1519

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

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. Użyte w rozporządzeniu określenia oznaczają:

1) osoby zajmujące kierownicze stanowiska w ministerstwie — 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.

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 realizuje w Ministerstwie Obrony Narodowej, zwanym dalej „ministerstwem", zadania określone w § 4, a także pełni nadrzędną rolę w resortowym systemie ochrony informacji niejawnych i jest obowiązany do:

1) określania, w porozumieniu z Szefem SKW, propozycji dotyczących kierunków działania i zasadniczych zadań dla pionów ochrony jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, zwanych dalej „jednostkami organizacyjnymi", oraz przedkładania ich do akceptacji Ministrowi Obrony Narodowej;

2) koordynowania i nadzorowania przedsięwzięć realizowanych przez pełnomocników w zakresie ochrony informacji niejawnych w celu zapewnienia jednolitego i skutecznego systemu ochrony informacji niejawnych w jednostkach organizacyjnych;

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

4) opiniowania i uzgadniania projektów dokumentów organizacyjno-etatowych zawierających struktury oraz zadania pionów ochrony jednostek organizacyjnych;

5) opiniowania projektów dokumentów decyzyjnych i rozkazodawczych regulujących problematykę ochrony informacji niejawnych, wydawanych przez kierowników jednostek organizacyjnych bezpośrednio podporządkowanych:

   a) osobom zajmującym kierownicze stanowiska ministerstwa,

   b) kierownikom komórek organizacyjnych ministerstwa;

6) wykonywania zadań związanych z realizacją funkcji gestora specjalistycznego sprzętu ochrony informacji niejawnych, w tym określania potrzeb modernizacji i kierunków rozwoju tego sprzętu;

7) opracowywania, w porozumieniu z Szefem SKW, programów szkolenia specjalistycznego dla kandydatów na stanowiska kierowników kancelarii tajnej, zastępców kierowników i inne stanowiska służbowe w kancelariach tajnych oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych;

8) organizowania szkolenia:

a) określonego w art. 19 ust. 2 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą", prowadzonego przez SKW, dla osób z jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, dla osób zajmujących kierownicze stanowiska w ministerstwie oraz dla kierowników komórek organizacyjnych ministerstwa, z wyłączeniem stanowisk pozostających w strukturach Organizacji Traktatu Północnoatlantyckiego (NATO) i Unii Europejskiej (UE),

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

— Inspektoratu Wsparcia Sił Zbrojnych,

— Komendy Głównej Żandarmerii Wojskowej,

— Dowództwa Wojsk Lądowych,

— Dowództwa Marynarki Wojennej,

— Dowództwa Sił Powietrznych,

c) specjalistycznego dla kandydatów na kierowników, zastępców kierowników i inne stanowiska w kancelariach tajnych, kancelariach tajnych międzynarodowych oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, z jednostek organizacyjnych, o których mowa w lit. b;

9) wydawania specjalistycznych wytycznych do działalności pionów ochrony jednostek organizacyjnych;

10) nadzorowania działalności merytorycznej pionów ochrony oraz zarządzania kontroli stanu zabezpieczenia informacji niejawnych w jednostkach i komórkach organizacyjnych;

11) rozliczania funkcjonalnego pełnomocników ochrony kierowników jednostek organizacyjnych, o których mowa w pkt 8 lit. a;

12) uzgadniania rocznych planów zasadniczych przedsięwzięć jednostek organizacyjnych, o których mowa w pkt 8 lit. a, w zakresie zamierzeń realizowanych przez piony ochrony tych jednostek;

13) sporządzania i przedkładania Ministrowi Obrony Narodowej okresowych analiz, sprawozdań, meldunków oraz wniosków dotyczących przestrzegania przepisów o ochronie informacji niejawnych w jednostkach organizacyjnych, o których mowa w pkt 5;

14) wydawania opinii w sprawach dotyczących ochrony informacji niejawnych;

15) przygotowywania projektów decyzji Ministra Obrony Narodowej w sprawie udostępnienia informacji niejawnych w przypadkach określonych w art. 21 ust. 4 pkt 1, art. 34 ust. 5 i 9, art. 54 ust. 7 i 8 ustawy.

