrony IK uwzględniano w działalności poszczególnych ministrów i podległych jej organów.

3.4.3. 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.

3.4.4. 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 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.

3.4.5. 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. 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.

Natomiast 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.

3.4.6. 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 finansowej tworzonej na podstawie art. 26 ust. 4 ustawy o zarządzaniu kryzysowym.

3.5. Środowisko naukowe

NPOIK stwarza wiele nowych możliwości w zakresie badań naukowych, prac rozwojowych i programów wdrożeniowych dla środowiska naukowego.

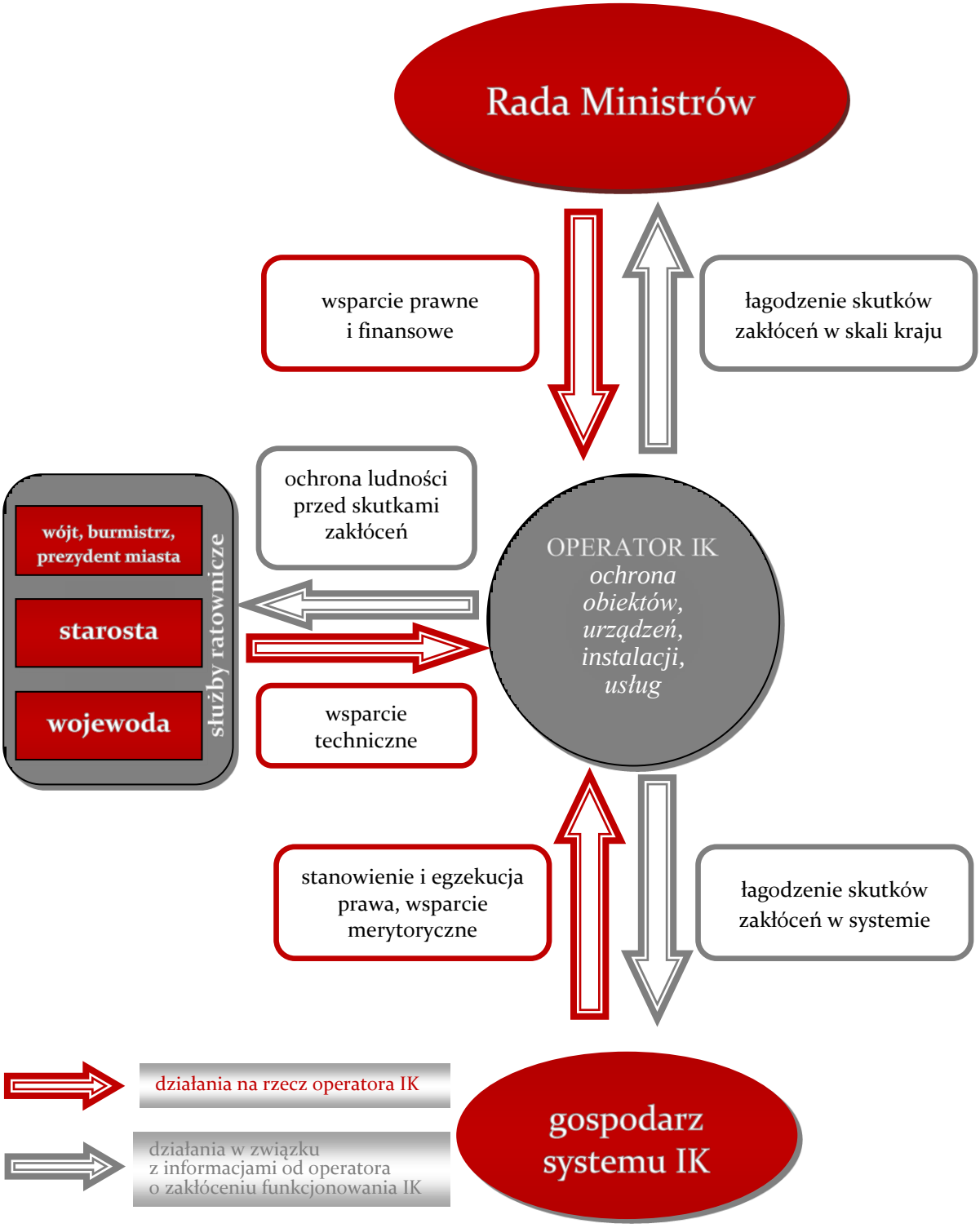
Dla realizacji Programu niezbędne jest opracowanie narzędzi, pozwalających na efektywniejsze działanie wszystkich zainteresowanych stron. Jednostki i środowisko naukowe są źródłem wiedzy w tym zakresie oraz stanowią wsparcie eksperckie dla uczestników Programu.

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,
- testowanie, ocenę i wdrażanie technologii ochrony IK,
- opracowanie i wdrożenie metodyki oceny ryzyka zniszczenia lub zaprzestania funkcjonowania IK, w tym narzędzi informatycznych,
- opracowanie i wdrożenie metodyki oceny podatności IK na zagrożenia oraz skutków zniszczenia lub zaprzestania funkcjonowania IK,
- opracowanie i wdrożenie metodyki oceny współzależności między systemami IK,
- przygotowanie wytycznych oraz opisy najlepszych praktyk w zakresie ochrony IK,
- działania promocyjne na rzecz osiągnięcia celów Programu.

Powyższe zadania będą realizowane w formie:

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



Rys. 4. Główne podmioty uczestniczące w procesie ochrony IK i ich role.

4. Ochrona infrastruktury krytycznej

Jak wspomniano wcześniej, ochronę infrastruktury krytycznej należy pojmować jako proces:

- 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.

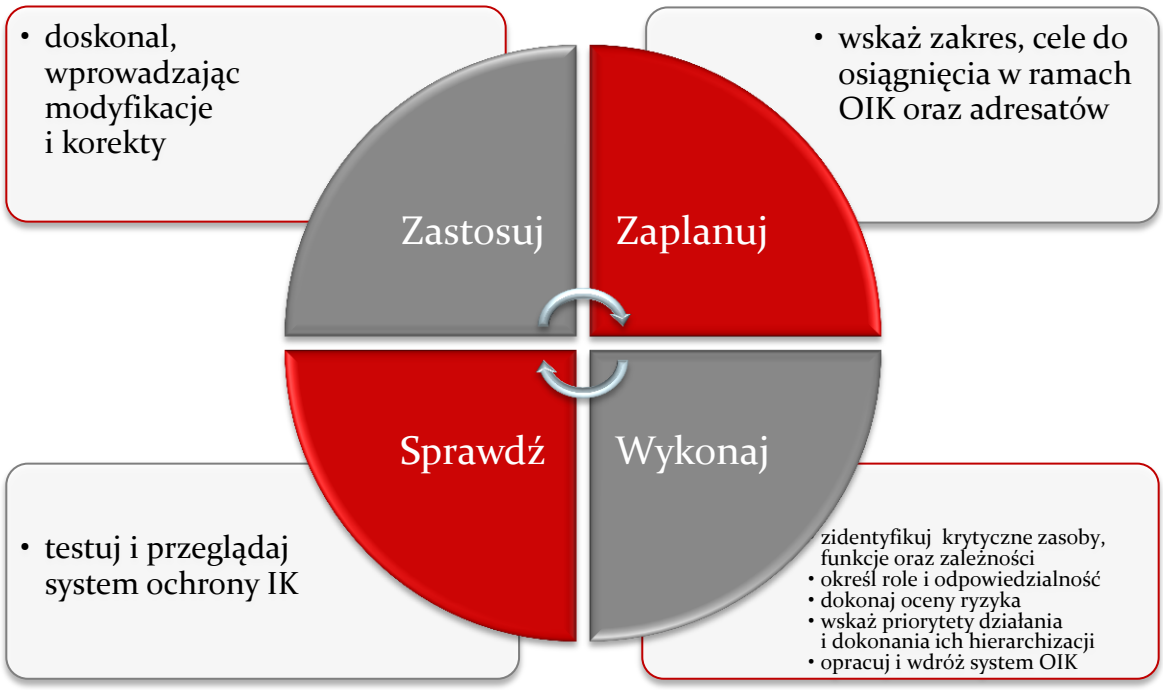
Tak rozumiany proces ochrony infrastruktury krytycznej składa się z następujących etapów:

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[2]. 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 nas 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.

