Warszawa, dnia 26 lutego 2020 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja
Komisja Administracji i Spraw Wewnętrznych
***
Podkomisja nadzwyczajna
do rozpatrzenia rządowego projektu
ustawy o zmianie ustawy o zarządzaniu
kryzysowym oraz niektórych innych
ustaw (druk nr 203)

S P R A W O Z D A N I E P O D K O M I S J I

Podkomisja nadzwyczajna po rozpatrzeniu rządowego projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (druk nr 203) na posiedzeniach w dniach: 12 i 26 lutego 2020 r przedkłada sprawozdanie o tym projekcie ustawy.

Sprawozdawca

/-/Edward Siarka

IX kadencja/druk nr 203

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, urządzenia, instalacji lub operatora 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:

---

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.

„c) planowanie w zakresie wspierania Sił Zbrojnych Rzeczypospolitej Polskiej oraz wojsk sojuszniczych w przypadku realizacji na terytorium Rzeczypospolitej Polskiej zobowiązań sojuszniczych w ramach Organizacji Traktatu Północnoatlantyckiego z zakresu zarządzania kryzysowego;”,

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

„9a) ryzyku – należy przez to rozumieć kombinację prawdopodobieństwa wystąpienia zagrożenia ze skutkami wystąpienia zagrożenia;

9b) ryzyku dla infrastruktury krytycznej – należy przez to rozumieć kombinację prawdopodobieństwa wystąpienia zagrożenia lub podatności na wystąpienie zagrożenia ze skutkami 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 wartości 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 z ich skutkami, 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 podmioty wskazane w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony innych 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 zagrożenia hybrydowego, przeciwdziałanie mu i reagowanie na nie.”;

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;

7) organizacyjne i techniczne możliwości wspierania Sił Zbrojnych Rzeczypospolitej Polskiej oraz wojsk sojuszniczych w razie 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 oraz określenia celów strategicznych służących ograniczeniu ryzyka opracowuje się Raport o zagrożeniach bezpieczeństwa narodowego, zwany dalej „Raportem”.

2. Raport zawiera:

1) identyfikację i charakterystykę oraz skutki wystąpienia zagrożeń:

a) o istotnym wpływie na funkcjonowanie państwa i możliwości jego rozwoju, w szczególności mogących mieć istotne znaczenie dla bezpieczeństwa narodowego, w tym międzynarodowej pozycji oraz potencjałów ekonomicznego i obronnego,

b) których skutki mogą:

- godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, w szczególności w suwerenność, niepodległość i nienaruszalność jego terytorium,
- zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach,
- oddziaływać, obok oddziaływania na Rzeczpospolitą Polską, także na inne państwa,
- dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie,

c) występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów międzynarodowych,

d) o charakterze terrorystycznym mogących doprowadzić do sytuacji kryzysowej,

e) cyberbezpieczeństwa mogących 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, przyjętego 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),

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. Raporty cząstkowe zawierają elementy, o których mowa w ust. 2, z wyjątkiem charakterystyk zagrożeń.

5. Opracowanie raportów cząstkowych koordynuje dyrektor Rządowego Centrum Bezpieczeństwa, zwanego dalej „Centrum”, z wyłączeniem części dotyczącej zagrożeń:

1) o charakterze terrorystycznym mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Szef Agencji Bezpieczeństwa Wewnętrznego, oraz
2) cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

6. Na podstawie otrzymanych raportów cząstkowych dyrektor Centrum opracowuje projekt Raportu, z wyłączeniem części, o których mowa w ust. 5, które opracowują, odpowiednio, Szef Agencji Bezpieczeństwa Wewnętrznego i Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

7. Dyrektor Centrum przedkłada projekt Raportu Radzie Ministrów co trzy lata.

8. Rada Ministrów przyjmuje Raport w drodze uchwały.

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

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 dyrektor Centrum opracowuje streszczenie istotnych elementów krajowej oceny ryzyka w rozumieniu decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 347 z 20.12.2013, str. 924, L 250 z 04.10.2018, str. 1 oraz L 77A z 20.03.2019, str. 1).

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

Art. 5ab. 1. Plany zarządzania ryzykiem zawierają:

1) charakterystykę zagrożeń, w tym zagrożeń dotyczących infrastruktury krytycznej uwzględnionej w wykazach, o których mowa w art. 5c pkt 1 lub 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) dyrektor Centrum – 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 staroście.

4. Powiatowy plan zarządzania ryzykiem starosta przekazuje właściwemu wojewodzie.

Art. 5ac. 1. Dyrektor Centrum, opracowując projekt Krajowego Planu Zarządzania Ryzykiem, uwzględnia plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów.

2. Minister właściwy do spraw rozwoju regionalnego opiniuje projekt Krajowego Planu Zarządzania Ryzykiem pod względem spójności z programami strukturalnymi.

3. Dyrektor Centrum przedkłada Radzie Ministrów projekt Krajowego Planu Zarządzania Ryzykiem.

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

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

1) dyrektor Centrum – 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 staroście.

3. Powiatowy plan reagowania kryzysowego starosta przekazuje właściwemu 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) zasady 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 modułów zadaniowych pogrupowanych w katalogi;
5) załączniki 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 Centrum przedkłada Radzie Ministrów projekt Krajowego Planu 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 Centrum i stanowią załączniki funkcjonalne do Krajowego Planu Reagowania Kryzysowego.

Art. 5af. Plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych zawierają:

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) 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 i 5 oraz art. 5af pkt 2 i 3;
2) 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.[2)]), wraz z ich opisem;
3) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem.

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

1) elementy, o których mowa w art. 5ae ust. 1 pkt 1–3 i 5 oraz art. 5af pkt 2 i 3;
2) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem.

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

[2)] 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.

2. Cykl planowania realizują właściwe organy administracji publicznej oraz uczestnicy 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 dyrektor Centrum opracowuje streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem w rozumieniu decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Tekst mający znaczenie dla EOG).

2. Dyrektor Centrum 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, urządzenia, instalacje i usługi wchodzące w skład systemów, o których mowa w art. 3 pkt 2, z uwzględnieniem ich znaczenia dla funkcjonowania państwa i zaspokojenia potrzeb obywateli;
4) szczegółowe kryteria pozwalające wyodrębnić obiekty, urządzenia, instalacje i usługi wchodzące w skład systemów, o których mowa w art. 3 pkt 2, na obszarze województwa, z uwzględnieniem ich

znaczenia dla funkcjonowania organów administracji publicznej oraz zaspokojenia potrzeb obywateli na obszarze województwa;

5) wskazanie 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. Projekt programu opracowuje dyrektor Centrum we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych oraz wojewodami.”,

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

„3a. Na potrzeby opracowania projektu programu dyrektor Centrum przekazuje, na rok przed dniem przystąpienia do jego opracowania, organom, o których mowa w ust. 3, zakres informacji niezbędnych do przygotowania programu 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 dyrektorowi Centrum, nie później niż na sześć 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 niedostępności usług, o których mowa w pkt 2;

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

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

3d. Dyrektor Centrum, mając na względzie zapewnienie spójności i kompletności programu, może wystąpić o przekazanie także innych propozycji niż określone w ust. 3b, jeżeli uzna, że ich umieszczenie w programie jest niezbędne.

3e. Dyrektor Centrum przedkłada projekt programu Radzie Ministrów.”,

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 Centrum:

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, o których mowa w art. 3 pkt 2, krajowy wykaz obiektów, urządzeń, instalacji lub usług wchodzących w skład infrastruktury krytycznej, z uwzględnieniem podziału na poszczególne systemy, zwany dalej „wykazem krajowym”; wykaz krajowy ma charakter niejawny;

2) opracowuje wyciągi z wykazu krajowego dotyczące obiektów, urządzeń, instalacji lub usług znajdujących się w systemie, o którym mowa w art. 3 pkt 2, oraz przekazuje je ministrom kierującym działami administracji rządowej lub kierownikom urzędów centralnych odpowiedzialnym za dany system;

3) opracowuje wyciągi z wykazu krajowego dotyczące obiektów, urządzeń, instalacji lub usług znajdujących się na obszarze danego województwa oraz przekazuje właściwemu wojewodzie;

4) informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, urządzeń, instalacji lub operatorów usług o ich ujęciu w wykazie krajowym;

5) zatwierdza plany ochrony infrastruktury krytycznej po ich uzgodnieniu z ministrem kierującym działem administracji rządowej lub kierownikiem urzędu centralnego odpowiedzialnymi za system, o którym mowa w art. 3 pkt 2.

Art. 5d. 1. Dyrektor Centrum sporządza i prowadzi wykaz zawierający europejską infrastrukturę krytyczną 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 Centrum sporządza we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych wykaz obiektów, urządzeń, instalacji lub usług wchodzących w skład infrastruktury krytycznej, z uwzględnieniem podziału na poszczególne systemy, o których mowa w art. 3 pkt 2, 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 kryteriów, o których mowa w art. 5b ust. 2 pkt 4, wojewódzki wykaz obiektów, urządzeń, instalacji i usług wchodzących w skład infrastruktury krytycznej, z uwzględnieniem podziału na systemy, o których mowa w art. 3 pkt 2, zwany dalej „wykazem wojewódzkim”; wykaz wojewódzki ma charakter niejawny;
2) opracowuje wyciągi z wykazu wojewódzkiego oraz przekazuje je ministrom kierującym działami administracji rządowej lub kierownikom urzędów centralnych odpowiedzialnym za system, o którym mowa w art. 3 pkt 2;
3) przekazuje wykaz wojewódzki dyrektorowi Centrum;
4) informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, urządzeń, instalacji lub usług o ich ujęciu w wykazie wojewódzkim;
5) zatwierdza plany ochrony infrastruktury krytycznej ujętej w wykazie wojewódzkim.

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

1) opracowywanie 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 art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560, z 2019 r. poz. 2020 i 2248) 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 tej ustawy.

3. Do zadań operatora infrastruktury krytycznej należy:

1) bieżące monitorowanie stopnia wdrożenia planów ochrony infrastruktury krytycznej;
2) sporządzanie i przekazywanie informacji w zakresie zapewnienia ochrony infrastruktury krytycznej na żądanie:
   a) dyrektora Centrum,
   b) właściwego ministra kierującego działem administracji rządowej 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 wojewody;
3) współpraca z organami administracji publicznej oraz dyrektorem Centrum 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, w terminie 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 jej ochrony 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 infrastruktury krytycznej;
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 infrastruktury krytycznej w przypadkach, o których mowa w pkt 2–4.

4. Operator infrastruktury krytycznej przekazuje, w terminie do dnia 31 marca każdego roku, raport o stanie ochrony infrastruktury krytycznej dyrektorowi Centrum oraz odpowiednio:

1) właściwemu ministrowi kierującemu działem administracji rządowej 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 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 infrastruktury krytycznej wyznacza koordynatora w terminie 30 dni od dnia otrzymania informacji, o której mowa w art. 5c pkt 4 i art. 5f pkt 4, oraz informacji o ujęciu infrastruktury krytycznej w wykazie europejskiej infrastruktury krytycznej.

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, 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 ujętej w wykazie, o którym mowa w art. 5c pkt 1, albo
   b) „zastrzeżone” – w przypadku zajmowania stanowiska koordynatora w strukturze organizacyjnej operatora infrastruktury krytycznej ujętej w wykazie, 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 Centrum oraz:

1) właściwego ministra kierującego działem administracji rządowej 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 wojewodę.

Art. 5j. Koordynator może przedkładać rekomendacje organowi zarządzającemu operatora infrastruktury krytycznej w zakresie ochrony jego obiektów, urządzeń, instalacji i usług ujętych w wykazach, o których mowa w art. 5c pkt 1, art. 5d ust. 1 lub 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 Centrum we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych na bieżąco rozpoznaje obiekty, w tym obiekty budowlane, urządzenia, instalacje i usługi, będące w fazie projektowania lub budowy, mogące potencjalnie spełniać kryteria, o których mowa w art. 5b ust. 2 pkt 3, zwane dalej „potencjalną infrastrukturą krytyczną".

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

3. Na podstawie ustaleń poczynionych z inwestorem lub operatorem infrastruktury krytycznej lub ministrami kierującymi działami administracji rządowej lub kierownikami urzędów centralnych dyrektor Centrum ujmuje obiekt, urządzenie, instalację lub usługę w wykazie potencjalnej infrastruktury krytycznej.

4. Dyrektor Centrum powiadamia inwestora lub operatora infrastruktury krytycznej o jej ujęciu w wykazie potencjalnej infrastruktury krytycznej.

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

Art. 5m. 1. Plan ochrony infrastruktury krytycznej zawiera:

1) dane ogólne:

   a) obejmujące nazwę i lokalizację infrastruktury krytycznej,

b) pozwalające zidentyfikować operatora infrastruktury krytycznej, w tym jego nazwę, adres i siedzibę oraz numery REGON, NIP i KRS,

c) pozwalające zidentyfikować zarządzającego przedsiębiorstwem w imieniu operatora infrastruktury krytycznej, w tym jego nazwę, adres i siedzibę, numery REGON, NIP i KRS;

2) dane o infrastrukturze krytycznej obejmujące:

a) charakterystykę procesów, stosowanych technologii i podstawowe parametry techniczne,

b) plan (mapę**)** z naniesioną lokalizacją obiektów**,** urządzeń, instalacji lub systemu, o którym mowa w art. 3 pkt 2, i zaznaczonymi elementami zapewniającymi bezpieczeństwo infrastruktury krytycznej,

c) opis funkcjonalnych połączeń z innymi obiektami, urządzeniami, instalacjami, 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 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:

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 tej infrastruktury 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 kierującym działem administracji rządowej lub kierownikiem urzędu centralnego odpowiedzialnym za system, o którym mowa w art. 3 pkt 2, w skład którego wchodzi infrastruktura krytyczna, albo
2) właściwym 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, tryb oraz terminy opracowywania oraz zatwierdzania planów ochrony infrastruktury krytycznej, mając na względzie potrzebę zapewnienia ciągłości funkcjonowania infrastruktury krytycznej.

Art. 5n. 1. W przypadku gdy dla obiektów, urządzeń, instalacji i usług infrastruktury krytycznej istnieją, tworzone na podstawie odrębnych przepisów, plany odpowiadające wymogom planu ochrony infrastruktury krytycznej, zawierające elementy, o których mowa w art. 5m ust. 1, operator infrastruktury krytycznej, który posiada plan opracowany na podstawie odrębnych przepisów i odpowiadający wymogom planu ochrony infrastruktury krytycznej, przedkłada ten plan dyrektorowi Centrum w celu uznania spełnienia tych wymogów.

2. 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) użyte w art. 6a w ust. 1, w art. 6b w ust. 1-4 i 6, w art. 6c w ust. 1 i w art. 13 w ust. 3 w różnym przypadku wyrazy „Rządowego Centrum Bezpieczeństwa” zastępuje się użytym w odpowiednim przypadku wyrazem „Centrum”;

10) w art. 8 w ust. 2 pkt 3 otrzymuje brzmienie:

„3) minister właściwy do spraw zagranicznych;”;

11) w art. 9 w ust. 1:

a) po pkt 2 dodaje się pkt 2a w brzmieniu:

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

b) pkt 5 otrzymuje brzmienie:

„5) opiniowanie projektów Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego;”;

12) w art. 10 w ust. 1 skreśla się wyrazy „zwane dalej „Centrum”,”;

13) 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 w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków;”,

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 11 wyraz „Zarządzania” zastępuje się wyrazem „Reagowania”,

h) 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, przyjętego 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), w okresie jego obowiązywania.”;

14) 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 zarządzania 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 przypadku wystąpienia sytuacji kryzysowej w zakresie organizacyjnym, technicznym i finansowym;

3) opiniowanie projektów planów zarządzania kryzysowego;

4) opiniowanie wykazu, o którym mowa w art. 5c pkt 1, w ramach swojej właściwości;

5) wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.”;

15) 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, 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) 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.”;

16) 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. 4 dodaje się ust. 4a w brzmieniu:

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

17) 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;

18) 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;

19) 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.”;

20) w art. 21a:

a) ust. 2 otrzymuje brzmienie:

„2. Operatorzy infrastruktury krytycznej niezwłocznie informują dyrektora Centrum oraz właściwe 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, o którym mowa w ust. 3, po wysłaniu komunikatu, niezwłocznie przekazuje dyrektorowi Centrum informację o liczbie kart SIM użytkowników końcowych, do których komunikat został wysłany i którym komunikat został dostarczony.”;

21) 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 oraz 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 (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …).”.

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 tej ustawy;";

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 tej ustawy, 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 tej ustawy, 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 aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych”;

2) w art. 1:

a) ust. 1 otrzymuje brzmienie:

„1. Ustawa określa szczególne uprawnienia przysługujące ministrowi właściwemu do spraw aktywów państwowych 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”.”,

b) w ust. 2:

– pkt 1 otrzymuje brzmienie:

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

– 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).”;

3) 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 aktywów państwowych 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.”;

4) 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.”;

5) 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, urządzeń, instalacji 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, 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 (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …);”.

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 zdarzenia 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 w celu zapobieżenia takiemu zdarzeniu 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, 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, 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, zostaną sporządzone po raz pierwszy 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.

2. Plany reagowania kryzysowego, o których mowa w art. 5ae ustawy zmienianej w art. 1, zostaną sporządzone po raz pierwszy 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 dotychczasowym 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, zostaną sporządzone po raz pierwszy 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, zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy.

3. Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, pozostaje w mocy do czasu sporządzenia wykazów, o których mowa w art. 5c pkt 1, art. 5d ust. 1 i art. 5f pkt 1 ustawy zmienianej w art. 1.

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 terminie 30 dni od dnia wejścia w życie niniejszej ustawy. Przepisu art. 5i ust. 2 nie stosuje się.

Art. 16. Raport, o którym mowa w art. 5h ust. 1 ustawy zmienianej w art. 1, 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 terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 18. Przepis art. 26 ust. 4a ustawy zmienianej w art. 1 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 dotychczasowym zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 5a ust. 9, art. 5m ust. 6 oraz art. 5n ust. 2 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.