1821

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ

z dnia 19 października 2005 r.

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

Na podstawie art. 18a ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) szczegółowe zadania pełnomocników ochrony w jednostkach organizacyjnych podległych i nadzorowanych przez Ministra Obrony Narodowej, zwanych dalej „jednostkami organizacyjnymi", w tym dotyczące koordynowania oraz nadzorowania działalności pionów ochrony przez pełnomocników ochrony bezpośrednio nadrzędnych jednostek organizacyjnych;

2) szczególne wymagania w zakresie ochrony fizycznej informacji niejawnych;

3) tryb opracowywania oraz podstawowe wymagania, jakim powinny odpowiadać plany ochrony jednostek organizacyjnych, niezbędne elementy planów ochrony, a także sposób nadzorowania ich realizacji;

4) podział stref bezpieczeństwa na rodzaje, a także warunki dostępu do tych stref.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) komórka organizacyjna Ministerstwa Obrony Narodowej — Sekretariat Ministra Obrony Narodowej, departament, generalny zarząd, samodzielny zarząd, biuro, szefostwo;

2) ochrona fizyczna — zespół przedsięwzięć ochronnych realizowanych przez warty i służby wewnętrzne lub garnizonowe, oddziały wart cywilnych, specjalistyczne uzbrojone formacje ochronne przedsiębiorców, przez portierów i dozorców, a także przez psy wartownicze;

3) pełnomocnik ochrony — pełnomocnika do spraw ochrony informacji niejawnych kierownika jednostki organizacyjnej;

4) system ochrony jednostki organizacyjnej — zespół przedsięwzięć organizacyjno-technicznych obejmujących ochronę fizyczną i techniczną obiektów wojskowych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne;

5) ustawa — ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

Rozdział 2

Szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych

§ 3. Do szczegółowych zadań pełnomocnika ochrony należy:

1) zapewnienie obsługi kancelaryjnej w jednostce organizacyjnej;

2) sprawowanie nadzoru nad funkcjonowaniem kancelarii tajnej, tajnej-zagranicznej oraz innych komórek organizacyjnych, przechowujących, przetwarzających, wytwarzających, przekazujących i prowadzących ewidencję materiałów niejawnych;

3) prowadzenie wykazu stanowisk i prac zleconych oraz wykazu osób dopuszczonych do pracy lub służby na stanowiskach w jednostce organizacyjnej, z którymi może się wiązać dostęp do informacji niejawnych;

4) prowadzenie wykazu przedsiębiorców realizujących na rzecz jednostki organizacyjnej umowy lub zadania związane z dostępem do informacji niejawnych;

5) prowadzenie postępowań sprawdzających zwykłych, w tym kontrolnych postępowań sprawdzających, podejmowanie decyzji dotyczących wydania lub odmowy wydania poświadczenia bezpieczeństwa, cofnięcia poświadczenia bezpieczeństwa, a także decyzji o umorzeniu lub zawieszeniu postępowania sprawdzającego; powiadamianie o tym osób upoważnionych do obsady stanowiska służbowego, służby ochrony państwa oraz osób sprawdzanych;

6) opracowywanie projektów dokumentów normujących ochronę informacji niejawnych w jednostce organizacyjnej, a w tym:

   a) szczegółowych wymagań w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone",

   b) planu postępowania z materiałami zawierającymi informacje niejawne stanowiącymi tajemnicę państwową, w razie wprowadzenia stanu nadzwyczajnego, i jego uaktualnianie,

c) wykazu podstawowych rodzajów dokumentów niejawnych, wytwarzanych w jednostce organizacyjnej, zawierających informacje niejawne stanowiące tajemnicę służbową, z przeznaczeniem dla celów szkoleniowych;

7) opracowywanie programów szkolenia oraz organizacja szkolenia podstawowego i uzupełniającego dla osób pełniących służbę wojskową oraz zatrudnionych w jednostce organizacyjnej;

8) zapewnienie ochrony systemów i sieci teleinformatycznych funkcjonujących w jednostce organizacyjnej, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne;

9) prowadzenie kontroli ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w jednostce organizacyjnej;

10) organizowanie kontroli rocznych stanu ochrony informacji niejawnych oraz szkolenie członków komisji biorących udział w tych kontrolach;

11) informowanie kierownika jednostki organizacyjnej oraz pełnomocnika ochrony bezpośrednio nadrzędnej jednostki organizacyjnej o naruszeniu przepisów o ochronie informacji niejawnych, a także kierownika właściwej jednostki organizacyjnej Wojskowych Służb Informacyjnych w przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne" lub wyższą;

12) prowadzenie postępowań wyjaśniających okoliczności naruszenia przepisów o ochronie informacji niejawnych oraz przedstawianie wyników tych postępowań i wynikających z nich wniosków kierownikowi jednostki organizacyjnej, a także pełnomocnikowi ochrony bezpośrednio nadrzędnej jednostki organizacyjnej;

13) zapewnienie ochrony fizycznej jednostki organizacyjnej, a w tym:

a) opracowanie planu ochrony jednostki organizacyjnej i jego bieżąca aktualizacja,

b) sprawowanie nadzoru nad funkcjonowaniem systemu ochrony jednostki organizacyjnej,

c) organizowanie systemu przepustkowego i nadzorowanie realizacji przedsięwzięć w tym zakresie,

d) nadawanie uprawnień do wstępu do stref bezpieczeństwa, obiektów podlegających szczególnej ochronie oraz obszarów chronionych, z wyłączeniem pomieszczeń, w których występują systemy ochrony kryptograficznej,

e) współudział w opracowywaniu programów organizacyjno-użytkowych dotyczących zabezpieczenia fizycznego obiektów jednostki organizacyjnej oraz opracowywanie projektów organizacyjno-użytkowych dotyczących kancelarii tajnych oraz innych pomieszczeń, w których są wytwarzane, przetwarzane, przekazywane lub przechowywane materiały niejawne;

14) zapewnienie ochrony informacji niejawnych podczas ćwiczeń, treningów sztabowych, narad i szkoleń;

15) współudział w opracowywaniu umów i instrukcji bezpieczeństwa przemysłowego dotyczących zlecenia przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej wykonania zadań związanych z dostępem do informacji niejawnych;

16) nadzorowanie, szkolenie i doradztwo w zakresie wykonywania przez przedsiębiorców lub jednostki naukowe, z którymi jednostka organizacyjna zawarła umowę, obowiązku ochrony przekazanych im informacji;

17) współdziałanie w zakresie ochrony informacji niejawnych z właściwymi jednostkami organizacyjnymi służb ochrony państwa oraz bieżące informowanie kierownika jednostki organizacyjnej o przebiegu tego współdziałania;

18) przekazywanie właściwym jednostkom organizacyjnym Wojskowych Służb Informacyjnych danych wymaganych do prowadzenia ewidencji osób dopuszczonych do pracy lub służby na stanowiskach, z którymi wiąże się dostęp do informacji niejawnych stanowiących tajemnicę służbową, oznaczonych klauzulą „poufne", a także danych o osobach, którym wydano decyzję o odmowie wydania poświadczenia bezpieczeństwa lub o cofnięciu poświadczenia bezpieczeństwa;

19) informowanie Wojskowych Służb Informacyjnych o zleceniu przedsiębiorcy lub jednostce naukowej umowy albo zadania wiążącego się z dostępem do informacji niejawnych stanowiących tajemnicę państwową oraz przesłanie kopii instrukcji bezpieczeństwa przemysłowego;

20) przedstawianie kierownikowi jednostki organizacyjnej propozycji dotyczących wyznaczenia osoby odpowiedzialnej za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę lub jednostkę naukową obowiązku ochrony przekazanych im informacji niejawnych w związku z wykonywanymi umowami albo zadaniami związanymi z dostępem do informacji niejawnych.