2. Pełnomocnicy ochrony dowódców rodzajów Sił Zbrojnych, Dowódcy Operacyjnego Sił Zbrojnych, Inspektoratu Wsparcia Sił Zbrojnych, Inspektoratu Uzbrojenia, Inspektoratu Wojskowej Służby Zdrowia, Dowódcy Garnizonu Warszawa, Komendanta Głównego Żandarmerii Wojskowej i innych osób funkcyjnych, którym podporządkowano jednostki organizacyjne, realizują zadania wymienione w § 4 oraz koordynują i nadzorują realizację zadań w zakresie ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych podporządkowanych tym osobom i są obowiązani do:

1) określania propozycji dotyczących zasadniczych zadań dla pionów ochrony podporządkowanych jednostek organizacyjnych oraz przedkładania ich do akceptacji swoim przełożonym;

2) kierowania pracami związanymi z opracowywaniem projektów aktów prawnych regulujących problematykę ochrony informacji niejawnych w podporządkowanych jednostkach organizacyjnych;

3) uzgadniania rocznych planów zasadniczych przedsięwzięć podporządkowanych jednostek organizacyjnych w zakresie zamierzeń realizowanych przez piony ochrony tych jednostek;

4) nadzorowania działalności merytorycznej pionów ochrony podporządkowanych jednostek organizacyjnych oraz prowadzenia w tych jednostkach kontroli stanu zabezpieczenia informacji niejawnych i przestrzegania przepisów o ochronie tych informacji, zgodnie z rocznym planem kontroli zatwierdzonym przez swojego przełożonego;

5) rozliczania funkcjonalnego pełnomocników ochrony kierowników podporządkowanych jednostek organizacyjnych;

6) sporządzania i przedkładania swoim przełożonym okresowych analiz, ocen, sprawozdań oraz wniosków dotyczących przestrzegania przepisów o ochronie informacji niejawnych w podporządkowanych jednostkach organizacyjnych.

3. Pełnomocnicy ochrony Szefa Inspektoratu Wsparcia Sił Zbrojnych, Komendanta Głównego Żandarmerii Wojskowej oraz dowódców rodzajów Sił Zbrojnych z wyłączeniem Dowództwa Wojsk Specjalnych, niezależnie od przedsięwzięć wyszczególnionych w ust. 2, organizują szkolenie:

1) określone w art. 19 ust. 2 pkt 1 ustawy, prowadzone przez SKW dla osób zatrudnionych w tych instytucjach i w podporządkowanych jednostkach organizacyjnych;

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 kierowników kancelarii tajnych, zastępców kierowników i inne stanowiska w kancelariach tajnych, kancelariach tajnych międzynarodowych oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, z jednostek organizacyjnych, o których mowa w pkt 1.

Rozdział 3

Szczegółowe zadania pełnomocników ochrony kierowników jednostek organizacyjnych

§ 4. 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 w razie wprowadzenia stanu nadzwyczajnego,

   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 stanu zabezpieczenia informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w jednostce organizacyjnej;

4) organizowanie w pierwszym kwartale każdego roku kalendarzowego 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) opracowywanie planów szkolenia podstawowego i uzupełniającego z zakresu ochrony informacji niejawnych oraz prowadzenie ewidencji wydanych zaświadczeń o ukończeniu szkolenia;

8) organizacja szkolenia z zakresu ochrony informacji niejawnych:

   a) podstawowego dla osób, o których mowa w art. 19 ust. 2 pkt 2 ustawy,

   b) podstawowego i uzupełniającego dla osób pełniących służbę lub zatrudnionych w jednostce organizacyjnej oraz wykonujących czynności zlecone związane z dostępem do informacji niejawnych;

9) szacowanie ryzyka oraz zarządzanie ryzykiem bezpieczeństwa informacji niejawnych w jednostce organizacyjnej;

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 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;

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

   a) określanie poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych oraz stosowanie odpowiednich do tego poziomu środków bezpieczeństwa fizycznego,

   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 oraz ochrony pomieszczeń, rejonów ćwiczeń, w których są one prowadzone;

17) prowadzenie, w postaci papierowej lub elektronicznej, wykazu umów i zadań związanych z dostępem do informacji niejawnych realizowanych przez przedsiębiorców na rzecz jednostki organizacyjnej;

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

19) nadzorowanie, szkolenie 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) 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 realizacji zadań, o których mowa w art. 15 ust. 4 ustawy, wymaga uzyskania opinii Pełnomocnika Ministra.

