Art. 23. 1. Zgłoszenie, o którym mowa w art. 22 ust. 1 pkt 2, zawiera:

1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
   a) wskazanie zadania publicznego, na które incydent miał wpływ,
   b) liczbę osób, na które incydent miał wpływ,
   c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
   d) zasięg geograficzny obszaru, którego dotyczy incydent,
   e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
5) informacje o przyczynie i źródle incydentu;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych działaniach naprawczych;
8) inne istotne informacje.

2. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu w podmiocie publicznym.

3. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 22 ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

4. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do podmiotu publicznego, o którym mowa w art. 4 pkt 7–15, o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

5. W zgłoszeniu podmiot publiczny, o którym mowa w art. 4 pkt 7–15, oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 24. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje, o których mowa w art. 13 ust. 1. Informacje te przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania ich w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Art. 25. Do podmiotu publicznego, o którym mowa w art. 4 pkt 7–15, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się przepisy rozdziału 3 w zakresie świadczenia usługi kluczowej, w związku z której świadczeniem został uznany za operatora usługi kluczowej.

Rozdział 6

Zadania CSIRT MON, CSIRT NASK i CSIRT GOV

Art. 26. 1. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów.

2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych, o których mowa w art. 4 pkt 7–15, sektorowych zespołów cyberbezpieczeństwa lub 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 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów.

3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością wskazaną w ust. 5–7, należy:

1) monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;

2) szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;

3) przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;

4) wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;

5) reagowanie na zgłoszone incydenty;

6) klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;

7) zmiana klasyfikacji incydentów poważnych i incydentów istotnych;

8) przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT;

9) przeprowadzanie w uzasadnionych przypadkach badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, zwanych dalej „rekomendacjami dotyczącymi stosowania urządzeń informatycznych lub oprogramowania”;

10) współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej, i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;

11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;

12) przekazywanie, w terminie do dnia 30 maja każdego roku, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;

13) wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącej cyberbezpieczeństwa;

14) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności:

   a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności,

   b) monitoruje wskaźniki zagrożeń cyberbezpieczeństwa,

   c) rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,

   d) prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa,

   e) wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,

   f) prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,

   g) współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa;

15) zapewnienie możliwości dokonywania zgłoszeń i przekazywania informacji, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1, oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń;

16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA).

4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu, którego koordynacja obsługi wymaga współpracy CSIRT, oraz określą we współpracy z sektorowymi zespołami cyberbezpieczeństwa sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu.

5. Do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez:

1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

2) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa w rozumieniu art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571) jest Minister Obrony Narodowej.

6. Do zadań CSIRT NASK należy:

1) koordynacja obsługi incydentów zgłaszanych przez:
   a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
   b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek, o których mowa w ust. 7 pkt 2,
   c) instytuty badawcze,
   d) Urząd Dozoru Technicznego,
   e) Polską Agencję Żeglugi Powietrznej,
   f) Polskie Centrum Akredytacji,
   g) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,
   h) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,
   i) dostawców usług cyfrowych, z wyjątkiem wymienionych w ust. 7 pkt 5,
   j) operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 5 i 7,
   k) inne podmioty niż wymienione w lit. a–j oraz ust. 5 i 7,
   l) osoby fizyczne;
2) tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach;
3) zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzących działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW (Dz. Urz. UE L 335 z 17.12.2011, str. 1).

7. Do zadań CSIRT GOV należy koordynacja obsługi incydentów zgłaszanych przez:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem wymienionych w ust. 5 i 6;
2) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane;
3) Narodowy Bank Polski;
4) Bank Gospodarstwa Krajowego;

5) inne niż wymienione w pkt 1–4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 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 jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

8. CSIRT MON, CSIRT NASK lub CSIRT GOV, który otrzymał zgłoszenie incydentu, a nie jest właściwy do koordynacji jego obsługi, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami.

9. Działalność CSIRT NASK jest finansowana w formie dotacji podmiotowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji.

10. CSIRT MON, CSIRT NASK i CSIRT GOV mogą, w drodze porozumienia, powierzyć sobie wzajemnie wykonywanie zadań w stosunku do niektórych rodzajów podmiotów, o których mowa w ust. 5–7. O zawarciu porozumienia CSIRT, który powierzył wykonywanie zadań, informuje podmioty, w stosunku do których nastąpiła zmiana CSIRT.