§ 4. 1. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych koordynuje realizację zadań w zakresie ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa oraz kierownikom komórek organizacyjnych Ministerstwa Obrony Narodowej i jest uprawniony do:

1) określania, w porozumieniu z Szefem Zarządu Ochrony Informacji Niejawnych Inspektoratu Wojskowych Służb Informacyjnych, propozycji dotyczących zasadniczych zadań i kierunków działania

dla pionów ochrony jednostek organizacyjnych oraz przedkładania ich do akceptacji Ministrowi Obrony Narodowej;

2) kierowania pracami związanymi z opracowaniem projektów dokumentów prawnych regulujących problematykę ochrony informacji niejawnych w jednostkach organizacyjnych;

3) opiniowania i uzgadniania projektów dokumentów wydawanych przez kierowników jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, regulujących problematykę ochrony informacji niejawnych w tych jednostkach;

4) opracowywania, w porozumieniu z Szefem Wojskowych Służb Informacyjnych, programów szkolenia specjalistycznego dla kierowników, zastępców kierowników i kancelistów kancelarii tajnych i tajnych-zagranicznych oraz kierowników i pracowników bibliotek, w których są przechowywane i ewidencjonowane niejawne wojskowe wydawnictwa specjalistyczne;

5) organizowania szkolenia:

a) uzupełniającego, o którym mowa w art. 54 ust. 3a ustawy, prowadzonego przez Wojskowe Służby Informacyjne dla pełnomocników ochrony i ich zastępców z jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa oraz kierownikom komórek organizacyjnych Ministerstwa Obrony Narodowej,

b) specjalistycznego dla osób pełniących służbę oraz zatrudnionych w pionach ochrony jednostek organizacyjnych, o których mowa w lit. a, z wyłączeniem dowództw rodzajów sił zbrojnych;

6) nadzorowania działalności merytorycznej pionów ochrony jednostek organizacyjnych, o których mowa w pkt 5 lit. a, oraz realizowania kontroli zleconych przez Ministra Obrony Narodowej;

7) sporządzania i przedkładania Ministrowi Obrony Narodowej analiz, sprawozdań, meldunków i wniosków dotyczących przestrzegania przepisów o ochronie informacji niejawnych w komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych, o których mowa w pkt 5 lit. a, z wyłączeniem Inspektoratu Wojskowych Służb Informacyjnych oraz jednostek organizacyjnych podporządkowanych Szefowi Wojskowych Służb Informacyjnych;

8) wydawania opinii w sprawach dotyczących ochrony informacji niejawnych.

2. Pełnomocnicy ochrony dowódców rodzajów sił zbrojnych i okręgów wojskowych, Komendanta Głównego Żandarmerii Wojskowej, Dowódcy Garnizonu Warszawa oraz dowódców związków taktycznych (równorzędnych) koordynują realizację zadań w zakresie ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych podległych tym osobom, sprawują nadzór nad ich działalnością merytoryczną i są uprawnieni do:

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

2) kierowania pracami związanymi z opracowaniem projektów dokumentów prawnych regulujących problematykę ochrony informacji niejawnych w podległych jednostkach organizacyjnych;

3) organizowania szkolenia uzupełniającego, o którym mowa w art. 54 ust. 3a ustawy, prowadzonego przez Wojskowe Służby Informacyjne dla pełnomocników ochrony i ich zastępców z podległych jednostek organizacyjnych;

4) organizowania szkolenia specjalistycznego dla osób pełniących służbę lub zatrudnionych w pionach ochrony podległych jednostek organizacyjnych;

5) uzgadniania rocznych planów zasadniczych przedsięwzięć pionów ochrony podległych jednostek organizacyjnych;

6) nadzorowania działalności merytorycznej pionów ochrony jednostek podległych, zgodnie z rocznym planem kontroli zatwierdzonym przez swojego przełożonego;

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

Rozdział 3

Szczególne wymagania w zakresie ochrony fizycznej informacji niejawnych

§ 5. W celu zapewnienia skutecznej ochrony informacji niejawnych, w jednostce organizacyjnej stosuje się środki ochrony fizycznej oraz wydziela strefy: administracyjną i bezpieczeństwa, a także określa pomieszczenia i obiekty (rejony) podlegające szczególnej ochronie.

§ 6. 1. System ochrony informacji niejawnych w jednostce organizacyjnej realizuje się przez ochronę fizyczną oraz przy wykorzystaniu technicznych środków ją wspomagających.

2. Ochronę fizyczną realizują warty i służby wewnętrzne lub garnizonowe, oddziały wart cywilnych, specjalistyczne uzbrojone formacje ochronne przedsiębiorców, a także portierzy i dozorcy.

3. W przypadku zagrożenia atakami terrorystycznymi siły ochronne, o których mowa w ust. 2, można wzmocnić siłami Żandarmerii Wojskowej.