Rozdział 4

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

§ 5. 1. Pełnomocnicy ochrony współdziałają z właściwymi jednostkami i komórkami organizacyjnymi SKW w zakresie:

1) bezpieczeństwa osobowego;

2) bezpieczeństwa przemysłowego;

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

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

5) wykorzystywania wyników działalności kontrolnej.

2. Współdziałanie pełnomocników ochrony z właściwymi jednostkami i komórkami organizacyjnymi 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 właściwymi jednostkami i komórkami organizacyjnymi SKW w zakresie ochrony informacji niejawnych jest realizowane przez:

1) przekazywanie przez SKW za pośrednictwem Pełnomocnika Ministra:

a) wyników inspekcji przeprowadzonych przez przedstawicieli organów bezpieczeństwa NATO i UE w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych,

b) dokumentów regulujących problematykę ochrony informacji niejawnych w NATO i UE celem 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;

2) udostępnianie pełnomocnikom ochrony przez właściwe jednostki 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 o faktach cofnięcia przedsiębiorcom realizującym umowy albo zadania związane z ochroną informacji niejawnych na rzecz jednostek organizacyjnych świadectwa bezpieczeństwa przemysłowego;

4) informowanie SKW przez pełnomocników ochrony:

a) 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,

b) o przypadkach naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych o klauzuli „poufne” lub wyższej;

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, 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

§ 6. W jednostkach organizacyjnych, w zakresie ochrony informacji niejawnych, prowadzi się następujące rodzaje szkoleń:

1) podstawowe;

2) uzupełniające;

3) specjalistyczne.

§ 7. 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 wyznaczone przez niego osoby, spośród personelu 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.

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

2. Szkolenie uzupełniające dla osób pełniących służbę lub zatrudnionych w jednostkach organizacyjnych organizuje i prowadzi pełnomocnik ochrony lub wyznaczeni przez niego pracownicy pionu ochrony, w przypadku istotnych zmian przepisów regulujących problematykę ochrony informacji niejawnych lub gdy uzasadniają to negatywne wyniki uzyskane przez jednostkę organizacyjną w czasie kontroli przestrzegania przepisów o ochronie informacji niejawnych.

3. Szkolenie prowadzi się w miejscu i terminach uzgodnionych z kierownikami komórek organizacyjnych jednostki organizacyjnej.

4. Szkolenie uzupełniające dla osób pełniących służbę wojskową lub zatrudnionych w komórkach organizacyjnych ministerstwa prowadzi, w przypadkach, o których mowa w ust. 2, w miejscu i terminach zaplanowanych przez kierowników tych komórek, Pełnomocnik Ministra lub wyznaczona przez niego osoba.

§ 9. 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) kierownika, zastępcę kierownika lub inne stanowisko służbowe w kancelarii tajnej, kancelarii tajnej międzynarodowej oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych.

3. Potrzeby w zakresie szkolenia osób, o których mowa w ust. 1, na rok następny zgłaszają corocznie:

1) Pełnomocnikowi Ministra:

a) kierownicy komórek organizacyjnych,

b) kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska w ministerstwie oraz kierownikom komórek organizacyjnych, a także kierownicy podległych im jednostek organizacyjnych, z zastrzeżeniem pkt 2;

2) pełnomocnikom ochrony kierowników jednostek organizacyjnych, o których mowa w § 3 ust. 3 — kierownicy komórek wewnętrznych tych jednostek oraz kierownicy podległych jednostek organizacyjnych odpowiednio według podległości.

4. Sporządzone na podstawie zapotrzebowań listy uczestników szkoleń, o których mowa w ust. 2 pkt 1—3, są przekazywane SKW w celu ewidencji i weryfikacji.

5. Szkolenie specjalistyczne, o którym mowa w ust. 2 pkt 1—3, organizują, zgodnie z właściwościami określonymi w ust. 3, odpowiednio Pełnomocnik Ministra i pełnomocnicy wymienieni w § 3 ust. 3, natomiast zajęcia szkoleniowe prowadzą żołnierze, funkcjonariusze lub pracownicy SKW.