11. Komunikat o zawarciu porozumienia, o którym mowa w ust. 10, ogłasza się w dzienniku urzędowym odpowiednio Ministra Obrony Narodowej, Ministra Cyfryzacji lub Agencji Bezpieczeństwa Wewnętrznego. W komunikacie wskazuje się informacje o:

1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami;

2) terminie, od którego porozumienie będzie obowiązywało.

Art. 27. 1. CSIRT GOV jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452, 650 i 730).

2. CSIRT MON jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 5 ust. 1 pkt 2a ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2017 r. poz. 1978 i 2405 oraz z 2018 r. poz. 650 i 1544).

3. W przypadku stwierdzenia, że incydent, którego obsługa jest koordynowana przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV, jest związany ze zdarzeniami, o których mowa w ust. 1 albo 2, koordynację obsługi incydentu przejmuje właściwy CSIRT MON lub CSIRT GOV.

Art. 28. 1. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV informuje na podstawie zgłoszenia incydentu poważnego dokonanego przez operatora usługi kluczowej inne państwa członkowskie Unii Europejskiej, których dotyczy ten incydent, za pośrednictwem Pojedynczego Punktu Kontaktowego.

2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV przekazuje, jeżeli pozwalają na to okoliczności, operatorowi usługi kluczowej zgłaszającemu incydent poważny informacje dotyczące działań podjętych po zgłoszeniu tego incydentu, które mogłyby pomóc w jego obsłudze.

3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić z wnioskiem do Pojedynczego Punktu Kontaktowego o przekazanie zgłoszenia incydentu poważnego, o którym mowa w ust. 1, pojedynczym punktom kontaktowym w innych państwach członkowskich Unii Europejskiej, których dotyczy ten incydent.

Art. 29. CSIRT MON, CSIRT NASK lub CSIRT GOV informuje inne państwa członkowskie Unii Europejskiej w przypadku, gdy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej, za pośrednictwem Pojedynczego Punktu Kontaktowego.

Art. 30. 1. Podmioty inne niż operatorzy usług kluczowych i dostawcy usług cyfrowych, w tym osoby fizyczne, mogą zgłosić incydent do CSIRT NASK. W zgłoszeniu należy podać:

1) nazwę podmiotu lub systemu informacyjnego, w którym wystąpił incydent;

2) opis incydentu;

3) inne istotne informacje.

2. Zgłoszenia incydentów od operatorów usług kluczowych oraz dostawców usług cyfrowych są traktowane priorytetowo względem zgłoszeń, o których mowa w ust. 1.

3. Zgłoszenia, o których mowa w ust. 1, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK.

4. Podmiot, o którym mowa w ust. 1, oznacza w zgłoszeniu informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 31. 1. CSIRT MON, CSIRT NASK i CSIRT GOV określa sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1, a także określa sposób dokonywania zgłoszeń i przekazywania informacji przy użyciu innych środków komunikacji – w przypadku braku możliwości dokonania zgłoszenia albo przekazania ich w postaci elektronicznej.

2. Komunikat zawierający informacje, o których mowa w ust. 1, CSIRT MON, CSIRT NASK i CSIRT GOV publikuje na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego.

Art. 32. 1. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego, incydentu istotnego i incydentu krytycznego.

2. W trakcie koordynacji obsługi incydentu poważnego, incydentu istotnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, incydentu istotnego lub krytycznego.

3. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do operatora usługi kluczowej o udostępnienie informacji technicznych związanych z incydentem poważnym lub krytycznym, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu.

4. CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowe zespoły cyberbezpieczeństwa na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od operatora usługi kluczowej, dostawcy usługi cyfrowej lub podmiotu publicznego, o którym mowa w art. 4 pkt 7–15, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.

Art. 33. 1. CSIRT MON, CSIRT NASK lub CSIRT GOV może przeprowadzić badanie urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

2. CSIRT MON, CSIRT NASK albo CSIRT GOV, podejmując badanie urządzenia informatycznego lub oprogramowania, informuje pozostałe CSIRT o fakcie podjęcia badań oraz urządzeniu informatycznym lub oprogramowaniu, którego badanie dotyczy.