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



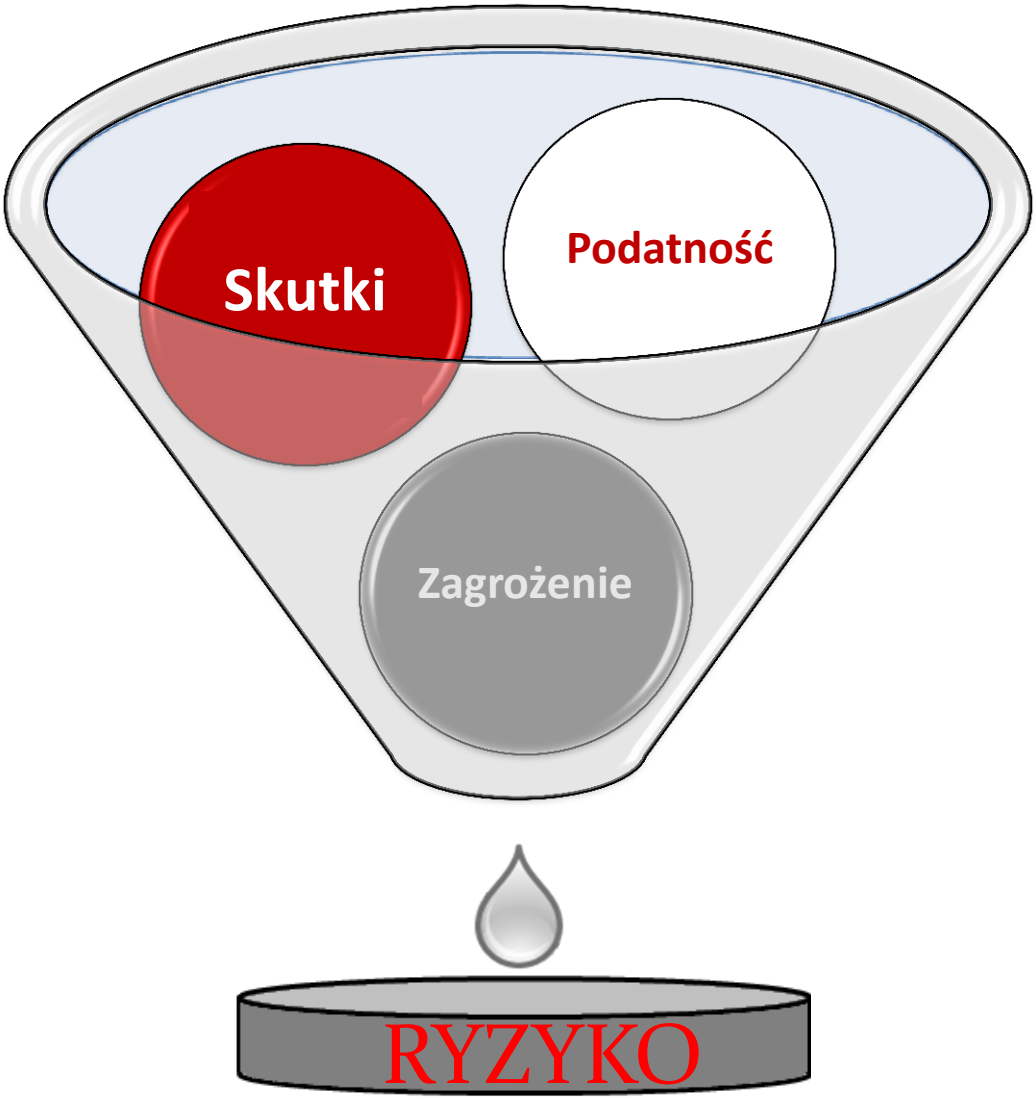
Rys. 5. Proces ochrony IK w cyklu Deminga.

4.1. Ocena ryzyka

Wszelkie działania podejmowane w celu podniesienia poziomu 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.

Na potrzeby systemu ochrony IK niezbędne jest wspólne podejście do oceny ryzyka zakłócenia funkcjonowania IK, pozwalające na porównywanie i ustalenie priorytetów ochrony we wszystkich systemach IK. Pierwszym elementem tego podejścia jest ustanowienie wspólnej definicji ryzyka i sposobu oceny jego podstawowych czynników.

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



Rys. 6 Ryzyko jako funkcja zagrożenia, podatności i skutków.

Na potrzeby Programu do oceny ryzyka wykorzystuje się metodę scenariuszową, która uwzględnia wszystkie trzy powyższe czynniki i odnosi się do obiektu, urządzenia, instalacji lub systemu IK. Zastosowanie scenariuszy wynika z różnych form i sposobów rozprzestrzeniania się zagrożeń oraz ich skutków, które są powiązane z podatnością IK i systemów zabezpieczeń.

Ocena ryzyka metodą scenariuszową składa się z następujących kroków:

1) identyfikacja zagrożeń i budowa scenariuszy,
2) określenie prawdopodobieństwa wystąpienia danego scenariusza,
3) określenie podatności IK oraz środków ochrony,
4) określenie skutków wystąpienia danego scenariusza,
5) ocena ryzyka zakłócenia IK w danym scenariuszu.

4.1.1. Identyfikacja zagrożeń i budowa scenariuszy

Identyfikując zagrożenia, należy odpowiedzieć sobie na pytanie: *jakie niekorzystne zdarzenia mogą dotknąć IK?* Raport o zagrożeniach bezpieczeństwa narodowego dostarcza podstawowych informacji o zagrożeniach zidentyfikowanych w kraju. Źródłem informacji o zagrożeniach występujących lokalnie mogą być, zgodnie z zasadą współpracy, władze województwa, powiatu i gminy, które identyfikują zagrożenia na potrzeby wykonania planów zarządzania kryzysowego.

W przypadku zagrożeń terrorystycznych ich identyfikacja jest poza zakresem kompetencji i możliwości operatorów IK oraz gospodarzy systemów IK. W tym obszarze muszą oni polegać na informacjach otrzymanych w ramach współpracy ze służbami ochrony państwa, w szczególności wykorzystując mechanizm opisany w art. 12a ustawy o zarządzaniu kryzysowym.

Zagrożenia wybrane do dalszej analizy powinny dotyczyć konkretnego obiektu, urządzenia, instalacji lub systemu IK i są podstawą opracowania scenariuszy rozwoju niekorzystnych zdarzeń. Scenariusze w kontekście ochrony IK mają wskazać obszary niepewności i czynniki, które wpływają na decyzje dotyczące systemu ochrony IK, które muszą zostać podjęte teraz i w przyszłości.

Ogólne wymagania w stosunku do scenariuszy budowanych na potrzeby ochrony IK przedstawiają się następująco:

- wiarygodność (scenariusz powinien dawać obiektywne wyniki, pozwalać na dalszą obróbkę, być uzupełniony o dodatkowe informacje faktograficzne),
- poprawność merytoryczna (scenariusz powinien być zgodny z zasadą funkcjonowania IK i obowiązującą teorią na temat zagrożeń),
- konsekwencja opisu (scenariusz powinien posiadać określoną strukturę organizacyjną i logiczną),
- funkcjonalność (scenariusz powinien być łatwy i możliwy do zastosowania),
- prostota (scenariusz powinien być łatwy do zrozumienia i akceptacji).

Ważnym aspektem jest poziom szczegółowości scenariuszy. Scenariusze zawierające dużą liczbę informacji pozwalają na dokładniejsze określenie prawdopodobieństwa wystąpienia scenariusza, identyfikację podatności oraz skutków wystąpienia scenariusza. Jednocześnie jednak w celu przedstawienia kompletnego obrazu ryzyka zakłócenia IK konieczna jest wielka ich liczba, co wymaga dużego przygotowania merytorycznego i wysiłku analitycznego. Scenariusze uboższe w informacje mogą być mniej liczne, ale wiąże się to z większą niepewnością w określeniu prawdopodobieństwa wystąpienia scenariusza, podatności oraz możliwych skutków. Dlatego ważne jest, aby budować scenariusze reprezentatywne dla danego typu zagrożenia.

4.1.2. Określenie prawdopodobieństwa wystąpienia danego scenariusza

Podobnie jak to miało miejsce w przypadku identyfikacji zagrożeń, źródłem informacji na temat prawdopodobieństwa może być „Raport o zagrożeniach bezpieczeństwa narodowego", opracowywany na poziomie krajowym oraz władz województwa, powiatu i gminy. W przypadku określenia prawdopodobieństwa zagrożeń terrorystycznych źródłem informacji są służby ochrony państwa.

Poza źródłami wymienionymi powyżej określenie prawdopodobieństwa wystąpienia danego scenariusza można osiągnąć w drodze:

a) analizy danych statystycznych[3],
b) analizy danych historycznych,
c) szacowania eksperckiego[4],
d) analizy studiów przypadków, które wystąpiły w kraju lub zagranicą,
e) modelowania matematycznego,
f) analizy HAZOP[5].

4.1.3. Określenie podatności IK oraz podatności środków ochrony

Podatność infrastruktury krytycznej i środków jej ochrony to cechy charakterystyczne, które czynią je wrażliwymi na zniszczenie, zakłócenie funkcjonowania, zmniejszenie potencjału lub efektywności działania oraz niewłaściwe wykorzystanie.

Podatność może być wykorzystana przez zagrożenie, które oddziałując na infrastrukturę, powoduje wystąpienie skutków w postaci zakłócenia funkcjonowania IK. Podatność nie powoduje szkody, ale jest warunkiem lub zbiorem warunków, które mogą umożliwić zagrożeniu oddziaływanie na IK. Podatność może pochodzić ze źródeł zarówno wewnętrznych względem IK, jak i zewnętrznych i istnieć tak długo, dopóki w samej IK nie nastąpią zmiany powodujące jej zmniejszenie lub usunięcie.

Wiele ocen podatności skupia się wyłącznie na ochronie fizycznej, jest to jednak tylko jeden z rodzajów ochrony IK. Oszacowanie podatności na zagrożenia powinno uwzględniać również czynnik ludzki, wykorzystanie do funkcjonowania IK systemów i sieci teleinformatycznych, techniczne aspekty budowy i eksploatacji IK oraz zależności i współzależności.

---

[3] Statystyki dotyczą przeszłości, wykorzystywane są przede wszystkim do dokonywania porównań, pokazują trendy i ewentualne efekty przyjętych przedsięwzięć.

[4] Powinno się go dokonywać w grupie składającej się ze specjalistów w różnych dziedzinach i różnych obszarach wiedzy i kompetencji.

[5] HAZOP *(Hazard and Operability Study)* – „Studium zagrożeń i zdolności operacyjnych" – metoda analityczna pozwalającą na wykrycie takich zdarzeń i scenariuszy zakłóceń funkcjonowania IK, które nie zostały zarejestrowane w przeszłości, a mimo to mogą (teoretycznie) wystąpić w przyszłości, jest strukturalną metodą identyfikacji potencjalnych zagrożeń występujących w procesach przemysłowych.

Wiele IK opiera się w swoim funkcjonowaniu na dostępie do usług oferowanych przez inne systemy IK, np.: zaopatrzenia w energię i paliwa, łączności, transportu czy sieci teleinformatycznych. Zakłócenie w którymś z tych systemów może wpłynąć na funkcjonowanie innych. Zależności między zarówno pojedynczą IK, jak i systemami IK muszą zostać uwzględnione w określeniu podatności.

4.1.4. Określenie skutków wystąpienia danego scenariusza

Skutki w rozumieniu Programu to negatywne oddziaływanie zniszczenia lub zakłócenia funkcjonowania IK na ludność, gospodarkę, środowisko i stabilność państwa.

W tym kontekście określenie skutków wystąpienia danego scenariusza obejmuje:

1) ludność:
   - liczbę zabitych,
   - liczbę rannych,
   - liczbę ewakuowanych,
   - liczbę ludzi, którzy utracili podstawowe usługi,
2) gospodarkę:
   - koszty wystąpienia danego scenariusza,
   - wpływ na gospodarkę na poziomie regionalnym i krajowym,
3) środowisko – długoterminowy wpływ na środowisko (zmiany i zakłócenia),
4) stabilności państwa – zakłócenia w realizacji konstytucyjnych obowiązków państwa.

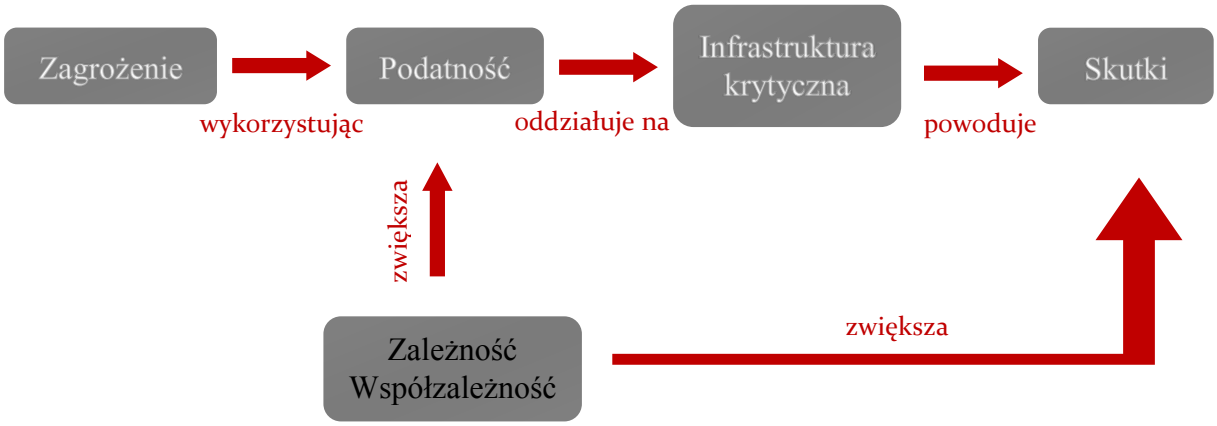
Skutki zakłócenia funkcjonowania IK mogą wystąpić bezpośrednio po niekorzystnym zdarzeniu lub być rozłożone w czasie. Ostateczna wielkość strat będzie zależeć zatem od czasu trwania zakłócenia i musi być uwzględniona w ich określeniu. Należy zwrócić uwagę także na takie zakłócenia funkcjonowania IK, które mogą eskalować do zdarzeń katastroficznych lub też wywoływać efekt domina[6].

Określenie skutków wystąpienia danego scenariusza dokonuje się z wykorzystaniem źródeł wskazanych w 4.1.2.

[6] Efekt domina – skumulowany skutek, powstający w liniowej sekwencji podobnych lub powiązanych ze sobą zdarzeń, w której jedno zdarzenie powoduje szereg kolejnych następujących po sobie zdarzeń i będący jednocześnie bezpośrednim i nieuniknionym wynikiem zdarzenia inicjującego. Sformułowania tego używa się zazwyczaj w odniesieniu do procesów gwałtownych, destrukcyjnych, niemożliwych do opanowania, po tym, gdy już zostaną zainicjowane.

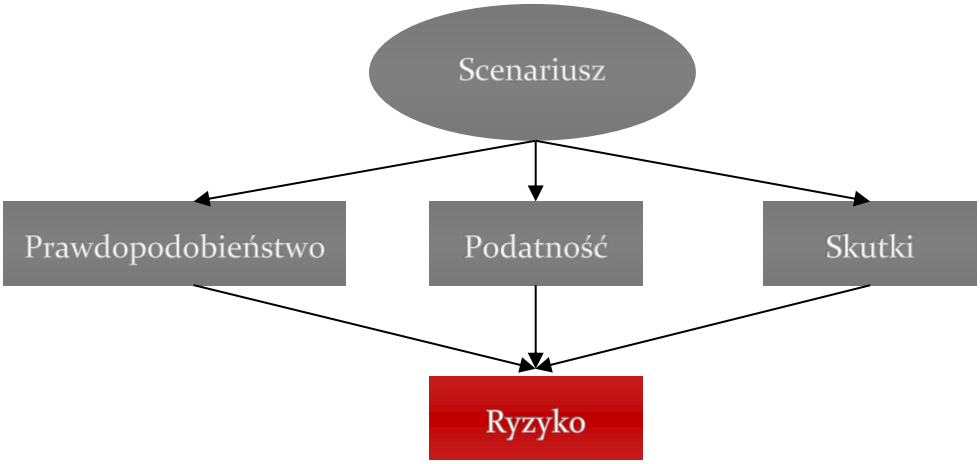
4.1.5. Ocena ryzyka zakłócenia IK w danym scenariuszu

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



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

Mając na uwadze, że określenia prawdopodobieństwa, podatności i skutków dla danego scenariusza dokonuje się niezależnie, połączenie ich w ryzyko zakłócenia IK w danym scenariuszu następuje w sposób pokazany poniżej:



Zarówno ryzyko, jak i jego czynniki mogą być mierzone ilościowo lub jakościowo (np. opisowo). Kiedy jest to możliwe i uzasadnione ze względu na łatwość porównywania, należy stosować miary ilościowe. Prawdopodobieństwo i skutki powinny być obszarem oceny ilościowej i jakościowej, natomiast podatność jakościowej. W każdym przypadku przydatne jest stosowanie skalowania (przypisania określonym wartościom prawdopodobieństwa, podatności i skutków skal np. 1–5) z użyciem zakresów liczbowych lub szczegółowego opisu. Korzystanie z zakresów liczbowych i/lub szczegółowych opisów skal jest konieczne, ponieważ takie pojęcia jak „niskie” lub „wysokie” są przedmiotem różnych interpretacji.

Określone w opisany powyżej sposób ryzyko powinno zostać poddane procesowi oceny. W procesie tym dokonuje się akceptacji ryzyka. 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.

Do czasu opracowania narzędzi pozwalających na dokonywanie oceny ryzyka zgodnie z zaproponowaną metodyką dopuszcza się stosowanie innych metod oceny ryzyka spełniających wymóg wiarygodności i porównywalności.

4.2. Rodzaje ochrony

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 ochronne mają na celu minimalizację ryzyka zakłócenia IK przez:

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

Na tak rozumianą ochronę składają się:

1) ochrona fizyczna – zespół przedsięwzięć minimalizujących ryzyko zakłócenia funkcjonowania IK przez osoby, które znalazły się na terenie IK w sposób nieautoryzowany; ochrona fizyczna obejmuje ochronę osób, rozumianą jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej, ochronę mienia, czyli działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do wstępu osób nieuprawnionych na teren chroniony, a także techniczne środki ochrony, czyli wykorzystanie w ochronie obiektów płotów, barier, systemów telewizji przemysłowej, systemów dostępowych itp. środków,
2) ochrona techniczna – zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z technicznymi

aspektami budowy i eksploatacji obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej; ochrona techniczna IK obejmuje:

- kwestie związane ze zgodnością budynków, urządzeń, instalacji i usług z obowiązującymi przepisami i normami np. budowlanymi, przeciwpożarowymi itp.,
- działania techniczne mające na celu zmniejszenie uzależnienia funkcjonowania IK od zewnętrznych usług,
- działania techniczne mające na celu zapewnienie ciągłości funkcjonowania IK,

3) ochrona osobowa – zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które, przez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu; ochronę tę należy zatem powiązać z pracownikami oraz innymi osobami czasowo przebywającymi w obrębie IK (usługodawcy, dostawcy, goście),

4) ochrona teleinformatyczna – zespół przedsięwzięć, procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych; oznacza to również ochronę przed cyberatakami, cyberprzestępstwami i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom,

5) ochrona prawna – zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z działalnością osób fizycznych lub przedsiębiorców (prywatnych krajowych lub zagranicznych), których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług IK; oznacza to zastosowanie narzędzi prawnych niedopuszczających, przez możliwość kontroli i ewentualnego blokowania lub ograniczania decyzji zarządów, do np. wrogiego przejęcia, fuzji czy też sprzedaży niektórych elementów infrastruktury, której efektem mogą być zakłócenia w jej funkcjonowaniu,

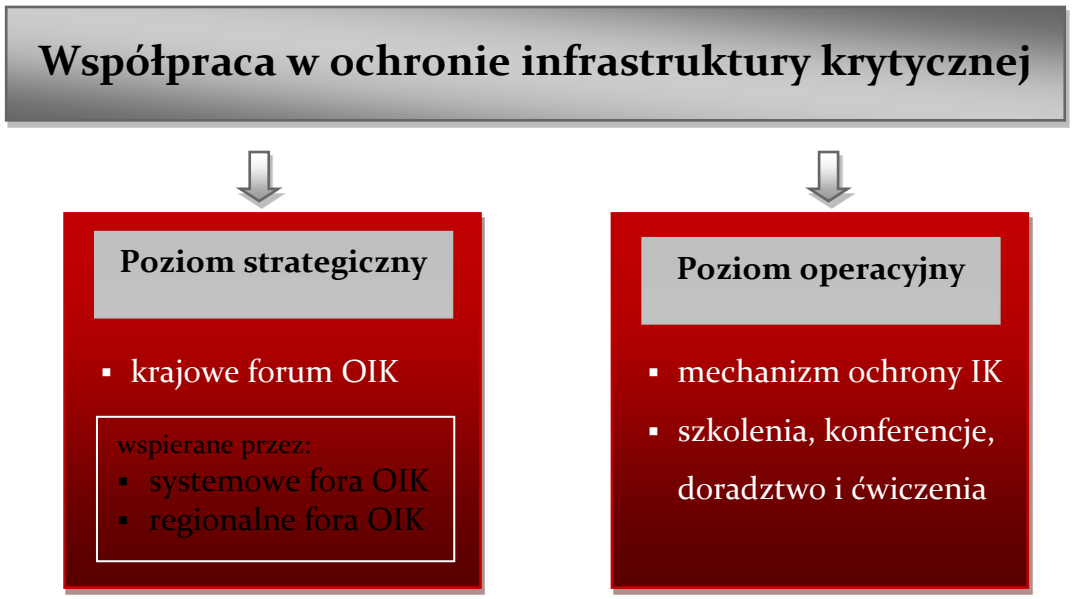
6) plany odtwarzania, rozumiane jako odtwarzanie funkcji realizowanych przez IK.

Zastosowanie konkretnych rodzajów ochrony powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK. W przypadku niewielkiego ryzyka nie ma konieczności stosowania wszystkich jej rodzajów.

4.3. 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 skuteczna, 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.

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 ramach partnerstwa publiczno-prywatnego[7] w zakresie ochrony infrastruktury krytycznej będzie odbywać się w trzech obszarach:

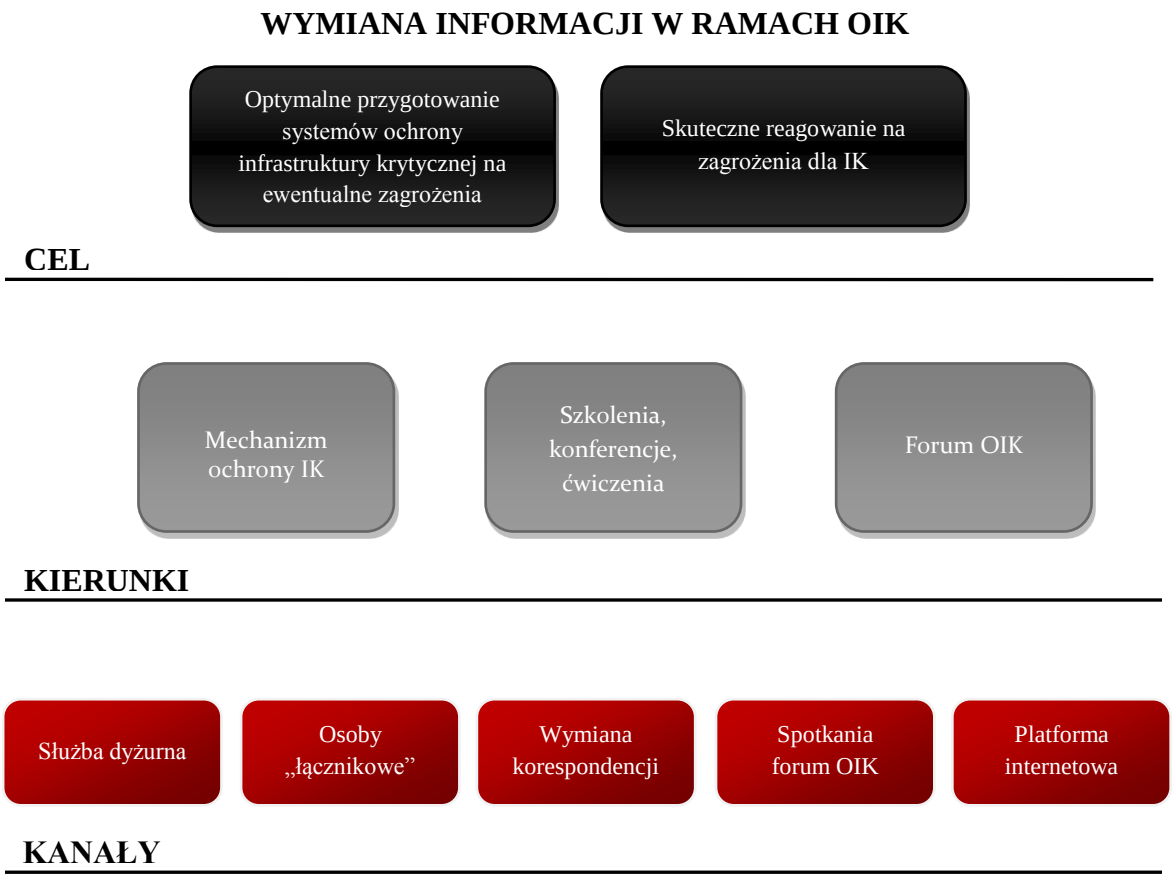
1) forum ochrony infrastruktury krytycznej,
2) bieżąca wymiana informacji przez bezpośrednie kontakty stron (mechanizm ochrony IK),
3) wspólne szkolenia, konferencje, doradztwo i organizacja ćwiczeń.

[7] Partnerstwo publiczno-prywatne w zakresie OIK oznacza jedynie rodzaj współpracy między jednostkami administracji publicznej a podmiotami prywatnymi przez wymianę wszelkich informacji mogących mieć wpływ na osiągnięcie celów NPOIK. W przeciwieństwie zatem do obecnie obowiązujących uregulowań partnerstwo w zakresie OIK nie jest oparte na umowie, jak również nie jest realizacją za wynagrodzeniem przez partnera prywatnego przedsięwzięcia na rzecz podmiotu publicznego.

Stronami w ramach omawianej wymiany informacji będą z jednej strony operatorzy IK, a z drugiej przedstawiciele administracji publicznej. 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 stworzonego systemu szybkiego powiadamiania i alarmowania o zagrożeniach,
- bieżące, bezpośrednie kontakty przedstawicieli stron – tzw. „łączników" z możliwością zorganizowania video-konferencji,
- wymianę korespondencji jawnej i niejawnej w tradycyjny sposób i z wykorzystaniem elektronicznych systemów wymiany informacji jawnych i niejawnych,
- cykliczne, wspólne spotkania w ramach prywatno-publicznych forów ochrony infrastruktury krytycznej,
- wspólną platformę internetową stworzoną specjalnie dla celów powiadamiania, 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 infrastruktury krytycznej i administracją publiczną,
- zwiększenie zaufania do operatorów jako firm odpowiedzialnych społecznie (CSR – *Corporate Social Responsibility*) 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.

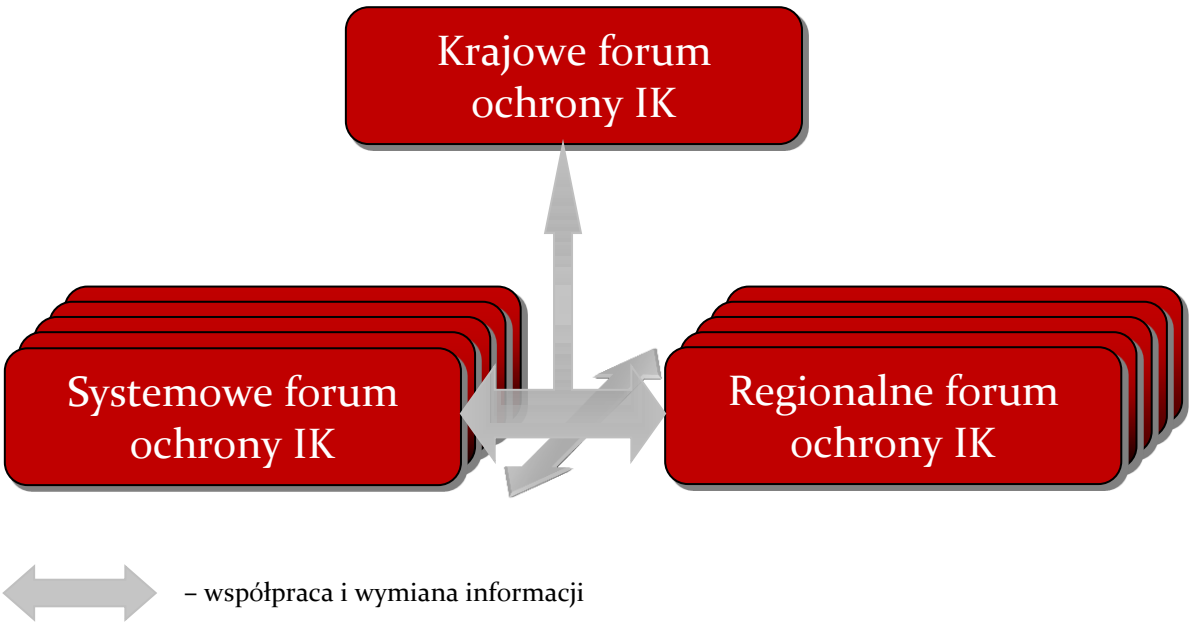
4.3.1. Forum ochrony infrastruktury krytycznej

Administracja ma unikalne możliwości 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 wypracowywanie propozycji rozwiązań.



Rys. 9. Schemat funkcjonowania forów ochrony IK.

4.3.1.1. 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). Zastępcą (zastępcami) przewodniczącego jest jeden z przedstawicieli operatorów IK[8]. Fora zbierają się:

- krajowe, przynajmniej raz w roku lub częściej, zależnie od okoliczności,
- systemowe, przynajmniej dwa razy w roku lub częściej, zależnie od okoliczności,
- wojewódzkie, przynajmniej raz na kwartał lub częściej, zależnie od okoliczności.

[8] Liczba i procedura wyboru zastępów zostanie określona na pierwszym posiedzeniu forum.

4.3.1.2. Funkcjonowanie forum

Podczas obrad forum poruszane są tematy mające strategiczne znaczenie dla ochrony infrastruktury krytycznej:

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.

4.3.2. Mechanizm ochrony IK (bieżąca wymiana informacji)

Bieżąca wymiana informacji będzie obejmować:

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 obejmujące obszary:
   - administracja publiczna,
   - sektor prywatny,
   - świat nauki

   oraz zawarte w nich obszary problemowe dotyczące systemów:
   - zaopatrzenia w energię, surowce energetyczne i paliwa,
   - łączności,

- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Platforma internetowa zostanie ustanowiona jako forum, na którym uczestnicy ochrony infrastruktury krytycznej będą ze sobą współpracować i wymieniać informacje na temat zagrożeń i podatności oraz opracowywać wytyczne do strategii i rozwiązań w celu ograniczenia ryzyka zakłócenia funkcjonowania IK, które mogą być później przedstawiane podczas obrad Forum ochrony IK. Zgodnie z założeniami platforma będzie się składać z grup (pokoi) systemowych oraz eksperckich grup doradczych. Członkami platformy będą operatorzy infrastruktury krytycznej, przedstawiciele organów administracji publicznej, agencji rządowych, a także inne zaangażowane podmioty. Platforma, przez systemowe i eksperckie grupy doradcze, ma na celu promocję ochrony IK wśród jej operatorów, w tym potrzeby inwestycji w tym zakresie.