6. Szkolenie specjalistyczne, o którym mowa w ust. 2 pkt 4, organizują i prowadzą zgodnie z właściwościami określonymi w ust. 3 odpowiednio Pełnomocnik Ministra albo pełnomocnicy ochrony wymienieni w § 3 ust. 3.

7. Szkolenie specjalistyczne, o którym mowa w ust. 2 pkt 4, prowadzi się zgodnie z programem szkolenia opracowanym przez Pełnomocnika Ministra w porozumieniu z SKW.

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

9. W uzasadnionych przypadkach szkolenie specjalistyczne może być organizowane w trybie roboczym z pominięciem terminów określonych w ust. 8.

10. Szkolenie specjalistyczne, o którym mowa w ust. 2, kończy się wydaniem zaświadczenia potwierdzającego jego odbycie.

Rozdział 6

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

§ 10. W celu zapewnienia skutecznej ochrony informacji niejawnych, w jednostce organizacyjnej stosuje się środki bezpieczeństwa fizycznego, wydziela się strefy ochronne oraz organizuje system przepustkowy.

§ 11. Zakres stosowania środków bezpieczeństwa fizycznego powinien być dostosowany do poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, wynikających z przeprowadzonej analizy.

§ 12. 1. Do środków bezpieczeństwa fizycznego zalicza się ochronę fizyczną i techniczne środki ją wspomagające.

2. Ochronę fizyczną stanowią warty wojskowe, oddziały wart cywilnych, specjalistyczne uzbrojone formacje ochronne oraz służby dyżurne realizujące zadania ochronne w jednostce organizacyjnej lub w konwoju, a także portierzy i dozorcy, zwani dalej „siłami ochronnymi".

3. W przypadku zagrożenia atakami terrorystycznymi ochronę fizyczną można wzmocnić siłami Żandarmerii Wojskowej.

§ 13. Służbę wartowniczą i ochronną organizuje się w oparciu o system posterunków i patroli.

§ 14. 1. Ochronę fizyczną informacji niejawnych wspomaga się technicznymi środkami, które tworzą w szczególności:

1) systemy ochrony technicznej obejmujące:

a) systemy alarmowe (SA) — zewnętrzne i wewnętrzne,

b) telewizyjne systemy nadzoru (TSN),

c) systemy kontroli dostępu (SKD);

2) zabezpieczenia mechaniczne obejmujące:

a) ściany i stropy o odpowiedniej konstrukcji,

b) drzwi odpowiedniej klasy oraz wzmocnienia drzwi standardowych,

c) szyby odporne na włamanie lub działanie fali detonacyjnej,

d) ogrodzenia, kraty i siatki stalowe zabezpieczające otwory okienne lub okna antywłamaniowe odpowiedniej klasy,

e) urządzenia do przechowywania materiałów niejawnych,

f) zamki i kłódki odpowiedniej klasy.

2. Systemy i urządzenia alarmowe muszą spełniać wymagania określone w Normie Obronnej NO-04-A004 — Obiekty wojskowe. Systemy alarmowe.

3. Zainstalowane systemy i urządzenia alarmowe remontuje się, konserwuje i poddaje przeglądom technicznym zgodnie z arkuszem normy obronnej NO-04-A004-8 Obiekty wojskowe. Systemy alarmowe. Eksploatacja.

§ 15. 1. W jednostce organizacyjnej, w której są przetwarzane informacje niejawne, tworzy się strefy ochronne, wprowadza system kontroli wejść i wyjść ze stref oraz określa uprawnienia do przebywania w tych strefach.

2. Strefy ochronne, o których mowa w ust. 1, stanowią oznaczony obszar, obiekt, kompleks budynków, budynek, a także fragment budynku, jedno lub kilka pomieszczeń, w których są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej.

3. Organizuje się następujące strefy ochronne:

1) strefa I, w której przebywanie wiąże się z możliwością bezpośredniego dostępu do informacji niejawnych, przy czym:

a) w strefie I mogą pracować lub pełnić służbę osoby posiadające poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyżej sklasyfikowanej informacji przetwarzanej w tej strefie,

b) wstęp osób (interesantów) niebędących żołnierzami albo pracownikami jednostki (komórki) organizacyjnej objętej strefą może nastąpić po uzyskaniu zgody kierownika tej jednostki (komórki organizacyjnej) lub uprawnionej przez niego osoby i pod nadzorem upoważnionego żołnierza lub pracownika, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie;

2) strefa II, w której przebywanie nie wiąże się z bezpośrednim dostępem do informacji niejawnych, przy czym:

a) w strefie II mogą pracować lub pełnić służbę osoby posiadające poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyżej sklasyfikowanej informacji przetwarzanej w tej strefie,

b) wstęp osób (interesantów) niebędących żołnierzami albo pracownikami jednostki (komórki) organizacyjnej objętej strefą może nastąpić po uzyskaniu zgody kierownika tej jednostki (komórki) organizacyjnej lub uprawnionej przez niego osoby i pod nadzorem upoważnionego żołnierza lub pracownika, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie;

3) strefa III, służąca do kontroli osób i pojazdów, w której przebywanie nie wiąże się z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne" lub „tajne", przy czym:

a) w strefie tej mogą pracować lub pełnić służbę osoby posiadające poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne" oraz osoby upoważnione przez kierownika jednostki organizacyjnej do dostępu do informacji niejawnych o klauzuli „zastrzeżone",

b) wstęp osób (interesantów) niebędących żołnierzami albo pracownikami jednostki (komórki) organizacyjnej objętej strefą może nastąpić pod nadzorem żołnierza lub pracownika, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie.

4. Wejście do I i II strefy ochronnej następuje wyłącznie ze strefy ochronnej III.

5. W strefie ochronnej I lub II można utworzyć:

1) strefę zabezpieczoną technicznie, chronioną przed podsłuchem, spełniającą dodatkowo następujące wymagania:

a) strefę wyposaża się w system sygnalizacji włamania i napadu,

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

c) strefa podlega regularnym inspekcjom przeprowadzanym nie rzadziej niż raz w roku oraz po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście mogło mieć miejsce,

d) w strefie nie mogą znajdować się linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny, które nie zostały uzgodnione z SKW;

2) pomieszczenie wzmocnione, spełniające następujące wymagania:

a) konstrukcję pomieszczenia, w tym ścian, podłogi, sufitu, okien, drzwi i zamków, uzgadnia się z SKW,

b) konstrukcja pomieszczenia powinna zapewniać ochronę równoważną odpowiednim szafom przeznaczonym do przechowywania informacji niejawnych o tej samej klauzuli tajności,

c) w pomieszczeniu wzmocnionym dopuszczalne jest przechowywanie informacji niejawnych poza odpowiednimi szafami.

6. Na czas sprzątania i wykonywania prac remontowych użytkownicy pomieszczeń objętych strefą ochronną zabezpieczają dokumenty niejawne w sposób uniemożliwiający przypadkowe ujawnienie ich treści osobom nieuprawnionym; sprzątanie oraz wykonywanie prac remontowych w tych pomieszczeniach może odbywać się wyłącznie w obecności ich użytkowników.

7. W przypadku gdy prace, o których mowa w ust. 6, wiążą się z bezpośrednim dostępem do informacji niejawnych, personel sprzątający lub techniczny musi posiadać poświadczenia bezpieczeństwa odpowiednie do klauzuli tych informacji; jeżeli prace porządkowe lub remontowe, które będą się wiązać z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, wykonuje podmiot zewnętrzny, musi on posiadać stosowne świadectwo bezpieczeństwa przemysłowego.

8. Osoby pełniące służby dyżurne i ochronne w strefach ochronnych muszą spełnić wymagania:

1) w stosunku do osób pełniących służby dyżurne i ochronne wewnątrz strefy I i II przepisy ust. 3 pkt 1 i 2 stosuje się odpowiednio;

2) osoby pełniące służby dyżurne i ochronne w strefie III muszą posiadać uprawnienia do dostępu do informacji niejawnych o klauzuli odpowiadającej klauzuli informacji, do których mogą mieć dostęp;

3) jeżeli służbę ochronną w strefie III wykonuje podmiot zewnętrzny i może wiązać się to z dostępem do informacji niejawnych o klauzuli „poufne", to musi on posiadać świadectwo bezpieczeństwa przemysłowego co najmniej III stopnia; w przypadku dostępu do informacji o klauzuli „zastrzeżone" osoby pełniące służbę ochronną w strefie III muszą posiadać uprawnienia do dostępu do informacji niejawnych o klauzuli co najmniej „zastrzeżone".

§ 16. 1. Strefy ochronne oznacza się następująco:

1) strefę I — tablicą w kształcie prostokąta o podstawie 19 cm i wysokości 13 cm z napisem koloru czarnego „Strefa ochronna I" o wysokości liter 2 cm na czerwonym tle lub linią ciągłą koloru czerwonego szerokości 10 cm;

2) strefę II — tablicą w kształcie prostokąta o podstawie 19 cm i wysokości 13 cm z napisem koloru czarnego „Strefa ochronna II" o wysokości liter 2 cm na żółtym tle lub linią ciągłą koloru żółtego szerokości 10 cm;

3) strefę III — tablicą w kształcie prostokąta o podstawie 19 cm i wysokości 13 cm z napisem koloru czarnego „Strefa ochronna III" o wysokości liter 2 cm na zielonym tle lub linią ciągłą koloru zielonego szerokości 10 cm.

2. Tablice, o których mowa w ust. 1, umieszcza się na drzwiach wejściowych do stref lub na ścianie przy drzwiach wejściowych albo na specjalnych stojakach.

3. Linie, o których mowa w ust. 1, oznacza się (w szczególności przez malowanie lub oklejenie) przed wejściem do strefy na całej szerokości obszaru, obiektu, budynku lub fragmentu budynku.

§ 17. 1. W celu uniemożliwienia osobom nieuprawnionym dostępu do III strefy ochronnej tworzy się system przepustkowy.

2. W ramach systemu przepustkowego stosuje się przepustki stałe, okresowe, jednorazowe, elektroniczne karty dostępu lub inne identyfikatory, imienne upoważnienia do wykonywania czynności kontrolnych, legitymacje poselskie lub senatorskie, legitymacje pracowników Najwyższej Izby Kontroli i Państwowej Inspekcji Pracy oraz zezwolenia stałe i jednorazowe wydawane przedstawicielom placówek dyplomatycznych państw obcych, a także przepustki samochodowe lub rozkazy wyjazdu w odniesieniu do pojazdów pozostających na wyposażeniu danej jednostki organizacyjnej.

3. Wejście do III strefy ochronnej odbywa się na podstawie:

1) ważnych przepustek (papierowych, elektronicznych kart dostępu) stałych, okresowych i jednorazowych z napisem „GOŚĆ";

2) imiennych stałych i jednorazowych upoważnień do wykonywania czynności kontrolnych, wystawionych przez uprawnione organy wojskowe i państwowe;

3) legitymacji, o których mowa w ust. 2;

4) zezwoleń stałych lub jednorazowych wydawanych cudzoziemcom.

4. Wjazd do III strefy ochronnej odbywa się na podstawie przepustek samochodowych stałych, okresowych, jednorazowych lub rozkazów wyjazdu (w odniesieniu do pojazdów samochodowych danej jednostki organizacyjnej). W przypadku innych pojazdów służbowych zgodę na wjazd wydaje oficer dyżurny jednostki organizacyjnej (kompleksu, obiektu) lub kierownik jednostki (komórki) organizacyjnej.

5. Do wejścia lub wjazdu bez przepustki do III strefy ochronnej obiektu jednostki organizacyjnej uprawnieni są strażacy udający się grupowo do gaszenia pożaru oraz pracownicy pogotowia ratunkowego lub awaryjnego w związku z zaistniałym wypadkiem lub awarią urządzeń elektrycznych, gazowych, wodno-kanalizacyjnych itp., a także funkcjonariusze Policji lub żołnierze Żandarmerii Wojskowej w przypadku wykonywania zadań związanych z bezpieczeństwem i ochroną porządku publicznego.

6. W sytuacjach określonych w ust. 5 strażakom, pracownikom pogotowia, funkcjonariuszom Policji lub żołnierzom Żandarmerii Wojskowej towarzyszą żołnierze (pracownicy) pełniący służbę dyżurną lub wchodzący w skład sił ochronnych jednostek (komórek) organizacyjnych.

7. Dokumenty, o których mowa w ust. 2, mogą, po przyznaniu stosownych uprawnień przez kierownika jednostki organizacyjnej, upoważniać także do wejścia do I i II strefy ochronnej.

Rozdział 7

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

§ 18. 1. Ochrona informacji niejawnych w jednostce organizacyjnej jest organizowana i realizowana na podstawie planu ochrony informacji niejawnych, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne", w razie wprowadzenia stanu nadzwyczajnego.

2. Plan ochrony informacji niejawnych opracowuje i aktualizuje, stosownie do pojawiających się zagrożeń, pełnomocnik ochrony, w porozumieniu z kierownikami komórek wewnętrznych jednostki organizacyjnej, a zatwierdza kierownik jednostki organizacyjnej.

§ 19. 1. Plan ochrony informacji niejawnych składa się z części graficznej i opisowej.

2. W części graficznej planu ochrony informacji niejawnych przedstawia się w szczególności rozmieszczenie:

1) budynków (pomieszczeń), z wyróżnieniem tych, w których są przetwarzane informacje niejawne. Wszystkie budynki przedstawia się w formie rzutu poziomego z góry i opisuje się je; w przypadku budynków wielokondygnacyjnych proponuje się wykonanie i opisanie rzutów poziomych poszczególnych kondygnacji, na których w poszczególnych pomieszczeniach są przetwarzane materiały niejawne;

2) technicznych środków wspomagających ochronę fizyczną informacji niejawnych;

3) stref ochronnych;

4) dróg oraz rejonów ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych, tajnych międzynarodowych oraz w innych komórkach organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych o klauzuli „ściśle tajne" lub „tajne".

3. Zestawienie podstawowych znaków umownych stosowanych w części graficznej planów ochrony informacji niejawnych stanowi załącznik do rozporządzenia.

4. Część graficzną planu ochrony informacji niejawnych wykonuje się w skali umożliwiającej naniesienie wszystkich elementów ochrony i urządzeń ją wspomagających.

5. W części opisowej planu ochrony informacji niejawnych zawiera się w szczególności:

1) charakterystykę jednostki organizacyjnej, a w niej:

a) pełną nazwę jednostki organizacyjnej,

b) rodzaj materiałów niejawnych występujących w jednostce organizacyjnej oraz sposób i tryb ich przetwarzania,

c) nazwy komórek organizacyjnych, z wyszczególnieniem numerów budynków oraz pomieszczeń, w których przetwarzane są informacje niejawne oznaczone klauzulą „poufne", „tajne" lub „ściśle tajne";

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

3) zastosowane środki bezpieczeństwa fizycznego:

a) rodzaj sił ochronnych oraz zasady organizacji i wykonywania przez nie zadań związanych z ochroną fizyczną informacji niejawnych,

b) rodzaje zabezpieczeń technicznych wykorzystywanych w ochronie informacji niejawnych;

4) opis granic stref ochronnych, sposobu ich ochrony, w tym organizację systemu przepustkowego lub kontroli dostępu;

5) zasady i sposób zdawania, przechowywania i wydawania kluczy użytku bieżącego i zapasowych do pomieszczeń oraz szaf, w których przechowywane są informacje niejawne, a także zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych;

6) procedury przyznawania uprawnień do wejścia, wyjścia i przebywania w strefach ochronnych I, II i III, w tym dla pracowników obsługi technicznej, personelu sprzątającego oraz interesantów;

7) sposób interwencji sił ochronnych i osób odpowiedzialnych za ochronę fizyczną w przypadkach wystąpienia sytuacji kryzysowych i wprowadzenia stanu nadzwyczajnego;

8) procedury ewakuacji i niszczenia informacji niejawnych oznaczonych klauzulą „tajne" lub „ściśle tajne", w tym w razie wprowadzenia stanu nadzwyczajnego;

9) siły i środki wydzielone do ewakuacji i zabezpieczenia dróg ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych oraz w innych komórkach organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych o klauzuli „ściśle tajne" lub „tajne";

10) działanie sił ochronnych, kierowników jednostek (komórek) organizacyjnych, pracowników pionu ochrony oraz wykonawców w poszczególnych wyższych stanach gotowości bojowej oraz podczas osiągnięcia zdolności do podjęcia działań, a także w sytuacjach awaryjnych takich jak klęska żywiołowa, katastrofa naturalna lub awaria techniczna, a zwłaszcza:

a) sposób działania sił ochronnych w poszczególnych sytuacjach kryzysowych oraz podczas osiągnięcia zdolności do podjęcia działań,

b) sposób i organizację wzmocnienia systemu ochrony informacji niejawnych w poszczególnych sytuacjach kryzysowych oraz podczas osiągnięcia zdolności do podjęcia działań w poszczególnych stanach, w tym sposób współdziałania sił ochronnych z Żandarmerią Wojskową, Policją oraz innymi organami porządkowymi,

c) przyjmowanie materiałów niejawnych od wykonawców przez kancelarie tajne, przygotowanie materiałów do zniszczenia, przekazania do archiwów oraz ewakuacji;

11) ewakuacja materiałów zawierających informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne"; określenie rejonów ewakuacji, sił i środków wydzielonych do ewakuacji oraz sposobu zabezpieczenia dróg ewakuacji materiałów niejawnych; współpraca z wojskowymi i cywilnymi służbami podczas ewakuacji materiałów niejawnych;

12) postępowanie z materiałami niejawnymi pozostawionymi w miejscu stałej dyslokacji oraz przeznaczonymi do zniszczenia.

§ 20. 1. Plan ochrony informacji niejawnych przechowuje pełnomocnik ochrony.

2. Wyciągi z planów ochrony informacji niejawnych dotyczące ochrony tych informacji w podległych komórkach organizacyjnych, poszczególnych kompleksach, budynkach i pomieszczeniach sporządza się w miarę potrzeb dla służb dyżurnych i sił ochronnych i przechowuje się je w ich pomieszczeniach.

3. Plan ochrony informacji niejawnych lub wyciągi z niego mogą być udostępnione, w niezbędnym zakresie, również osobom realizującym zadania przewidziane dla nich w tym planie, a także osobom kontrolującym.

§ 21. 1. Pełnomocnik ochrony nadzoruje realizację zadań wynikających z planu ochrony informacji niejawnych.

2. Pełnomocnik ochrony, w zakresie realizacji zadań, o których mowa w ust. 1, w razie wprowadzenia stanu nadzwyczajnego ma prawo żądać od kierowników komórek organizacyjnych udzielenia natychmiastowej pomocy.

Rozdział 8

Przepis dostosowujący i końcowy

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

2. Dokumenty, o których mowa w § 4 ust. 1 pkt 1 lit. c i d, należy opracować w terminie 1 roku od dnia wejścia w życie rozporządzenia.

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

Minister Obrony Narodowej: *T. Siemoniak*

[1)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Obrony Narodowej z dnia 21 czerwca 2007 r. w sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. U. Nr 126, poz. 876 oraz z 2008 r. Nr 57, poz. 345), które traci moc z dniem wejścia w życie niniejszego rozporządzenia na podstawie art. 189 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

Załącznik do rozporządzenia Ministra Obrony Narodowej
z dnia 2 listopada 2011 r. (poz. 1519)

ZESTAWIENIE PODSTAWOWYCH ZNAKÓW UMOWNYCH STOSOWANYCH W CZĘŚCI GRAFICZNEJ PLANÓW OCHRONY INFORMACJI NIEJAWNYCH

— służby dyżurne (OD — oficer dyżurny, DP — dyżurny biura przepustek)

— ogrodzenie

— brama

— furtka

— szlaban (zapora)

— drzwi

— drzwi objęte systemem kontroli dostępu (SKD)

— kołowrotek SKD

— bramka SKD

— chroniony budynek

— urządzenie alarmowe stosowane w ochronie zewnętrznej obiektu (budynku)

— urządzenie alarmowe stosowane w ochronie wewnętrznej obiektu (budynku)

— kamera telewizyjna wewnętrzna bez detektora ruchu

— kamera telewizyjna wewnętrzna z detektorem ruchu

— kamera telewizyjna zewnętrzna bez detektora ruchu

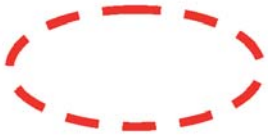
— kamera telewizyjna zewnętrzna z detektorem ruchu

— strefa ochronna I

— strefa ochronna II

— strefa ochronna III

— droga ewakuacji materiałów niejawnych



— rejon ewakuacji materiałów niejawnych