PREZES RADY MINISTRÓW

Warszawa */elektroniczny znacznik czasu/*

DKPL.WK.10.2.6.2020.ACY(12)

RM-10-6-20

UD46

Pani Elżbieta WITEK
Marszałek Sejmu

Szanowna Pani Marszałek,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi

projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw.

W załączeniu przedstawiam także opinię dotyczącą zgodności proponowanych regulacji z prawem Unii Europejskiej.

Jednocześnie informuję, że do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Prezes Rady Ministrów.

Z poważaniem,
Mateusz Morawiecki
Prezes Rady Ministrów
/podpisano kwalifikowanym podpisem elektronicznym/

Projekt

U S T A W A

z dnia

o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw[1)]

Art. 1. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398) wprowadza się następujące zmiany:

1) w art. 3:

a) pkt 1 otrzymuje brzmienie:

„1) sytuacji kryzysowej – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach, środowiska lub dziedzictwa kulturowego, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków lub zakłócenia obsługi tych organów;”,

b) w pkt 2 lit. f otrzymuje brzmienie:

„f) zaopatrzenia w wodę oraz odprowadzania ścieków,”,

c) po pkt 3 dodaje się pkt 3a w brzmieniu:

„3a) operatorze infrastruktury krytycznej – należy przez to rozumieć właściciela, posiadacza samoistnego lub posiadacza zależnego obiektu, instalacji, urządzenia lub usługi, które zostały ujęte w wykazie infrastruktury krytycznej;”,

d) w pkt 4 w lit. b średnik zastępuje się przecinkiem i dodaje się lit. c w brzmieniu:

„c) planowanie w zakresie wspierania Sił Zbrojnych Rzeczypospolitej Polskiej oraz wojsk sojuszniczych w przypadku realizacji na terytorium Rzeczypospolitej

---

[1)] Niniejszą ustawą zmienia się ustawy: ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, ustawę z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, ustawę z dnia 29 października 2010 r. o rezerwach strategicznych, ustawę z dnia 14 grudnia 2012 r. o odpadach, ustawę z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, ustawę z dnia 7 lutego 2014 r. o udziale zagranicznych funkcjonariuszy lub pracowników we wspólnych operacjach lub wspólnych działaniach ratowniczych na terytorium Rzeczypospolitej Polskiej oraz ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Polskiej zobowiązań sojuszniczych w ramach Organizacji Traktatu Północnoatlantyckiego;”,

e) po pkt 9 dodaje się pkt 9a i 9b w brzmieniu:

„9a) ryzyku – należy przez to rozumieć kombinację prawdopodobieństwa wystąpienia zagrożenia oraz skutków wystąpienia zagrożenia;

9b) ryzyku dla infrastruktury krytycznej – należy przez to rozumieć kombinację prawdopodobieństwa wystąpienia zagrożenia lub podatności na wystąpienie zagrożenia oraz skutków wystąpienia zagrożenia;”,

f) pkt 10 otrzymuje brzmienie:

„10) mapie ryzyka – należy przez to rozumieć mapę przedstawiającą obszar geograficzny objęty zasięgiem ryzyka lub opis tego obszaru, wraz ze wskazaniem poziomu ryzyka;”,

g) w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12–21 w brzmieniu:

„12) matrycy ryzyka – należy przez to rozumieć graficzny lub opisowy sposób przedstawienia kombinacji prawdopodobieństw wystąpienia zagrożeń oraz ich skutków, ze wskazaniem wartości ryzyka;

13) zarządzaniu ryzykiem – należy przez to rozumieć działania polegające na:

a) ocenie ryzyka, w tym:

– identyfikacji zagrożeń,

– analizie ryzyka,

– szacowaniu ryzyka,

b) planowaniu działań ograniczających ryzyko,

c) wdrażaniu działań ograniczających ryzyko,

d) osiąganiu gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej,

e) okresowej ocenie osiągniętych efektów;

14) analizie ryzyka – należy przez to rozumieć ocenę prawdopodobieństwa wystąpienia zagrożenia i opis jego możliwych skutków dla ludzi, gospodarki, infrastruktury, mienia w znacznych rozmiarach, środowiska lub dziedzictwa kulturowego, z uwzględnieniem scenariuszy zmian klimatu;

15) szacowaniu ryzyka – należy przez to rozumieć określenie poziomu akceptacji ryzyka z uwzględnieniem wyników analizy ryzyka oraz posiadanych sił i środków w zakresie organizacyjnym, technicznym i finansowym;

16) module zadaniowym – należy przez to rozumieć zestawienie przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez wykonawcę wskazanego w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony podmiotów wskazanych w siatce bezpieczeństwa;
17) planach zarządzania kryzysowego – należy przez to rozumieć plany zarządzania ryzykiem oraz plany reagowania kryzysowego;
18) planach zarządzania ryzykiem – należy przez to rozumieć Krajowy Plan Zarządzania Ryzykiem, plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany zarządzania ryzykiem;
19) planach reagowania kryzysowego – należy przez to rozumieć Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego;
20) zagrożeniu hybrydowym – należy przez to rozumieć zaplanowane i skoordynowane działania prowadzone przez podmioty państwowe lub niepaństwowe w sposób utrudniający przypisanie odpowiedzialności za nie sprawcy, które zmierzają do osiągnięcia celów politycznych, strategicznych lub wojskowych oraz mogą łączyć różne środki wywierania nacisku i uzależniania od potencjalnego agresora, takie jak polityczne, militarne, ekonomiczne, społeczne, prawne oraz informacyjne;
21) zarządzaniu sytuacją hybrydową – należy przez to rozumieć prognozowanie, przeciwdziałanie i reagowanie na zagrożenia hybrydowe.”;

2) w art. 4:
   a) w ust. 1 po pkt 1 dodaje się pkt 1a w brzmieniu:
      „1a) prowadzenie oceny ryzyka;”,
   b) w ust. 2 w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6 i 7 w brzmieniu:
      „6) organizacyjne i techniczne możliwości wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego, zgodnie z art. 25 ustawy;

7) organizacyjne i techniczne możliwości wsparcia Sił Zbrojnych Rzeczypospolitej Polskiej oraz wojsk sojuszniczych w przypadku ich użycia do realizacji zobowiązań sojuszniczych w ramach Organizacji Traktatu Północnoatlantyckiego na terytorium Rzeczypospolitej Polskiej.”;

3) uchyla się art. 5;

4) art. 5a otrzymuje brzmienie:

„Art. 5a. 1. W celu dokonania oceny ryzyka wystąpienia zagrożeń oraz określenia celów strategicznych służących ograniczeniu ryzyka wystąpienia zagrożeń opracowuje się Raport o zagrożeniach bezpieczeństwa narodowego, zwany dalej „Raportem”.

2. Raport zawiera:

1) identyfikację i charakterystykę zagrożeń oraz skutków ich wystąpienia, obejmujące zagrożenia:
   a) o istotnym wpływie na funkcjonowanie i możliwości rozwoju państwa, w szczególności mogące mieć istotne znaczenie dla bezpieczeństwa narodowego i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego,
   b) których skutki mogą:
      – godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, w szczególności w suwerenność, niepodległość i nienaruszalność terytorium,
      – zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach,
      – oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa,
      – dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie,
   c) występujące w rejonach napięć, konfliktów i kryzysów międzynarodowych, mające wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych,
   d) o charakterze terrorystycznym mogące doprowadzić do sytuacji kryzysowej,
   e) cyberbezpieczeństwa mogące doprowadzić do sytuacji kryzysowej;
2) analizę ryzyka z uwzględnieniem zagrożeń transgranicznych oraz zagrożeń o małym prawdopodobieństwie wystąpienia i katastrofalnych skutkach;
3) szacowanie ryzyka;

4) mapy ryzyka;
5) matrycę ryzyka;
6) określenie celów strategicznych służących ograniczeniu ryzyka, z uwzględnieniem:
   a) celów priorytetowych służących realizacji postanowień Ramowego programu działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof[2)], w okresie jego obowiązywania,
   b) hierarchizacji celów według kryterium ważności;
7) wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych;
8) hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych z uwzględnieniem regionalnych lub lokalnych inicjatyw;
9) ocenę realizacji celów strategicznych i przedsięwzięć niezbędnych do ich osiągnięcia;
10) wnioski i informacje przydatne przy opracowywaniu planów zarządzania kryzysowego.

3. Na potrzeby opracowania Raportu ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie opracowują raporty cząstkowe o zagrożeniach bezpieczeństwa narodowego, zwane dalej „raportami cząstkowymi”.

4. Raport cząstkowy zawiera:

1) identyfikację zagrożeń oraz skutków ich wystąpienia obejmujące zagrożenia:
   a) o istotnym wpływie na funkcjonowanie i możliwości rozwoju państwa, w szczególności mogące mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego,
   b) których skutki mogą:
      – godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, w szczególności w suwerenność, niepodległość i nienaruszalność terytorium,
      – zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach,

---

2) Ramowy program działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof został przyjęty w dniu 18 marca 2015 r. podczas Trzeciej Światowej Konferencji ONZ w sprawie ograniczenia ryzyka katastrof, która odbyła się w Sendai w dniach 14-18 marca 2015 r. (Rezolucja nr 69/283 Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych przyjęta w dniu 3 czerwca 2015 r. – A/RES/69/283).

– oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa,
– dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie,

c) występujące w rejonach napięć, konfliktów i kryzysów międzynarodowych, mające wpływ na bezpieczeństwo Rzeczypospolitej Polskiej lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych,
d) o charakterze terrorystycznym mogące doprowadzić do sytuacji kryzysowej,
e) cyberbezpieczeństwa mogące doprowadzić do sytuacji kryzysowej;

2) analizę ryzyka z uwzględnieniem zagrożeń transgranicznych oraz zagrożeń o małym prawdopodobieństwie wystąpienia i katastrofalnych skutkach;
3) szacowanie ryzyka;
4) mapy ryzyka;
5) matrycę ryzyka;
6) cele strategiczne służące ograniczeniu ryzyka z uwzględnieniem:
   a) celów priorytetowych służących realizacji postanowień Ramowego programu działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof, przyjętego podczas Trzeciej Światowej Konferencji ONZ, w okresie jego obowiązywania,
   b) hierarchizacji celów według kryterium ważności;
7) wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych;
8) hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych z uwzględnieniem regionalnych lub lokalnych inicjatyw;
9) ocenę realizacji celów strategicznych i przedsięwzięć niezbędnych do ich osiągnięcia;
10) wnioski i informacje, przydatne przy opracowywaniu planów zarządzania kryzysowego.

5. Opracowanie raportów cząstkowych koordynuje Rządowe Centrum Bezpieczeństwa, z wyłączeniem części:

1) dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Szef Agencji Bezpieczeństwa Wewnętrznego, oraz

2) dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

6. Na podstawie otrzymanych raportów cząstkowych Rządowe Centrum Bezpieczeństwa opracowuje Raport, z wyłączeniem części:

1) dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, którą opracowuje Szef Agencji Bezpieczeństwa Wewnętrznego,

2) dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, którą opracowuje Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

7. Dyrektor Rządowego Centrum Bezpieczeństwa przedkłada Raport Radzie Ministrów co trzy lata.

8. Rada Ministrów przyjmuje Raport w drodze uchwały.

9. Rada Ministrów określi, w drodze rozporządzenia, sposób i tryb opracowania raportów cząstkowych, biorąc pod uwagę zapewnienie terminowości i sprawności opracowania Raportu o zagrożeniach bezpieczeństwa narodowego.”;

5) po art. 5a dodaje się art. 5aa–5aj w brzmieniu:

„Art. 5aa. 1. Ocena ryzyka wynikająca z Raportu oraz wnioski, o których mowa w art. 5a ust. 2 pkt 10, są uwzględniane w planach zarządzania kryzysowego oraz w innych dokumentach opracowywanych przez organy administracji publicznej w zakresie zarządzania kryzysowego.

2. Na podstawie Raportu Rządowe Centrum Bezpieczeństwa opracowuje streszczenie istotnych elementów krajowej oceny ryzyka.

3. Dyrektor Rządowego Centrum Bezpieczeństwa udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny ryzyka.

Art. 5ab. 1. Plan zarządzania ryzykiem zawiera:

1) charakterystykę zagrożeń, w tym zagrożeń dotyczących infrastruktury krytycznej, uwzględnionej w wykazach, o których mowa w art. 5c pkt 1 i art. 5f pkt 1;

2) opis zasad współdziałania między podmiotami wskazanymi w siatce bezpieczeństwa;

3) uporządkowaną listę działań na rzecz ograniczenia ryzyka katastrof w zakresie organizacyjnym, technicznym i finansowym, z uwzględnieniem:

a) hierarchii działań,

b) ram czasowych ich realizacji,

c) podmiotów wiodących oraz współpracujących przy ich wykonywaniu,

d) sposobów finansowania oraz wysokości nakładów finansowych,

e) oceny osiągniętych efektów oraz wniosków z wdrożonych działań.

2. Plany zarządzania ryzykiem opracowują:

1) Rządowe Centrum Bezpieczeństwa – Krajowy Plan Zarządzania Ryzykiem;
2) ministrowie kierujący działami administracji rządowej – plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej;
3) kierownicy urzędów centralnych – plany zarządzania ryzykiem kierowników urzędów centralnych;
4) wojewodowie – wojewódzkie plany zarządzania ryzykiem;
5) starostowie – powiatowe plany zarządzania ryzykiem;
6) wójtowie (burmistrzowie, prezydenci miast) – gminne plany zarządzania ryzykiem.

3. Gminny plan zarządzania ryzykiem wójt (burmistrz, prezydent miasta) przekazuje właściwemu miejscowo staroście.

4. Powiatowy plan zarządzania ryzykiem starosta przekazuje właściwemu miejscowo wojewodzie.

Art. 5ac. 1. Rządowe Centrum Bezpieczeństwa, uwzględniając plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów, opracowuje Krajowy Plan Zarządzania Ryzykiem.

2. Minister właściwy do spraw rozwoju regionalnego opiniuje Krajowy Plan Zarządzania Ryzykiem pod względem spójności z programami strukturalnymi.

3. Dyrektor Rządowego Centrum Bezpieczeństwa przedkłada Radzie Ministrów Krajowy Plan Zarządzania Ryzykiem.

4. Rada Ministrów przyjmuje Krajowy Plan Zarządzania Ryzykiem w drodze uchwały.

Art. 5ad. 1. Plany reagowania kryzysowego opracowują:

1) Rządowe Centrum Bezpieczeństwa – Krajowy Plan Reagowania Kryzysowego;
2) ministrowie kierujący działami administracji rządowej – plany reagowania kryzysowego ministrów kierujących działami administracji rządowej;
3) kierownicy urzędów centralnych – plany reagowania kryzysowego kierowników urzędów centralnych;
4) wojewodowie – wojewódzkie plany reagowania kryzysowego;

5) starostowie – powiatowe plany reagowania kryzysowego;
6) wójtowie (burmistrzowie, prezydenci miast) – gminne plany reagowania kryzysowego.

2. Gminny plan reagowania kryzysowego wójt (burmistrz, prezydent miasta) przekazuje właściwemu miejscowo staroście.

3. Powiatowy plan reagowania kryzysowego starosta przekazuje właściwemu miejscowo wojewodzie.

Art. 5ae. 1. Krajowy Plan Reagowania Kryzysowego zawiera:

1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;
2) opis zasad współdziałania między uczestnikami, o których mowa w pkt 1, w tym wymiany informacji w relacjach krajowych i międzynarodowych;
3) zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych;
4) wykaz katalogów i modułów zadaniowych;
5) załączniki funkcjonalne określające:
   a) organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania,
   b) organizację łączności,
   c) zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,
   d) zasady oraz tryb oceniania i dokumentowania szkód,
   e) procedury uruchamiania rezerw strategicznych,
   f) procedury reagowania kryzysowego – standardowe procedury operacyjne,
   g) priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej,
   h) wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie reagowania kryzysowego.

2. Dyrektor Rządowego Centrum Bezpieczeństwa przedkłada Radzie Ministrów Krajowy Plan Reagowania Kryzysowego.

3. Rada Ministrów przyjmuje Krajowy Plan Reagowania Kryzysowego w drodze uchwały.

4. Plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych są uzgadniane z dyrektorem Rządowego

Centrum Bezpieczeństwa i stanowią załączniki funkcjonalne do Krajowego Planu Reagowania Kryzysowego.

Art. 5af. Plany reagowania kryzysowego ministrów i kierowników urzędów zawierają:

1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków;
2) określenie zadań w zakresie monitorowania zagrożeń;
3) wykaz przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych wraz z ich opisem;
4) określenie organizacji realizacji zadań z zakresu ochrony infrastruktury krytycznej.

Art. 5ag. Wojewódzkie plany reagowania kryzysowego zawierają:

1) elementy, o których mowa w art. 5ae ust. 1 pkt 1–3;
2) określenie zadań w zakresie monitorowania zagrożeń;
3) wykaz przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych wraz z ich opisem;
4) wykaz działań określonych planami działań krótkoterminowych, o których mowa w art. 92 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (Dz. U. z 2019 r. poz. 1396, z późn. zm.[3)]), wraz z ich opisem;
5) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa, wraz z ich opisem;
6) załączniki funkcjonalne, o których mowa w art. 5ae ust. 1 pkt 5.

Art. 5ah. Powiatowe i gminne plany reagowania kryzysowego zawierają:

1) elementy, o których mowa w art. 5ae ust. 1 pkt 1–3;
2) określenie zadań w zakresie monitorowania zagrożeń;
3) wykaz przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych, wraz z ich opisem;
4) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem;
5) załączniki funkcjonalne, o których mowa w art. 5ae ust. 1 pkt 5.

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2019 r. poz. 1403, 1495, 1501, 1527, 1579, 1680, 1712,1815, 2087 i 2166.

Art. 5ai. 1. Plany zarządzania kryzysowego podlegają systematycznej aktualizacji, w cyklu planowania nie dłuższym niż trzy lata.

2. Cykl planowania realizują właściwe organy administracji publicznej oraz podmioty przewidywane do realizacji przedsięwzięć określonych w planie zarządzania kryzysowego, w zakresie ich dotyczącym.

3. Plany zarządzania kryzysowego uzgadnia się z kierownikami jednostek organizacyjnych, w zakresie ich dotyczącym, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planie.

4. Plany postępowania na wypadek wystąpienia sytuacji kryzysowej, opracowane na podstawie odrębnych przepisów z wyłączeniem planów sporządzanych na czas zewnętrznego zagrożenia bezpieczeństwa państwa i na czas wojny, stanowią załączniki do planu reagowania kryzysowego właściwego organu administracji publicznej.

Art. 5aj 1. Na podstawie Raportu oraz planów zarządzania kryzysowego Rządowe Centrum Bezpieczeństwa opracowuje streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem.

2. Dyrektor Rządowego Centrum Bezpieczeństwa udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem.”;

6) w art. 5b:

a) ust. 2 i 3 otrzymują brzmienie:

„2. Program określa:

1) narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej;

2) ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy, o których mowa w art. 3 pkt 2;

3) szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, uwzględniając ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli;

4) szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej na obszarze województwa, uwzględniając ich znaczenie dla funkcjonowania organów administracji publicznej oraz zaspokojenia potrzeb obywateli na obszarze województwa;

5) wskazanie, w podziale na systemy, o których mowa w art. 3 pkt 2, usług kluczowych dla bezpieczeństwa państwa i jego obywateli oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców;
6) formy ochrony pozwalające zapewnić ciągłość funkcjonowania infrastruktury krytycznej, w szczególności w zakresie:
   a) zapewnienia bezpieczeństwa fizycznego,
   b) zapewnienia bezpieczeństwa technicznego,
   c) zapewnienia bezpieczeństwa osobowego,
   d) zapewnienia bezpieczeństwa teleinformatycznego,
   e) zapewnienia bezpieczeństwa prawnego,
   f) planów ciągłości działania i odtwarzania;
7) propozycje wymagań, standardów lub dobrych praktyk pozwalających zapewnić ciągłość funkcjonowania infrastruktury krytycznej.

3. Program opracowuje Rządowe Centrum Bezpieczeństwa we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych oraz wojewodami.”,

b) po ust. 3 dodaje się ust. 3a–3h w brzmieniu:

„3a. Na potrzeby opracowania programu Rządowe Centrum Bezpieczeństwa, na rok przed przystąpieniem do jego opracowania, przekazuje organom, o których mowa w ust. 3, zakres informacji niezbędnych do przygotowania opisu działań planowanych do określenia w programie oraz informuje o terminie przystąpienia do opracowania tego programu.

3b. Organy, o których mowa w ust. 3, każdy w zakresie swojej właściwości, przygotowują i przekazują Rządowemu Centrum Bezpieczeństwa, nie później niż na 6 miesięcy przed terminem opracowania projektu programu, propozycje rozwiązań planowanych do określenia w programie, wskazując:

1) wykaz funkcji, celów i zadań wymienionych w ustawie budżetowej w części dotyczącej układu zadaniowego wraz ze wskazaniem usług niezbędnych do ich realizacji;
2) usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców;

3) podatność na wystąpienie zagrożenia i potencjalne skutki wynikające z ograniczenia lub niedostępności usług, o których mowa w pkt 2, z uwzględnieniem zależności od infrastruktury krytycznej;

4) proponowane sposoby zmniejszenia podatności na wystąpienie zagrożenia i potencjalnych skutków usług, o których mowa w pkt 3;

5) propozycje wymagań, standardów lub dobrych praktyk pozwalających zapewnić ciągłość świadczenia usług wskazanych w pkt 2.

3c. Organy, o których mowa w ust. 3, przekazują Rządowemu Centrum Bezpieczeństwa, wraz z propozycjami rozwiązań wskazanymi w ust. 3b, dane stanowiące podstawę do ich przygotowania.

3d. Dyrektor Rządowego Centrum Bezpieczeństwa, mając na względzie zapewnienie spójności i kompletności programu, może wystąpić o przekazanie także innych informacji niż określone w ust. 3b, jeżeli uzna je za niezbędne do umieszczenia w programie.

3e. Rządowe Centrum Bezpieczeństwa uzgadnia zakres i sposób uwzględnienia propozycji rozwiązań, o których mowa w ust. 3b, z organami, o których mowa w ust. 3.

3f. Rządowe Centrum Bezpieczeństwa opracowuje program z uwzględnieniem propozycji, o których mowa w ust. 3b.

3g. Dyrektor Rządowego Centrum Bezpieczeństwa przedkłada program Radzie Ministrów.

3h. Rada Ministrów przyjmuje program w drodze uchwały.”,

c) ust. 5 otrzymuje brzmienie:

„5. Program podlega aktualizacji nie rzadziej niż raz na trzy lata.”,

d) uchyla się ust. 7 i 9;

7) po art. 5b dodaje się art. 5c–5n w brzmieniu:

„Art. 5c. Dyrektor Rządowego Centrum Bezpieczeństwa:

1) sporządza na podstawie kryteriów, o których mowa w art. 5b ust. 2 pkt 3, we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych odpowiedzialnymi za systemy, krajowy wykaz obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej z podziałem na poszczególne systemy, zwany dalej „wykazem krajowym”. Wykaz krajowy ma charakter niejawny;

2) opracowuje wyciągi z wykazu krajowego dotyczące obiektów, instalacji, urządzeń lub usług znajdujących się w danym systemie oraz przekazuje je ministrom lub kierownikom urzędów centralnych odpowiedzialnym za system, w skład którego wchodzi infrastruktura krytyczna;
3) opracowuje wyciągi z wykazu krajowego dotyczące obiektów, instalacji, urządzeń lub usług znajdujących się na obszarze danego województwa oraz przekazuje właściwemu wojewodzie;
4) informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług o ujęciu w wykazie krajowym;
5) zatwierdza plany ochrony infrastruktury krytycznej**,** po uzgodnieniu ich z ministrem lub kierownikiem urzędu centralnego odpowiedzialnym za system, w którego skład wchodzi infrastruktura krytyczna.