3. CSIRT MON, CSIRT NASK lub CSIRT GOV w przypadku identyfikacji podatności, o której mowa w ust. 1, składa wniosek w sprawie rekomendacji, o których mowa w ust. 4.

4. Pełnomocnik po uzyskaniu opinii Kolegium wydaje, zmienia lub odwołuje rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

5. Podmiot krajowego systemu cyberbezpieczeństwa może wnieść do Pełnomocnika zastrzeżenia do rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, nie później niż w terminie 7 dni od dnia otrzymania rekomendacji.

6. Pełnomocnik odnosi się do zastrzeżeń otrzymanych w trybie ust. 5 niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania, i podtrzymuje rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania albo wydaje zmienione rekomendacje.

7. Podmiot krajowego systemu cyberbezpieczeństwa informuje Pełnomocnika, na jego wniosek, o sposobie i zakresie uwzględnienia rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania.

8. Nieuwzględnienie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania stanowi podstawę do wystąpienia przez Pełnomocnika do organu sprawującego nadzór nad podmiotem, o którym mowa w ust. 7, z informacją o ich nieuwzględnieniu.

Art. 34. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.

2. CSIRT MON, CSIRT NASK i CSIRT GOV, koordynując obsługę incydentu, który doprowadził do naruszenia ochrony danych osobowych, współpracują z organem właściwym do spraw ochrony danych osobowych.

Art. 35. 1. CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym oraz informują o nim Rządowe Centrum Bezpieczeństwa.

2. Informacja, o której mowa w ust. 1, zawiera:

1) wstępną analizę potencjalnych skutków incydentu, z uwzględnieniem w szczególności:

   a) liczby użytkowników, których dotyczy incydent, w szczególności jeśli zakłóca świadczenie usługi kluczowej,

   b) momentu wystąpienia i wykrycia incydentu oraz czasu jego trwania,

   c) zasięgu geograficznego obszaru, którego dotyczy incydent;

2) rekomendację w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w art. 8 ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

3. Informacja, o której mowa w ust. 1, może zawierać wniosek o zwołanie Zespołu do spraw Incydentów Krytycznych, zwanego dalej „Zespołem".

4. W przypadku uzyskania informacji o zagrożeniach cyberbezpieczeństwa CSIRT MON, CSIRT NASK i CSIRT GOV mogą informować się wzajemnie oraz informować o tych zagrożeniach Rządowe Centrum Bezpieczeństwa. Przepisy ust. 2 i 3 stosuje się odpowiednio.

5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą publikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje, w niezbędnym zakresie, o podatnościach, incydentach krytycznych oraz o zagrożeniach cyberbezpieczeństwa, o ile przekazywanie informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów. Publikowane informacje nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych.

Art. 36. 1. Zespół jest organem pomocniczym w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynującym działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowe Centrum Bezpieczeństwa.

2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa.

3. Dyrektor Rządowego Centrum Bezpieczeństwa przewodniczy pracom Zespołu.

4. Obsługę prac Zespołu zapewnia Rządowe Centrum Bezpieczeństwa.

5. Do udziału w pracach Zespołu, z głosem doradczym, członkowie Zespołu mogą zapraszać przedstawicieli organów właściwych do spraw cyberbezpieczeństwa lub jednostek im podległych lub przez nie nadzorowanych, organów ścigania, wymiaru sprawiedliwości lub służb specjalnych.

6. W przypadku, o którym mowa w art. 35 ust. 3, albo na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 1, dyrektor Rządowego Centrum Bezpieczeństwa zawiadamia niezwłocznie członków Zespołu o terminie i miejscu posiedzenia Zespołu. Udział w posiedzeniu Zespołu może odbywać się za pośrednictwem środków komunikacji elektronicznej.

7. Zespół na posiedzeniu:

1) wyznacza jednomyślnie CSIRT koordynujący obsługę incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 1;

2) określa role pozostałych CSIRT oraz Rządowego Centrum Bezpieczeństwa w obsłudze incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 1;

3) określa sposób wymiany informacji technicznych dotyczących incydentu krytycznego obsługiwanego wspólnie przez CSIRT MON, CSIRT NASK lub Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV;

4) podejmuje decyzję o wystąpieniu przez dyrektora Rządowego Centrum Bezpieczeństwa z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego;

5) w przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 15 ust. 2 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, przygotowuje w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego.