Elektronicznie
podpisany przez
Grzegorz Paczowski
Data: 2013.12.30
12:14:21 +01'00'

DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 30 grudnia 2013 r.

Poz. 1660

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 19 grudnia 2013 r.

w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych

Na podstawie art. 18 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) miejsce i rolę Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, zwanego dalej „Pełnomocnikiem Ministra", oraz pełnomocników ochrony kierowników bezpośrednio nadrzędnych jednostek organizacyjnych w resortowym systemie ochrony informacji niejawnych;

2) szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

3) zakres, tryb i sposób współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych ze Służbą Kontrwywiadu Wojskowego, zwaną dalej „SKW";

4) rodzaje, szczegółowe cele oraz sposób organizacji szkoleń z zakresu ochrony informacji niejawnych;

5) zakres i szczególne wymagania dotyczące stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych oraz kryteria tworzenia stref ochronnych;

6) tryb opracowywania oraz niezbędne elementy planów ochrony informacji niejawnych, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego, a także sposób nadzorowania ich realizacji.

§ 2. 1. Użyte w rozporządzeniu określenia oznaczają:

1) osoby zajmujące kierownicze stanowiska ministerstwa – Ministra Obrony Narodowej, Sekretarza Stanu w Ministerstwie Obrony Narodowej, Szefa Sztabu Generalnego Wojska Polskiego, podsekretarzy stanu w Ministerstwie Obrony Narodowej, Dyrektora Generalnego Ministerstwa Obrony Narodowej;

2) rozliczanie funkcjonalne – rozliczanie z realizacji zadań prowadzone przez osoby niebędące przełożonymi w hierarchii służbowej, które zgodnie z odpowiednimi dokumentami kompetencyjnymi nadzorują realizację zadań w specjalistycznych dziedzinach działalności;

3) kancelarie tajne międzynarodowe – funkcjonujące w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych kancelarie tajne zagraniczne, przetwarzające informacje niejawne międzynarodowe, wobec których wymagane jest utworzenie odrębnego systemu kancelaryjnego.

2. Ilekroć w rozporządzeniu jest mowa o pionie ochrony, należy przez to rozumieć, w zależności od szczebla jednostki organizacyjnej, departament, oddział, zespół, wydział lub sekcję ochrony informacji niejawnych jako wyodrębnioną komórkę organizacyjną do spraw ochrony informacji niejawnych w rozumieniu art. 15 ust. 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą”.

Rozdział 2

Miejsce i rola Pełnomocnika Ministra oraz pełnomocników ochrony kierowników bezpośrednio nadrzędnych jednostek organizacyjnych w resortowym systemie ochrony informacji niejawnych

§ 3. 1. Pełnomocnik Ministra pełni nadrzędną rolę w resortowym systemie ochrony informacji niejawnych.

2. Pełnomocnik Ministra realizuje w Ministerstwie Obrony Narodowej, zwanym dalej „ministerstwem”, zadania określone w § 5 oraz:

1) określa, w porozumieniu z Szefem SKW, propozycje dotyczące kierunków działania i zasadniczych zadań dla pionów ochrony jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, zwanych dalej „jednostkami organizacyjnymi”, oraz przedkłada je do akceptacji Ministrowi Obrony Narodowej;

2) koordynuje i nadzoruje przedsięwzięcia realizowane przez pełnomocników ochrony w zakresie ochrony informacji niejawnych w celu zapewnienia jednolitego i skutecznego systemu ochrony informacji niejawnych w jednostkach organizacyjnych;

3) kieruje pracami związanymi z opracowywaniem projektów aktów prawnych regulujących problematykę ochrony informacji niejawnych w jednostkach organizacyjnych;

4) opiniuje i uzgadnia projekty dokumentów organizacyjno-etatowych w zakresie struktur oraz zadań pionów ochrony jednostek organizacyjnych;

5) wykonuje zadania związane z realizacją funkcji gestora specjalistycznego sprzętu ochrony informacji niejawnych, w tym określa potrzeby modernizacji i kierunki rozwoju tego sprzętu;

6) opracowuje, w porozumieniu z Szefem SKW, programy szkolenia specjalistycznego dla kandydatów na stanowiska kierowników kancelarii tajnej i kancelarii tajnej międzynarodowej, zastępców kierowników i inne stanowiska służbowe w kancelariach tajnych i kancelariach tajnych międzynarodowych, zwanych dalej „pracownikami kancelarii”, oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych;

7) organizuje szkolenia:

   a) określone w art. 19 ust. 2 pkt 1 ustawy, prowadzone przez SKW, dla osób z jednostek organizacyjnych bezpośrednio podporządkowanych:

      – Ministrowi Obrony Narodowej,

      – osobom zajmującym kierownicze stanowiska ministerstwa,

      – kierownikom komórek organizacyjnych ministerstwa,

   b) specjalistyczne z zakresu bezpieczeństwa teleinformatycznego, prowadzone przez SKW, dla inspektorów bezpieczeństwa teleinformatycznego i administratorów systemu teleinformatycznego pełniących służbę lub zatrudnionych w komórkach organizacyjnych ministerstwa i jednostkach organizacyjnych, o których mowa w lit. a, z wyłączeniem:

      – dowództw Rodzajów Sił Zbrojnych,

      – Inspektoratu Uzbrojenia,

      – Inspektoratu Wsparcia Sił Zbrojnych,

      – Dowództwa Garnizonu Warszawa,

      – Komendy Głównej Żandarmerii Wojskowej,

   c) specjalistyczne dla kandydatów na pracowników kancelarii tajnej i kancelarii tajnej międzynarodowej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, z jednostek organizacyjnych, o których mowa w lit. b,

   d) specjalistyczne uzupełniające dla pracowników kancelarii tajnej i kancelarii tajnej międzynarodowej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, z jednostek organizacyjnych, o których mowa w lit. b;

8) wydaje specjalistyczne wytyczne do działalności pionów ochrony jednostek organizacyjnych w zakresie ochrony informacji niejawnych;

9) nadzoruje działalność merytoryczną pionów ochrony oraz zarządza kontrolę ochrony informacji niejawnych i przestrzegania przepisów o ochronie tych informacji w jednostkach organizacyjnych i komórkach organizacyjnych ministerstwa;

10) rozlicza funkcjonalnie pełnomocników ochrony kierowników jednostek organizacyjnych, o których mowa w pkt 7 lit. a;

11) uzgadnia roczne plany zasadniczych przedsięwzięć jednostek organizacyjnych, o których mowa w pkt 7 lit. a, w zakresie zamierzeń realizowanych przez piony ochrony tych jednostek;

12) sporządza i przedkłada Ministrowi Obrony Narodowej okresowe analizy, sprawozdania, meldunki oraz wnioski dotyczące funkcjonowania systemu ochrony informacji niejawnych w jednostkach organizacyjnych, o których mowa w pkt 7 lit. a;

13) wydaje opinie w sprawach dotyczących ochrony informacji niejawnych;

14) przygotowuje projekty pisemnych upoważnień lub zgód Ministra Obrony Narodowej w sprawie udostępnienia informacji niejawnych w przypadkach określonych w art. 21 ust. 4 pkt 1, art. 34 ust. 5 i 9 oraz art. 54 ust. 7 i 8 ustawy.

§ 4. 1. Pełnomocnicy ochrony kierowników jednostek organizacyjnych, którym podporządkowano jednostki organizacyjne, realizują zadania wymienione w § 5 oraz koordynują i nadzorują realizację zadań w zakresie ochrony informacji niejawnych przez pełnomocników ochrony jednostek organizacyjnych podporządkowanych tym osobom oraz:

1) określają propozycje dotyczące zadań dla pionów ochrony podporządkowanych jednostek organizacyjnych i przedkładają je do akceptacji przełożonym;

2) kierują pracami związanymi z opracowywaniem projektów dokumentów decyzyjnych regulujących problematykę ochrony informacji niejawnych w podporządkowanych jednostkach organizacyjnych;

3) uzgadniają roczne plany zasadniczych przedsięwzięć podporządkowanych jednostek organizacyjnych w zakresie zamierzeń realizowanych przez piony ochrony tych jednostek;

4) nadzorują działalność merytoryczną pionów ochrony podporządkowanych jednostek organizacyjnych oraz prowadzą w tych jednostkach kontrole ochrony informacji niejawnych i przestrzegania przepisów o ochronie tych informacji;

5) rozliczają funkcjonalnie pełnomocników ochrony kierowników podporządkowanych jednostek organizacyjnych;

6) sporządzają i przedkładają swoim przełożonym okresowe analizy, oceny, sprawozdania oraz wnioski dotyczące przestrzegania przepisów o ochronie informacji niejawnych w podporządkowanych jednostkach organizacyjnych;

7) opiniują i uzgadniają projekty dokumentów organizacyjno-etatowych w zakresie struktur oraz zadań pionów ochrony podporządkowanych jednostek organizacyjnych.

2. Pełnomocnicy ochrony dowódców rodzajów Sił Zbrojnych, Szefa Inspektoratu Wsparcia Sił Zbrojnych, Komendanta Głównego Żandarmerii Wojskowej oraz Dowódcy Garnizonu Warszawa realizują zadania określone w ust. 1 oraz organizują szkolenia:

1) określone w art. 19 ust. 2 pkt 1 ustawy, prowadzone przez SKW dla osób pełniących służbę lub zatrudnionych w dowództwach rodzajów Sił Zbrojnych, Inspektoracie Wsparcia Sił Zbrojnych, Komendzie Głównej Żandarmerii Wojskowej, Dowództwie Garnizonu Warszawa oraz jednostkach organizacyjnych im podporządkowanych;

2) specjalistyczne z zakresu bezpieczeństwa teleinformatycznego, prowadzone przez SKW dla inspektorów bezpieczeństwa teleinformatycznego i administratorów systemu teleinformatycznego pełniących służbę lub zatrudnionych w jednostkach organizacyjnych, o których mowa w pkt 1;

3) specjalistyczne dla kandydatów na stanowiska w kancelariach tajnych i kancelariach tajnych międzynarodowych oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, z jednostek organizacyjnych, o których mowa w pkt 1;

4) specjalistyczne uzupełniające dla pracowników kancelarii tajnej i kancelarii tajnej międzynarodowej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, z jednostek organizacyjnych, o których mowa w pkt 1.

Rozdział 3

Szczegółowe zadania pełnomocników ochrony kierowników jednostek organizacyjnych

§ 5. 1. Do szczegółowych zadań pełnomocnika ochrony należy:

1) opracowywanie i przedstawianie do akceptacji kierownikowi jednostki organizacyjnej projektów dokumentów regulujących ochronę informacji niejawnych w jednostce organizacyjnej, w tym:
   a) dokumentacji określającej sposób i tryb przetwarzania w jednostce organizacyjnej informacji niejawnych o klauzuli „poufne”,
   b) instrukcji dotyczącej sposobu i trybu przetwarzania w jednostce organizacyjnej informacji niejawnych o klauzuli „zastrzeżone” oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony,
   c) dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą,
   d) planu ochrony informacji niejawnych w jednostce organizacyjnej, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego, zwanego dalej „planem ochrony informacji niejawnych”,
   e) decyzji (rozkazu) kierownika jednostki organizacyjnej w sprawie organizacji systemu przepustkowego w jednostce organizacyjnej;
2) zapewnienie ochrony systemów teleinformatycznych funkcjonujących w jednostce organizacyjnej, w których są przetwarzane informacje niejawne, poprzez nadzór nad przestrzeganiem zasad i procedur z zakresu ochrony informacji niejawnych;
3) prowadzenie kontroli ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w jednostce organizacyjnej;
4) organizowanie kontroli okresowych ewidencji, materiałów i obiegu dokumentów zawierających informacje niejawne w jednostce organizacyjnej oraz nadzorowanie ich przebiegu;
5) prowadzenie zwykłych i kontrolnych postępowań sprawdzających;
6) prowadzenie, w postaci papierowej lub elektronicznej, i aktualizowanie wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto, obejmującego wyłącznie informacje, o których mowa w art. 15 ust. 1 pkt 8 ustawy;
7) planowanie szkolenia z zakresu ochrony informacji niejawnych oraz prowadzenie ewidencji wydanych zaświadczeń o ukończeniu szkolenia;
8) organizowanie szkolenia z zakresu ochrony informacji niejawnych:
   a) podstawowego dla osób, o których mowa w art. 19 ust. 2 pkt 2 ustawy, prowadzonego wspólnie z SKW,
   b) podstawowego i uzupełniającego dla osób pełniących służbę lub zatrudnionych w jednostce organizacyjnej oraz wykonujących czynności zlecone związane z dostępem do informacji niejawnych;
9) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych w jednostce organizacyjnej, a w szczególności szacowanie ryzyka;
10) zapewnienie obsługi kancelaryjnej w jednostce organizacyjnej;
11) wdrożenie wytycznych, zaleceń i instrukcji dotyczących postępowania z informacjami niejawnymi międzynarodowymi, wydawanymi przez krajową władzę bezpieczeństwa;
12) sprawowanie nadzoru nad funkcjonowaniem kancelarii tajnej i kancelarii tajnej międzynarodowej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych;
13) informowanie kierownika jednostki organizacyjnej oraz pełnomocnika ochrony bezpośrednio nadrzędnej jednostki organizacyjnej o naruszeniu w jednostce organizacyjnej przepisów o ochronie informacji niejawnych, a także kierownika właściwej jednostki organizacyjnej SKW w przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne” lub wyższą;

14) prowadzenie postępowań wyjaśniających okoliczności naruszenia przepisów o ochronie informacji niejawnych oraz przedstawianie wyników tych postępowań i wynikających z nich wniosków kierownikowi jednostki organizacyjnej, a w przypadkach naruszenia przepisów dotyczących bezpieczeństwa informacji niejawnych międzynarodowych o klauzuli stanowiącej odpowiednik klauzuli „zastrzeżone” także Szefowi SKW;

15) zapewnienie bezpieczeństwa fizycznego informacji niejawnych w jednostce organizacyjnej, w tym:

a) stosowanie środków bezpieczeństwa fizycznego odpowiednich do poziomu zagrożeń,

b) organizowanie stref ochronnych oraz systemu wejść i wyjść z tych stref,

c) określanie zasad wstępu do stref ochronnych oraz nadawanie uprawnień do wstępu do tych stref;

16) zapewnienie właściwej ochrony informacji niejawnych podczas ćwiczeń, treningów sztabowych, narad, odpraw i szkoleń w rejonach i pomieszczeniach, w których są one prowadzone;

17) prowadzenie, w postaci papierowej lub elektronicznej, wykazu zawartych z przedsiębiorcami przez jednostkę organizacyjną umów i zadań związanych z dostępem do informacji niejawnych;

18) udział w opracowywaniu umów i instrukcji bezpieczeństwa przemysłowego dotyczących zlecenia przedsiębiorcy wykonania umów lub zadań związanych z dostępem do informacji niejawnych;

19) nadzorowanie, kontrola i doradztwo w zakresie wykonywania przez przedsiębiorców, z którymi jednostka organizacyjna zawarła umowę, obowiązku ochrony informacji niejawnych wytworzonych lub przekazanych przedsiębiorcy w związku z realizacją umowy;

20) w przypadku gdy umowy związane z dostępem do informacji niejawnych nie są realizowane bezpośrednio u zleceniodawcy, a na rzecz innej jednostki organizacyjnej, przy realizacji pkt 17–19 uczestniczą pełnomocnicy ochrony tych jednostek organizacyjnych;

21) sporządzanie i przedkładanie kierownikowi jednostki organizacyjnej okresowych analiz, ocen, sprawozdań oraz wniosków dotyczących przestrzegania w jednostce organizacyjnej przepisów o ochronie informacji niejawnych.

2. Powierzenie pełnomocnikowi ochrony wykonywania innych zadań niż te, o których mowa w ust. 1, wymaga uzyskania pozytywnej opinii Pełnomocnika Ministra.

Rozdział 4

Zakres, tryb i sposób współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych z SKW

§ 6. 1. Pełnomocnicy ochrony współdziałają z SKW w zakresie:

1) bezpieczeństwa osobowego;

2) bezpieczeństwa przemysłowego;

3) identyfikowania zagrożeń dla bezpieczeństwa informacji niejawnych przetwarzanych w jednostkach organizacyjnych;

4) organizowania i prowadzenia szkoleń z problematyki ochrony informacji niejawnych;

5) wykorzystywania wyników działalności kontrolnej;

6) bezpieczeństwa teleinformatycznego, w szczególności w zakresie akredytacji bezpieczeństwa systemów teleinformatycznych.

2. Współdziałanie pełnomocników ochrony z SKW odbywa się w trybie:

1) bezpośrednich albo korespondencyjnych kontaktów;

2) bieżących konsultacji dotyczących wspólnych obszarów działania;

3) uzgadniania szczegółów organizacyjnych i technicznych dotyczących realizacji wspólnie prowadzonych szkoleń.

3. Współdziałanie pełnomocników ochrony z SKW w zakresie ochrony informacji niejawnych jest realizowane przez:

1) przekazywanie przez SKW pełnomocnikom ochrony jednostek organizacyjnych za pośrednictwem Pełnomocnika Ministra:
   a) wyników inspekcji przeprowadzonych przez przedstawicieli organów bezpieczeństwa Organizacji Traktatu Północnoatlantyckiego, zwanej dalej „NATO”, i Unii Europejskiej, zwanej dalej „UE”, w jednostkach organizacyjnych,
   b) dokumentów regulujących problematykę ochrony informacji niejawnych w NATO i UE w celu ich dalszej dystrybucji,
   c) opracowywanych przez SKW projektów zaleceń, wytycznych i innych dokumentów regulujących problematykę ochrony informacji niejawnych, w celu zachowania spójności ich treści z aktami prawnymi wydawanymi przez Ministra Obrony Narodowej – do zaopiniowania przez pełnomocników ochrony;
2) udostępnianie pełnomocnikom ochrony przez SKW:
   a) materiałów informacyjnych o zagrożeniach mogących mieć wpływ na bezpieczeństwo informacji niejawnych przetwarzanych w jednostkach organizacyjnych,
   b) wniosków oraz zaleceń wynikających z przeprowadzonych przez SKW kontroli stanu zabezpieczenia informacji niejawnych w jednostkach organizacyjnych w celu eliminowania występujących nieprawidłowości oraz usprawnienia systemu ochrony informacji niejawnych;
3) informowanie przez SKW pełnomocników ochrony, za pośrednictwem Pełnomocnika Ministra, o cofnięciu przedsiębiorcom realizującym umowy albo zadania związane z dostępem do informacji niejawnych na rzecz jednostek organizacyjnych świadectw bezpieczeństwa przemysłowego;
4) informowanie SKW przez pełnomocników ochrony jednostek organizacyjnych zlecających umowę o zawieranych przez jednostki organizacyjne umowach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą, zakończeniu wykonania umowy, a także o przypadkach naruszenia przez przedsiębiorcę, z którym zawarto umowę, przepisów o ochronie informacji niejawnych;
5) udostępnianie przez pełnomocników ochrony upoważnionym przedstawicielom SKW informacji i dokumentów niezbędnych do przeprowadzenia czynności realizowanych w ramach postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego;
6) zapraszanie przedstawicieli SKW do udziału w prowadzonych przez pełnomocników ochrony szkoleniach oraz odprawach rozliczeniowo-zadaniowych dla pracowników pionów ochrony;
7) wzajemne informowanie się o toczących się postępowaniach karnych przeciwko osobom pełniącym służbę lub zatrudnionym w jednostce organizacyjnej:
   a) posiadającym poświadczenia bezpieczeństwa wydane przez SKW,
   b) w stosunku do których SKW prowadzi postępowanie sprawdzające – w sprawach o przestępstwa umyślne ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe, a także o przypadkach skazania prawomocnym wyrokiem za wyżej wymienione przestępstwa;
8) wzajemne przekazywanie danych osób, które w wyniku przeprowadzonych postępowań sprawdzających lub kontrolnych postępowań sprawdzających otrzymały odpowiednio:
   a) poświadczenie bezpieczeństwa,
   b) decyzję o odmowie wydania poświadczenia bezpieczeństwa,
   c) decyzję o cofnięciu posiadanego poświadczenia bezpieczeństwa.

Rozdział 5

Szkolenie w zakresie ochrony informacji niejawnych

§ 7. W jednostkach organizacyjnych przeprowadza się następujące rodzaje szkoleń:

1) podstawowe;
2) uzupełniające;
3) specjalistyczne;
4) specjalistyczne uzupełniające.

§ 8. 1. Celem szkolenia podstawowego jest zapoznanie osób pełniących służbę wojskową oraz zatrudnionych w jednostce organizacyjnej:

1) z tematyką określoną w art. 19 ust. 1 ustawy;

2) z instrukcją dotyczącą sposobu i trybu przetwarzania w jednostce organizacyjnej informacji niejawnych o klauzuli „zastrzeżone”;

3) ze sposobem i trybem przetwarzania w jednostce organizacyjnej informacji niejawnych o klauzuli „poufne”;

4) z zasadami ochrony informacji niejawnych międzynarodowych – w przypadku przetwarzania tego typu informacji w jednostce organizacyjnej lub przed wyjazdem zagranicznym wiążącym się z dostępem do informacji niejawnych NATO lub UE.

2. Szkolenie podstawowe organizuje i przeprowadza pełnomocnik ochrony lub wyznaczeni przez niego pracownicy pionu ochrony, w miejscu oraz w terminach ustalonych z kierownikami komórek organizacyjnych.

3. Szkolenie podstawowe kończy się wydaniem zaświadczenia, którego wzór stanowi załącznik do rozporządzenia wydanego na podstawie art. 20 ust. 2 ustawy, oraz odebraniem od osoby przeszkolonej oświadczenia o zapoznaniu się z przepisami o ochronie informacji niejawnych.

§ 9. 1. Celem szkolenia uzupełniającego jest uaktualnianie wiedzy uzyskanej podczas szkolenia podstawowego w zakresie ochrony informacji niejawnych.

2. Szkolenie uzupełniające dla osób pełniących służbę wojskową lub zatrudnionych w jednostkach organizacyjnych stosownie do potrzeb organizuje i przeprowadza pełnomocnik ochrony lub wyznaczeni przez niego pracownicy pionu ochrony.

3. Szkolenie uzupełniające przeprowadza się w miejscu i terminach uzgodnionych z kierownikami komórek organizacyjnych; do przeprowadzenia szkolenia dopuszcza się wykorzystanie platformy „e-learning”.

4. Szkolenie uzupełniające dla osób pełniących służbę wojskową lub zatrudnionych w komórkach organizacyjnych ministerstwa przeprowadza, w miejscu i terminach zaplanowanych przez kierowników tych komórek, Pełnomocnik Ministra lub wyznaczona przez niego osoba.

§ 10. 1. Celem szkolenia specjalistycznego jest przygotowanie osób, o których mowa w ust. 2, do wykonywania obowiązków służbowych.

2. Szkoleniem specjalistycznym obejmuje się kandydatów na:

1) pełnomocnika ochrony i zastępcę pełnomocnika ochrony;

2) administratora systemu teleinformatycznego, w którym przetwarza się informacje niejawne;

3) pracownika pionu ochrony pełniącego funkcję inspektora bezpieczeństwa teleinformatycznego;

4) pracowników kancelarii tajnej, kancelarii tajnej międzynarodowej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych.

§ 11. 1. Szkoleniem specjalistycznym uzupełniającym, w cyklu nie dłuższym niż pięcioletni, obejmuje się pracowników kancelarii tajnej i kancelarii tajnej międzynarodowej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, z jednostek organizacyjnych.

2. Celem szkolenia specjalistycznego uzupełniającego jest uzupełnienie wiedzy specjalistycznej osób, o których mowa w ust. 1.

§ 12. 1. Potrzeby w zakresie szkolenia osób, o których mowa w § 10 ust. 2, na rok następny zgłaszają corocznie:

1) Pełnomocnikowi Ministra:
   a) kierownicy komórek organizacyjnych ministerstwa,
   b) kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska ministerstwa oraz kierownikom komórek organizacyjnych ministerstwa, a także kierownicy podległych im jednostek organizacyjnych;
2) pełnomocnikom ochrony kierowników jednostek organizacyjnych, o których mowa w § 4 ust. 2 – kierownicy komórek organizacyjnych tych jednostek oraz kierownicy podległych jednostek organizacyjnych odpowiednio według podległości.

2. Listy uczestników szkoleń, o których mowa w § 10 ust. 2 pkt 1–3, sporządzone na podstawie zapotrzebowań, są przekazywane SKW w celu ewidencji i weryfikacji.

3. Szkolenie specjalistyczne, o którym mowa w § 10 ust. 2 pkt 1–3, organizują, zgodnie z właściwościami określonymi w ust. 1, odpowiednio Pełnomocnik Ministra i pełnomocnicy wymienieni w § 4 ust. 2; zajęcia szkoleniowe przeprowadzają żołnierze, funkcjonariusze lub pracownicy SKW zgodnie z programem szkolenia opracowanym przez SKW.

4. Szkolenie specjalistyczne, o którym mowa w § 10 ust. 2 pkt 4, oraz szkolenie specjalistyczne uzupełniające, organizują i przeprowadzają, zgodnie z właściwościami określonymi w ust. 1, odpowiednio Pełnomocnik Ministra albo pełnomocnicy ochrony wymienieni w § 4 ust. 2.

5. Szkolenie specjalistyczne, o którym mowa w § 10 ust. 2 pkt 4, oraz szkolenie specjalistyczne uzupełniające, przeprowadza się zgodnie z programem szkolenia opracowanym przez Pełnomocnika Ministra w porozumieniu z Szefem SKW.

6. Terminy szkoleń, o których mowa w § 10 ust. 2 pkt 1–3, Pełnomocnik Ministra oraz pełnomocnicy ochrony wymienieni w § 4 ust. 2 ustalają w porozumieniu z SKW do dnia 30 listopada roku kalendarzowego na rok następny.

7. W uzasadnionych przypadkach szkolenie specjalistyczne może być organizowane w trybie roboczym, z pominięciem terminów określonych w ust. 6.

8. Szkolenie specjalistyczne, o którym mowa w § 10 ust. 2, oraz szkolenie specjalistyczne uzupełniające, kończy się wydaniem zaświadczenia potwierdzającego jego odbycie.

Rozdział 6

Zakres i szczególne wymagania dotyczące stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych oraz kryteria tworzenia stref ochronnych

§ 13. 1. W celu zapewnienia w jednostce organizacyjnej skutecznej ochrony informacji niejawnych stosuje się środki bezpieczeństwa fizycznego obejmujące przedsięwzięcia organizacyjne, ochronę fizyczną i ochronę techniczną.

2. Ochrona fizyczna obejmuje zespół przedsięwzięć mających na celu zapewnienie stałej kontroli nad materiałami niejawnymi i jest realizowana przez osoby przeszkolone, w tym przez siły ochronne i służby dyżurne zapewniające między innymi kontrolę dostępu do pomieszczeń lub obszarów, rejonów, stref, w których są przetwarzane informacje niejawne, oraz nadzór nad technicznymi środkami wspomagającymi ochronę fizyczną, a także reagowanie na sygnały alarmowe lub techniczne.

3. Ochronę techniczną stanowią zabezpieczenia uniemożliwiające lub opóźniające wtargnięcie osób nieuprawnionych w sposób niezauważony lub z użyciem siły do pomieszczeń, obszarów, rejonów, stref, w których są przetwarzane informacje niejawne.

§ 14. 1. Zabezpieczenia służące do ochrony fizycznej informacji niejawnych tworzą w szczególności:

1) bariery fizyczne chroniące granice pomieszczeń, obszarów, rejonów, stref, w których są przetwarzane informacje niejawne, w tym w szczególności ogrodzenia, przegrody budowlane, zabezpieczenia mechaniczne, a także urządzenia do przechowywania materiałów niejawnych;

2) system kontroli dostępu obejmujący system elektroniczny lub rozwiązanie organizacyjne, stosowane w celu zagwarantowania uzyskiwania dostępu do pomieszczeń, obszarów, rejonów, stref, w których są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;

3) system alarmowy służący do wykrywania i sygnalizowania naruszenia chronionych granic pomieszczeń, obszarów, rejonów oraz stref;

4) telewizyjny system nadzoru stosowany do obserwowania i rejestrowania sytuacji w nadzorowanym obszarze, rejonie, strefie oraz do weryfikacji zdarzeń alarmowych;

5) system kontroli osób i przedmiotów obejmujący system elektroniczny lub rozwiązanie organizacyjne polegające na kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych, stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia do stref ochronnych rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia materiałów niejawnych z budynków lub obiektów;

6) depozytory przeznaczone do przechowywania telefonów komórkowych i innych urządzeń rejestrujących obraz i dźwięk;

7) depozytory kluczy przeznaczone do bezpiecznego zdawania, przechowywania i pobierania kluczy do pomieszczeń i urządzeń, w których przetwarzane są informacje niejawne.

2. Systemy alarmowe, elektroniczne systemy kontroli dostępu, telewizyjne systemy nadzoru muszą spełniać wymagania o standardzie nie niższym niż określony w Normie Obronnej NO-04-A004 – Obiekty wojskowe. Systemy alarmowe.

§ 15. 1. Tworzy się następujące strefy ochronne:

1) strefę ochronną I – obejmującą pomieszczenie, zespół pomieszczeń lub obszar, w którym informacje niejawne są przetwarzane, w taki sposób, że wstęp do tego pomieszczenia, zespołu pomieszczeń lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji, przy czym spełnione są następujące wymagania:
   a) granice strefy są wyraźnie określone i zabezpieczone,
   b) w planie ochrony informacji niejawnych wskazana jest najwyższa klauzula tajności przetwarzanych informacji niejawnych,
   c) osoby pracujące lub pełniące służbę w strefie muszą posiadać odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby w tej strefie,
   d) w strefie mogą przebywać wyłącznie osoby, którym nadano stałe lub okresowe uprawnienia do dostępu do tej strefy,
   e) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. c i d, przetwarzane informacje niejawne chroni się przed możliwością dostępu do nich tych osób oraz zapewnia się nadzór osoby uprawnionej;

2) strefę ochronną II – obejmującą pomieszczenie, zespół pomieszczeń lub obszar, w którym informacje niejawne są przetwarzane, w taki sposób, że wstęp do tego pomieszczenia, zespołu pomieszczeń lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji, przy czym spełnione są następujące wymagania:
   a) granice strefy są wyraźnie określone i zabezpieczone,
   b) osoby pracujące lub pełniące służbę w tej strefie muszą posiadać odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby w tej strefie,
   c) w strefie mogą przebywać wyłącznie osoby, którym nadano stałe lub okresowe uprawnienia do dostępu do tej strefy,
   d) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. b i c, zapewnia się nadzór osoby uprawnionej;

3) strefę ochronną III – obejmującą pomieszczenie, zespół pomieszczeń lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów, przy czym:
   a) w strefie tej mogą przebywać osoby, którym nadano stałe lub okresowe uprawnienia dostępu do tej strefy,
   b) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. a, zapewnia się nadzór osoby uprawnionej,
   c) w kompleksach, w których dyslokowanych jest więcej niż jedna jednostka organizacyjna, zasady wejścia do strefy ochronnej III ustala kierownik jednostki organizacyjnej, który jest odpowiedzialny za organizację i funkcjonowanie systemu ochrony całego kompleksu, w porozumieniu z kierownikami jednostek organizacyjnych stacjonujących na terenie tego kompleksu.

2. Wejście do strefy ochronnej I lub strefy ochronnej II następuje wyłącznie ze strefy ochronnej.

3. W strefie ochronnej I lub II można utworzyć specjalną strefę ochronną, chronioną przed podsłuchem, spełniającą odpowiednio wymagania zawarte w ust. 1 pkt 1 i 2 oraz dodatkowo następujące warunki:

1) strefę wyposaża się w system sygnalizacji włamania i napadu;

2) strefa pozostaje zamknięta, gdy nikogo w niej nie ma, albo jest chroniona, gdy ktoś w niej przebywa;

3) strefa podlega okresowym inspekcjom przeprowadzanym według zaleceń SKW, a także po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście mogło mieć miejsce;

4) w strefie nie mogą znajdować się linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny, których umieszczenie w strefie nie zostało uzgodnione z SKW;

5) wnoszenie przedmiotów do strefy odbywa się na zasadach określonych w procedurach bezpieczeństwa opracowanych dla tej strefy.

4. Dopuszcza się możliwość organizacji dodatkowego systemu kontroli dostępu w ramach strefy ochronnej I i II, jeżeli jest to podyktowane względami bezpieczeństwa przetwarzanych w jednostce organizacyjnej informacji niejawnych.

5. Strefę ochronną można utworzyć tymczasowo w celu realizacji zamierzeń związanych z dostępem do informacji niejawnych w warunkach zastanych po zapewnieniu ciągłej ochrony fizycznej tej strefy.

6. W przypadku gdy ochrona fizyczna jednostki organizacyjnej oraz prace związane z utrzymaniem infrastruktury tej jednostki, w szczególności sprzątanie, konserwacje, naprawy i remonty, wiążą się z bezpośrednim dostępem do informacji niejawnych, personel sprawujący ochronę, sprzątający lub techniczny musi posiadać uprawnienie do dostępu do informacji niejawnych odpowiednie do klauzuli tych informacji; jeżeli ochrona fizyczna jednostki organizacyjnej lub prace związane z utrzymaniem infrastruktury tej jednostki wiążą się z dostępem do informacji niejawnych o klauzuli „poufne” lub wyższej i wykonuje je podmiot zewnętrzny, musi on posiadać stosowne świadectwo bezpieczeństwa przemysłowego.

7. W strefie ochronnej I i strefie ochronnej II przetwarza się informacje niejawne do klauzuli „ściśle tajne” włącznie.

8. W strefie ochronnej III przetwarza się informacje niejawne do klauzuli „poufne” włącznie, bez możliwości przetwarzania w systemach teleinformatycznych informacji o klauzuli „poufne”.

9. Przetwarzanie informacji niejawnych o klauzuli „poufne” lub wyższej w systemach teleinformatycznych odbywa się w strefie ochronnej I lub w strefie ochronnej II, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

10. Przekazywanie informacji niejawnych pomiędzy elementami systemów teleinformatycznych odbywa się w strefie ochronnej, na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

11. Newralgiczne elementy systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, w szczególności serwery, systemy zarządzania siecią, kontrolery sieciowe umieszcza się w strefie ochronnej z uwzględnieniem wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

§ 16. 1. Strefy ochronne oznacza się czytelnie, w następujący sposób:

1) strefę ochronną I – tablicą w kształcie prostokąta z napisem koloru czarnego „STREFA OCHRONNA I” na czerwonym tle;

2) strefę ochronną II – tablicą w kształcie prostokąta z napisem koloru czarnego „STREFA OCHRONNA II” na żółtym tle;

3) strefę ochronną III – tablicą w kształcie prostokąta z napisem koloru czarnego „STREFA OCHRONNA III” na zielonym tle.

2. Tablice, o których mowa w ust. 1, umieszcza się przy wejściu do strefy, w widocznych miejscach. Można odstąpić od oznaczania strefy ochronnej III, jeśli jest to uzasadnione względami ochrony informacji niejawnych.

§ 17. 1. W warunkach tymczasowych, poza miejscem stałej lokalizacji jednostki organizacyjnej, można odstąpić od oznaczania stref ochronnych, jeśli demaskowałoby to stanowiska lub punkty dowodzenia (kierowania) lub inne urządzenia.

2. Organizacja stref ochronnych oraz sposób ich oznaczania w przypadku przetwarzania informacji niejawnych w mobilnych systemach teleinformatycznych odbywa się na podstawie wyników procesu szacowania ryzyka, o których mowa w art. 49 ust. 1 ustawy, w sposób określony w dokumentacji bezpieczeństwa systemu teleinformatycznego.

Rozdział 7

Tryb opracowywania oraz niezbędne elementy planów ochrony informacji niejawnych, a także sposób nadzorowania ich realizacji

§ 18. 1. Ochrona informacji niejawnych w jednostce organizacyjnej jest organizowana i realizowana na podstawie planu ochrony informacji niejawnych.

2. Plan ochrony informacji niejawnych opracowuje i aktualizuje pełnomocnik ochrony, w porozumieniu z osobą odpowiedzialną za ochronę obiektów jednostki organizacyjnej.

3. Opracowanie planu ochrony informacji niejawnych poprzedza przeprowadzenie analizy ryzyka, w tym szacowanie ryzyka i opracowanie dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.

4. Zmiany poziomu zagrożeń, lokalizacji stref ochronnych lub zmiany struktury jednostki organizacyjnej wymagają aktualizacji planu ochrony informacji niejawnych.

5. Aktualizację planu ochrony informacji niejawnych może przeprowadzać pełnomocnik ochrony samodzielnie po upoważnieniu przez kierownika jednostki organizacyjnej.

§ 19. 1. Plan ochrony informacji niejawnych zawiera w szczególności:

1) określenie granic stref ochronnych oraz klauzul informacji niejawnych przetwarzanych w strefie ochronnej I, a także procedur nadawania uprawnień do przebywania w strefach ochronnych i sposobu realizacji kontroli dostępu do tych stref;

2) określony dla jednostki organizacyjnej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, przedstawiony w dokumentacji, o której mowa w art. 43 ust. 4 ustawy;

3) zasady i sposób przechowywania, wydawania i zdawania kluczy użytku bieżącego i zapasowych do pomieszczeń oraz urządzeń, w których są przechowywane materiały niejawne, a także zasady ustalania, zmiany i deponowania haseł lub kodów (szyfrów), w przypadku stosowania zamków szyfrowych oraz zasady ustalania, zmiany i deponowania haseł administracyjnych do niejawnych systemów teleinformatycznych;

4) procedury postępowania z materiałami niejawnymi o klauzuli „ściśle tajne” lub „tajne” w razie wprowadzenia stanu nadzwyczajnego;

2. W planie ochrony informacji niejawnych uwzględnia się funkcjonowanie jednostki organizacyjnej w trakcie szkolenia, ćwiczeń oraz osiągania wyższych stanów gotowości bojowej.

§ 20. 1. Realizację zadań wynikających z planu ochrony informacji niejawnych nadzoruje pełnomocnik ochrony poprzez sprawdzenie funkcjonowania:

1) ochrony fizycznej informacji niejawnych;

2) technicznych środków wspomagających ochronę informacji niejawnych;

3) systemu przepustkowego i kontroli dostępu, przechowywania, wydawania oraz zdawania kluczy i kodów oraz przestrzegania zasad używania urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w strefach ochronnych.

2. Pełnomocnik ochrony, w zakresie realizacji zadań, o których mowa w ust. 1, współdziała z Żandarmerią Wojskową, Policją, jednostkami organizacyjnymi stacjonującymi w tym samym kompleksie (obiekcie) wojskowym oraz innymi organami porządkowymi i siłami ratowniczymi stosownie do zawartych porozumień w tym zakresie.

Rozdział 8

Przepisy przejściowe i końcowe

§ 21. 1. Organizację stref ochronnych należy dostosować do wymagań określonych w rozporządzeniu w terminie 2 lat od dnia jego wejścia w życie.

2. Plany ochrony informacji niejawnych należy dostosować do wymagań określonych w rozporządzeniu w terminie jednego roku od dnia jego wejścia w życie.

§ 22. Traci moc rozporządzenie Ministra Obrony Narodowej z dnia 2 listopada 2011 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. U. Nr 252, poz. 1519).

§ 23. Rozporządzenie wchodzi w życie z dniem 1 stycznia 2014 r.

Minister Obrony Narodowej: *T. Siemoniak*