Art. 5d. 1. Dyrektor Rządowego Centrum Bezpieczeństwa sporządza wykaz zawierający europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską, zwany dalej „wykazem europejskiej infrastruktury krytycznej”. Wykaz europejskiej infrastruktury krytycznej ma charakter niejawny.

2. W przypadku infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej, ujętej w wykazie europejskiej infrastruktury krytycznej, przepisy art. 5c pkt 2–5 stosuje się odpowiednio.

Art. 5e. 1. Dyrektor Rządowego Centrum Bezpieczeństwa sporządza, we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych, wykaz obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej z podziałem na poszczególne systemy, będących w fazie projektowania lub budowy, mogących potencjalnie spełniać kryteria, o których mowa w art. 5b ust. 2 pkt 3, zwany dalej „wykazem potencjalnej infrastruktury krytycznej”.

2. W przypadku infrastruktury krytycznej, ujętej w wykazie potencjalnej infrastruktury krytycznej, przepisy art. 5c pkt 2–4 stosuje się odpowiednio.

Art. 5f. Wojewoda:

1) sporządza na podstawie szczegółowych kryteriów, o których mowa w art. 5b ust. 2 pkt 4, wojewódzki wykaz obiektów, instalacji, urządzeń i usług wchodzących

w skład infrastruktury krytycznej z podziałem na systemy, zwany dalej „wykazem wojewódzkim”. Wykaz wojewódzki ma charakter niejawny;

2) opracowuje wyciągi z wykazu wojewódzkiego oraz przekazuje ministrom kierującym działami administracji rządowej i kierownikom urzędów centralnych odpowiedzialnym za dany system;
3) przekazuje wykaz wojewódzki dyrektorowi Rządowego Centrum Bezpieczeństwa;
4) informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług o ujęciu w wykazie wojewódzkim;
5) zatwierdza plany ochrony infrastruktury krytycznej ujętej w wykazie wojewódzkim.

Art. 5g. 1. Operator infrastruktury krytycznej zapewnia ochronę infrastruktury krytycznej, w szczególności przez:

1) opracowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej;
2) utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej, do czasu jej pełnego odtworzenia;
3) zapewnienie zdolności do ochrony informacji niejawnych w związku z realizacją przedsięwzięć w zakresie ochrony infrastruktury krytycznej.

2. Operator infrastruktury krytycznej będący jednocześnie operatorem usługi kluczowej w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560, z 2019 r. poz. 2020 i 2248 oraz z 2020 r. poz. …) uwzględnia w planach ochrony infrastruktury krytycznej dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych określoną w przepisach wydanych na podstawie art. 10 ust. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. Do zadań operatora infrastruktury krytycznej należy:

1) opracowywanie i wdrażanie planów ochrony infrastruktury krytycznej oraz bieżące monitorowanie stopnia wdrożenia planów;
2) sporządzanie i przekazywanie informacji w zakresie realizacji zapewnienia ochrony infrastruktury krytycznej, na żądanie:
   a) dyrektora Rządowego Centrum Bezpieczeństwa,
   b) właściwego ministra odpowiedzialnego za jeden z systemów, o których mowa w art. 3 pkt 2, albo

c) właściwego kierownika urzędu centralnego odpowiedzialnego za jeden z systemów, o których mowa w art. 3 pkt 2, albo

d) właściwego terytorialnie wojewody;

3) zapewnienie współpracy z organami administracji publicznej oraz dyrektorem Rządowego Centrum Bezpieczeństwa przez przekazywanie i odbieranie informacji o:

a) zdarzeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej,

b) spodziewanym lub zaobserwowanym zwiększeniu zapotrzebowania na usługi lub produkty dostarczane przez operatorów infrastruktury krytycznej,

c) spodziewanych przerwach lub zakłóceniach w dostawach usług lub produktów dostarczanych przez operatorów infrastruktury krytycznej.

Art. 5h. 1. Operator infrastruktury krytycznej sporządza do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

2. Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące ochrony infrastruktury krytycznej w zakresie:

1) zapewnienia bezpieczeństwa fizycznego;

2) zapewnienia bezpieczeństwa technicznego;

3) zapewnienia bezpieczeństwa osobowego;

4) zapewnienia bezpieczeństwa teleinformatycznego;

5) zapewnienia bezpieczeństwa prawnego;

6) planów ciągłości działania i odtwarzania.

3. Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem:

1) rozwiązań zawartych w planie ochrony infrastruktury krytycznej operatora;

2) wystąpienia ryzyka dla infrastruktury krytycznej zidentyfikowanego w planie ochrony infrastruktury krytycznej;

3) incydentów i zdarzeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w planie ochrony infrastruktury krytycznej;

4) wyników przeprowadzonych kontroli i audytów odnoszących się do zabezpieczeń zawartych w planie ochrony infrastruktury krytycznej;

5) opisu działań podjętych przez operatora w przypadkach, o których mowa w pkt 2–4.

4. Operator infrastruktury krytycznej przekazuje raport o stanie ochrony infrastruktury krytycznej dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio:

1) właściwemu ministrowi odpowiedzialnemu za jeden z systemów, o których mowa w art. 3 pkt 2, albo
2) właściwemu kierownikowi urzędu centralnego odpowiedzialnemu za jeden z systemów, o których mowa w art. 3 pkt 2, albo
3) właściwemu terytorialnie wojewodzie.

5. Raport o stanie ochrony infrastruktury krytycznej sporządza się z zachowaniem przepisów o ochronie informacji niejawnych.

Art. 5i. 1. W celu zapewnienia realizacji zadań, o których mowa w art. 5g ust. 3 i art. 5h ust. 1, operator infrastruktury krytycznej wyznacza koordynatora do spraw ochrony infrastruktury krytycznej, zwanego dalej „koordynatorem”.

2. Operator ochrony infrastruktury krytycznej wyznacza koordynatora w terminie 30 dni od dnia otrzymania informacji, o której mowa w art. 5c pkt 4, art. 5d ust. 2 i art. 5f pkt 4.

3. Koordynatorem może być osoba, która:

1) jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej;
2) korzysta z pełni praw publicznych;
3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem organizacji, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej;
4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli co najmniej:
   a) „poufne” w przypadku zajmowania stanowiska koordynatora w strukturze organizacyjnej operatora infrastruktury krytycznej, o którym mowa w art. 5c pkt 1, albo

b) „zastrzeżone” w przypadku zajmowania stanowiska koordynatora w strukturze organizacyjnej operatora infrastruktury krytycznej, o którym mowa w art. 5f pkt 1.

4. Koordynator podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej.

5. O wyznaczeniu koordynatora operator infrastruktury krytycznej informuje niezwłocznie dyrektora Rządowego Centrum Bezpieczeństwa oraz:

1) właściwego ministra odpowiedzialnego za jeden z systemów, o których mowa w art. 3 pkt 2, albo
2) właściwego kierownika urzędu centralnego odpowiedzialnego za jeden z systemów, o których mowa w art. 3 pkt 2, albo
3) właściwego terytorialnie wojewodę.

Art. 5j. Koordynator może przedkładać rekomendacje organowi zarządzającemu operatora infrastruktury krytycznej w zakresie ochrony jego obiektów, instalacji, urządzeń i usług ujętych w wykazach, o których mowa w art. 5c pkt 1, art. 5d ust. 1 i art. 5f pkt 1.

Art. 5k. Operator infrastruktury krytycznej zapewnia koordynatorowi organizacyjne i techniczne warunki realizacji zadań, o których mowa w art. 5g ust. 3 i art. 5h ust. 1, w tym dostęp do dokumentów i informacji.

Art. 5l. 1. Dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z odpowiednimi ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych na bieżąco rozpoznaje obiekty budowlane, urządzenia, instalacje i usługi, będące w fazie projektowania lub budowy, potencjalnie spełniające kryteria, o których mowa w art. 5b ust. 2 pkt 3, zwane dalej „potencjalną infrastrukturą krytyczną”.

2. Obiekt, instalację, urządzenie lub usługę uznaje się za potencjalną infrastrukturę krytyczną, jeżeli z założeń projektowych wynika, że będzie ona kluczowa dla bezpieczeństwa państwa i jego obywateli oraz będzie służyć zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, oraz spełni kryteria, o których mowa w art. 5b ust. 2 pkt 3.

3. W celu wyznaczenia potencjalnej infrastruktury krytycznej dyrektor Rządowego Centrum Bezpieczeństwa prowadzi rozmowy z inwestorem lub operatorem infrastruktury krytycznej.

4. Dyrektor Rządowego Centrum Bezpieczeństwa w rozmowach przedstawia stanowisko uzgodnione z ministrami i kierownikami urzędów centralnych, których przedstawiciele mogą brać udział w rozmowach.

5. Na podstawie ustaleń będących wynikiem rozmów dyrektor Rządowego Centrum Bezpieczeństwa ujmuje obiekt, instalację, urządzenie lub usługę w wykazie potencjalnej infrastruktury krytycznej.

6. Dyrektor Rządowego Centrum Bezpieczeństwa powiadamia inwestora lub operatora infrastruktury krytycznej o ujęciu w wykazie potencjalnej infrastruktury krytycznej.

7. Dyrektor Rządowego Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy, o których mowa w art. 3 pkt 2, przedstawia inwestorowi informacje oraz dokumenty, pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub podczas realizacji inwestycji.

Art. 5m. 1. Operator opracowuje plan ochrony infrastruktury krytycznej, który zawiera:

1) dane ogólne:
   a) obejmujące nazwę i lokalizację infrastruktury krytycznej,
   b) pozwalające zidentyfikować operatora infrastruktury krytycznej, w tym nazwę, adres i siedzibę oraz numery REGON, NIP i KRS,
   c) pozwalające zidentyfikować zarządzającego przedsiębiorstwem w imieniu operatora infrastruktury krytycznej, w tym nazwę, adres i siedzibę, numery REGON, NIP i KRS;
2) dane infrastruktury krytycznej obejmujące:
   a) charakterystykę procesów, stosowanych technologii i podstawowe parametry techniczne,
   b) plan (mapę) z naniesieniem lokalizacji obiektów, instalacji, urządzeń lub systemu z zaznaczeniem elementów zapewniających bezpieczeństwo infrastruktury krytycznej,
   c) opis funkcjonalnych połączń z innymi obiektami, instalacjami, urządzeniami lub usługami;
3) charakterystykę:

a) zagrożeń i ryzyka dla infrastruktury krytycznej wraz z przewidywanymi scenariuszami rozwoju zdarzeń,

b) zależności infrastruktury krytycznej od pozostałych systemów infrastruktury krytycznej oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach infrastruktury krytycznej,

c) organizacyjnych i technicznych elementów zapewniających bezpieczeństwo infrastruktury krytycznej,

d) zasobów właściwych terytorialnie organów, możliwych do wykorzystania w celu ochrony infrastruktury krytycznej;

4) warianty:

a) działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej,

b) zapewnienia ciągłości funkcjonowania infrastruktury krytycznej,

c) odtwarzania infrastruktury krytycznej;

5) zasady współpracy z właściwymi miejscowo:

a) centrami zarządzania kryzysowego,

b) organami administracji publicznej.

2. Operator infrastruktury krytycznej może zawrzeć w planie ochrony infrastruktury krytycznej dodatkowe elementy, biorąc pod uwagę specyfikę infrastruktury krytycznej lub charakterystykę zagrożeń.

3. Do planu ochrony infrastruktury krytycznej stosuje się przepisy o ochronie informacji niejawnych lub o ochronie tajemnicy przedsiębiorstwa.

4. Operator infrastruktury krytycznej uzgadnia plan ochrony infrastruktury krytycznej z:

1) ministrem lub kierownikiem urzędu centralnego odpowiedzialnym za system, w którego skład wchodzi infrastruktura krytyczna, albo

2) właściwym terytorialnie wojewodą.

5. Plan ochrony infrastruktury krytycznej, w zależności od charakterystyki infrastruktury krytycznej, podlega również uzgodnieniu, w zakresie ich dotyczącym, z właściwym terytorialnie:

1) komendantem wojewódzkim Państwowej Straży Pożarnej;

2) komendantem wojewódzkim (Stołecznym) Policji;

3) dyrektorem regionalnego zarządu gospodarki wodnej Wód Polskich;

4) wojewódzkim inspektorem nadzoru budowlanego;

5) wojewódzkim lekarzem weterynarii;

6) państwowym wojewódzkim inspektorem sanitarnym;

7) dyrektorem urzędu morskiego.

6. Rada Ministrów określi, w drodze rozporządzenia, sposób i tryb opracowywania oraz zatwierdzania planów ochrony infrastruktury krytycznej, mając na względzie potrzebę zapewnienia ciągłości funkcjonowania infrastruktury krytycznej.

Art. 5n. 1. W przypadku gdy dla obiektów, instalacji i usług infrastruktury krytycznej istnieją, tworzone na podstawie odrębnych przepisów, plany odpowiadające wymogom planu ochrony infrastruktury krytycznej, operator infrastruktury krytycznej, który posiada plan opracowany na podstawie odrębnych przepisów i odpowiadający wymogom planu ochrony infrastruktury krytycznej, przedkłada ten plan dyrektorowi Rządowego Centrum Bezpieczeństwa w celu uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

2. Plan odpowiadający wymogom planu ochrony infrastruktury krytycznej zawiera elementy, o których mowa w art. 5m ust. 1.

3. Dyrektor Rządowego Centrum Bezpieczeństwa, kierując się potrzebą zapewnienia ciągłości funkcjonowania infrastruktury krytycznej oraz postanowieniami programu, uznaje spełnienie obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

4. Rada Ministrów określi, w drodze rozporządzenia, tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej, uwzględniając potrzebę zapewnienia ciągłości funkcjonowania infrastruktury krytycznej.”;

8) w art. 6:

a) w ust. 1 pkt 5 otrzymuje brzmienie:

„5) współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie jej ochrony.”,

b) uchyla się ust. 5–7;

9) w art. 9 po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) monitorowanie i rekomendowanie Radzie Ministrów działań dotyczących zarządzania sytuacją hybrydową;”;

10) w art. 10 po ust. 2a dodaje się ust. 2b i 2c w brzmieniu:

„2b. Dyrektor Centrum reprezentuje Centrum w zakresie realizacji zadań, o których mowa w art. 5a ust. 5–7, art. 5aa ust. 2, art. 5ab ust. 2 pkt 1, art. 5ac ust. 1, art. 5ad ust. 1, art. 5aj ust. 1, art. 5b ust. 3, 3a–3c i 3e–3g, art. 11 oraz art. 11a.

2c. Dyrektor Centrum wykonuje zadania, o których mowa w art. 5a ust. 7, art. 5aa ust. 3, art. 5ac ust. 3, art. 5ae ust. 2 i 4, art. 5aj ust. 2, art. 5b ust. 3d i 3g, art. 5c, art. 5d ust. 1, art. 5e ust. 1, art. 5l, art. 5n ust. 3, art. 6a ust. 1, art. 6b, art. 6c, art. 14 ust. 3 i 4, art. 20b oraz art. 21a.”;

11) w art. 11 w ust. 2:

a) w pkt 1:

– lit. b otrzymuje brzmienie:

„b) opracowywanie i aktualizowanie Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego,”,

– w lit. g średnik zastępuje się przecinkiem i dodaje się lit. h w brzmieniu:

„h) uzgadnianie planów zarządzania kryzysowego sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych;”,

b) uchyla się pkt 2a;

c) pkt 3 otrzymuje brzmienie:

„3) przygotowanie uruchamiania, w przypadku zaistnienia zagrożeń, procedur związanych z reagowaniem kryzysowym;”,

d) pkt 6 otrzymuje brzmienie:

„6) współdziałanie z podmiotami, komórkami i jednostkami organizacyjnymi Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej, Organizacji Narodów Zjednoczonych oraz innych organizacji międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej;”,

e) pkt 9 otrzymuje brzmienie:

„9) realizacja zadań stałego dyżuru Prezesa Rady Ministrów w ramach podwyższania gotowości obronnej państwa;”,

f) uchyla się pkt 10 i 10a,

g) w pkt 15 kropkę zastępuje się średnikiem i dodaje się pkt 16 w brzmieniu:

„16) pełnienie funkcji koordynatora oraz krajowego punktu kontaktowego dla Organizacji Narodów Zjednoczonych do spraw wdrażania Ramowego

Programu Działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof, w okresie jego obowiązywania.”;

12) w art. 12:

a) ust.1 otrzymuje brzmienie:

„1. Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują, w zakresie swojej właściwości, zadania dotyczące zarządzania kryzysowego, w tym:

1) opracowują plany zarządzania kryzysowego;
2) organizują, prowadzą i koordynują szkolenia i ćwiczenia z zakresu zarządzania kryzysowego oraz biorą udział w ćwiczeniach krajowych i międzynarodowych;
3) współpracują z operatorami infrastruktury krytycznej przy tworzeniu planów ochrony infrastruktury krytycznej oraz planów zarządzaniu kryzysowego.”;

b) uchyla się ust. 2 i 2a;

c) ust. 2c otrzymuje brzmienie:

„2c. Do zadań zespołów, o których mowa w ust. 2b, należy:

1) dokonywanie okresowej oceny ryzyka oraz elementów, o których mowa w art. 5a ust. 2 pkt 5 i 6, na potrzeby Raportu;
2) dokonywanie okresowej oceny gotowości do reagowania w zakresie organizacyjnym, technicznym i finansowym;
3) opiniowanie projektów planów zarządzania kryzysowego;
4) opiniowanie wykazu infrastruktury krytycznej w ramach swojej właściwości;
5) wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.”;

13) po art. 13 dodaje się art. 13a w brzmieniu:

„Art. 13a. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie wdrażają Ramowy Program Działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof oraz przekazują dyrektorowi Centrum, w wyznaczonym terminie, raporty dotyczące jego wdrażania oraz inne informacje, niezbędne do realizacji przez Centrum zadania, o którym mowa w art. 11 ust. 2 pkt 16.”;

14) w art. 14:

a) w ust. 2:

– pkt 3 otrzymuje brzmienie:

„3) organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych;”,

– uchyla się pkt 6 i 6a,

b) po ust. 3 dodaje się ust. 3a w brzmieniu:

„3a.Wytyczne do wojewódzkich planów zarządzania kryzysowego mogą zostać wydane w każdym czasie i są wydawane niezależnie od cyklu planowania.”,

c) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. Wojewoda przekazuje dyrektorowi Centrum zatwierdzony wojewódzki plan zarządzania kryzysowego.”;

15) w art. 17 w ust. 2:

a) pkt 3 otrzymuje brzmienie:

„3) organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych;”,

b) uchyla się pkt 5 i 5a;

16) w art. 19 w ust. 2:

a) pkt 3 otrzymuje brzmienie:

„3) organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych;”,

b) uchyla się pkt 5 i 5a;

17) art. 20b otrzymuje brzmienie:

„Art. 20b. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, starostowie, wójtowie, burmistrzowie, prezydenci miast, operatorzy infrastruktury krytycznej oraz inwestorzy potencjalnej infrastruktury krytycznej są obowiązani do udzielania dyrektorowi Centrum, w wyznaczonym terminie, żądanych przez niego informacji i wyjaśnień niezbędnych do realizacji zadań Centrum określonych w ustawie.”;

18) w art. 21a:

a) ust. 2 otrzymuje brzmienie:

„2. Operatorzy infrastruktury krytycznej niezwłocznie informują dyrektora Centrum oraz właściwe terytorialnie wojewódzkie centrum zarządzania

kryzysowego o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej.”,

b) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu:

„3a. Obowiązek, o którym mowa w ust. 3, nie obejmuje wysyłania komunikatu użytkownikom końcowym, których karty SIM są zainstalowane i wykorzystywane w urządzeniach telemetrycznych.

3b. Operator, po wysłaniu komunikatu, niezwłocznie przekazuje dyrektorowi Centrum informację o liczbie kart SIM użytkowników końcowych, do których komunikat został wysłany i do których komunikat został dostarczony.”;

19) w art. 26 po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. Środki finansowe z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem oraz reagowaniem w przypadku wystąpienia sytuacji kryzysowej, a także usuwaniem jej skutków i odtwarzaniem zasobów.”.

Art. 2. W ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2018 r. poz. 2142 i 2245 oraz z 2019 r. poz. 1495) w art. 5 w ust. 2 pkt 5 otrzymuje brzmienie:

„5) obiekty, w tym obiekty budowlane, urządzenia, instalacje i usługi wchodzące w skład infrastruktury krytycznej ujęte w wykazach, o których mowa w art. 5c pkt 1, art. 5d ust. 1 i art. 5f pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”.

Art. 3. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27) wprowadza się następujące zmiany:

1) w art. 5 w ust. 1 pkt 2a otrzymuje brzmienie:

„2a) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …), a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;”;

2) w art. 32a ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców, ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych, zwaną dalej „oceną bezpieczeństwa”.”;

3) w art. 32aa ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców, ABW wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania”, prowadzi go i koordynuje jego funkcjonowanie.”.

Art. 4. W ustawie z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843) w art. 89 w ust. 1 pkt 7d otrzymuje brzmienie:

„7d) jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, w tym bezpieczeństwo podmiotów objętych wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …), a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób;”.

Art. 5. W ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2019 r. poz. 692) w art. 24 ust. 5 otrzymuje brzmienie:

„5. W przypadku wprowadzenia poziomu ochrony 3 stosuje się odpowiednio art. 21 i art. 25 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U z 2019 r. poz. 1398 oraz z 2020 r. poz. …).”.

Art. 6. W ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2016 r. poz. 2012) wprowadza się następujące zmiany:

1) tytuł ustawy otrzymuje brzmienie:

„o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych”;

2) w art. 1 ust. 1 otrzymuje brzmienie:

„1. Ustawa określa szczególne uprawnienia przysługujące ministrowi właściwemu do spraw energii w spółkach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w wykazach, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …), zwanych dalej „spółkami”.”;

3) w art. 1 w ust. 2:

a) pkt 1 otrzymuje brzmienie:

„1) w sektorze energii elektrycznej – infrastrukturę służącą do wytwarzania, dystrybucji albo przesyłania energii elektrycznej;”,

b) pkt 3 otrzymuje brzmienie:

„3) w sektorze paliw gazowych – infrastrukturę służącą do produkcji, wydobycia, rafinacji, przetwarzania, magazynowania, dystrybucji, przesyłania paliw gazowych gazociągami oraz terminale skroplonego gazu ziemnego (LNG).”;

4) w art. 2:

a) w ust. 2 uchyla się pkt 5,

b) ust. 3 otrzymuje brzmienie:

„3. Sprzeciw jest wyrażany w formie decyzji administracyjnej, w terminie 30 dni od dnia otrzymania przez ministra właściwego do spraw energii od

pełnomocnika do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5, informacji o podjęciu przez organy spółki uchwały lub dokonaniu przez zarząd spółki czynności prawnej, o której mowa w ust. 1 i 2, jednak nie później niż w terminie 45 dni od dnia ich dokonania.”,

c) ust. 5 otrzymuje brzmienie:

„5. W przypadku złożenia wniosku o ponowne rozpatrzenie sprawy termin na jej załatwienie wynosi 30 dni od dnia otrzymania wniosku.”;

5) w art. 5 ust. 4 otrzymuje brzmienie:

„4. Pełnomocnik do spraw ochrony infrastruktury krytycznej może być koordynatorem do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”

6) w art. 6 ust. 3 otrzymuje brzmienie:

„3. Pełnomocnik do spraw ochrony infrastruktury krytycznej sporządza dla zarządu spółki oraz rady nadzorczej raport o stanie ochrony infrastruktury krytycznej. Raport jest sporządzany co kwartał lub na żądanie zarządu spółki lub rady nadzorczej. Raport zawiera informacje dotyczące ochrony infrastruktury krytycznej w zakresie:

1) zapewnienia bezpieczeństwa fizycznego;
2) zapewnienia bezpieczeństwa technicznego;
3) zapewnienia bezpieczeństwa osobowego;
4) zapewnienia bezpieczeństwa teleinformatycznego;
5) zapewnienia bezpieczeństwa prawnego;
6) planów ciągłości działania i odtwarzania.”.

Art. 7. W ustawie z dnia 29 października 2010 r. o rezerwach strategicznych (Dz. U. z 2017 r. poz. 1846) w art. 8 w ust. 4 pkt 1 otrzymuje brzmienie:

„1) analizy i oceny możliwości wystąpienia zagrożeń wykonywane w ramach opracowywania planów zarządzania kryzysowego, o których mowa w art. 3 pkt 17 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;”.

Art. 8. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2019 r. poz. 701, 730, 1403 i 1579) w art. 25 w ust. 6i pkt 2 otrzymuje brzmienie:

„2) stanowiącego element obiektów, instalacji, urządzeń i usług ujętych w wykazach, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …);”.

Art. 9. W ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2019 r. poz. 2418) w art. 4 w pkt 8 lit. b otrzymuje brzmienie:

„b) obiekty ujęte w wykazach, sporządzonych na podstawie art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …), oraz wchodzące w ich skład i powiązane z nimi systemy;”.

Art. 10. W ustawie z dnia 7 lutego 2014 r. o udziale zagranicznych funkcjonariuszy lub pracowników we wspólnych operacjach lub wspólnych działaniach ratowniczych na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2018 r. poz. 1802) w art. 4 ust. 4 otrzymuje brzmienie:

„4. W przypadku gdy wspólna operacja jest prowadzona w związku z zaistnieniem lub w celu zapobieżenia zdarzeniu o charakterze terrorystycznym w rozumieniu art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2019 r. poz. 796) lub gdy zachodzi konieczność bezzwłocznego prowadzenia wspólnego działania ratowniczego, wniosek, o którym mowa w ust. 1 pkt 1, kierowany jest przez właściwy organ do organu państwa wysyłającego, w trybie określonym w ust. 2, równocześnie z wnioskiem do ministra właściwego do spraw wewnętrznych o wyrażenie zgody. W przypadku braku zgody wspólna operacja lub wspólne działanie ratownicze nie mogą być prowadzone, a jeżeli zostały rozpoczęte, muszą zostać zakończone w terminie nie dłuższym niż 24 godziny od otrzymania przez organ wnioskujący informacji o braku zgody.”.

Art. 11. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248) wprowadza się następujące zmiany:

1) w art. 10 w ust. 4 wyrazy ,,właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami ,,operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”;
2) w art. 15 w ust. 7 w pkt 2 wyrazy ,,właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami ,,operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”;
3) w art. 26:

a) w ust. 2 wyrazy ,,właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1" zastępuje się wyrazami ,,operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a",

b) w ust. 5 pkt 1 otrzymuje brzmienie:

„1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;",

c) w ust. 7 pkt 5 i 6 otrzymują brzmienie:

„5) inne niż wymienione w pkt 1–4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;".

Art. 12. 1. Streszczenie istotnych elementów krajowej oceny ryzyka, o którym mowa w art. 5aa ust. 2 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, zostanie sporządzone po raz pierwszy w terminie do dnia 31 grudnia 2020 r.

2. Streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o którym mowa w art. 5aj ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, zostanie sporządzone po raz pierwszy w terminie do dnia 31 grudnia 2020 r.

Art. 13. 1. Plany zarządzania ryzykiem, o których mowa w art. 5ab ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, zostaną sporządzone w terminie do dnia 8 sierpnia 2020 r. Plany sporządzone po raz pierwszy nie zawierają oceny osiągniętych efektów oraz wniosków z wdrożonych działań, o których mowa w art. 5ab ust. 1 pkt 3 lit. e ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą.

2. Plany reagowania kryzysowego, o których mowa w art. 5ae–5ah ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, zostaną sporządzone w terminie 12 miesięcy od dnia sporządzenia planów zarządzania ryzykiem.

3. Plany zarządzania kryzysowego, sporządzone i zatwierdzone na podstawie ustawy zmienianej w art. 1 w brzmieniu obowiązującym przed dniem wejścia w życie niniejszej ustawy, pozostają w mocy do czasu sporządzenia planów, o których mowa w ust. 1 i 2.

Art. 14. 1. Kryteria, o których mowa w art. 5b ust. 2 pkt 3 i 4 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Wykazy, o których mowa w art. 5c pkt 1, art. 5d ust. 1 i art. 5f pkt 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 15. Operatorzy infrastruktury krytycznej wyznaczą po raz pierwszy koordynatorów do spraw ochrony infrastruktury krytycznej w rozumieniu art. 5i ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

Art. 16. Raport, o którym mowa w art. 5h ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, sporządza się po raz pierwszy za rok 2020.

Art. 17. Operatorzy infrastruktury krytycznej zapewnią zdolność do ochrony informacji niejawnych zgodnie z art. 5g ust. 1 pkt 3 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 18. Przepis art. 26 ust. 4a ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, ma zastosowanie po raz pierwszy do opracowania budżetów jednostek samorządu terytorialnego na 2021 r.

Art. 19. Przepisy wykonawcze wydane na podstawie art. 5a ust. 6 oraz art. 6 ust. 7 ustawy zmienianej w art. 1, w brzmieniu obowiązującym przed dniem wejścia w życie niniejszej ustawy, zachowują moc do czasu wejścia w życie przepisów wykonawczych wydanych na podstawie art. 5a ust. 9 oraz art. 5m ust. 6 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą, jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 20. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

UZASADNIENIE

I. Wstęp

Projektowane zmiany w założeniu zmierzają do wzmocnienia systemu zarządzania kryzysowego w szczególności w zakresie zarządzania ryzykiem i ochrony ludności z uwzględnieniem postanowień *decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności* oraz *Ramowego programie działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof.*

W odniesieniu do konieczność uregulowania kwestii zarządzania ryzykiem – jest to wymogiem spełnienia warunkowości podstawowej w kolejnej perspektywie finansowej UE na lata 2021–2027. Zadania w zakresie zarządzania ryzykiem zostały określone w *decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności*. Opracowanie dokumentów planistycznych w obszarze zarządzania ryzykiem jest bezpośrednio powiązane z jednym z warunków podstawowych kolejnej perspektywy finansowej, który mówi o osiągnięciu *Skutecznych ram zarządzania ryzykiem.*

Wymogi te wprost wskazują na konieczność opracowania planu zarządzania ryzykiem, na szczeblu krajowym lub regionalnym, powiązanego ze strategiami adaptacji do zmian klimatu. Należy wskazać na art. 6 ww. decyzji, zgodnie z którym państwa członkowskie opracowują oceny ryzyka na szczeblu krajowym lub niższym oraz udostępniają Komisji Europejskiej streszczenie istotnych elementów tych ocen (pierwsze udostępnienia miało mieć miejsce do dnia 22 grudnia 2015 r.).

Cele wynikające z Unijnego Mechanizmu Ochrony Ludności powiązane są z priorytetami określonymi podczas Trzeciej Światowej Konferencji ONZ, która odbyła się w 2015 r. w Sendai. Jednym z podstawowych wymogów przyjętego wówczas *Ramowego programu działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof* jest realizacja przedsięwzięć zgodnie z opracowanymi przez poszczególne państwa celami strategicznymi, zarówno na szczeblu centralnym, jak i lokalnym. Głównym celem Ramowego Programu jest znaczące ograniczenie liczby śmiertelnych ofiar katastrof oraz zminimalizowanie wpływu katastrof na ciągłość podstawowych procesów realizowanych przez państwo (w tym kluczowych usług zapewniających ochronę życia i zdrowia obywateli oraz funkcjonowanie administracji i gospodarki).

Zgodnie z obowiązującą od dnia 21 marca 2019 r. decyzją Parlamentu Europejskiego i Rady (UE) 2019/420 z dnia 13 marca 2019 r. zmieniającą decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności, wszystkie działania na rzecz skutecznego zapobiegania klęskom żywiołowym i katastrofom spowodowanym przez człowieka powinny być spójne z *Ramowym programem.* Unia Europejska odegrała wiodącą rolę w negocjacjach w sprawie *Ramowego programu*, a wiele jego zaleceń opiera się na istniejących politykach i programach UE w zakresie zarządzania ryzykiem katastrof. Ponadto Komisja Europejska opracowała w 2016 r. *Plan działania na rzecz realizacji Ramowego programu z Sendai na lata 2015–2030 w sprawie ograniczania ryzyka katastrof*, który ma przyczynić się do wdrożenia przez państwa członkowskie postanowień *Ramowego programu.*

Biuro Narodów Zjednoczonych ds. ograniczenia ryzyka katastrof (UNDRR) otrzymało zadanie wsparcia krajów członkowskich we wdrażaniu postanowień *Ramowego Programu*. Współpraca realizowana jest poprzez wyznaczone przez poszczególne kraje punkty kontaktowe.

Według obowiązujących w Polsce regulacji, ocena ryzyka aktualizowana jest w cyklu dwuletnim w *Raporcie o zagrożeniach bezpieczeństwa narodowego* oraz w raportach cząstkowych do *Raportu* sporządzanych przez ministrów, kierowników urzędów centralnych oraz wojewodów. Dokumenty te stanowią podstawę opracowywanego, również cyklicznie, *Krajowego Planu Zarządzania Kryzysowego* oraz planów zarządzania kryzysowego na wszystkich szczeblach administracji. Brak jest jednak prawnego uregulowania kompleksowego podejścia do kwestii zarządzania ryzykiem. Przede wszystkim nie istnieje obowiązek opracowywania planów zarządzania ryzykiem oraz dokumentów, których założeniem jest informowanie Komisji Europejskiej, przez cykliczne przedkładanie, tj.: *Streszczenia istotnych elementów krajowej oceny ryzyka* oraz *Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem*. Zgodnie z Unijnym Mechanizmem Ochrony Ludności, streszczenia przekazuje się do dnia 31 grudnia 2020 r., a następne co trzy lata oraz jeśli zajdą ważne zmiany.

Konieczne jest wprowadzenie przepisów zobowiązujących podmioty zaangażowane w proces zarządzania ryzykiem do opracowania i aktualizowania dokumentów w tym zakresie, a także wdrażania *Ramowego programu działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof*. Wskazane jest dostosowanie terminologii do regulacji unijnych, co stworzy efektywne narzędzia do prowadzenia oceny ryzyka i zarządzania nim.

Proponuje się ujednolicenie terminów cyklów planistycznych krajowych z unijnymi, gdyż obowiązujące przepisy krajowe przewidują cykl 2-letni, podczas gdy unijne regulacje wskazują na 3-letnie cykle planistyczne. Dostosowania do procesu oceny ryzyka wymaga także *Raport o zagrożeniach bezpieczeństwa narodowego*. Dokonanie korelacji między regulacjami krajowymi a unijnymi będzie odbywać się bez konieczności opracowywania od podstaw nowych dokumentów planistycznych, lecz z wykorzystaniem już opracowanych i funkcjonujących.

Tak więc *Raport o zagrożeniach bezpieczeństwa narodowego* w dalszym ciągu dotyczyć będzie oceny ryzyka. Raport zostanie sporządzony na podstawie raportów cząstkowych do *Raportu o zagrożeniach bezpieczeństwa narodowego* sporządzanych przez ministrów, kierowników urzędów centralnych oraz wojewodów. Jednostki samorządu terytorialnego nie mają obowiązku opracowywania raportów cząstkowych. Po przeprowadzeniu oceny ryzyka i wskazaniu najistotniejszych zagrożeń dla bezpieczeństwa narodowego, konieczne jest określenie celów strategicznych służących ograniczeniu ryzyka ich wystąpienia, z wykorzystaniem istniejących zapisów oraz wniosków zawierających hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do ich osiągnięcia, z uwzględnieniem regionalnych lub lokalnych inicjatyw, czyli podejmowanych na obszarze województwa. Istotne jest bowiem zrozumienie, że dopiero prawidłowo przeprowadzona ocena ryzyka identyfikuje zagrożenia i obszary, w których konieczne jest podjęcie działań, w tym zwiększenie nakładów finansowych na przedsięwzięcia ograniczające ryzyko katastrof.

W przypadku planów zarządzania kryzysowego – opracowywane do tej pory plany zarządzania kryzysowego podzielone zostaną na plany zarządzania ryzykiem oraz plany reagowania kryzysowego, tj.:

- ✓ plany zarządzania ryzykiem w odniesieniu do działań uczestników zarządzania kryzysowego w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do przejmowania nad nią kontroli,
- ✓ plany reagowania kryzysowego w odniesieniu do działań uczestników zarządzania kryzysowego w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków.

Ww. rozwiązania zostały już zapoczątkowane – ostatnia wersja *Krajowego planu zarządzania kryzysowego* z 2018 r. została podzielona na dwie części:

- ✓ cześć A odnoszącą się do zarządzania ryzykiem, czyli de facto dwóch pierwszych faz zarządzania kryzysowego: zapobiegania i przygotowania,

- ✓ część B, która dotyczyła reagowania i odbudowy.

Dokonany podział był pierwszym krokiem do ostatecznego rozdzielenia KPZK na osobne dokumenty. Krajowy Plan Zarządzania Ryzykiem w założeniu dotyczyć będzie przedsięwzięć mających na celu niedopuszczenie do sytuacji kryzysowej i przygotowanie struktur zarządzania kryzysowego na wypadek jej wystąpienia.

Informacje dotyczące szczegółowych przedsięwzięć, które do tej pory stanowiły część *Raportu o zagrożeniach bezpieczeństwa narodowego*, oraz zadania i obowiązki uczestników zarządzania kryzysowego dla faz: zapobieganie i przygotowanie, które stanowiły część A *Krajowego Planu Zrządzania Kryzysowego*, zostaną przeniesione do planu zarządzania ryzykiem na szczeblu krajowym. Konieczna będzie analiza i uzupełnienie wymienionych przedsięwzięć, z uwzględnieniem elementu służącemu ich weryfikacji, aby ustalić czy ich realizacja wpłynęła na ograniczenie ryzyka. Podobnie będzie wyglądać konstrukcja planów zarządzania ryzykiem na pozostałych szczeblach.

Przewiduje się wprowadzenie dla organów administracji rządowej obowiązku wdrażania *Ramowego Programu Działań na lata 2015–2030 na rzecz ograniczenia ryzyka katastrof* oraz pełnienie przez Rządowe Centrum Bezpieczeństwa funkcji krajowego punktu kontaktowego dla Organizacji Narodów Zjednoczonych do spraw jego wdrażania.

W procesach oceny i zarządzania ryzykiem nie sposób nie uwzględniać zagrożeń dotyczących infrastruktury krytycznej. Dlatego też ujęcie zagrożeń jej dotyczących znajdzie odzwierciedlenie w planach zarządzania ryzykiem oraz planach reagowania kryzysowego.

Przewiduje się wzmocnienie ochrony infrastruktury krytycznej przez wdrożenie rozwiązań minimalizujących skutki zakłócenia jej funkcjonowania dla ludności – w tym z zastosowaniem narzędzi zarządzania ryzykiem przewidzianych w ww. zmianach. Charakterystyka zagrożeń dotyczących infrastruktury krytycznej zostanie uwzględniona w planach zarządzania ryzykiem oraz planach reagowania kryzysowego.

Ponadto w odniesieniu do zmian dotyczących infrastruktury krytycznej – istotną zmianą jest to, iż zostanie dokonany jej podział na taką, której zniszczenie lub zakłócenie będzie miało niekorzystny wpływ na:

- ✓ funkcjonowanie państwa i zaspokojenia potrzeb obywateli,
- ✓ lokalną społeczność danego województwa.

Projekt wskazuje na sposób wyłaniania i umieszczania w wykazie obiektów, instalacji, urządzeń lub usług z ich podziałem na „infrastrukturę krajową” oraz „infrastrukturę wojewódzką”. W drugim przypadku natomiast kompetencje w zakresie wyłaniania i umieszczania wyłonionej infrastruktury w stosownych wykazach przypadną wojewodzie. Ochrona infrastruktury krytycznej nie może odbywać się z pominięciem czynnika ludzkiego.

Jednocześnie wyodrębniona do oddzielnego wykazu zostanie europejska infrastruktura krytyczna. Powstanie również wykaz tzw. potencjalnej infrastruktury krytycznej – czyli wykaz obiektów, instalacji, urządzeń lub usług będących w fazie projektowania lub budowy, a mogących spełniać kryteria właściwe dla infrastruktury krytycznej istotnej dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.

Planowane jest wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u wszystkich operatorów infrastruktury krytycznej. Operatorzy infrastruktury krytycznej we wszystkich systemach infrastruktury krytycznej będą wyznaczać osobę koordynującą działania na linii operator – organy administracji publicznej.

Projekt wprowadza ujednolicenie terminologii w obszarze szkoleń i ćwiczeń z zakresu zarządzania kryzysowego na poziomie ministra kierującego działem administracji rządowej oraz kierownika urzędu centralnego oraz zadanie w postaci wskazania, iż mają oni możliwość zarządzania, organizacji i prowadzenia szkoleń i ćwiczeń z zakresu zarządzania kryzysowego – w odniesieniu do ćwiczeń krajowych, jak również udziału w ćwiczeniach międzynarodowych.

Na poziomie województwa, powiatu oraz gminy zunifikowano brzmienie przepisów dotyczących szkoleń i ćwiczeń, dając podstawy prawne do wspólnego uczestnictwa w ćwiczeniach na różnych szczeblach, stosownie do lokalnych lub krajowych potrzeb.

II. Szczegółowe zmiany w ustawie o zarządzaniu kryzysowym

1) *Definicje (projektowane zmiany w słowniczku ustawy o zarządzaniu kryzysowym (art. 3 ustawy z.k.)*

Sytuacja kryzysowa

Definicja sytuacji kryzysowej zostanie uzupełniona o kwestie dotyczące dziedzictwa kulturowego. Projekt nowelizacji w definicji sytuacji kryzysowej uwzględnia postanowienia decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności, która w art. 2

określa, że „Ochrona zapewniana w ramach unijnego mechanizmu obejmuje przede wszystkim ludzi, lecz także środowisko naturalne i mienie, w tym dziedzictwo kulturowe, i chroni je przed wszystkimi rodzajami klęsk żywiołowych i katastrof spowodowanych przez człowieka, w tym następstwami ataków terrorystycznych".

Ponadto decyzja Parlamentu Europejskiego i Rady 2019/420 z dnia 13 marca 2019 r. zmieniająca decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności rozszerzyła katalog zagrożeń, jak też działań podejmowanych w sytuacji wystąpienia klęsk żywiołowych i katastrof spowodowanych przez człowieka. Brak regulacji dotyczących ochrony dziedzictwa kulturowego mógłby powodować, iż problematyka ta nie zostanie włączona do budowanego obecnie systemu przygotowań na zdarzenia nadzwyczajne, w szczególności w administracji publicznej różnych szczebli, między innymi poprzez podejmowane działania planistyczno-organizacyjne, szkoleniowe i kontrolne. Ponadto pozbawia instytucje kultury, w których zgromadzone są zbiory, a które stanowią dziedzictwo narodowe, z korzystania z zasobów ludzkich i sprzętowych, podmiotów wyspecjalizowanych w prowadzeniu akcji ratowniczych.

Za ujęciem tego obszaru w projektowanych zmianach przemawiają zarówno doświadczenia historyczne, jak również olbrzymie straty w dziedzictwie kultury w wyniku klęsk żywiołowych w Rzeczypospolitej Polskiej, w tym w szczególności powodzi w 1997 r.

Uzupełnienie dotychczasowej treści definicji o wskazanie istoty zakłóceń funkcjonowania organów administracji publicznej związane jest z faktem, iż przepisy ustawy o zarządzaniu kryzysowym przede wszystkim statuują oraz wskazują obowiązki i kompetencje organów administracji publicznej w ramach systemu zarządzania kryzysowego. Ich niezakłócona działalność jest gwarantem działań podejmowanych na rzecz szeroko rozumianej ochrony ludności.

Systemy infrastruktury krytycznej

Infrastruktura krytyczna definiowana jest co do zasady jak dotychczas. To systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli, kluczowe dla funkcjonowania państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Zmianie ulegnie jedynie nazwa jednego z jedenastu systemów infrastruktury krytycznej. Zmiana dotyczy dodania w systemie zaopatrzenia w wodę kwestii odprowadzania ścieków. Kwestie zbiorowego zaopatrzenia w wodę są nierozerwalnie związane z odprowadzaniem ścieków, co znajduje odzwierciedlenie w aktach rangi ustawowej, m.in. ustawie z dnia 4 września 1997 r. o działach administracji rządowej, gdzie w ramach działu gospodarka wodna wskazuje się sprawy określenia zasad i warunków zbiorowego zaopatrzenia w wodę przeznaczoną do spożycia przez ludzi oraz zbiorowego odprowadzania ścieków, czy też ustawie z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, w której określa się zasady działalności przedsiębiorstw wodociągowo-kanalizacyjnych, tworzenia warunków do zapewnienia ciągłości dostaw i odpowiedniej jakości wody oraz niezawodnego odprowadzania i oczyszczania ścieków.

Tym samym proponowana w projekcie nowa nazwa systemu „zaopatrzenia w wodę oraz odprowadzania ścieków" skorelowana jest z przyjętą w innych aktach terminologią.

Ponadto w zakresie infrastruktury krytycznej – wprowadzono definicję operatora infrastruktury krytycznej. Tak jak obecnie będą to właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń lub usług infrastruktury krytycznej, które zostały ujęte w wykazie infrastruktury krytycznej.

Operator infrastruktury krytycznej

Wprowadzono do słowniczka pojęcie operatora infrastruktury krytycznej jako właściciela, posiadacza samoistnego lub posiadacza zależnego obiektu, instalacji, urządzenia lub usługi, które zostały ujęte w wykazie infrastruktury krytycznej.

Planowanie cywilne

Pojęcie planowania cywilnego zostało przeredagowane tak, aby w swojej treści zawierało aspekt planowania w zakresie wspierania operacji sojuszniczych prowadzonych w ramach Organizacji Traktatu Północnoatlantyckiego na terytorium Rzeczypospolitej Polskiej.

Ryzyko

Mając na względzie konieczność zarządzania ryzykiem – projekt wprowadza szereg definicji odnoszących się do kwestii ryzyka, począwszy od zdefiniowania „ryzyka", jak również definicji „ryzyka dla infrastruktury krytycznej". Istotną różnicą między tymi

pojęciami jest uwzględnianie w przypadku ryzyka dla infrastruktury krytycznej kwestii podatności.

Redefiniowano pojęcie mapy ryzyka, ponadto wprowadza się pojęcia: matrycy, ryzyka, zarządzania ryzykiem, analizy ryzyka oraz szacowania ryzyka.

Moduł zadaniowy

Zdefiniowano, funkcjonujące już w praktyce, pojęcie modułu zadaniowego, jako zestawienia przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez wykonawcę wskazanego w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony podmiotów wskazanych w siatce bezpieczeństwa.

Plany

Słowniczek do projektu zostaje uzupełniony o definicję planów zarządzania kryzysowego, planów zarządzania ryzykiem oraz planów reagowania kryzysowego.

Zagrożenia hybrydowe / zarządzanie sytuacją hybrydową

Do materii ustawy wprowadza się pojęcia zagrożenia hybrydowego, przez które należy rozumieć zaplanowane i skoordynowane działania prowadzone przez podmioty państwowe lub niepaństwowe w sposób utrudniający przypisanie odpowiedzialności za nie sprawcy. Działanie te zmierzają do osiągnięcia celów politycznych i strategicznych oraz łączą różne środki wywierania nacisku i uzależniania od potencjalnego agresora, takie jak polityczne, militarne, ekonomiczne, społeczne, prawne oraz informacyjne.

Hybrydowość niesie za sobą złożoność i wielopłaszczyznowość, a skutki działań mogą zaistnieć zarówno na terenie całego kraju, jak i na jego części. Działania te cechują się tym, że są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego jednoznaczne zidentyfikowanie progu wojny.

Najważniejszą rolę w przeciwdziałaniu zagrożeniom hybrydowym powinny odgrywać instytucje układu pozamilitarnego z obszaru ogniw ochronnych, gospodarczych, informacyjnych i systemu kierowania wspierane przez siły zbrojne, bowiem nie ma możliwości wyznaczenia dla całości działań hybrydowych podmiotu wiodącego. Ważną rolę odstraszającą odgrywają także siły zbrojne, które muszą mieć możliwość reagowania w sytuacji wystąpienia zagrożeń hybrydowych na wypadek niespodziewanej eskalacji kryzysu. Wojskowe środki używane w ramach działań hybrydowych mogą bowiem

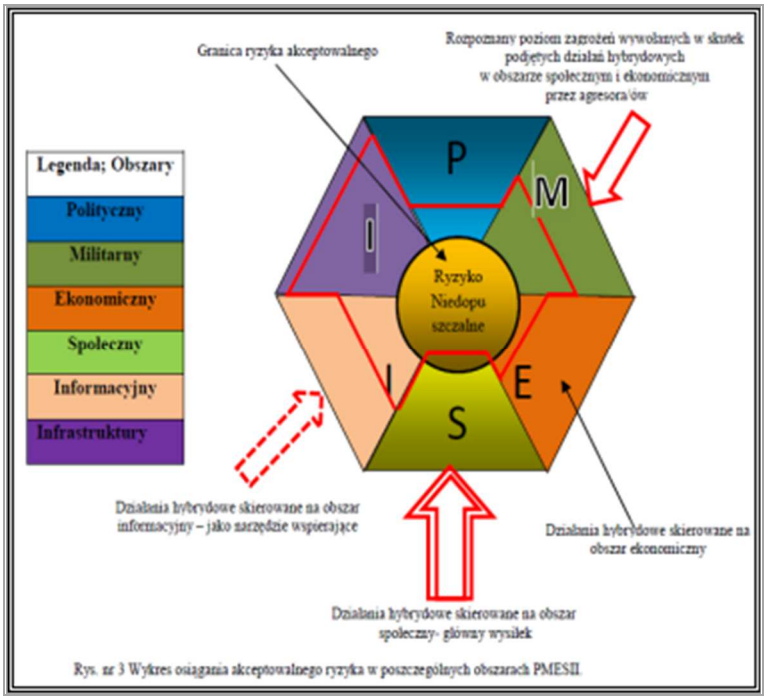
kamuflować przygotowania do faktycznego użycia sił zbrojnych (np. niezapowiedziane ćwiczenia militarne, którym towarzyszy duża koncentracja sił zbrojnych).

Skuteczną odpowiedzią na zagrożenia spowodowane działaniami hybrydowymi to ich wczesne rozpoznanie i efektywne reagowanie. Konieczne jest zrozumienie mechanizmów powstawania zagrożeń, a w konsekwencji oszacowanie ryzyka wystąpienia zagrożeń w warunkach normalnego funkcjonowania państwa. Niezbędna jest umiejętność szybkiego reagowania na pierwsze oznaki działań hybrydowych oraz elastyczna, efektywna i skoordynowana reakcja układu militarnego i pozamilitarnego. Podejście takie zapewni wypracowanie odpowiedniej strategii do przeciwdziałania zagrożeniom hybrydowym, a tym samym będzie miało także efekt odstraszający od dalszej eskalacji kryzysu.

Działania hybrydowe charakteryzują się tym, że mogą występować w poszczególnych obszarach PMESII[1] lub w kilku równocześnie. Do przeprowadzenia skutecznych działań hybrydowych muszą być zagwarantowane odpowiednie warunki dla powodzenia realizacji zakładanych celów. Dotychczasowe doświadczenia oraz te z przeszłości wskazują, iż obszar społeczny oraz ekonomiczny i informacyjny są najbardziej podatne na działania hybrydowe.

Potencjalny przeciwnik prowadząc działania w danym obszarze lub obszarach wybiera najbardziej podatne i najmniej odporne obszary.

[1] PMESII – segmentacja środowiska bezpieczeństwa. Dzieli otoczenie na obszar: polityczny, militarny, ekonomiczny, społeczny, infrastruktury, informacyjny.



Rys. nr 3 Wykres osiągania akceptowalnego ryzyka w poszczególnych obszarach PMESII

Powodzenie działań hybrydowych w wybranych obszarach oddziałuje na pozostałe obszary, zmniejszając ich odporność, a zwiększając podatność. De facto w wyniku działań hybrydowych każdy obszar PMESII może pośrednio zostać zaatakowany nawet bez konkretnej ingerencji agresora.

Należy zaznaczyć, że jedną z cech działań hybrydowych jest ich niska przewidywalność oraz możliwość utajnienia prawdziwych intencji przez potencjalnego przeciwnika zwłaszcza w fazie przygotowawczej.

Potencjalny przeciwnik, dysponując szerokim wachlarzem możliwych narzędzi do zastosowania, znając najbardziej podatne obszary, wykorzysta je w sposób jak najbardziej nieprzewidywalny, a scenariusz działań raz podjętych ulegnie modyfikacji i będzie skierowany na różne obszary w zależności od ich odporności i podjętych przeciwdziałań.

Do realizacji działań hybrydowych potencjalny agresor będzie używać różnych dostępnych przez siebie narzędzi (ataków terrorystycznych, organizacji przestępczych, cyberataku, dezinformacji, niekontrolowanej migracji, blokady gospodarczej i dyskryminacji gospodarczej, spekulacji finansowych, incydentów granicznych, niezapowiedzianych ćwiczeń przy granicy państwa, naruszeń granicy państwowej, zakłóceń systemu zaopatrzenia, celowego manipulowania chorobami zakaźnymi wśród ludzi, jak np. wąglik, i rozpowszechnienia chorób zwierząt, jak np.: afrykański pomór świń,

itp.) w zależności od celów i rozpoznanych obszarów PMESII danego podmiotu w szczególności do obszarów najbardziej podatnych.

Skutki zagrożenia zarówno dla ludności, gospodarki, mienia, infrastruktury czy środowiska będą zależały od rodzaju i skali zdarzeń. W związku z tym należy się liczyć z możliwością paraliżu systemów finansowych, bankowych, telekomunikacyjnych, opieki zdrowotnej, zaopatrzenia w energię, paliwa, żywność i wodę, zakłócenia funkcjonowania struktur państwa, jego rozwoju gospodarczego, bezpieczeństwa przemysłowego w obszarach strategicznych gospodarki, dezinformacją, aż po bezpośrednie zagrożenie dla zdrowia i życia ludności oraz utratę suwerenności i integralności terytorialnej. W skrajnym przypadku działania hybrydowe mogą doprowadzić również do wystąpienia kryzysu polityczno-militarnego.

Wobec różnorodności możliwych zagrożeń, działania instytucji państwa powinny przebiegać według procedur przyjętych dla konkretnych zagrożeń, z uwzględnieniem złożoności poszczególnych scenariuszy[2].

Obok pojęcia zagrożenia hybrydowego – projekt wprowadza kwestie zarządzania sytuacją hybrydową, przez którą należy rozumieć prognozowanie, przeciwdziałanie i reagowanie na zagrożenia hybrydowe. Znajdzie ona odzwierciedlenie w zadaniach Rządowego Zespołu Zarządzania Kryzysowego;

2) *Planowanie cywilne (zmiany w art. 4 ustawy z.k.)*

Projektowana zmiana brzmienia w art. 4 ustawy z.k. polega na uzupełnieniu katalogu zadań z zakresu planowania cywilnego o prowadzenie oceny ryzyka.

Dodatkowo przewiduje się uzupełnienie przesłanek niezbędnych do właściwej realizacji zadań z zakresu planowania cywilnego przede wszystkim o:

- ✓ organizacyjne i techniczne możliwości wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego, zgodnie z art. 25 ustawy o zarządzaniu kryzysowym;
- ✓ organizacyjne i techniczne możliwości wsparcia Sił Zbrojnych Rzeczypospolitej Polskiej oraz wojsk sojuszniczych w przypadku ich użycia przy realizacji zobowiązań sojuszniczych w ramach Organizacji Traktatu Północnoatlantyckiego na terytorium

[2] Materiał opracowany we współpracy z ekspertami Centrum Doktryn i Szkolenia Sił Zbrojnych.

Rzeczypospolitej Polskiej;

3) *Art. 5 – zmiana porządkowa*

Propozycja zmierza do uchylenia regulacji dotyczących planów zarządzania kryzysowego w obecnej formie. Zostaną one ujęte w nowej formule w jednostkach redakcyjnych, tak aby zachować kolejność i korelacje Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów zarządzania kryzysowego;

4) *Raport o zagrożeniach bezpieczeństwa narodowego / plany zarządzania ryzykiem / plany reagowania kryzysowego*

Projekt przewiduje opracowywanie Raportu o zagrożeniach bezpieczeństwa narodowego (dalej „Raport") w celu dokonania oceny ryzyka wystąpienia zagrożeń oraz określenia celów strategicznych służących ograniczeniu ryzyka wystąpienia zagrożeń. Projekt wskazuje, z jakich elementów będzie składał się Raport. Wskazuje również zadania w zakresie jego opracowywania, zarówno od strony podmiotów koordynujących, tj. dyrektora Centrum, Szefa ABW oraz Pełnomocnika ds. Cyberbezpieczeństwa, jak również ze strony podmiotów koordynowanych, tj. ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów.

Projektowana regulacja wskazuje, iż na potrzeby opracowania Raportu ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie opracowują tzw. raporty cząstkowe o zagrożeniach bezpieczeństwa narodowego, których elementy składowe zostały wskazane w projektowanej regulacji.

Projekt przewiduje, iż opracowanie raportów cząstkowych koordynuje Rządowe Centrum Bezpieczeństwa, z wyłączeniem części:

- ✓ dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Szef Agencji Bezpieczeństwa Wewnętrznego, oraz
- ✓ dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

Na podstawie otrzymanych raportów cząstkowych Rządowe Centrum Bezpieczeństwa opracowuje Raport, z wyłączeniem części:

- ✓ dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, którą opracowuje Szef Agencji Bezpieczeństwa Wewnętrznego,
- ✓ dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, którą opracowuje Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

Projekt wskazuje dyrektora Rządowego Centrum Bezpieczeństwa jako właściwego do przedkładania Raportu Radzie Ministrów co trzy lata (Rada Ministrów przyjmuje Raport w drodze uchwały);

5) *Ocena ryzyka oraz wnioski wynikające z Raportu*

Projekt wskazuje, iż ocena ryzyka wynikająca z Raportu oraz wnioski z Raportu są uwzględniane w planach zarządzania kryzysowego oraz w innych dokumentach opracowywanych w tym zakresie przez organy administracji publicznej w zakresie zarządzania kryzysowego.

Ponadto na podstawie Raportu Rządowe Centrum Bezpieczeństwa opracowuje streszczenie istotnych elementów krajowej oceny ryzyka, które dyrektor Rządowego Centrum Bezpieczeństwa udostępnia Komisji Europejskiej.

Plany zarządzania ryzykiem

Projekt – definiując plany zarządzania ryzykiem – wskazuje wspólne elementy tych planów. Plany zarządzania ryzykiem zawierają bowiem takie same elementy na wszystkich szczeblach zarządzania kryzysowego.

Plany zarządzania ryzykiem opracowują:

- ✓ Rządowe Centrum Bezpieczeństwa – Krajowy Plan Zarządzania Ryzykiem,
- ✓ ministrowie kierujący działami administracji rządowej – plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej,
- ✓ kierownicy urzędów centralnych – plany zarządzania ryzykiem kierowników urzędów centralnych,
- ✓ wojewodowie – wojewódzkie plany zarządzania ryzykiem,
- ✓ starostowie – powiatowe plany zarządzania ryzykiem,
- ✓ wójtowie (burmistrzowie, prezydenci miast) – gminne plany zarządzania ryzykiem.

W przypadku gminnych planów zarządzania ryzykiem – wójt (burmistrz, prezydent miasta) przekazuje je właściwemu miejscowo staroście. Natomiast powiatowy plan zarządzania ryzykiem starosta przekazuje właściwemu miejscowo wojewodzie.

Na szczeblu centralnym natomiast – Rządowe Centrum Bezpieczeństwa, uwzględniając plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów, opracowuje Krajowy Plan Zarządzania Ryzykiem. Minister właściwy do spraw rozwoju regionalnego opiniuje Krajowy Plan Zarządzania Ryzykiem pod względem spójności z programami strukturalnymi.

Tak opracowany plan na szczeblu krajowym dyrektor Rządowego Centrum Bezpieczeństwa przedkłada Radzie Ministrów, która przyjmuje ten plan w drodze uchwały.

Plany reagowania kryzysowego

Projekt definiuje plany reagowania kryzysowego jako Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego. Projekt wskazuje elementy dla poszczególnych rodzajów planów, uwzględniając specyfikę każdego ze szczebli zarządzania kryzysowego.

Przez analogię do rozwiązań dotyczących planów zarządzania ryzykiem oraz uporządkowania treści przepisów projekt wskazuje, iż plany reagowania kryzysowego opracowują:

- ✓ Rządowe Centrum Bezpieczeństwa – Krajowy Plan Reagowania Kryzysowego,
- ✓ ministrowie kierujący działami administracji rządowej – plany reagowania kryzysowego ministrów kierujących działami administracji rządowej,
- ✓ kierownicy urzędów centralnych – plany reagowania kryzysowego kierowników urzędów centralnych,
- ✓ wojewodowie – wojewódzkie plany reagowania kryzysowego,
- ✓ starostowie – powiatowe plany zarządzania ryzykiem,
- ✓ wójtowie (burmistrzowie, prezydenci miast) – gminne plany reagowania kryzysowego.

W ww. kolejności wskazano również rodzaje planów reagowania kryzysowego wraz określeniem elementów charakterystycznych dla danego planu.

Novum zawartym w projekcie jest to, iż Krajowy Plan Reagowania Kryzysowego

będzie opracowywany przez Rządowe Centrum Bezpieczeństwa, a dyrektor Rządowego Centrum Bezpieczeństwa będzie każdorazowo przedkładał ten plan Radzie Ministrów. Zakłada się, iż Rada Ministrów będzie przyjmować Krajowy Plan Reagowania Kryzysowego Rządowego w drodze uchwały.

Natomiast plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych będą uzgadniane z dyrektorem Rządowego Centrum Bezpieczeństwa i stanowić będą załączniki funkcjonalne do Krajowego Planu Reagowania Kryzysowego.

Projekt zawiera ponadto normę, która nakazuje Rządowemu Centrum Bezpieczeństwa opracowanie streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, w oparciu o treści Raportu oraz planów zarządzania kryzysowego. Opracowanie te dyrektor Rządowego Centrum Bezpieczeństwa udostępnia Komisji Europejskiej;

6) *Narodowy Program Ochrony Infrastruktury Krytycznej*

W treści Narodowego Programu Ochrony Infrastruktury Krytycznej (dalej „NPOIK") znajdą odzwierciedlenie zmiany w obszarze infrastruktury krytycznej, m.in. zmiana nazewnictwa jednego z systemów w definicji infrastruktury krytycznej, podział infrastruktury krytycznej na dwa szczeble – krajowy oraz wojewódzki, jak również wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u wszystkich operatorów infrastruktury krytycznej.

Projekt przewiduje identyfikację oraz wyznaczanie infrastruktury krytycznej w zależności od przypadku, w którym jej zniszczenie lub zakłócenie miałoby niekorzystny wpływ na:

- ✓ funkcjonowanie państwa lub na dany system infrastruktury krytycznej,
- ✓ lokalną społeczność danego województwa.

Projekt uwzględnia ww. zmiany nadające nowy kształt NPOIK-u. Zdefiniowano na nowo elementy NPOIK, jak również sposób jego opracowywania. Wprowadzono w odniesieniu do NPOIK nowy, trzyletni okres planistyczny.

Wskazano również nowe brzmienie przepisu dotyczącego szczegółowych kryteriów wyłaniania infrastruktury krytycznej, co w założeniu ma pozwolić wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej,

biorąc pod uwagę ich znaczenie dla funkcjonowania państwa, danego systemu lub lokalnej społeczności danego województwa oraz zaspokojenia potrzeb obywateli.

Projekt zawiera również normy, które określają sposób opracowywania NPOIK we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych oraz wojewodami;

7) *Wyznaczanie infrastruktury krytycznej*

W nowym ujęciu przewiduje się funkcjonowanie następujących wykazów infrastruktury krytycznej, tj.

- ✓ wykazu krajowego – sporządzanego przez dyrektora RCB na podstawie kryteriów, o których mowa w NPOIK, we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych odpowiedzialnymi za systemy, obejmującego obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej z podziałem na poszczególne systemy;
- ✓ wykazu europejskiej infrastruktury krytycznej – sporządzanego przez dyrektora RCB, zawierającego europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską;
- ✓ wykazu potencjalnej infrastruktury krytycznej – sporządzanego przez dyrektora Rządowego Centrum Bezpieczeństwa, we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych odpowiedzialnymi za systemy, obejmującego obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej z podziałem na poszczególne systemy, będące w fazie projektowania lub budowy, mogące potencjalnie spełniać kryteria, o których mowa w NPOIK;
- ✓ wykazu wojewódzkiego – sporządzanego przez właściwego miejscowo wojewodę na podstawie szczegółowych kryteriów, o których mowa w NOPIK, obejmującego obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej z podziałem na systemy zlokalizowanej na terenie danego województwa.

Projekt przewiduje, iż dyrektor Rządowego Centrum Bezpieczeństwa opracowuje wyciągi z wykazu krajowego dotyczące obiektów, instalacji, urządzeń lub usług znajdujących się w danym systemie oraz przekazuje je ministrom kierującym działami

administracji rządowej i kierownikom urzędów centralnych odpowiedzialnym za dany system. Ponadto opracowuje wyciągi z wykazu krajowego dotyczące obiektów, instalacji, urządzeń lub usług znajdujących się na obszarze danego województwa oraz przekazuje właściwemu wojewodzie.

O ujęciu w wykazie krajowym dyrektor RCB informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług jak również zatwierdza plany ochrony infrastruktury krytycznej ujęte w tym wykazie, po zasięgnięciu opinii ministra kierującego działem administracji rządowej i kierownika urzędu centralnego odpowiedzialnego za system.

W odniesieniu do wykazu potencjalnej infrastruktury krytycznej – obiekt, instalację, urządzenie lub usługę uznaje się za potencjalną infrastrukturę krytyczną, w przypadku gdy z założeń projektowych wynika, że będzie ona kluczowa dla bezpieczeństwa państwa i jego obywateli oraz będzie służyć zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, oraz spełni kryteria, o których mowa w NOPIK. W celu wyznaczenia potencjalnej infrastruktury krytycznej dyrektor Rządowego Centrum Bezpieczeństwa prowadzi rozmowy z inwestorem lub operatorem infrastruktury krytycznej. Dyrektor Rządowego Centrum Bezpieczeństwa w rozmowach przedstawia stanowisko uzgodnione z ministrami i kierownikami urzędów centralnych odpowiedzialnych za systemy, których przedstawiciele mogą brać udział w rozmowach.

Na podstawie ustaleń będących wynikiem rozmów, dyrektor dokonuje ujęcia obiektu, instalacji, urządzenia lub usługi w wykazie potencjalnej infrastruktury krytycznej – dyrektor Rządowego Centrum Bezpieczeństwa powiadamia inwestora lub operatora infrastruktury krytycznej o ujęciu w wykazie potencjalnej infrastruktury krytycznej.

Dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy przedstawia inwestorowi informacje oraz dokumenty, pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub realizacji przy realizacji inwestycji.

W odniesieniu do wojewody natomiast opracowuje on wyciągi z wykazu wojewódzkiego oraz przekazuje ministrom kierującym działami administracji rządowej i kierownikom urzędów centralnych odpowiedzialnym za dany system, jak również przekazuje wykaz wojewódzki dyrektorowi Rządowego Centrum Bezpieczeństwa.

Ponadto informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług o ujęciu w wykazie wojewódzkim oraz zatwierdza plany ochrony infrastruktury krytycznej ujętej w wykazie wojewódzkim.

W zakresie ochrony infrastruktury krytycznej projekt porządkuje czynności w zakresie zapewnienia jej ochrony przez operatorów infrastruktury krytycznej. Do zadań operatora infrastruktury krytycznej należy:

- ✓ opracowywanie i wdrażanie planów ochrony infrastruktury krytycznej oraz bieżące monitorowanie stopnia wdrożenia planów;
- ✓ sporządzanie i przekazywanie informacji w zakresie realizacji zadań dotyczących ochrony infrastruktury krytycznej na żądanie dyrektora Rządowego Centrum Bezpieczeństwa oraz właściwego ministra odpowiedzialnego za jeden z systemów albo właściwego kierownika urzędu centralnego odpowiedzialnego za jeden z systemów infrastruktury krytycznej, albo właściwego terytorialnie wojewody;
- ✓ zapewnienie współpracy z organami administracji publicznej oraz dyrektorem Rządowego Centrum Bezpieczeństwa, przez przekazywanie i odbieranie informacji o:
    - o zdarzeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej,
    - o spodziewanym lub zaobserwowanym zwiększeniu zapotrzebowania na usługi lub produkty dostarczane przez operatorów infrastruktury krytycznej,
    - o spodziewanych przerwach lub zakłóceniach w dostawach usług lub produktów dostarczanych przez operatorów infrastruktury krytycznej.

Operator infrastruktury krytycznej będzie sporządzał do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące ochrony infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania. Raport o stanie ochrony infrastruktury krytycznej sporządza się m.in. z uwzględnieniem rozwiązań zawartych w planie ochrony infrastruktury krytycznej operatora, możliwości wystąpienia ryzyka zidentyfikowanego w planie ochrony infrastruktury krytycznej, incydentów i zdarzeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, które nie

były uwzględnione w planie ochrony infrastruktury krytycznej, wyników przeprowadzonych kontroli i audytów odnoszących się do zabezpieczeń zawartych w planie ochrony infrastruktury krytycznej.

Operator infrastruktury krytycznej przekazuje tak sporządzony raport o stanie ochrony infrastruktury krytycznej dyrektorowi Rządowego Centrum Bezpieczeństwa oraz właściwemu ministrowi odpowiedzialnemu za jeden z systemów albo właściwemu kierownikowi urzędu centralnego odpowiedzialnemu za jeden z systemów, albo właściwemu terytorialnie wojewodzie.

W celu realizacji ww. obowiązków operator infrastruktury krytycznej wyznacza osobę koordynującą działania na linii operator – organy administracji publicznej, tj. koordynatora ochrony infrastruktury krytycznej.

Należy w tym miejscu przypomnieć jak od strony organizacyjno-prawnej wygląda stan faktyczny w zakresie osób funkcyjnych zajmujących się, ze strony operatorów infrastruktury krytycznej, utrzymywaniem kontaktów z podmiotami państwowymi, właściwymi w zakresie ochrony infrastruktury krytycznej. Przepis art. 6 ust. 5a ustawy z.k. nakłada obowiązek wyznaczenie osoby do kontaktów. Jednakże regulacja ta nie jest w żaden sposób kompletna. Poza czynnością wyznaczenia osoby do kontaktów – brak jest przepisów, które wskazywałyby np. na zakres zadań takiej osoby czy też opisywałyby procedury z jej udziałem. Taki mechanizm nie pojawia się zarówno w ustawie z.k., jak i na poziomie aktów wykonawczych do ustawy o z.k.

Z jednej strony mamy bowiem do czynienia z celowym wyodrębnieniem osoby do wykonywania określonych funkcji, z drugiej strony jednak brak jest wskazania szczegółowych wymagań i obowiązków. Można więc przyjąć, iż jeden operator infrastruktury krytycznej wyznaczy osobę odpowiednio przygotowaną i zajmującą w strukturze organizacyjnej miejsce gwarantujące poprawne i efektywne wykonywanie powierzonych czynności. W innych przypadkach natomiast może to być osoba, wyznaczona wyłącznie w celu wypełnienia obowiązku zawartego w przepisach, w rzeczywistości jednak nieposiadająca realnych narzędzi realizacji powierzonych zadań.

Dotychczasowa praktyka wskazuje na ogromne zróżnicowanie zarówno przygotowania do pełnienia obowiązków, jak i ich faktycznej realizacji. Dlatego też rozwiązaniem, mającym być efektywnie działającym narzędziem systemowym w zakresie ochrony infrastruktury krytycznej, a nie jedynie „skrzynką kontaktową”, jest dokonanie

instytucjonalizacji osoby do utrzymywania kontaktów, tj. zastąpienie jej funkcją „koordynatora ochrony infrastruktury krytycznej”, któremu jednocześnie zostaną przyznane stosowne kompetencje.

Mając na względzie, iż w obecnym stanie prawnym operatorzy infrastruktury krytycznej mają obowiązek zapewnienia współpracy z administracją publiczną w zakresie ochrony infrastruktury krytycznej czy też wyznaczania osób do utrzymywania kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej – proponowane rozwiązania w założeniu stanowią więc usprawnienie rozwiązań w tym zakresie, z wykorzystaniem funkcjonujących już, choć nie do końca efektywnych rozwiązań.

Projekt zmian dotyczy powoływania koordynatorów ochrony infrastruktury krytycznej we wszystkich systemach infrastruktury krytycznej, o których mowa w art. 3 pkt 2 ustawy z.k. – co jest analogią do obecnie wyznaczonych osób kontaktowych, funkcjonujących u operatorów infrastruktury krytycznej.

W projekcie wskazuje się sposób powoływania koordynatora przez operatora infrastruktury krytycznej, w oparciu o określone kryteria, sposób umiejscowienia koordynatora w strukturze organizacyjnej operatora infrastruktury krytycznej, jak również wskazuje się zadania koordynatora oraz rozwiązania zapewniające ciągłość jego działania i umożliwiające wykonywanie przez niego zadań. Proponowane rozwiązania mają na celu zagwarantowanie efektywnego wykonywania zadań przez koordynatora.

Projekt przewiduje, iż operator infrastruktury krytycznej wyznacza, w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie, koordynatora ochrony infrastruktury krytycznej

Kryteria wyboru koordynatora zostały ustalone w następujący sposób – koordynatorem może być osoba, która:

- ✓ jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej,
- ✓ korzysta z pełni praw publicznych,
- ✓ posiada odpowiednią wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem organizacji, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej,

- ✓ nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe,
- ✓ spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli co najmniej:
    - o „poufne” w przypadku zajmowania stanowiska koordynatora w strukturze organizacyjnej „krajowego” operatora infrastruktury krytycznej albo
    - o „zastrzeżone” w przypadku zajmowania stanowiska koordynatora w strukturze organizacyjnej „wojewódzkiego” operatora infrastruktury krytycznej.

Projekt wskazuje na bezpośrednie podporządkowanie koordynatora organowi zarządzającemu operatora infrastruktury krytycznej. Takie umiejscowienie w strukturze organizacyjnej operatora jest gwarancją prawidłowej i efektywnej realizacji zadań powierzonych koordynatorowi. Bezpośredni dostęp do organu zarządzającego jest konieczny np. ze względu na czynności koordynujące opracowywanie i wdrażanie planów ochrony infrastruktury krytycznej. Czynności związane z realizacją tego zadania wiążą się np. z procesem zbierania danych w ramach struktury organizacyjnej operatora w określonym przedziale czasowym w trakcie sporządzania planów, jak również określonych działań w trakcie ich wdrażania – co wymaga wydawania dyspozycji określonym strukturom organizacyjnym operatora.

Operator infrastruktury krytycznej ma obowiązek niezwłocznego informowania o wyznaczeniu koordynatora dyrektora Centrum oraz ministra odpowiedzialnego za dany system infrastruktury krytycznej albo kierownika urzędu centralnego za dany system infrastruktury krytycznej, albo właściwego wojewodę.

Projekt określa ponadto zadania koordynatora oraz mechanizmy, które mają zapewnić kwestie organizacyjne i techniczne realizacji tych zadań, wskazując na rolę, jaką ma pełnić, będący pracownikiem operatora, koordynator – tj. rolę koordynującą realizację przedsięwzięć prowadzonych przez operatora infrastruktury krytycznej w zakresie ochrony jego obiektów, instalacji, urządzeń i usług ujętych w jednolitym wykazie infrastruktury krytycznej.

Projekt przewiduje, iż operator infrastruktury krytycznej zapewnia koordynatorowi organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do dokumentów i informacji.

Ponadto przewidziano, iż operator infrastruktury krytycznej w związku z realizacją przedsięwzięć w zakresie ochrony jego obiektów, instalacji, urządzeń i usług zapewnia zdolność do ochrony informacji niejawnych. Należy bowiem przyjąć, że informacje wrażliwe wytworzone w ramach opracowywania, uzgadniania oraz realizacji planów ochrony infrastruktury krytycznej oraz informacje wymieniane z właściwymi organami administracji publicznej o zidentyfikowanych zagrożeniach lub zakłóceniach infrastruktury krytycznej oraz podejmowanych działaniach w celu jej ochrony lub odtworzenia powinny być klasyfikowane jako informacje niejawne. Regulacja, spójnie z duchem ustawy o ochronie informacji niejawnych, pozostawia operatorom infrastruktury krytycznej decyzję w odniesieniu do sposobów zapewnienia ochrony informacji niejawnych, w zależności od poziomu niejawności wytwarzanych informacji.

Mając z kolei na uwadze przekazywane do operatorów infrastruktury krytycznej informacje niejawne, stwierdzić należy, iż z wieloletniej praktyki Centrum wynika, iż przekazywane operatorom informacje posiadają najczęściej klauzulę „zastrzeżone". Biorąc pod uwagę konieczność niewprowadzania nadmiernych obciążeń kosztowych, zarówno na operatorów infrastruktury krytycznej, jak i na współpracującą z nimi administrację, nie jest konieczne wprowadzanie rozwiązań ponad wymagane dla klauzuli „zastrzeżone". W celu ułatwienia przetwarzania u operatorów infrastruktury krytycznej informacji niejawnych o klauzuli „zastrzeżone" oraz wymiany takich informacji z Centrum, Centrum jako gestor SNPI OPAL zachęca operatorów infrastruktury krytycznej do zaimplementowania takiego systemu u operatorów.

Jeżeli jednak podmioty administracji publicznej przewidują przekazywanie informacji niejawnych o wyższych klauzulach niż „zastrzeżone", możliwe jest przeprowadzanie postępowań sprawdzających wobec wybranych pracowników operatorów infrastruktury krytycznej do wyższych klauzul. Wnioskowanie o wyznaczenie takich osób do operatora powinno posiadać określenie klauzuli niejawności informacji, która będzie przesyłana z konkretnego urzędu. Ponadto wskazane jest odstąpienie od pobierania kosztów postępowania sprawdzającego, jako że jest ono prowadzone ze względu na uzasadniony wniosek administracji.

Istotną zmianą w zakresie ochrony infrastruktury krytycznej jest wskazanie w materii ustawowej elementów planów ochrony infrastruktury krytycznej oraz wskazanie zasad ich uzgadniania i zatwierdzania. Regulacje ustawowe w tym zakresie uzupełnione będą aktem wykonawczym do ustawy, w którym Rada Ministrów określi wyłącznie sposób i tryb opracowania oraz zatwierdzania planów ochrony infrastruktury krytycznej;

8) *art. 6 ustawy z.k. – zmiany porządkowe*

Wprowadzenie regulacji doprecyzowujących zadania operatorów infrastruktury krytycznej w zakresie ich ochrony oraz wyznaczenie koordynatora spowodowało konieczność doprecyzowania przepisów art. 6 ustawy z.k. przez nadanie nowego brzmienia w ust. 1 pkt 5, co będzie czyniło przepisy aktu normatywnego czytelnymi, oraz uchylenia ust. 5–7, m.in. wprowadzenie instytucji koordynatora powoduje konieczność uchylenia ust. 5a, który dotyczy wyznaczania osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej;

9) *Rządowy Zespół Zarządzania Kryzysowego*

Projekt przewiduje nowe zadanie dla Rządowego Zespołu Zarządzania Kryzysowego, tj. monitorowanie i rekomendowanie Radzie Ministrów działań dotyczących zarządzania sytuacją hybrydową.

10) *Dyrektor Rządowego Centrum Bezpieczeństwa / Rządowe Centrum Bezpieczeństwa*

Zmiana o charakterze porządkowym i doprecyzowującym – projektowane zmiany w art. 10 ustawy z.k. polegają na wskazaniu, które zadania określone w ustawie z.k. realizuje bezpośrednio dyrektor Centrum, a które zadania Centrum – reprezentowane przez dyrektora;

11) *Zadania Centrum*

W zadaniach Centrum doprecyzowany przepis, w którym wskazano, iż realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa odbywa się na rzecz Prezesa Rady Ministrów (realizacja zadań stałego dyżuru Prezesa Rady Ministrów w ramach gotowości obronnej państwa). Zmiany w obszarze tworzenia planów spowodowały uzupełnienie katalogu zadań o konieczność opracowywania i aktualizowania Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego.

Dodatkowo do nowych zadań należeć będzie uzgadnianie planów sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów

centralnych oraz przygotowywanie uruchamiania, w przypadku zaistnienia zagrożeń, procedur związanych z reagowaniem kryzysowym.

Nowe zadania w obszarze współpracy międzynarodowej powodują konieczność odzwierciedlenia w treści zadań. Dlatego też wskazano, iż do zadań Centrum należy:

- ✓ współdziałanie z podmiotami, komórkami i jednostkami organizacyjnymi Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej, Organizacji Narodów Zjednoczonych oraz innych organizacji międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej,
- ✓ pełnienie funkcji krajowego punktu kontaktowego dla Organizacji Narodów Zjednoczonych oraz koordynatora do spraw wdrażania Ramowego Programu Działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof;

12) *Realizacja przez ministrów i kierowników urzędów centralnych zadań dotyczących zarządzania kryzysowego*

Zmiany w zakresie zadań ministrów zostały skorelowane z ogólnymi zmianami dotyczącymi kwestii planowania. Do zadań ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych dotyczących zarządzania kryzysowego, realizowanych w zakresie swojej właściwości należeć będzie:

- ✓ opracowywanie planów zarządzania kryzysowego (zarówno planów zarządzania kryzysowego jak i planów reagowania kryzysowego),
- ✓ organizowanie, prowadzenie i koordynacja szkolenia i ćwiczenia z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych (celem jest to sformalizowanie na szczeblu ministrów i kierowników urzędów centralnych możliwości zarówno organizowania, prowadzenia i koordynowania szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udziału w ćwiczeniach krajowego lub międzynarodowego z zakresu zarządzania kryzysowego, co w założeniu ma umożliwić doskonalenie umiejętności podejmowania bez zwłoki adekwatnych do sytuacji decyzji na szczeblu kierownictwa – tak jak ma to miejsce w przypadku wystąpienia realnej sytuacji kryzysowej),
- ✓ współpraca z operatorami infrastruktury krytycznej przy tworzeniu planów ochrony infrastruktury krytycznej oraz planu zarządzaniu kryzysowego (w szczególności w

przypadku ministrów będących koordynatorami poszczególnych systemów infrastruktury krytycznej).

Redefiniowaniu uległy zadania zespołów zarządzania kryzysowego ministrów i kierowników – nowy katalog zadań zespołów zarządzania kryzysowego na tym szczeblu wygląda następującą:

- ✓ dokonywanie okresowej oceny ryzyka na potrzeby Raportu,
- ✓ dokonywanie okresowej oceny gotowości do reagowania w zakresie organizacyjnym, technicznym i finansowym,
- ✓ opiniowanie projektów planów zarządzania kryzysowego,
- ✓ opiniowanie wykazu infrastruktury krytycznej w ramach swoich właściwości,
- ✓ wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom;

13) *Wdrażanie Ramowego Programu Działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof*

Dodanie art. 13a ma na celu realizację skutecznego wdrażania Ramowego Programu Działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof – oprócz wskazania Centrum jako punktu kontaktowego, przewiduje się, iż ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie będą ten program wdrażać oraz przekazywać dyrektorowi Centrum, w wyznaczonym terminie, raporty dotyczące wdrażania oraz inne informacje, niezbędne do realizacji zadań w tym zakresie przez Centrum;

14) *Wojewoda – ćwiczenia*

Jak wspomniano już wcześniej – na wszystkich szczeblach zarządzania przewiduje się wprowadzenie jednolitej terminologii w kwestii organizowania, prowadzenia i koordynacji szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udziału w ćwiczeniach krajowych i międzynarodowych. Tak samo sformułowany przepis będzie również funkcjonował na szczeblu wojewody.

W celu uporządkowania przepisów – uchyla się zadania wojewody związane z zapobieganiem, przeciwdziałaniem i usuwaniem skutków zdarzeń o charakterze terrorystycznym oraz współpracy w tym zakresie z Szefem ABW. Zasady prowadzenia

działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie prowadzenia tychże działań znajdują się w ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452). Dlatego też uznano, iż wskazywanie zadań w tym zakresie w ustawie z.k. jest zbędne.

Analogiczne rozwiązanie zastosowano w przypadku starosty oraz wójta, burmistrza i prezydenta miasta.

Ponadto doprecyzowano przepis, wskazując, iż zatwierdzony wojewódzki plan zarządzania kryzysowego wojewoda przekazuje dyrektorowi Centrum;

15) *Starosta – ćwiczenia*

W zakresie zadań starosty, podobnie jak na pozostałych szczeblach zarządzania kryzysowego, dokonano korelacji terminologii w zakresie organizowania, prowadzenia i koordynacji szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udziału (możliwości brania udziału) w ćwiczeniach krajowych i międzynarodowych;

16) *Wójt, burmistrz, prezydent miasta – ćwiczenia*

Analogicznie do ww. rozwiązań – na poziomie wójta, burmistrza i prezydenta miasta należy do nich organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych;

17) *Art. 20b zmiana porządkowa*

W związku z wprowadzeniem definicji operatora infrastruktury krytycznej treść art. 20b ustawy z.k. została stosownie przeredagowana;

18) *„ALERT RCB”*

Wprowadza się przepis, który umożliwia niewysyłanie operatorowi komunikatu do kart SIM zainstalowanych i wykorzystywanych w urządzeniach telemetrycznych, np. miernikach, lokalizatorach GPS i innych urządzeniach przesyłających na odległość dane pomiarowe.

Powszechne jest bowiem gromadzenie danych, pozwalających na skuteczniejsze ich wykorzystywanie i w rezultacie optymalizacje procesów, w jakich są one wykorzystywane. Telemetria znajduje zastosowanie w procesach, które na bieżąco kontrolują dane dotyczące funkcjonowania elementów systemów wielu przedsiębiorstw. Zastosowanie systemów z kartami SIM (telemetrycznymi) umożliwia na bieżąco

otrzymywanie informacji o działaniu poszczególnych systemów. Dostęp do bieżących danych, obrazujących działanie poszczególnych elementów, pozwala na dokonywanie stosownych zmian w zachodzących procesach w czasie rzeczywistym. Ponadto w przypadku awarii jakiegoś elementu systemu – osoby odpowiedzialne otrzymują o tym informację – mogą więc natychmiast podjąć stosowne działania naprawcze.

Innym przykładem jest system lokalizacji GPS za pomocą kart SIM (telemetrycznych). Znajduje on zastosowanie zarówno w monitorowaniu transportu drogowego jak i w zdalnym określaniu lokalizacji pojazdów. Stosowanie takiego rozwiązania przynosi korzyść w postaci stałego monitoringu pojazdów i zdolności optymalizowania ich tras. Możliwe jest również monitorowanie parametrów funkcjonowania tych pojazdów, np. poziomu paliwa, prędkości, z jakimi się poruszają, czy też liczby przejechanych kilometrów.

Powyżej wskazano tylko dwa przykłady używania kart SIM operatorów, na które nie ma potrzeby wysyłania ALERT-ów RCB. Projekt przewiduje, iż operator, stosownie do swoich możliwości technicznych, może podjąć decyzję o niewysyłaniu komunikatu do użytkownika końcowego, jeżeli będzie to karta SIM znajdującą się w urządzeniu telemetrycznym.

Takie rozwiązanie pozwoli wysyłać komunikaty przede wszystkim do osób fizycznych na zagrożonym obszarze.

Ponadto proponuje się, aby operator, po wysłaniu komunikatu, niezwłocznie przekazywał dyrektorowi Centrum informację o liczbie kart SIM użytkowników końcowych, do których komunikat został wysłany, oraz posiadaną informację o liczbie kart SIM użytkowników końcowych, do których komunikat został dostarczony. Operator przekazuje te dane z uwzględnieniem obszaru, na który komunikat został wysłany, zgodnie z żądaniem dyrektora Centrum.

Dane liczbowo-obszarowe pozyskiwane w ten sposób są danymi niezbędnymi do budowania mapy ze wskazaniem zagrożenia, obszaru objętego zagrożeniem oraz szacunkową liczbą osób, które mogą być dotknięte skutkami tychże zagrożeń.

Pozyskiwane w ten sposób dane pozwolą również na ocenę skuteczności tego systemu oraz wskazanie ewentualnych kierunków jego dalszego rozwoju;

19) *Alokacja środków finansowych na potrzeby zarządzania kryzysowego*

Doprecyzowaniu ulega regulacja dotycząca dysponowania środkami finansowymi z rezerwy celowej na potrzeby zarządzania kryzysowego. Przewiduje się, iż środki finansowe z rezerwy celowej będą mogły być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem oraz reagowaniem w przypadku wystąpienia sytuacji kryzysowej, a także usuwaniem jej skutków i odtwarzaniem zasobów.

III. Zmiany w innych ustawach

Zmiany w innych ustawach mają przede wszystkim charakter wynikowy, jak również dokonują poprawek w zakresie błędnych odniesień do ustawy o zarządzaniu kryzysowym w innych ustawach. W przypadku zmian w ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii (…) zmiany mają również charakter merytoryczny – są one powiązane tematycznie z projektowanymi zmianami, gdyż dotyczą tematyki ochrony infrastruktury krytycznej.

Art. 2 – zmiany w ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia doprecyzowują przepis art. 5 ust. 2 pkt 5 tej ustawy w zakresie zmiany odniesień zawartych w tym przepisie do nowej systematyki ustawy z.k. Obiekty, w tym obiekty budowlane, urządzenia, instalacje i usługi wchodzące w skład infrastruktury krytycznej ujęte w wykazach: krajowym, europejskim oraz wojewódzkim.

Art. 3 – zmiany w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu są zmianami wynikowymi, dotyczą art. 5 ust. 1 pkt 2a, art. 32a ust. 1 oraz art. 32aa ust. 1, zostały wprowadzone w związku ze zmianą systematyki ustawy z.k.

Art. 4 – zmiana w ustawie z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych w art. 89 w ust. 1 w pkt 7d jest zmianą *stricte* wynikową – dostosowuje przepisy ustawy p.z.p. do nowej systematyki ustawy z.k.

Art. 5 – zmiana w ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich w art. 24 w ust. 5 polega na usunięciu odwołań do nieistniejących przepisów art. 23 i art. 24 ustawy z.k. Pozostawia się natomiast, nadal aktualne odwołania do przepisów art. 21 i art. 25 ustawy z.k.

Art. 6 – zmiany w ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub

grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych obejmują poniższe kwestie.

Zmiany w tytule ustawy oraz w art. 1 ust. 1 polegają na usunięciu odniesienia do grup kapitałowych i mają charakter stricte porządkowy. Uprawnienia przysługujące ministrowi właściwemu do spraw energii są realizowane w odniesieniu do poszczególnych spółek, prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujęte w jednolitym wykazie obiektów instalacji, urządzeń i usług, a nie w odniesieniu do grup kapitałowych, w których skład wchodzą te spółki. W obowiązujących przepisach brak jest regulacji pozwalających na powołanie pełnomocnika w grupie kapitałowej, mając na względzie fakt, że przepis, zgodnie z którym kandydat na pełnomocnika powinien być pracownikiem spółki (ustawa nie przesądza, której spółki, czy wszystkich spółek grupy kapitałowej, czy spółek posiadających obiekty infrastruktury krytycznej, czy wyłącznie spółki dominującej).

Proponowane zmiany w art. 1 w ust. 2 pkt 1 i 3 przewidują objęcie przepisami ustawy o szczególnych uprawnieniach mienia spółek – operatorów infrastruktury krytycznej – służących do dystrybucji energii elektrycznej i paliw gazowych. Umożliwi to przeciwdziałanie czynnościom tych przedsiębiorców będących operatorami systemów dystrybucyjnych w sektorze energii elektrycznej i paliw gazowych (których mienie zostało ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług stanowiących infrastrukturę krytyczną), stanowiącym zagrożenie dla infrastruktury krytycznej. Obecnie w wykazie obiektów infrastruktury krytycznej zostało ujęte mienie jednej spółki dystrybucyjnej służące do dystrybucji energii elektrycznej, natomiast mienie żadnego z podmiotów zajmujących się dystrybucją paliw gazowych nie jest aktualnie ujęte w tym wykazie. Nie można wykluczyć, że w przyszłości wykazem objęte zostanie mienie innych spółek – operatorów systemu dystrybucyjnego, jeśli zostanie ono uznane za istotne dla funkcjonowania systemu lub jego części.

Natomiast uchylenie pkt 5 w art. 2 ust. 2 sprowadza się do usunięcia z katalogu uchwał organu spółki tych, które mogą zostać objęte sprzeciwem ministra właściwego do spraw energii: uchwały o przyjęciu planu rzeczowo-finansowego, planu działalności inwestycyjnej i wieloletniego planu strategicznego z uwagi na fakt, że plany te mają charakter deklaratoryjny, zawierają zakładane kierunki rozwoju spółki, a uchwała organu spółki o przyjęciu takiego planu nie jest jednoznaczna z jego realizacją. Realizacja przyjętych

założeń w odniesieniu do istotnych obszarów działalności spółki wymaga podjęcia przez jej organy odrębnych uchwał, które w przypadku, gdy stanowić będą rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej, mogą zostać objęte sprzeciwem ministra właściwego do spraw energii (o ile będą się one mieścić w katalogu czynności wymienionych w ustawie).