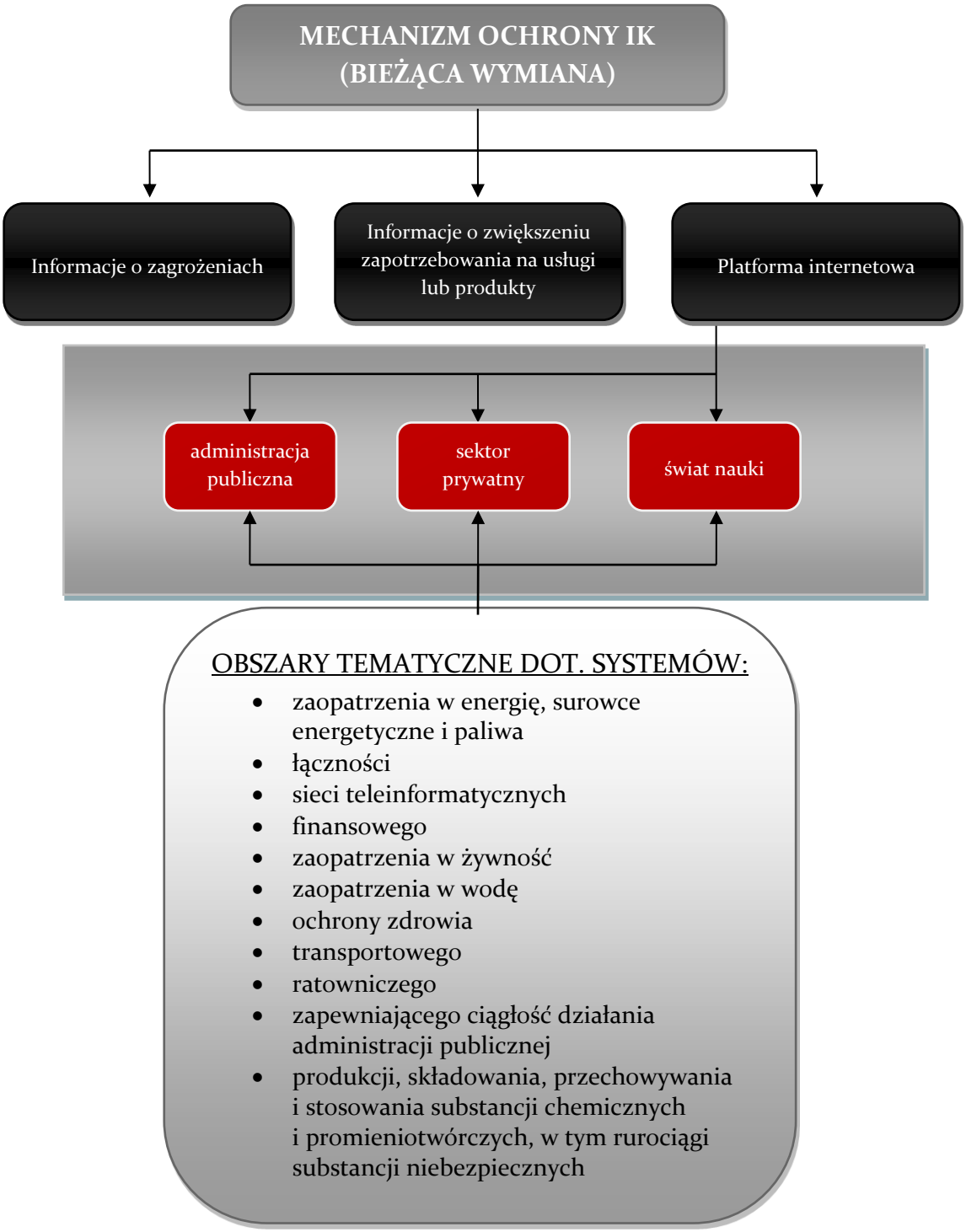
O tym, jakie informacje będą wymieniane w ramach internetowej platformy, decydują sami jej członkowie, tym niemniej nawet wymiana informacji o zagrożeniach czy zidentyfikowanych podatnościach może korzystnie wpływać na wizerunek wszystkich podmiotów systemu IK, oznaczając dojrzałość w podejściu do prowadzenia 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.

Eksperckie grupy doradcze prowadzą doradztwo w zakresie szeroko rozumianej ochrony infrastruktury krytycznej. Składają się ze specjalistów w danej dziedzinie zarówno z wewnątrz, jak i z zewnątrz mechanizmu. RCB będzie prowadzić aktywne działania mające na celu:

- pozyskanie zewnętrznych ekspertów,
- stworzenie bazy ekspertów,
- pośrednictwo w kontaktach między operatorami OIK a ekspertami.

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.

4.3.3. 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 innymi działaniami o charakterze szkoleniowym. Działania te obejmują:

a) udzielanie wsparcia merytorycznego (na zasadzie doradztwa oraz szkoleń na rzecz operatorów) przez podmioty administracji publicznej w zakresie rodzajów ochrony i w zakresie funkcjonowania wewnętrznych mechanizmów ochrony infrastruktury krytycznej i zarządzania kryzysowego,
b) udział w ćwiczeniach z zakresu ochrony infrastruktury krytycznej,
c) udział w konferencjach z zakresu ochrony infrastruktury krytycznej,
d) integrację środowisk odpowiedzialnych za ochronę infrastruktury krytycznej.

4.3.3.1. 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 wykonujących zadania ochronne 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:

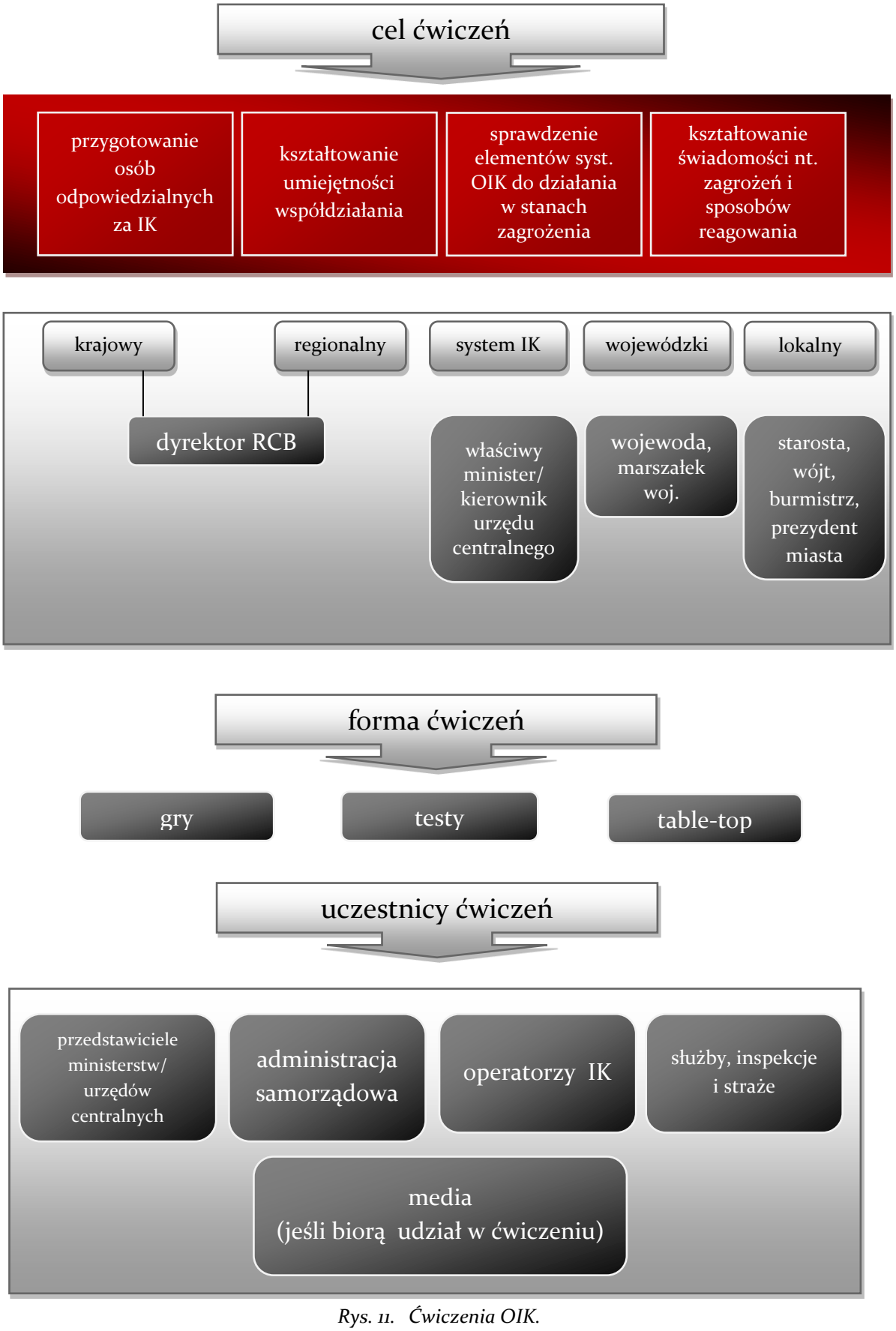
1) dyrektor Rządowego Centrum Bezpieczeństwa – w odniesieniu do ćwiczenia prowadzonego w formie:
   a) ćwiczeń o zasięgu krajowym,
   b) ćwiczeń regionalnych, obejmujących obszar dwóch lub więcej województw,
2) minister odpowiedzialny za system IK – w odniesieniu do ćwiczeń organizowanych w ramach kierowanego 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.

Do obowiązków organizatora ćwiczenia należy:

1) opracowywanie planów przeprowadzania ćwiczeń oraz uzgadnianie tych planów w zakresie terminów i zakresu ćwiczeń z dyrektorem Rządowego Centrum Bezpieczeństwa,
2) określenie celu i efektu przeprowadzenia ćwiczenia,
3) zapewnianie właściwych warunków do realizacji ćwiczenia,
4) przygotowanie dokumentacji ćwiczenia,
5) zapewnianie środków finansowych na pokrycie kosztów związanych z organizacją i realizacją ćwiczenia,
6) przekazanie dyrektorowi Rządowego Centrum Bezpieczeństwa do wiadomości zatwierdzonego przez organizatora ćwiczeń sprawozdania z przeprowadzonych ćwiczeń.

Założenia ćwiczenia określają w szczególności:

1) cele i efekt końcowy przeprowadzenia ćwiczenia, w układzie: przeszkolić (kogo?), doskonalić (co?, jakie elementy?), zgrywać (kogo z czym?, kim?), sprawdzić (kogo?, co?), służyć (komu?, czemu?) itp.,
2) zakres ćwiczenia, w formie ogólnych zagadnień szkoleniowych przewidzianych do realizacji w trakcie całego ćwiczenia,
3) formę/rodzaj/zasięg ćwiczenia,
4) terminy przeprowadzenia ćwiczenia i/lub jego poszczególnych etapów (jeżeli wystąpią),
5) miejsce przeprowadzenia ćwiczenia oraz wskazanie uczestników i terminu przeprowadzenia rekonesansu rejonu ćwiczenia, jeżeli ćwiczenie realizowane będzie w terenie (ćwiczenie praktyczne),
6) harmonogram przygotowania ćwiczenia,
7) termin osiągnięcia gotowości do ćwiczenia,
8) strukturę kierownictwa ćwiczenia, wyszczególnienie osób funkcyjnych z podaniem stanowiska, imienia i nazwiska oraz pozostałych uczestników ćwiczenia wraz ze strukturą organizacyjną ćwiczenia,
9) zakres dokumentacji ćwiczenia.



Rys. 11. Ćwiczenia OIK.

5. Wdrożenie Programu

Wdrożenie Programu powinno być zgodne z jego celami i priorytetami i wymaga podjęcia szeregu skoordynowanych działań. W ujęciu przedmiotowym wdrożenie Programu obejmuje:

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

5.1. Działania organizacyjno-prawne

Działania organizacyjno-prawne obejmują:

1) organizację i aktywację działalności forów oraz mechanizmu ochrony IK – perspektywa krótkoterminowa (RCB + gospodarze systemów IK + operatorzy IK + wojewodowie),
2) wprowadzenie w aktach prawnych niezbędnych zmian, ułatwiających ochronę i odtworzenie IK przez jej operatorów – perspektywa średnioterminowa (Rada Ministrów + gospodarze systemów IK + RCB),
3) opracowanie, uzgodnienie i wdrożenie mechanizmów motywujących do aktywnego udziału w Programie dla operatorów IK oraz wsparcia sił i środków pozostających w dyspozycji lokalnych władz i podległych im służb, inspekcji i straży – perspektywa długoterminowa (Rada Ministrów + gospodarze systemów IK + RCB + operatorzy IK),
4) integrację systemów ochrony obowiązkowej, ochrony szczególnej i ochrony IK – perspektywa długoterminowa (Rada Ministrów + gospodarze systemów IK + RCB + operatorzy IK + wojewodowie).

5.2. Działania techniczne

Działania techniczne w ramach wdrożenia Programu obejmują:

1) uruchomienie i utrzymanie internetowej platformy wymiany informacji – perspektywa krótkoterminowa (RCB),
2) opracowanie procedur prowadzenia kontroli i audytów wewnętrznych – perspektywa średnioterminowa (RCB + gospodarze systemów IK + operatorzy IK),
3) opracowanie i wdrożenie metodyki oceny ryzyka zakłócenia funkcjonowania IK – perspektywa średnioterminowa (RCB + gospodarze systemów IK + operatorzy IK + środowisko naukowe),
4) opracowanie standardów (norm) dotyczących poszczególnych rodzajów ochrony IK – perspektywa długoterminowa (RCB + gospodarze systemów IK + operatorzy IK + środowisko naukowe + pozostali partnerzy).

5.3. Działania edukacyjne i szkoleniowe

Działania edukacyjne i szkoleniowe mają decydujące znaczenie dla skuteczności Programu. Podniesienie poziomu świadomości i wiedzy uczestniczących w ochronie IK przyczyni się do zwiększenia efektywności i podniesienia jakości wszystkich etapów ochrony IK. Działania z tego zakresu będą prowadzone wśród obecnych uczestników ochrony IK i obejmują:

1) przeprowadzenie inicjujących szkoleń z zakresu ochrony IK i Programu dla operatorów IK oraz gospodarzy systemów IK – perspektywa krótkoterminowa (RCB);
2) opracowanie programu szkoleń i stałe działania edukacyjno-uświadamiające dla operatorów IK i administracji publicznej – perspektywa średniookresowa (RCB + gospodarze systemów IK + operatorzy IK);
3) opracowanie i wydawanie broszur informacyjnych oraz poradników z zakresu ochrony IK dla operatorów IK i administracji publicznej – perspektywa średniookresowa (RCB + gospodarze systemów IK + operatorzy IK);
4) racjonalizację programów nauczania w szkołach oraz programów kształcenia w szkołach wyższych – perspektywa długoterminowa (szkoły + uczelnie + RCB + gospodarze systemów IK + operatorzy IK).

5.4. Program strategiczny

RCB, we współpracy z ministrami odpowiedzialnymi za systemy IK, będzie dążyć do przygotowania i przedstawienia do zatwierdzenia Ministrowi Nauki i Szkolnictwa Wyższego przez Komitet Sterujący Narodowego Centrum Badań i Rozwoju projektu *strategicznego programu badań naukowych i prac rozwojowych w zakresie podniesienia bezpieczeństwa IK* w ramach badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa[9].

[9] Zgodnie z art. 17 pkt 1 ustawy z dnia 30 kwietnia 2010 r. o Narodowym Centrum Badań i Rozwoju (Dz. U. Nr 96, poz. 616, z późn. zm.), do zadań Komitetu Sterującego należy przygotowywanie i przedstawianie Ministrowi Nauki i Szkolnictwa Wyższego do zatwierdzenia projektów strategicznych programów badań naukowych i prac rozwojowych, w których ramach realizowane są badania naukowe lub prace rozwojowe, o których mowa w art. 2 pkt 5 ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (Dz. U. Nr 96, poz. 615, z późn. zm.) – „badania naukowe lub prace rozwojowe na rzecz obronności i bezpieczeństwa państwa".

5.5. 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.

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

5.6. Finansowanie Programu

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 ustawy o zarządzaniu kryzysowym.

6. Międzynarodowy aspekt ochrony infrastruktury krytycznej

W Polsce, podobnie jak i w innych krajach, działająca sprawnie i w sposób niezakłócony infrastruktura ma coraz większy wpływ na obywateli, struktury administracji
i gospodarkę. Proces ten niekiedy doprowadza do uzależnienia się w takim stopniu, że dysfunkcja danej infrastruktury może prowadzić do skutków wykraczających poza granice własnego kraju. Ustalenie skali współzależności i podjęcie skutecznych działań celem jego zredukowania wymaga nawiązania i prowadzenia współpracy ze wszystkimi krajami i organizacjami międzynarodowymi, które podzielają te cele.

6.1. 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).

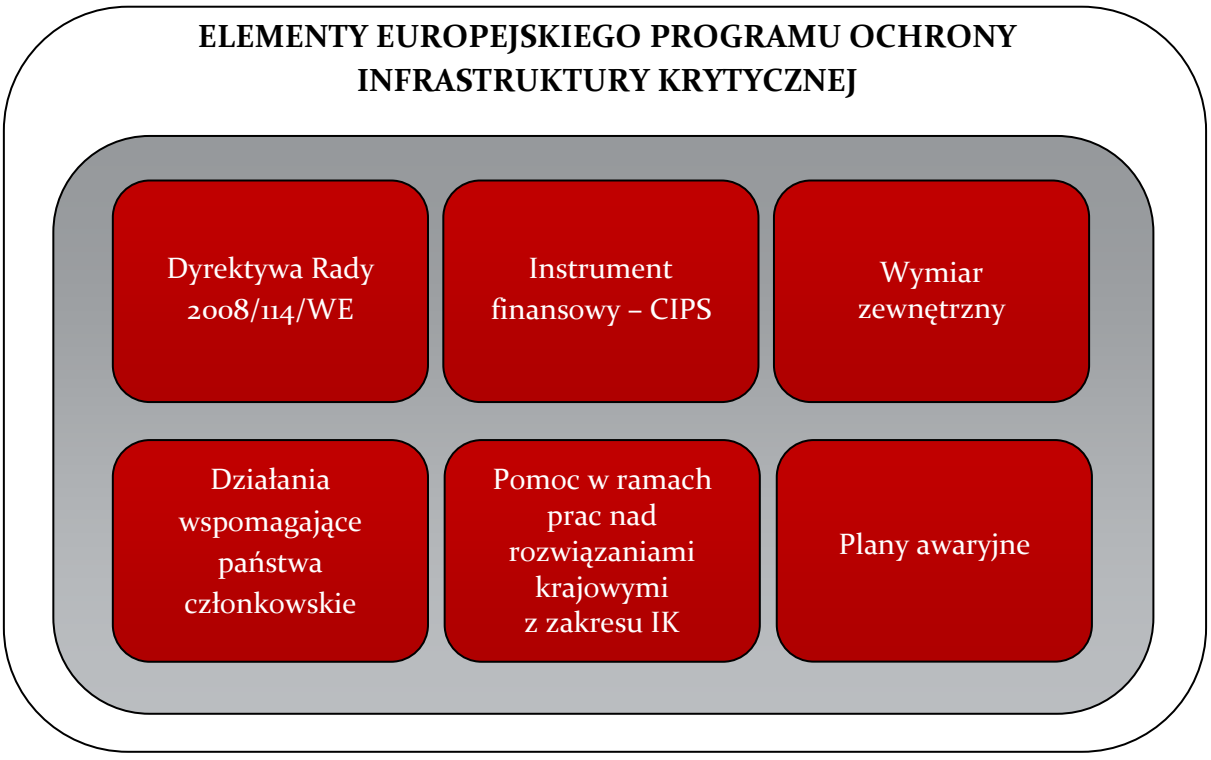
Na działania w ramach Europejskiego Programu Ochrony Infrastruktury Krytycznej składają się:

- 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,
- instrument finansujący działania z zakresu ochrony infrastruktury krytycznej – decyzja Rady z dnia 12 lutego 2007 r. ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa" – CIPS,
- działania wspomagające państwa członkowskie w implementacji dyrektywy (m.in. projekt sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej – 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,
- plany awaryjne.

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 infrastrukturę krytyczną jako składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji, jeżeli jej zakłócenie lub zniszczenie będzie miało wpływ na co najmniej dwa państwa członkowskie, staje się ona europejską infrastrukturą krytyczną.

Europejska infrastruktura krytyczna, na chwilę obecną, wyznaczana jest w dwóch sektorach – sektorze energii i sektorze transportu. Zgodnie z przepisami ww. dyrektywy w przyszłym roku będzie poddana przeglądowi, w którego ramach poruszona zostanie również kwestia poszerzenia zakresu dyrektywy o inne sektory. Priorytet nadano sektorowi technologii informacyjno-komunikacyjnych.

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



Rys. 12. Elementy Europejskiego Programu Ochrony Infrastruktury Krytycznej.

6.2. Współpraca międzynarodowa w zakresie ochrony IK

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

Współpraca może odbywać się w ramach działań wspólnych oraz indywidualnych i jest prowadzona w celu:

- wzmocnienia możliwości ochrony krajowej IK,
- skorzystania w zakresie ochrony IK z doświadczeń innych państw,
- pozyskania informacji i wiedzy przydatnych w doskonaleniu systemu ochrony IK w Polsce,
- identyfikacji współzależności między państwami,
- identyfikacji infrastruktury kluczowej dla wzajemnych relacji,
- budowy globalnej kultury bezpieczeństwa.

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

7. Ocena skuteczności Programu

Biorąc pod uwagę fakt, że system ochrony IK jest budowany w Polsce po raz pierwszy oraz że jest to zadanie niezwykle złożone, a przyjęta metoda nowatorska w skali kraju, w pierwszym okresie funkcjonowania Programu trudno będzie określić mierniki obrazujące skuteczność i efekty jego stosowania. Jak pokazują doświadczenia innych krajów, budowa skutecznie działającego systemu ochrony IK może zająć Polsce kilka lat i taki okres przewidywany jest na wprowadzenie i przetestowanie zaproponowanych w NPOIK rozwiązań oraz obserwację ich skuteczności.

7.1. Przewidywane efekty Programu

Efektem Programu będzie osiągnięcie celu strategicznego i celów operacyjnych. Biorąc jednak pod uwagę, że efekty te pojawią w dłuższej perspektywie czasowej, bliższe efekty Programu obejmować będą:

- podniesienie poziomu wiedzy na temat infrastruktury krytycznej, jej znaczenia dla bezpieczeństwa państwa, zagrożeń, którym może ona podlegać, i ochrony przed tymi zagrożeniami,
- ostateczne ukształtowanie się, na podstawie doświadczeń, ról i zakresu odpowiedzialności w procesie ochrony IK oraz wprowadzenie mechanizmu koordynacji współpracy,
- przeprowadzenie oceny ryzyka zakłócenia funkcjonowania IK z uwzględnieniem wszystkich typów zagrożeń,
- ustalenie hierarchii priorytetów odtwarzania IK,
- opracowanie przez operatorów IK akceptowalnego oraz oczekiwanego poziomu ryzyka zakłócenia funkcjonowania IK, pozostającej w ich władaniu,
- wykrycie obszarów ryzyka nieakceptowalnego i podjęcie działań naprawczych,
- usprawnienie przepływu informacji między operatorami IK a administracją publiczną,
- ustalenie zakresu wsparcia operatora IK przez administrację publiczną w sytuacjach kryzysowych,
- wprowadzenie w aktach prawnych niezbędnych zmian, ułatwiających ochronę i odtworzenie IK,
- rozpoczęcie prac nad generowaniem i upublicznianiem dobrych praktyk w dziedzinie ochrony IK,
- rozpoczęcie prac nad standaryzacją form i zasad ochrony IK.

7.2. Wprowadzenie kontroli poziomu ochrony IK

Ocena poziomu ochrony IK powinna korelować z zasadami partnerstwa i współodpowiedzialności obowiązującymi dla całego Programu. Dlatego główny nacisk powinien być położony na wdrożenie przez operatorów IK kontroli wewnętrznej według zasad opracowanych we współpracy z administracją publiczną. Dodatkowo zagadnienia związane z ochroną IK muszą zostać włączone w bieżącą działalność służb, inspekcji i straży realizujących swoje zadania ustawowe.

7.3. 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.

7.4. Ćwiczenia z udziałem służb ratowniczych i ochronnych

Sprawdzenie funkcjonowania współpracy między uczestnikami ochrony IK będzie realizowane w formie ćwiczeń potencjalnych sytuacji awaryjnych z udziałem służb ratowniczych i ochronnych (Policja, PSP, pogotowie ratunkowe). Ćwiczenia będą prowadzone w sposób opisany w pkt 4.3.3.1. Wnioski z ćwiczeń będą przekazywane do wiadomości ministra odpowiedzialnego za system IK oraz do dyrektora RCB.

7.5. Wdrożenie procesu analitycznego w zakresie efektów stosowania programu i opracowanie dokumentów ewaluacyjnych

Do czasu opracowania całościowych i mierzalnych wskaźników obrazujących efektywność programu RCB będzie sporządzać raporty obrazujące następujące zmiany:

- liczbę operatorów IK, u których wyznaczono osoby odpowiedzialne za kontakty z administracją,
- liczbę obiektów posiadających zatwierdzony plan ochrony,
- liczbę operatorów stosujących kontrolę wewnętrzną i audyt ochrony IK,
- liczbę ćwiczeń w podziale na poszczególne systemy IK w porównaniu do lat ubiegłych,
- liczbę aktywnych uczestników forów i platformy internetowej.

Raporty sporządzane będą 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.

8. Definicje i skróty użyte w dokumencie

8.1. Definicje

cyberatak – celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni,

cyberprzestępstwo – czyn zabroniony popełniony w obszarze cyberprzestrzeni,

cyberprzestrzeń[10] – jest rozumiana jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235), wraz z powiązaniami między nimi oraz relacjami z użytkownikami,

cyberterroryzm – przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni,

gospodarz systemu IK – minister kierujący działem administracji rządowej odpowiedzialny za system infrastruktury krytycznej,

infrastruktura krytyczna – zgodnie z art. 3 pkt 2 ustawy o zarządzaniu kryzysowym – 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. IK obejmuje systemy:

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

Narodowy Program Ochrony Infrastruktury Krytycznej – zgodnie z art. 5b ust. 1 ustawy o zarządzaniu kryzysowym dokument, którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej,

[10] Definicje pochodzą z projektu Polityki Bezpieczeństwa Cyberprzestrzeni Rzeczypospolitej Polskiej.

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 2005 r. Nr 145, poz. 1221, z późn. zm.),

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 2012 r. poz. 461, 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) z udziałem Sił Zbrojnych Rzeczypospolitej Polskiej, Policji, PSP i formacji obrony cywilnej,

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.

8.2. 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