Zmiana proponowana w art. 2 w ust. 3 polega na wydłużeniu terminów, w których minister właściwy do spraw energii może zgłosić sprzeciw wobec określonych czynności spółki stanowiących rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej z 14 do 30 dni od dnia otrzymania informacji od pełnomocnika oraz z 30 do 45 dni od dnia ich dokonania. Przedmiotowa zmiana jest uzasadniona potrzebą uzyskania przez ministra właściwego do spraw energii czasu niezbędnego na dokonanie wszechstronnej, kompleksowej oceny planowanych przez spółkę czynności w kontekście zagrożenia dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej. Przyjęty w obowiązujących przepisach 14-dniowy termin na przeprowadzenie postępowania i wydanie decyzji administracyjnej często w skomplikowanych sprawach jest zbyt krótki. Ponadto proponuje się wydłużenie z 14 do 30 dni terminu na załatwienie sprawy w przypadku złożenia wniosku o ponowne rozpatrzenie sprawy.

W art. 5 natomiast ust. 4 otrzymuje brzmienie, w którym przewiduje się, iż pełnomocnik do spraw ochrony infrastruktury krytycznej może być koordynatorem do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5i ust.1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Zmiana w art. 6 ust. 3 ma na celu ujednolicenie, z wymogami określonymi w projektowanym art. 5e ust. 2 ustawy o zarządzaniu kryzysowym, zakresu informacji, które powinien zawierać raport o stanie ochrony infrastruktury krytycznej.

Art. 7 – zmiany w ustawie z dnia 29 października 2010 r. o rezerwach strategicznych w art. 8 w ust. 4 w pkt 1 jest zmianą wynikową, dostosowującą przepisy ustawy r.s. do nowej systematyki ustawy z.k.

Art. 8 – zmiana w ustawie z dnia 14 grudnia 2012 r. o odpadach (w art. 25 ust. 6i pkt 2) jest również zmianą wynikową, dostosowującą przepisy tej ustawy do nowej systematyki ustawy z.k.

Art. 9 – zmiany w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej w art. 4 w pkt 8 lit. b jest zmianą wynikową, dostosowującą przepisy tej ustawy do nowej systematyki ustawy z.k.

Art. 10 – zmiana w ustawie z dnia 7 lutego 2014 r. o udziale zagranicznych funkcjonariuszy lub pracowników we wspólnych operacjach lub wspólnych działaniach ratowniczych na terytorium Rzeczypospolitej Polskiej – w art. 4 ust. 4 ww. ustawy znajduje się błędne wskazanie odniesienia do pojęcia zdarzenia o charakterze terrorystycznym, wskazujące w tym zakresie ustawę z.k. zamiast ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych.

Art. 11 – zmiany w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w art. 4 w pkt 8 lit. b są zmianami wynikowymi dostosowującymi przepisy tej ustawy do nowej systematyki ustawy z.k.

IV. Przepisy przejściowe i końcowe

Projekt przewiduje, iż streszczenie istotnych elementów krajowej oceny ryzyka, w brzmieniu nadanym projektowaną ustawą, zostanie sporządzone w terminie do dnia 31 grudnia 2020 r.

Streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, w brzmieniu nadanym projektowaną ustawą, zostanie po raz pierwszy sporządzone w terminie do dnia 31 grudnia 2020 r.

Plany zarządzania ryzykiem, w brzmieniu nadanym projektowaną ustawą, zostaną sporządzone w terminie do dnia 8 sierpnia 2020 r. Plany sporządzone po raz pierwszy nie zawierają oceny osiągniętych efektów i wniosków z wdrożonych działań.

Plany reagowania kryzysowego, w brzmieniu nadanym projektowaną ustawą, zostaną sporządzone w terminie 12 miesięcy od dnia sporządzenia planów zarządzania ryzykiem.

Plany zarządzania kryzysowego sporządzone i zatwierdzone na podstawie dotychczasowych przepisów, przed dniem wejścia w życie projektowanej ustawy, pozostają w mocy do czasu sporządzenia planów zarządzania ryzykiem oraz planów reagowania kryzysowego.

Kryteria wyłaniania infrastruktury krytycznej zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie projektowanej ustawy.

Wykazy infrastruktury krytycznej, tj. krajowy, europejski oraz wojewódzki, zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie projektowanej ustawy.

Operatorzy infrastruktury krytycznej wyznaczą po raz pierwszy koordynatorów do spraw ochrony infrastruktury krytycznej w terminie 30 dni od dnia wejścia w życie projektowanej ustawy.

Raport o stanie ochrony infrastruktury krytycznej, w brzmieniu nadanym projektowaną ustawą, sporządza się po raz pierwszy za rok 2020.

Operatorzy infrastruktury krytycznej zapewnią zdolność do ochrony informacji niejawnych w terminie 18 miesięcy od dnia wejścia w życie projektowanej ustawy.

Projektowany przepis art. 26 ust. 4a ustawy z.k. będzie miał zastosowanie po raz pierwszy do opracowania budżetów jednostek samorządu terytorialnego na 2021 r.

Przepisy wykonawcze dotyczące sporządzania Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów ochrony infrastruktury krytycznej zachowują moc do czasu wejścia w życie nowych aktów wykonawczych, jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie projektowanych rozwiązań.

Przewidziano 14-dniowy termin wejścia w życie regulacji zawartych w projekcie ustawy.

Projekt ustawy jest zgodny z prawem Unii Europejskiej oraz nie zawiera norm technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i w związku z powyższym nie podlega procedurze notyfikacji.

Projektowana ustawa nie wymaga przedstawienia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu.

Nazwa projektu Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw **Ministerstwo wiodące i ministerstwa współpracujące** Dyrektor Rządowego Centrum Bezpieczeństwa **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan nadbryg. Marek Kubiak, dyrektor Rządowego Centrum Bezpieczeństwa **Kontakt do opiekuna merytorycznego projektu** Pani Beata Janowczyk, Szef Wydziału Oceny Ryzyka i Planowania Cywilnego (pkt I rozwiązań zawartych w projekcie) tel. 22 361-69-30, tel. kom. 785-700-195 e-mail: beata.janowczyk@rcb.gov.pl Pan Witold Skomra, Doradca w Rządowym Centrum Bezpieczeństwa (pkt II rozwiązań zawartych w projekcie) tel. 22 361-68-17, tel. kom. 785-700-176 e-mail: witold.skomra@rcb.gov.pl	**Data sporządzenia** **16.01.2020** **Źródło:** Inne **Nr w wykazie prac** UD46 (projekt procedowany w archiwalnym wykazie prac RM pod numerem UD523)

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

I. Zapewnienie formalno-prawnych podstaw zarządzania ryzykiem, które jest wymogiem spełnienia warunkowości podstawowej w kolejnej perspektywie finansowej UE na lata 2021–2027.

Zadania w zakresie zarządzania ryzykiem zostały określone w *decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności*. Opracowanie dokumentów planistycznych w obszarze zarządzania ryzykiem jest bezpośrednio powiązane z jednym z warunków podstawowych kolejnej perspektywy finansowej, który mówi o osiągnięciu *Skutecznych ram zarządzania ryzykiem*.

Wskazuje się wprost na konieczność opracowania planu zarządzania ryzykiem na szczeblu krajowym lub regionalnym, powiązanego ze strategiami adaptacji do zmian klimatu. Ponadto państwa członkowskie opracowują oceny ryzyka na szczeblu krajowym lub niższym oraz udostępniają Komisji Europejskiej tzw. streszczenie istotnych elementów tych ocen.

Cele wynikające z Unijnego Mechanizmu Ochrony Ludności powiązane są z priorytetami przyjętymi podczas Trzeciej Światowej Konferencji ONZ, która odbyła się w 2015 r. w Sendai. Jednym z podstawowych wymogów *Ramowego programie działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof* jest realizacja przedsięwzięć zgodnie z przyjętymi przez poszczególne państwa celami strategicznymi, zarówno na szczeblu centralnym, jak i lokalnym. Biuro Narodów Zjednoczonych ds. ograniczenia ryzyka katastrof (UNDRR) otrzymało zadanie wsparcia krajów członkowskich we wdrażaniu postanowień Programu. Współpraca realizowana jest przez wyznaczone w poszczególnych krajach punkty kontaktowe.

Według obowiązujących w Polsce regulacji, ocena ryzyka aktualizowana jest w cyklu dwuletnim w *Raporcie o zagrożeniach bezpieczeństwa narodowego* oraz w raportach cząstkowych do *Raportu* sporządzanych przez ministrów, kierowników urzędów centralnych oraz wojewodów. Dokumenty te stanowią podstawę opracowywanego, również cyklicznie, *Krajowego Planu Zarządzania Kryzysowego* oraz planów zarządzania kryzysowego na wszystkich szczeblach administracji. Brak jest formalno-prawnych podstaw dotyczących kwestii zarządzania ryzykiem. Przede wszystkim nie ma obowiązku opracowywania planów zarządzania ryzykiem oraz dokumentów, których założeniem jest poinformowanie Komisji Europejskiej o spełnieniu wymaganych zapisów, tj. *Streszczenia istotnych elementów krajowej oceny ryzyka* oraz *Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem*.

II. Zapewnienie formalno-prawnych rozwiązań związanych z zachowaniem ciągłości świadczenia usług kluczowych realizowanych w systemach wskazanych w art. 3 ust 2 ustawy o zarządzaniu kryzysowym. Identyfikacja usług świadczonych przez operatorów infrastruktury krytycznej oraz ich znacząca współzależność ze względu na potencjalne skutki zakłócenia zarówno w odniesieniu do funkcjonowania państwa, jak i społeczeństwa.

Minimalizacja skutków zakłócenia przez wprowadzenie procesów oceny i zarządzania ryzykiem oraz uwzględnienie zagrożeń dotyczących infrastruktury krytycznej. Ujęcie zagrożeń dla infrastruktury krytycznej w planach zarządzania ryzykiem oraz planach reagowania kryzysowego.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

I. Propozycje zawarte w przedkładanym projekcie nowelizacji w założeniu nie mają kompleksowo dokonać transpozycji regulacji zawartych w *decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności* (dalej „decyzja UMOL"). Decyzja UMOL, co do zasady, jest bowiem wiążąca dla tych podmiotów, do których jest adresowana – w tym przypadku państw UE – i jest stosowana bezpośrednio.

Zakres proponowanej nowelizacji w tym obszarze obejmuje kwestie, które wymagają uregulowania w polskim prawodawstwie, gdyż dotyczą wdrożenia zintegrowanego podejścia do zarządzania ryzykiem, obejmującego cały cykl zarządzania, od oceny ryzyka przez przygotowanie planów zarządzania nim oraz wdrażanie środków zapobiegawczych i zapewniających gotowość do ich użycia. Według obowiązującego w Polsce prawa, ocena ryzyka na potrzeby planowania cywilnego aktualizowana jest w cyklu dwuletnim w *Raporcie o zagrożeniach bezpieczeństwa narodowego* oraz w raportach cząstkowych do *Raportu* sporządzanych przez ministrów, kierowników urzędów centralnych oraz wojewodów. Dokumenty te stanowią podstawę opracowywanego, również cyklicznie, *Krajowego Planu Zarządzania Kryzysowego* oraz planów zarządzania kryzysowego ministrów, kierowników urzędów centralnych i wojewodów.

Na chwilę obecną regulacje zawarte w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym nie pozwalają w pełni odzwierciedlać w planach zarządzania kryzysowego kwestii dotyczących zarządzania ryzykiem. Istnieje zatem konieczność opracowywania planów zarządzania ryzykiem, na szczeblu krajowym lub odpowiednio niższym, powiązanych ze strategiami adaptacji do zmian klimatu. Niezbędne jest wskazanie m.in. podmiotów odpowiedzialnych za ich opracowanie, zakresu merytorycznego czy cyklu planistycznego.

Posiadanie planów zarządzania ryzykiem stało się o tyle istotne, iż są one niezbędne do spełnienia tzw. warunkowości *ex ante* w perspektywie finansowej UE na lata 2021–2027, a co będzie miało przełożenie na pozyskiwanie środków finansowych w ramach polityki spójności z Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności oraz Europejskiego Funduszu Morskiego i Rybackiego.

Dodatkowo, zgodnie z obowiązującą od dnia 21 marca 2019 r. decyzją Parlamentu Europejskiego i Rady (UE) 2019/420 z dnia 13 marca 2019 r. zmieniającą decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności, wszystkie działania na rzecz skutecznego zapobiegania klęskom żywiołowym i katastrofom spowodowanym przez człowieka powinny być spójne z *Ramowym programem działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof*. Jednym z jego podstawowych wymogów jest realizacja przedsięwzięć zgodnie z opracowanymi przez poszczególne państwa strategiami ograniczenia ryzyka katastrof, zarówno na szczeblu centralnym, jak i lokalnym.

Dokonanie korelacji między regulacjami krajowymi a unijnymi będzie odbywać się bez konieczności opracowywania od podstaw nowych dokumentów planistycznych, lecz z wykorzystaniem już opracowanych i funkcjonujących.

Raport o zagrożeniach bezpieczeństwa narodowego w dalszym ciągu dotyczyć będzie oceny ryzyka. Po jej przeprowadzeniu i wskazaniu najistotniejszych zagrożeń dla bezpieczeństwa narodowego, konieczne jest określenie celów strategicznych służących ograniczeniu ryzyka ich wystąpienia, z wykorzystaniem istniejących zapisów oraz wniosków zawierających hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do ich osiągnięcia, z uwzględnieniem regionalnych lub lokalnych inicjatyw, czyli podejmowanych na obszarze województwa. Istotne jest bowiem zrozumienie, że dopiero prawidłowo przeprowadzona ocena ryzyka identyfikuje zagrożenia i obszary, w których konieczne jest podjęcie działań, w tym zwiększenie nakładów finansowych na przedsięwzięcia ograniczające ryzyko katastrof. Ta część *Raportu* będzie stanowiła wypełnienie obowiązku strategii.

Przygotowywane do tej pory plany zarządzania kryzysowego podzielone zostaną na plany zarządzania ryzykiem (dotyczące działań w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do jej wystąpienia) oraz plany reagowania kryzysowego (w odniesieniu do działań w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków).

Informacje dotyczące szczegółowych przedsięwzięć, które do tej pory stanowiły część *Raportu*, oraz zadania i obowiązki uczestników zarządzania kryzysowego dla faz: zapobieganie i przygotowanie, które stanowiły część *Krajowego Planu Zrządzania Kryzysowego*, zostaną przeniesione do planu zarządzania ryzykiem na szczeblu krajowym. Konieczna będzie analiza i uzupełnienie wymienionych przedsięwzięć, z uwzględnieniem elementu służącemu ich weryfikacji, aby ustalić, czy ich realizacja wpłynęła na ograniczenie ryzyka. Podobnie będzie wyglądać konstrukcja planów zarządzania ryzykiem na pozostałych szczeblach.

Przewiduje się wprowadzenie dla organów administracji rządowej obowiązku wdrażania *Ramowego programu działań na lata 2015–2030 na rzecz ograniczenia ryzyka katastrof* oraz pełnienie przez Rządowe Centrum Bezpieczeństwa funkcji krajowego punktu kontaktowego dla Organizacji Narodów Zjednoczonych do spraw jego wdrażania.

Wskazane jest także dostosowanie terminologii do regulacji unijnych, co stworzy efektywne narzędzia do prowadzenia oceny ryzyka i zarządzania nim. Jednocześnie należy ujednolicić terminy cyklów planistycznych krajowych z unijnymi, gdyż obowiązujące przepisy krajowe przewidują cykl 2-letni, podczas gdy unijne regulacje wskazują na 3-letnie cykle planistyczne.

II. Zostanie dokonana identyfikacja usług kluczowych oraz ich współzależności. Przewiduje się uwzględnienie w planach zarządzania ryzykiem oraz planach reagowania kryzysowego zagrożeń dla infrastruktury krytycznej.
Opracowane zostaną kryteria umożliwiające wyłanianie operatorów infrastruktury krytycznej oraz pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, przeprowadzony zostanie podział na infrastrukturę krytyczną, której zniszczenie lub zakłócenie będzie miało niekorzystny wpływ na:

– funkcjonowanie państwa i zaspokojenia potrzeb obywateli,
– zaspokojenie potrzeb lokalnych społeczności danego województwa.

W przypadku pierwszym sposób wyłaniania i umieszczania w wykazie pozostanie na dotychczasowych zasadach. W drugim przypadku natomiast kompetencje w zakresie wyłaniania i umieszczania infrastruktury krytycznej przypadną wojewodzie.

Ponadto przewiduje się wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u wszystkich operatorów infrastruktury krytycznej. Operatorzy infrastruktury krytycznej we wszystkich systemach będą wyznaczać osoby koordynujące działania na linii operator – organy administracji publicznej, co jest analogią do obecnie wyznaczonych osób kontaktowych, funkcjonujących u operatorów infrastruktury krytycznej. Zmiana ta nie generuje dodatkowych kosztów dla operatorów IK, natomiast wprowadza efektywnie działające narzędzie systemowe w zakresie ochrony infrastruktury krytycznej, czyli dokonuje instytucjonalizacji osoby do utrzymywania kontaktów, tj. zastąpienie jej funkcją „koordynatora ochrony infrastruktury krytycznej". Koordynatorowi jednocześnie zostaną przyznane stosowne kompetencje. Koordynator będzie realizował działania przypisane ustawowo operatorowi i w jego imieniu.

Elementem weryfikującym poprawność planu ochrony infrastruktury krytycznej będzie raport zawierający w szczególności informacje dotyczące funkcjonowania ochrony infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania.

Raportowanie o stanie IK w obowiązującym stanie prawnym dotyczy tylko systemu zaopatrzenia w energię, surowce energetyczne i paliwa. Dotychczas raporty te w powyżej wskazanym systemie sporządzane były z częstotliwością raz na kwartał. W odniesieniu do pozostałych systemów obowiązywało raportowanie doraźne. W projekcie ustawy obowiązek okresowego raportowania został rozszerzony na wszystkie systemy, a cykl raportowania został ujednolicony i wydłużony do 12 miesięcy. W dalszym ciągu w przypadku wystąpienia incydentu naruszającego bezpieczeństwo infrastruktury krytycznej, operator zobowiązany będzie do doraźnego sporządzania raportów.

Raport o stanie ochrony infrastruktury krytycznej sporządzany będzie m.in. z uwzględnieniem rozwiązań zawartych w planie ochrony infrastruktury krytycznej operatora, możliwości wystąpienia ryzyka zidentyfikowanego w planie ochrony infrastruktury krytycznej, incydentów i zdarzeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, które nie były uwzględnione w planie ochrony infrastruktury krytycznej, wyników przeprowadzonych kontroli i audytów odnoszących się do zabezpieczeń zawartych w planie ochrony infrastruktury krytycznej. Z tytułu jego sporządzania operatorzy nie będą ponosić dodatkowych kosztów.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Obowiązek opracowania planów zarządzania ryzykiem jest wdrażany w innych krajach UE, co wynika z postanowienia decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności. Brak jest danych dotyczących legislacji w innych państwach w tym obszarze.
Kraje ONZ, zgodnie z ustalonym harmonogramem, wdrażają Ramowy programu działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof na podstawie Porozumienia zawartego podczas Trzeciej Światowej Konferencji ONZ, która odbyła się w 2015 r. w Sendai.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Mieszkańcy	38,4 mln	Dane GUS za I półrocze 2018 r.	Wzrost bezpieczeństwa ludności związany z ograniczeniem ryzyka katastrof oraz związaną z tym utratą życia, zdrowia, mienia, jak również strat

			ekonomicznych, społecznych, kulturowych i środowiskowych.
Ministrowie	19		Przekonstruowanie nowych edycji raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów zarządzania kryzysowego, które należało będzie opracowywać jako plany zarządzania ryzykiem i plany reagowania kryzysowego.
Kierownicy urzędów centralnych	40		Przekonstruowanie nowych edycji raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów zarządzania kryzysowego, które należało będzie opracowywać jako plany zarządzania ryzykiem i plany reagowania kryzysowego.
Wojewodowie	16		Przekonstruowanie nowych edycji raportów cząstkowych do Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów zarządzania kryzysowego, które należało będzie opracowywać jako plany zarządzania ryzykiem i plany reagowania kryzysowego.
Dyrektor Rządowego Centrum Bezpieczeństwa	1		Przekonstruowanie nowych edycji Raportu o zagrożeniach bezpieczeństwa narodowego oraz Krajowego Planu Zarządzania Kryzysowego, który należało będzie opracować jako plan zarządzania ryzykiem i plan reagowania kryzysowego.
Powiaty	380		Przekonstruowanie planów zarządzania kryzysowego, które należało będzie opracowywać jako plany zarządzania ryzykiem i plany reagowania kryzysowego.
Gminy	2 478		Przekonstruowanie planów zarządzania kryzysowego, które należało będzie opracowywać jako plany zarządzania ryzykiem i plany reagowania kryzysowego.
Operatorzy Infrastruktury krytycznej	128	Dane własne	Wyznaczenie osoby koordynującej działania na linii operator – organy administracji publicznej, tzw. koordynatorów ochrony infrastruktury krytycznej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Dyskusje nad potrzebą wdrożenia procesu zarządzania ryzykiem, zgodnie z wytycznymi Unijnego Mechanizmu Ochrony Ludności oraz Ramowym programem działań na lata 2015–2030 w sprawie ograniczenia ryzyka katastrof, trwały w Polsce od wielu lat.

Decydujące rozmowy dotyczyły konieczności spełnienia warunków podstawowych kolejnej perspektywy finansowej. Spotkania tego dotyczące odbyły się w Ministerstwie Inwestycji i Rozwoju, Ministerstwie Środowiska, z udziałem przedstawicieli ww. ministerstw oraz Ministerstwa Spraw Wewnętrznych i Administracji oraz Rządowego Centrum Bezpieczeństwa. Konkluzją było uznanie, że jedynym sposobem na spełnienie warunkowości *ex ante* jest nowelizacja ustawy o zarządzaniu kryzysowym.

Stosownie do postanowień § 36 ust. 1 i § 38 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, udostępniony został projekt *ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw*, a właściwe podmioty zostały bezpośrednio poinformowane o zamieszczeniu projektu.

Podmioty, którym został przedstawiony projekt: Prezes Prokuratorii Generalnej Rzeczypospolitej Polskiej; Prezes Urzędu Ochrony Konkurencji i Konsumentów; Główny Geodeta Kraju; Główny Inspektor Ochrony Środowiska; Główny Inspektor Sanitarny; Główny Lekarz Weterynarii; Komendant Główny Państwowej Straży Pożarnej; Komendant Główny Policji; Komendant Główny Straży Granicznej; Komendant Główny Żandarmerii Wojskowej; Komendant Służby Ochrony Państwa; Prezes Państwowej Agencji Atomistyki; Prezes Urzędu Lotnictwa Cywilnego; Szef Biura Bezpieczeństwa Narodowego; Szef Agencji Bezpieczeństwa Wewnętrznego; Szef Agencji Wywiadu; Szef Obrony Cywilnej Kraju; Szef Służby Kontrwywiadu Wojskowego; Szef Służby Wywiadu Wojskowego; Szef Sztabu Generalnego Wojska Polskiego; Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa; Pełnomocnik Rządu do spraw Strategicznej Infrastruktury Energetycznej; Wojewodowie – wszyscy; Zarząd Główny Związku Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej; Zarząd Główny Polskiego Czerwonego Krzyża; Operatorzy infrastruktury krytycznej – wszyscy; Orange Polska S.A.; P4 Sp. z o.o.; Polkomtel Sp. z o.o.; T-Mobile S.A.; Polska Izba Informatyki i Telekomunikacji; Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji; Polska Izba Komunikacji Elektronicznej; Polskie Towarzystwo Informatyczne; Stowarzyszenie Inżynierów Telekomunikacji.

Zgłoszone w trakcie konsultacji i opiniowania uwagi dotyczyły treści rozwiązań zawartych w projekcie ustawy. Część uwag powielała się. Część uwag przyjęto i w oparciu o nie przeredagowano projekt ustawy. Większość uwag stała się bezprzedmiotowa, ponieważ w międzyczasie podjęto decyzję o usunięciu z projektu propozycji przepisów, do których były one zgłaszane.

Projekt ustawy nie podlegał konsultacjom z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym.

Na etapie konsultacji do projektu ustawy nie został zgłoszony żaden wniosek w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0–10)*
Dochody ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Ustawa nie będzie mieć wpływu na budżet państwa oraz budżety jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Rozwiązania zawarte w ustawie wprowadzają w głównej mierze dodatkowe formalno-prawne narzędzia realizacji ustawowych obowiązków organów zarządzania kryzysowego, w ramach posiadanych na te zadania środków finansowych.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0–10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
Niemierzalne	(dodaj/usuń)							
	(dodaj/usuń)							

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Ustawa nie będzie miała wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe. Brak wpływu projektowanej regulacji na sytuację ekonomiczną i społeczną rodziny, a także osób niepełnosprawnych oraz osób starszych.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐tak ☐nie ☒nie dotyczy
☐zmniejszenie liczby dokumentów ☐zmniejszenie liczby procedur ☐skrócenie czasu na załatwienie sprawy ☐inne: …	☒zwiększenie liczby dokumentów ☐zwiększenie liczby procedur ☐wydłużenie czasu na załatwienie sprawy ☐inne: …
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐tak ☐nie ☒ nie dotyczy

Komentarz:

Ustawa powoduje przekonstruowanie obecnie opracowywanych dokumentów planistycznych. Zostanie opracowany Raport o zagrożeniach bezpieczeństwa narodowego w nowym kształcie.

Przewiduje cykliczne sporządzanie streszczenia istotnych elementów krajowej oceny ryzyka oraz streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem (w brzmieniu przewidzianym projektowaną ustawą zostanie sporządzona w terminie do dnia 31 grudnia 2020 r.).

Sporządzone zostaną w nowej formule plany zarządzania ryzykiem w brzmieniu przewidzianym niniejszym projektem ustawy zostaną sporządzone w terminie do dnia 8 sierpnia 2020 r. Plany sporządzane po raz pierwszy nie będą zawierać oceny osiągniętych efektów i wniosków z wdrożonych działań w zakresie organizacyjnym, technicznym i finansowym na rzecz ograniczenia ryzyka katastrof.

Zostaną również sporządzone plany reagowania kryzysowego – termin ich sporządzenia to 12 miesięcy od dnia sporządzenia planów zarządzania ryzkiem.

W odniesieniu do infrastruktury krytycznej – opracowane zostaną kryteria wyłaniania infrastruktury krytycznej w terminie 24 miesięcy od dnia wejścia w życie ustawy oraz sporządzone zostaną wykazy infrastruktury krytycznej na podstawie nowych kryteriów – również w terminie 24 miesięcy od dnia wejścia w życie ustawy.

Operator infrastruktury krytycznej będzie sporządzał raport o stanie ochrony infrastruktury krytycznej. Regulacja przewiduje, iż raport będzie sporządzany za rok poprzedzający w terminie do dnia 31 marca każdego roku.

Przyjęto, iż raport jako dokument o charakterze sprawozdawczym powinien stanowić roczne podsumowanie realizacji działań podejmowanych w zakresie ochrony infrastruktury krytycznej.

Raport o stanie ochrony infrastruktury krytycznej jest przekazywany dyrektorowi Centrum oraz odpowiednio:

- ✓ właściwemu ministrowi odpowiedzialnemu za dany system infrastruktury krytycznej albo
- ✓ właściwemu kierownikowi urzędu centralnego odpowiedzialnemu za dany system infrastruktury krytycznej, albo
- ✓ właściwemu terytorialnie wojewodzie.

W celu realizacji zadań w zakresie ochrony infrastruktury krytycznej – operatorzy powołają koordynatorów. Do uprawnień koordynatora, któremu operator zapewnia warunki do wykonywania zadań, zalicza się m.in. możliwość przedkładania rekomendacji organowi zarządzającemu operatora w zakresie ochrony jego obiektów, instalacji urządzeń i usług.

Ponadto przewidziano, iż operator infrastruktury krytycznej w związku z realizacją przedsięwzięć w zakresie ochrony jego obiektów, instalacji, urządzeń i usług zapewnia zdolność do ochrony informacji niejawnych. Należy bowiem przyjąć, że informacje wrażliwe wytworzone w ramach opracowywania, uzgadniania oraz realizacji planów ochrony infrastruktury krytycznej oraz informacje wymieniane z właściwymi organami administracji publicznej o zidentyfikowanych zagrożeniach lub zakłóceniach infrastruktury krytycznej oraz podejmowanych działaniach w celu jej ochrony lub odtworzenia powinny być klasyfikowane jako informacje niejawne. Regulacja, zgodnie z postanowieniami ustawy o ochronie informacji niejawnych, pozostawia operatorom infrastruktury krytycznej decyzję w odniesieniu do sposobów zapewnienia ochrony informacji niejawnych, w zależności od poziomu niejawności wytwarzanych informacji.

Informacje niejawne przekazywane operatorom posiadają najczęściej klauzulę „zastrzeżone". W niektórych wypadkach niezbędnym jest przekazywanie informacji o klauzuli „poufne". Jeżeli jednak podmioty administracji publicznej przewidują przekazywanie informacji niejawnych o wyższych klauzulach niż „zastrzeżone", możliwe jest przeprowadzanie postępowań sprawdzających wobec wybranych pracowników operatorów infrastruktury krytycznej do wyższych klauzul. Samo złożenie ankiety bezpieczeństwa już pozwala na uzyskanie dostępu do dokumentów oznaczonych klauzulą „poufne". Ponadto ustawa umożliwia odstąpienie od pobierania kosztów postępowania sprawdzającego, jako że jest ono prowadzone ze względu na uzasadniony wniosek administracji. Nowelizacja nie nakłada obowiązku posiadania własnej kancelarii niejawnej. Wgląd do dokumentów o klauzulo „poufne" może być realizowany w urzędach wojewódzkich. Rozwiązania dotyczące raportowania i ochrony informacji zostały uzgodnione z operatorami IK w trybie roboczym.

9. Wpływ na rynek pracy

Ustawa nie będzie miała wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☒środowisko naturalne ☒sytuacja i rozwój regionalny ☐inne: …	☒demografia ☒mienie państwowe	☒informatyzacja ☒zdrowie

Omówienie wpływu	Zapisy wdrożą zarządzanie ryzykiem, którego celem jest m.in. poprawa bezpieczeństwa, w tym – znaczne ograniczenie globalnej śmiertelności w wyniku katastrof; – znaczne ograniczenie liczby osób na świecie, które ucierpią w wyniku katastrof; – ograniczenie bezpośrednich strat ekonomicznych spowodowanych katastrofami; – znaczne ograniczenie szkód spowodowanych katastrofami w zakresie krytycznej infrastruktury i zakłócenia podstawowych usług, takich jak służba zdrowia czy edukacji.

11. Planowane wykonanie przepisów aktu prawnego

W przepisach przejściowych i końcowych projektu ustawy wskazano graniczne terminy proponowanych rozwiązań.

Streszczenie (…) oraz Krajowa ocena ryzyka (…)

Projekt przewiduje, iż streszczenie istotnych elementów krajowej oceny ryzyka oraz streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem w brzmieniu przewidzianym projektowaną ustawą zostaną sporządzone w terminie do dnia 31 grudnia 2020 r.

Plany zarządzania kryzysowego

Plany zarządzania ryzykiem w brzmieniu przewidzianym niniejszym projektem ustawy zostaną sporządzone w terminie do dnia 8 sierpnia 2020 r. Plany sporządzane po raz pierwszy nie będą zawierać oceny osiągniętych efektów i wniosków z wdrożonych działań w zakresie organizacyjnym, technicznym i finansowym na rzecz ograniczenia ryzyka katastrof.

Plany reagowania kryzysowego w brzmieniu przewidzianym niniejszym projektem ustawy zostaną sporządzone w terminie 12 miesięcy od dnia sporządzenia planów zarządzania ryzkiem.

Infrastruktura krytyczna

Przewiduje się, iż kryteria wyłaniania infrastruktury krytycznej uwzględniające regulacje zawarte w projekcie ustawy zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie ustawy.

Wykazy infrastruktury krytycznej sporządzone na podstawie tych kryteriów zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie ustawy.

Operatorzy infrastruktury krytycznej wyznaczą po raz pierwszy koordynatorów do spraw ochrony infrastruktury krytycznej w terminie 30 dni od dnia wejścia w życie projektowanej ustawy.

Raporty o stanie ochrony infrastruktury krytycznej zostaną sporządzane przez koordynatorów do spraw ochrony infrastruktury krytycznej po raz pierwszy za rok 2020.

Operatorzy infrastruktury krytycznej zapewnią zdolność do ochrony informacji niejawnych w terminie 18 miesięcy od dnia wejścia w życie projektowanej ustawy.

Regulacje dotyczące kwestii dotyczących finansowania zadań z zakresu zarządzania kryzysowego będą miały zastosowanie po raz pierwszy do opracowania budżetów jednostek samorządu terytorialnego na 2021 r.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Ewaluacja będzie odbywać się w formie ćwiczeń z zakresu zarządzania kryzysowego, testujących rozwiązania zawarte w dokumentach planistycznych oraz kontrole realizacji zadań/przedsięwzięć przeprowadzane przez uprawnione do tego podmioty (np. kontrole prowadzone przez NIK).

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

-

Raport

z konsultacji projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw

1. Przedmiot konsultacji publicznych oraz opiniowania.

Przedmiotem konsultacji publicznych był projekt nowelizacji ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UD 523). Projekt dokonuje przede wszystkim zmian w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym oraz zmian w następujących ustawach:

1) ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
2) ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych;
3) ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

2. Przebieg konsultacji publicznych i opiniowania oraz wskazanie podmiotów, które wzięły w nich udział.

Stosownie do postanowień § 36 ust. 1 i 38 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, udostępniony został projekt *ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw* a właściwe podmioty bezpośrednie poinformowane o zamieszczeniu projektu.

Podmioty, którym został przedstawiony projekt: Prezes Prokuratorii Generalnej Rzeczypospolitej Polskiej; Prezes Urzędu Ochrony Konkurencji i Konsumentów; Główny Geodeta Kraju; Główny Inspektor Ochrony Środowiska; Główny Inspektor Sanitarny; Główny Lekarz Weterynarii; Komendant Główny Państwowej Straży Pożarnej; Komendant Główny Policji; Komendant Główny Straży Granicznej; Komendant Główny Żandarmerii Wojskowej; Komendant Służby Ochrony Państwa; Prezes Państwowej Agencji Atomistyki; Prezes Urzędu Lotnictwa Cywilnego; Szef Biura Bezpieczeństwa Narodowego; Szef Agencji

Bezpieczeństwa Wewnętrznego; Szef Agencji Wywiadu; Szef Obrony Cywilnej Kraju; Szef Służby Kontrwywiadu Wojskowego; Szef Służby Wywiadu Wojskowego; Szef Sztabu Generalnego Wojska Polskiego; Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa; Pełnomocnik Rządu do spraw Strategicznej Infrastruktury Energetycznej; Wojewodowie – wszyscy; Zarząd Główny Związku Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej; Zarząd Główny Polskiego Czerwonego Krzyża; Operatorzy infrastruktury krytycznej – wszyscy; Orange Polska S.A.; P4 Sp. z o.o.; Polkomtel Sp. z o.o.; T-Mobile S.A.; Polska Izba Informatyki i Telekomunikacji; Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji; Polska Izba Komunikacji Elektronicznej; Polskie Towarzystwo Informatyczne; Stowarzyszenie Inżynierów Telekomunikacji.

Zgłoszone w trakcie konsultacji i opiniowania uwagi dotyczyły treści rozwiązań zawartych w projekcie ustawy. Część uwag powielała się. Część uwag przyjęto i w oparciu o nie przeredagowano projekt ustawy. Większość uwag, tym wskazane w pkt 3 „Opis (…)" stała się bezprzedmiotowa ponieważ w międzyczasie podjęto decyzję o usunięciu z projektu propozycji przepisów, do których były one zgłaszane.

3. Opis najważniejszych uwag zgłaszanych w konsultacjach publicznych i opiniowaniu.

1) Wskazywano, iż definicja „klęski żywiołowej" zawarta w słowniczku projekcie ustawy o zarządzaniu kryzysowym różni się od definicję klęski żywiołowej, która znajduje się w ustawie o stanie klęski żywiołowej. Tym samym dwie definicji funkcjonujące w obrocie prawnym mogłyby powodować wątpliwości interpretacyjne przy ich stosowaniu.
   Obok definicji sytuacji kryzysowej wątpliwości budziły inne definicje, w tym definicja „zagrożeń hybrydowych".
2) Zdaniem opiniujących zbędne było wprowadzenie podziału planów zarządzania kryzysowego na plany zarządzania ryzykiem oraz plany reagowania kryzysowego. Podnoszono, iż w praktyce w miejsce tworzenia rozbudowanych powinno się dążyć do opracowywania wyłącznie maksymalnie użytecznych planów, które pozwalałyby korzystać z wypracowanych algorytmów i procedur.
   Dlatego też proponowano rozważyć ujęcie kwestii związanych z zarządzaniem ryzykiem w ramach raportów cząstkowych o zagrożeniach bezpieczeństwa narodowego, które już w chwili obecnej zawierają podobne treści. Natomiast plany reagowania kryzysowego tworzyć w ten sposób, aby były maksymalnie użyteczne i ograniczały się wyłącznie do charakterystyki zagrożeń oraz procedur postępowania na wypadek ich wystąpienia.
3) Postulowano konieczność usunięcia z projektu ustawy tych przepisów, które dotyczą

obowiązku wdrożenia minimalnych wymagań w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego infrastruktury krytycznej.

Rozwiązanie polegające na określeniu w rozporządzaniu Rady Ministrów minimalnych wymagań wobec operatorów infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego powodowałoby, po stronie operatora, nadmierne obciążenie finansowe, co w konsekwencji może prowadzić do utraty przez niego płynności finansowej i doprowadzić do zagrożenia likwidacją lub upadłością.

4) Zakwestionowano propozycje odnoszące się do możliwości ujęcia projektowanego lub budowanego obiektu budowlanego, urządzenia, instalacji i usługi w wykazie infrastruktury krytycznej. Budziło to bowiem obawy przedsiębiorców, ponieważ w związku z tym przepisem podmiot publiczny potencjalnie będzie miał możliwość ingerencji na etapie planowania i budowy w infrastrukturę usługową prywatnego podmiotu. Ze względu na możliwe oddziaływanie na wolność działalności gospodarczej wnioskowano o usunięcie regulujących te kwestie przepisów. Argumentowano, iż niezależnie od obowiązków ustawowych każdy przedsiębiorca finansujący budowę i utrzymanie swojej infrastruktury dąży do tego, aby była ona odpowiednio chroniona i zapewniała ciągłość działania przedsiębiorcy, gdyż to na jej podstawie świadczy on swoje usługi wobec klientów.
5) Wskazano, iż możliwość tworzenia sztabów koordynacyjnych na poszczególnych szczeblach zarządzania kryzysowego, będzie powodować trudności interpretacyjne w zakresie kompetencji takiego sztabu w odniesieniu do uprawnień osób kierujących akcją na miejscu zdarzenia czy też kompetencji zespołów zarządzania kryzysowego.
6) Wątpliwości budziły regulacje dotyczące tzw. Centralnej Bazy Magazynowej, tj. kwestii kto będzie wyposażał i utrzymywał Centralną Bazę Magazynową.
   Zdaniem zgłaszających uwagi brak było m.in. informacji o możliwości dysponowania sprzętem znajdującym się w Centralnej Bazie Magazynowej w czasie wojny lub po wprowadzeniu jednego ze stanów nadzwyczajnych.

4. Przedstawienie wyników zasięgnięcia opinii, dokonania konsultacji albo uzgodnienia projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym.

Projekt ustawy nie podlegał konsultacjom z właściwymi organami i instytucjami Unii

Europejskiej, w tym Europejskim Bankiem Centralnym.

Projekt ustawy nie podlega notyfikacji.

5. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa, wraz ze wskazaniem kolejności dokonania zgłoszeń albo informacji o ich braku.

Na etapie konsultacji do projektu rozporządzenia nie został zgłoszony żaden wniosek w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa.

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego

Na podstawie art. 5a ust. 9 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz …) zarządza się, co następuje:

§ 1. Rozporządzenie określa sposób i tryb opracowania Raportu o zagrożeniach bezpieczeństwa narodowego, zwanego dalej „Raportem”.

§ 2. 1. W celu sporządzenia Raportu ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie, zwani dalej „wykonawcami”, w zakresie swojej właściwości, opracowują raporty cząstkowe o zagrożeniach bezpieczeństwa narodowego, zwane dalej „raportami cząstkowymi”.

2. Raport cząstkowy opracowany przez kierownika urzędu centralnego może być włączany do raportu cząstkowego ministra, któremu kierownik podlega lub przez którego jest nadzorowany.

§ 3. 1. Wykonawca sporządza raport cząstkowy i przedkłada go dyrektorowi Rządowego Centrum Bezpieczeństwa, zwanego dalej „dyrektorem Centrum”.

2. W przypadku zagrożeń, o których mowa w art. 5a ust. 2 pkt 1 lit. d ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym zwaną dalej „ustawą”, wykonawca przedkłada raport cząstkowy Szefowi Agencji Bezpieczeństwa Wewnętrznego, zwanemu dalej „Szefem ABW”.

3. W przypadku zagrożeń, o których mowa w art. 5a ust. 2 pkt 1 lit. e ustawy, wykonawca przedkłada raport cząstkowy Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa, zwanemu dalej „Pełnomocnikiem”.

§ 4. 1. Dyrektor Centrum, w terminie 30 dni od dnia otrzymania raportu cząstkowego może zgłosić uwagi dotyczące zakresu, i formy raportu cząstkowego lub jego części, w tym

wskazać na konieczność uzupełnienia raportu cząstkowego o elementy wynikające z raportów cząstkowych sporządzonych przez innych wykonawców.

2. Wykonawca rozpatruje uwagi, o których mowa w ust. 1, oraz w razie konieczności dokonuje zmian w raporcie cząstkowym w terminie 14 dni, a następnie przekazuje go ponownie dyrektorowi Centrum.

3. Wykonawca powiadamia pisemnie dyrektora Centrum o przyczynach nieuwzględnienia uwag.

4. Przepisy ust. 1–3 stosuje się odpowiednio do:

1) Szefa ABW w zakresie, o którym mowa w § 3 ust. 2;

2) Pełnomocnika w zakresie, o którym mowa w § 3 ust. 3.

§ 5. Wykonawca dokonuje systematycznej aktualizacji raportów cząstkowych oraz nie rzadziej niż raz na trzy lata przedkłada raport cząstkowy, zgodnie w właściwością dyrektorowi Centrum, Szefowi ABW oraz Pełnomocnikowi. Przepisy § 3–4 stosuje się odpowiednio.

§ 6. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[1)]

PREZES RADY MINISTRÓW

1) Niniejsze rozporządzenie było poprzedzone rozporządzeniem Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. poz. 540), które na podstawie art. 19 ustawy z dnia … o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (Dz. U. poz. …) utraciło moc z dniem wejścia w życie niniejszego rozporządzenia.

UZASADNIENIE

Wstęp

Projektowane rozporządzenie stanowi wykonanie upoważnienia zawartego w 5a ust. 9 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej „ustawa z.k.”).

Celem projektowanych przepisów jest określenie sposobu i trybu opracowania Raportu o zagrożeniach bezpieczeństwa narodowego (dalej „Raport”).

Projekt wskazuje, iż w celu sporządzenia Raportu ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie, zwani dalej „wykonawcami”, w zakresie swojej właściwości, opracowują raporty cząstkowe o zagrożeniach bezpieczeństwa narodowego, zwane dalej „raportami cząstkowymi”.

Raport cząstkowy opracowany przez kierownika urzędu centralnego może być włączany do raportu cząstkowego ministra, któremu kierownik podlega lub przez którego jest nadzorowany.

Po opracowaniu raportów cząstkowych – jego wykonawca przedkładają je dyrektorowi Rządowego Centrum Bezpieczeństwa (dalej „Centrum”).

W przypadku zagrożeń, o których mowa w art. 5a ust. 2 pkt 1 lit. d ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym zwaną dalej „ustawą”, – tj. zagrożeń o charakterze terrorystycznym mogących doprowadzić do sytuacji kryzysowej – wykonawca przedkłada raport cząstkowy Szefowi Agencji Bezpieczeństwa Wewnętrznego, zwanemu dalej „Szefem ABW”.

Natomiast w odniesieniu do zagrożeń, o których mowa w art. 5a ust. 2 pkt 1 lit. e ustawy, – tj. zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej – wykonawca przedkłada raport cząstkowy Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa (dalej „Pełnomocnik”).

Dyrektor Centrum, w terminie 30 dni od dnia otrzymania raportu cząstkowego może zgłosić uwagi dotyczące zakresu, i formy raportu cząstkowego lub jego części, w tym wskazać na konieczność uzupełnienia raportu cząstkowego o elementy wynikające z raportów cząstkowych sporządzonych przez innych wykonawców.

Wykonawca ma obowiązek odniesienia się do uwaga dyrektora Centrum – rozpatruje więc uwagi oraz w razie konieczności dokonuje zmian w raporcie cząstkowym w terminie 14

dni, a następnie przekazuje raport cząstkowy dyrektorowi Centrum. W przypadku nieuwzględnienia uwag – wykonawca powiadamia pisemnie dyrektora Centrum o tym fakcie.

Analogiczny tryb postępowania z raportami cząstkowymi projekt przewiduje w przypadku ich przekazania Szefowi ABW oraz Pełnomocnikowi.

Na podstawie otrzymanych raportów cząstkowych oraz z uwzględnieniem treści sporządzonych przez Szefa ABW oraz Pełnomocnika – sporządzany jest Raport, który dyrektor Centrum przedkłada Radzie Ministrów.

Projekt wskazuje, iż wykonawca dokonuje systematycznej aktualizacji raportów cząstkowych oraz nie rzadziej niż raz na trzy lata przedkłada raport cząstkowy, zgodnie w właściwością dyrektorowi Centrum, Szefowi ABW oraz Pełnomocnikowi.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest objęty prawem Unii Europejskiej oraz nie zawiera norm technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i w związku z powyższym nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego **Ministerstwo wiodące i ministerstwa współpracujące** Rządowe Centrum Bezpieczeństwa **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan nadbryg. Marek Kubiak, dyrektor Rządowego Centrum Bezpieczeństwa **Kontakt do opiekuna merytorycznego projektu** Pani Beata Janowczyk, Szef Wydziału Oceny Ryzyka i Planowania Cywilnego tel. 22 361-69-30, tel. kom. 785-700-195 e-mail: beata.janowczyk@rcb.gov.pl	**Data sporządzenia** **22.07.2019** **Źródło:** Upoważnienie ustawowe Art. 5a ust. 9 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym **Nr w wykazie prac** …

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Celem projektowanych przepisów jest określenie sposobu i trybu opracowania Raportu o zagrożeniach bezpieczeństwa narodowego (dalej „Raport").

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projektowane przepisy rozporządzenia Rady Ministrów mają zapewnić w efektywny sposób weryfikację treści raportów cząstkowych o zagrożeniach bezpieczeństwa narodowego, opracowywanych przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów.

Ww. raporty cząstkowe przedkładane są dyrektorowi RCB, Szefowi ABW (w zakresie zagrożeń terrorystycznych) oraz Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa (w zakresie zagrożeń w cyberprzestrzeni mogących doprowadzić do sytuacji kryzysowej).

Na podstawie otrzymanych raportów cząstkowych oraz z uwzględnieniem treści sporządzonych przez Szefa ABW oraz Pełnomocnika – sporządzany jest Raport, który dyrektor Centrum przedkłada Radzie Ministrów.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak danych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Ministrowie kierujący działami administracji rządowej			Opracowanie i przedłożenie raportu cząstkowego o zagrożeniach bezpieczeństwa narodowego
Kierownicy urzędów centralnych			Opracowanie i przedłożenie raportu cząstkowego o zagrożeniach bezpieczeństwa narodowego
Wojewodowie			Opracowanie i przedłożenie raportu cząstkowego o zagrożeniach bezpieczeństwa narodowego
Pełnomocnik Rządu ds. Cyberbezpieczeństwa			Analiza raportów cząstkowych. Opracowanie Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń terrorystycznych.

Szef Agencji Bezpieczeństwa Wewnętrznego			Analiza raportów cząstkowych. Opracowanie Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej.
Dyrektor Rządowego Centrum Bezpieczeństwa			Analiza raportów cząstkowych. Opracowanie Raportu o zagrożeniach bezpieczeństwa narodowego oraz jego przedłożenie Radzie Ministrów.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie będzie mieć wpływu na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	----------

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł,	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							

ceny stałe z …… r.)	rodzina, obywatele oraz gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐tak ☐nie ☒nie dotyczy
☐zmniejszenie liczby dokumentów ☐zmniejszenie liczby procedur ☐skrócenie czasu na załatwienie sprawy ☐inne: …	☐zwiększenie liczby dokumentów ☒zwiększenie liczby procedur ☐wydłużenie czasu na załatwienie sprawy ☐inne: …
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐tak ☐nie ☒nie dotyczy

9. Wpływ na rynek pracy

Projekt rozporządzenia nie będzie miał wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐środowisko naturalne ☐sytuacja i rozwój regionalny ☐inne: …	☐demografia ☐mienie państwowe	☐informatyzacja ☐zdrowie

Omówienie wpływu	Projekt rozporządzenia nie będzie miał wpływu na ww. obszary.

11. Planowane wykonanie przepisów aktu prawnego

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
----
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Projekt

R O Z P O R Z Ą D Z E N I E R A D Y M I N I S T R Ó W

z dnia

w sprawie planów ochrony infrastruktury krytycznej

Na podstawie art. 5m ust. 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz …) zarządza się, co następuje:

§ 1. Rozporządzenie określa sposób i tryb opracowywania oraz aktualizacji planów ochrony infrastruktury krytycznej opracowywanych przez operatorów infrastruktury krytycznej.

§ 2. 1. Operator infrastruktury krytycznej opracowuje plan ochrony infrastruktury krytycznej, zwany dalej „planem”, w terminie 9 miesięcy od daty otrzymania od dyrektora Rządowego Centrum Bezpieczeństwa, zwanego dalej „dyrektorem Centrum”, informacji o ujęciu w wykazie, o których mowa w art. 5c pkt 4 i art. 5f pkt 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą”.

2. Operator infrastruktury krytycznej opracowuje plan w postaci papierowej i elektronicznej.

§ 3. 1. Operator infrastruktury krytycznej przekazuje plan do uzgodnienia:

1) ministrowi lub kierownikowi urzędu centralnego, w którego właściwości znajduje się system, w którym została ujęta dana infrastruktura krytyczna;
2) właściwemu terytorialnie wojewodzie.

2. Podmioty, o których mowa w ust. 1, uzgadniają plan w terminie 45 dni od dnia jego otrzymania.

§ 4. 1. Operator infrastruktury krytycznej przekazuje plan do uzgodnienia, w zależności od charakterystyki infrastruktury krytycznej, właściwemu terytorialnie:

1) komendantowi wojewódzkiemu Państwowej Straży Pożarnej;
2) komendantowi wojewódzkiemu (Stołecznemu) Policji;
3) dyrektorowi regionalnego zarządu gospodarki wodnej;
4) wojewódzkiemu inspektorowi nadzoru budowlanego;
5) wojewódzkiemu lekarzowi weterynarii;
6) państwowemu wojewódzkiemu inspektorowi sanitarnemu;

7) dyrektorowi urzędu morskiego.

2. Podmiot, o którym mowa w ust. 1, uzgadnia plan w terminie 30 dni od dnia jego otrzymania.

§ 5. 1. Podmiot, o którym mowa w § 3 ust. 1 i § 4 ust. 1, może odmówić uzgodnienia planu w całości lub części w przypadku:

1) niespełnienia wymogów, o których mowa art. 5ł ustawy;
2) przedstawienia rozwiązań, które nie gwarantują bezpieczeństwa infrastruktury krytycznej;
3) braku spójności z Narodowym Programem Ochrony Infrastruktury Krytycznej, o którym mowa w art. 5b ust. 1 ustawy.

2. Odmowa uzgodnienia planu wymaga pisemnego uzasadnienia oraz wskazania elementów wymagających poprawy lub uzupełnienia.

§ 6. 1. Operator infrastruktury krytycznej przekazuje poprawiony plan lub wskazuje przyczyny nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu w terminie 14 dni od otrzymania odmowy uzgodnienia planu.

2. Podmiot, o którym mowa w § 3 ust. 1 i § 4 ust. 1 ust. 1, uzgadnia plan w terminie 14 dni od dnia otrzymania poprawionego planu lub wyjaśnień nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu. Przepis § 5 stosuje się odpowiednio.

3. W przypadku ponownej odmowy uzgodnienia planu w całości lub części, operator infrastruktury krytycznej sporządza protokół rozbieżności zawierający w szczególności: wskazanie podmiotu, który zgłosił uwagę, przytoczenie treści zgłoszonej uwagi oraz stanowisko operatora infrastruktury krytycznej, w tym przedstawienie powodów nieuwzględnienia uwagi.

§ 7. 1. Operator infrastruktury krytycznej przedkłada plan do zatwierdzenia dyrektorowi Centrum w terminie 14 dni od daty dokonania ostatniego uzgodnienia.

2. W przypadku odmowy uzgodnienia planu w całości lub części operator infrastruktury krytycznej dołącza do planu protokół rozbieżności, o którym mowa w § 6 ust. 3.

§ 8. 1. Dyrektor Centrum zatwierdza plan w terminie 90 dni od daty przedłożenia. Przepisy § 5 i § 6 ust. 1 i 2 stosuje się odpowiednio.

2. W przypadku gdy do planu dołączono protokół rozbieżności, o którym mowa w § 6 ust. 3, dyrektor Centrum zatwierdza plan po ich rozpatrzeniu.

§ 9. 1. Aktualizacja planów odbywa się w zależności od potrzeb, nie rzadziej jednak niż raz na dwa lata.

2. Wprowadzone zmiany wymagają uzgodnienia i zatwierdzenia, w trybie określonym w § 3–7.

§ 10. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

UZASADNIENIE

Wstęp

Projektowane rozporządzenie stanowi wykonanie upoważnienia zawartego w 5m ust. 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej „ustawa z.k.”).

Projektowane rozporządzenie określa sposób i tryb opracowywania oraz aktualizacji ochrony infrastruktury krytycznej opracowywanych przez operatorów infrastruktury krytycznej.

Projekt przewiduje, iż operator infrastruktury krytycznej opracowuje plan ochrony infrastruktury krytycznej (dalej „plan”), w terminie 9 miesięcy od daty otrzymania od dyrektora Rządowego Centrum Bezpieczeństwa, zwanego dalej „dyrektorem Centrum”, informacji o ujęciu w odpowiednim wykazie infrastruktury krytycznej (o której mowa w art. 5c pkt 4 i art. 5f pkt 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą”).

Operator infrastruktury krytycznej opracowuje plan w postaci papierowej i elektronicznej.

Po opracowaniu planu – operator infrastruktury krytycznej przekazuje plan do uzgodnienia:

1) ministrowi lub kierownikowi urzędu centralnego, we właściwości którego znajduje się system, w którym została ujęta dana infrastruktura krytyczna;

2) właściwemu terytorialnie wojewodzie.

Ww. podmioty uzgadniają plan w terminie 45 dni od dnia jego otrzymania.

Dodatkowo operator infrastruktury krytycznej przekazuje plan do uzgodnienia, w zależności od charakterystyki infrastruktury krytycznej, właściwemu terytorialnie:

1) komendantowi wojewódzkiemu Państwowej Straży Pożarnej;

2) komendantowi wojewódzkiemu (Stołecznemu) Policji;

3) dyrektorowi regionalnemu zarządu gospodarki wodnej;

4) wojewódzkiemu inspektorowi nadzoru budowlanego;

5) wojewódzkiemu lekarzowi weterynarii;

6) państwowemu wojewódzkiemu inspektorowi sanitarnemu;

7) dyrektorowi urzędu morskiego.

2. Ww. podmioty uzgadniają plan w terminie 30 dni od dnia jego otrzymania.

Projekt przewiduje, iż ww. podmioty mogą odmówić uzgodnienia planu w całości lub części w przypadku gdy:

1) plan nie spełnia wymogów ustawowych – brak jest jego istotnych elementów;

2) przedstawia rozwiązania, które nie gwarantują bezpieczeństwa infrastruktury krytycznej;

3) brak jest spójności treści planu z Narodowym Programem Ochrony Infrastruktury Krytycznej.

Odmowa uzgodnienia planu wymaga pisemnego uzasadnienia oraz wskazania elementów wymagających poprawy lub uzupełnienia.

Operator infrastruktury krytycznej przekazuje poprawiony plan lub wskazuje przyczyny nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu w terminie 14 dni od otrzymania odmowy uzgodnienia planu.

Ponowne uzgadnianie planu przez właściwe podmioty następuje w terminie 14 dni od dnia otrzymania poprawionego planu lub wyjaśnień nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu.

W przypadku ponownej odmowy uzgodnienia planu w całości lub części, o której mowa w operator infrastruktury krytycznej sporządza protokół rozbieżności zawierający w szczególności: wskazanie podmiotu, który zgłosił uwagę, przytoczenie treści zgłoszonej uwagi oraz stanowisko operatora infrastruktury krytycznej, w tym przedstawienie powodów nieuwzględnienia uwagi.

Operator infrastruktury krytycznej przedkłada plan do zatwierdzenia dyrektorowi Centrum w terminie 14 dni od daty dokonania ostatniego uzgodnienia. W przypadku odmowy uzgodnienia planu w całości lub części operator infrastruktury krytycznej dołącza do planu protokół rozbieżności.

Dyrektor Centrum zatwierdza plan w terminie 90 dni od daty przedłożenia. W przypadku odmowy zatwierdzenia planu do dalszego postępowania z takim planem stosuje się odpowiednio przepisy dotyczące uzgadniania planów. W przypadku gdy do planu dołączono protokół rozbieżności, o którym mowa w § 6 ust. 3, dyrektor Centrum zatwierdza plan po ich rozpatrzeniu.

Aktualizacja planów odbywa się w zależności od potrzeb, nie rzadziej jednak niż raz na dwa lata. Wprowadzone zmiany wymagają uzgodnienia i zatwierdzenia, w trybie przewidzianym dla uzgodnienia i zatwierdzenia planu pierwotnego.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest objęty prawem Unii Europejskiej oraz nie zawiera norm technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i w związku z powyższym nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie planów ochrony infrastruktury krytycznej **Ministerstwo wiodące i ministerstwa współpracujące** Rządowe Centrum Bezpieczeństwa **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan nadbryg. Marek Kubiak, dyrektor Rządowego Centrum Bezpieczeństwa **Kontakt do opiekuna merytorycznego projektu** Pan Witold Skomra, Doradca w Rządowym Centrum Bezpieczeństwa tel. 22 361-68-17, tel. kom. 785-700-176 e-mail: witold.skomra@rcb.gov.pl	**Data sporządzenia** **22.07.2019** **Źródło:** Upoważnienie ustawowe Art. 5m ust. 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym **Nr w wykazie prac** …

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Celem projektowanych przepisów jest określenie sposobu i trybu opracowywania oraz aktualizacji ochrony infrastruktury krytycznej przez operatorów infrastruktury krytycznej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projekt przewiduje, iż operator infrastruktury krytycznej opracowuje plan ochrony infrastruktury krytycznej (dalej „plan"), w terminie 9 miesięcy od daty otrzymania od dyrektora Rządowego Centrum Bezpieczeństwa, zwanego dalej „dyrektorem Centrum", informacji o ujęciu w odpowiednim wykazie infrastruktury krytycznej (o której mowa w art. 5c pkt 4 i art. 5f pkt 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą").
Operator infrastruktury krytycznej opracowuje plan w postaci papierowej i elektronicznej.
Po opracowaniu planu - operator infrastruktury krytycznej przekazuje plan do uzgodnień ministrowi lub kierownikowi urzędu centralnego, we właściwości którego znajduje się system, w którym została ujęta dana infrastruktura krytyczna lub właściwemu terytorialnie wojewodzie.

Dodatkowo operator infrastruktury krytycznej przekazuje plan do uzgodnienia, w zależności od charakterystyki infrastruktury krytycznej, właściwemu terytorialnie: komendantem wojewódzkim Państwowej Straży Pożarnej, komendantem wojewódzkim Policji, dyrektorem regionalnego zarządu gospodarki wodnej, wojewódzkim inspektorem nadzoru budowlanego, wojewódzkim lekarzem weterynarii, państwowym wojewódzkim inspektorem sanitarnym, dyrektorem urzędu morskiego.

Projekt wskazuje terminy w jakich odbywa się proces uzgadniania planów ochrony infrastruktury krytycznej.

Projektowana regulacja wskazuje ponadto obowiązki dyrektora Centrum w zakresie zatwierdzania planów ochrony infrastruktury krytycznej oraz terminy w jakich ma to nastąpić.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak danych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operator infrastruktury krytycznej			Opracowanie i przedłożenie planu ochrony infrastruktury krytycznej.
Kierownik urzędu centralnego, we właściwości którego znajdują się system, w którym została ujęta dana			Uzgadnianie planu ochrony infrastruktury krytycznej

infrastruktura krytyczna			
Wojewoda			Uzgadnianie planu ochrony infrastruktury krytycznej
Minister, we właściwości którego znajduje się system, w którym została ujęta dana infrastruktura krytyczna			Uzgadnianie planu ochrony infrastruktury krytycznej
Komendant wojewódzki PSP			Uzgadnianie planu ochrony infrastruktury krytycznej
Komendantem wojewódzki Policji;			Uzgadnianie planu ochrony infrastruktury krytycznej
Dyrektor RZGW			Uzgadnianie planu ochrony infrastruktury krytycznej
Wojewódzki Inspektorat Nadzoru budowlanego			Uzgadnianie planu ochrony infrastruktury krytycznej
Wojewódzki lekarz weterynarii			Uzgadnianie planu ochrony infrastruktury krytycznej
Wojewódzki inspektorem sanitarny			Uzgadnianie planu ochrony infrastruktury krytycznej
Dyrektor urzędu morskiego.			Uzgadnianie planu ochrony infrastruktury krytycznej
Dyrektor Rządowego Centrum Bezpieczeństwa			Zatwierdzanie planu ochrony infrastruktury krytycznej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie będzie mieć wpływu na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego.

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	----------

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐tak ☐nie ☒nie dotyczy
☐zmniejszenie liczby dokumentów ☐zmniejszenie liczby procedur ☐skrócenie czasu na załatwienie sprawy ☐inne: …	☐zwiększenie liczby dokumentów ☒zwiększenie liczby procedur ☐wydłużenie czasu na załatwienie sprawy ☐inne: …
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐tak ☐nie ☒nie dotyczy

9. Wpływ na rynek pracy

Projekt rozporządzenia nie będzie miał wpływu na rynek pracy.
10. Wpływ na pozostałe obszary

☐środowisko naturalne ☐sytuacja i rozwój regionalny ☐inne: …	☐demografia ☐mienie państwowe	☐informatyzacja ☐zdrowie

Omówienie wpływu	Projekt rozporządzenia nie będzie miał wpływu na ww. obszary.

11. Planowane wykonanie przepisów aktu prawnego
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
----
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Projekt

R O Z P O R Z Ą D Z E N I E R A D Y M I N I S T R Ó W

z dnia

w sprawie uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej

Na podstawie art. 5n ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz …) zarządza się, co następuje:

§ 1. Rozporządzenie określa tryb uznania spełnienia obowiązku posiadania planu ochrony odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

§ 2. 1. Operator infrastruktury krytycznej przekazuje plan, o którym mowa w art. 5n ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwany dalej „planem”, w terminie 9 miesięcy od daty otrzymania od dyrektora Rządowego Centrum Bezpieczeństwa, zwanego dalej „dyrektorem Centrum”, informacji o ujęciu w wykazie, o której mowa w art. 5c pkt 4 lub art. 5f pkt 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej „ustawą”.

2. Operator infrastruktury krytycznej przekazuje plan w postaci papierowej lub elektronicznej.

§ 3. Dyrektor Centrum dokonuje analizy planu pod kątem zgodności z elementami planu ochrony infrastruktury krytycznej, o których mowa w art. 5m ust. 1 ustawy, w terminie 90 dni od dnia otrzymania.

§ 4. 1. Dyrektor Centrum może odmówić uzgodnienia planu w całości lub części w przypadku niespełnienia wymogów, o których mowa art. 5m ust. 1 ustawy.

2. Odmowa uzgodnienia planu wymaga pisemnego uzasadnienia oraz wskazania elementów wymagających poprawy lub uzupełnienia.

§ 5. Operator infrastruktury krytycznej przekazuje poprawiony plan lub przedkłada wyjaśnienia w przypadku nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu w terminie 90 dni od otrzymania odmowy uzgodnienia planu.

§ 6. Dyrektor Centrum dokonuje ponownej analizy planu, z uwzględnieniem wyjaśnień operatora infrastruktury krytycznej, o których mowa w § 5, w terminie 90 dni od dnia

otrzymania poprawionego planu lub wyjaśnień nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu.

§ 7. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

UZASADNIENIE

Wstęp

Projektowane rozporządzenie stanowi wykonanie upoważnienia zawartego w art. 5n ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz …) (dalej „ustawa z.k.”).

Projektowane rozporządzenie określa tryb uznania spełnienia obowiązku posiadania planu ochrony odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

Zgodnie bowiem z art. 5n. ustawy z.k. – w przypadku gdy dla obiektów, instalacji i usług infrastruktury krytycznej istnieją, tworzone na podstawie odrębnych przepisów, plany odpowiadające wymogom planu ochrony infrastruktury krytycznej, operator infrastruktury krytycznej, który posiada plan opracowany na podstawie odrębnych przepisów i odpowiadający wymogom planu ochrony infrastruktury krytycznej, przedkłada ten plan dyrektorowi Rządowego Centrum Bezpieczeństwa (dalej „Centrum”) w celu uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

Plan odpowiadający wymogom planu ochrony infrastruktury krytycznej powinien zawiera elementy charakterystyczne dla planu ochrony infrastruktury krytycznej, o których mowa w art. 5m ust. 1 ustawy z.k.

Projekt przewiduje, iż operator infrastruktury krytycznej przekazuje ww. plan dyrektorowi Centrum w terminie 9 miesięcy od daty otrzymania od dyrektora Centrum informacji o ujęciu w wykazie infrastruktury krytycznej. Operator infrastruktury krytycznej przekazuje plan w postaci papierowej lub elektronicznej.

Następnie dyrektor Centrum dokonuje analizy otrzymanego planu pod kątem zgodności z elementami planu ochrony infrastruktury krytycznej, o których mowa w art. 5m ust. 1 ustawy z.k., w terminie 90 dni od dnia otrzymania.

Dyrektor Centrum może odmówić uzgodnienia planu w całości lub części w przypadku niespełnienia wymogów, o których mowa art. 5m ust. 1 ustawy z.k. Jednakże odmowa uzgodnienia planu wymaga pisemnego uzasadnienia oraz wskazania elementów wymagających poprawy lub uzupełnienia.

Operator infrastruktury krytycznej przekazuje poprawiony plan lub przedkłada wyjaśnienia w przypadku nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu w terminie 90 dni od otrzymania odmowy uzgodnienia planu.

Dyrektor Centrum dokonuje ponownej analizy planu, z uwzględnieniem wyjaśnień operatora infrastruktury krytycznej w terminie 90 dni od dnia otrzymania poprawionego planu lub wyjaśnień nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest objęty prawem Unii Europejskiej oraz nie zawiera norm technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i w związku z powyższym nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej Ministerstwo wiodące i ministerstwa współpracujące Rządowe Centrum Bezpieczeństwa Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Pan nadbryg. Marek Kubiak, dyrektor Rządowego Centrum Bezpieczeństwa Kontakt do opiekuna merytorycznego projektu Pan Witold Skomra, Doradca w Rządowym Centrum Bezpieczeństwa tel. 22 361-68-17, tel. kom. 785-700-176 e-mail: witold.skomra@rcb.gov.pl	**Data sporządzenia** **03.10.2019** **Źródło:** Upoważnienie ustawowe Art. 5n ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym **Nr w wykazie prac** …

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowane rozporządzenie określa tryb uznania spełnienia obowiązku posiadania planu ochrony odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projektowane rozporządzenie określa tryb uznania spełnienia obowiązku posiadania planu ochrony odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

Projekt przewiduje, iż operator infrastruktury krytycznej przekazuje ww. plan dyrektorowi Centrum w terminie 9 miesięcy od daty otrzymania od dyrektora Centrum informacji o ujęciu w wykazie infrastruktury krytycznej. Operator infrastruktury krytycznej przekazuje plan w postaci papierowej lub elektronicznej.

Następnie dyrektor Centrum dokonuje analizy otrzymanego planu pod kątem zgodności z elementami planu ochrony infrastruktury krytycznej, o których mowa w art. 5m ust. 1 ustawy z.k., w terminie 90 dni od dnia otrzymania.

Dyrektor Centrum może odmówić uzgodnienia planu w całości lub części w przypadku niespełnienia wymogów, o których mowa art. 5m ust. 1 ustawy z.k. Jednakże odmowa uzgodnienia planu wymaga pisemnego uzasadnienia oraz wskazania elementów wymagających poprawy lub uzupełnienia.

Operator infrastruktury krytycznej przekazuje poprawiony plan lub przedkłada wyjaśnienia w przypadku nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu w terminie 90 dni od otrzymania odmowy uzgodnienia planu.

Dyrektor Centrum dokonuje ponownej analizy planu, z uwzględnieniem wyjaśnień operatora infrastruktury krytycznej w terminie 90 dni od dnia otrzymania poprawionego planu lub wyjaśnień nieuwzględnienia uwag będących podstawą odmowy uzgodnienia planu.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak danych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operator infrastruktury krytycznej			Przedłożenie planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej.
Dyrektor Rządowego Centrum Bezpieczeństwa			Uznanie spełnienia obowiązku posiadania planu ochrony odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Rozporządzenie nie będzie mieć wpływu na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	----------

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz							

	gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: …	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: …
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy

9. Wpływ na rynek pracy

Projekt rozporządzenia nie będzie miał wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne: …	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Projekt rozporządzenia nie będzie miał wpływu na ww. obszary.

11. Planowane wykonanie przepisów aktu prawnego

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

---

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