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

2. Ze względu na sposób pełnienia służby na posterunkach rozróżnia się następujące ich rodzaje:

1) posterunki stałe;

2) posterunki ruchome.

3. W zależności od miejsca pełnienia służby na posterunkach rozróżnia się posterunki zewnętrzne i wewnętrzne, natomiast ze względu na czas pełnienia służby posterunki dzieli się na dwuzmienne, trzyzmienne i doraźne.

4. Patrole, w składzie dwóch i więcej wartowników, organizuje się w obiektach wojskowych, w których inne sposoby ochrony są nieefektywne.

§ 8. 1. Ochrona fizyczna informacji niejawnych powinna być wspomagana środkami technicznymi, które stanowią w szczególności:

1) systemy i urządzenia alarmowe obejmujące:

   a) systemy sygnalizacji włamania i napadu (SSWiN) — zewnętrzne i wewnętrzne,

   b) systemy telewizji przemysłowej (STVP) — zewnętrzne i wewnętrzne,

   c) systemy kontroli dostępu (SKD);

2) łączność wartownicza i służb dyżurnych:

   a) przewodowa,

   b) radiowa lub radiotelefoniczna;

3) oświetlenie obiektów:

   a) zewnętrzne, w tym oświetlenie obwodnic,

   b) wewnętrzne,

   c) awaryjne magazynów i pomieszczeń;

4) ogrodzenia:

   a) z siatki,

   b) z siatki i drutu kolczastego lub ostrzowego,

   c) z paneli metalowych,

   d) z typowych prefabrykowanych pełnych lub ażurowych elementów żelbetowych;

5) wieże wartownicze;

6) umocnienia inżynieryjne:

   a) zapory inżynieryjne,

   b) punkty (gniazda) oporu,

   c) stanowiska ogniowe;

7) zabezpieczenia mechaniczne:

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

   e) szafy stalowe odpowiedniej klasy,

   f) zamki i kłódki.

2. Zastosowane w ochronie informacji niejawnych systemy powinny posiadać deklarację zgodności ich wykonania w odpowiedniej klasie, natomiast urządzenia wykorzystane do ich budowy odpowiednie certyfikaty lub świadectwa kwalifikacyjne. Systemy i urządzenia powinny spełniać parametry określone w normie obronnej NO-04-A004 — Obiekty wojskowe. Systemy alarmowe.

3. W wartowniach obiektów, których ochrona jest wspomagana zewnętrznymi i wewnętrznymi systemami alarmowymi, należy utrzymywać grupę wartowników ze zmiany czuwającej lub patrol interwencyjny, w gotowości do natychmiastowego udania się w rejon naruszonego sektora ochranianego obiektu.

§ 9. 1. W jednostce organizacyjnej, w której są wytwarzane, przetwarzane, przechowywane lub przekazywane materiały niejawne, wydziela się strefy: administracyjną i bezpieczeństwa, a także określa pomieszczenia i obiekty (rejony) podlegające szczególnej ochronie.

2. Strefę bezpieczeństwa stanowi oznaczony i chroniony obszar, obiekt, fragment budynku, kompleks, jedno lub kilka pomieszczeń z ograniczoną liczbą wejść i wyjść, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę państwową lub służbową o klauzuli „poufne”.

3. Strefę administracyjną stanowi obszar przylegający do strefy bezpieczeństwa, w którym jest zapewniona kontrola ruchu osób i pojazdów.

4. W zależności od sposobu przetwarzania, wytwarzania, przechowywania i przekazywania informacji niejawnych w obszarach zaliczonych do strefy bezpieczeństwa, ustanawia się:

1) strefę bezpieczeństwa klasy I — jeżeli informacje niejawne stanowiące tajemnicę państwową lub służbową o klauzuli „poufne” są wytwarzane, przetwarzane, przechowywane lub przekazywane w taki sposób, że wejście do strefy praktycznie oznacza bezpośredni dostęp do tych informacji; w strefie tej mogą przebywać osoby posiadające poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyżej sklasyfikowanej informacji przechowywanej, przetwarzanej lub wytwarzanej w tym obszarze, z zastrzeżeniem ust. 5; wstęp osób niebędących żołnierzami albo pracownikami komórki organizacyjnej objętej strefą (interesantów) może nastąpić po uzyskaniu

zgody kierownika tej komórki i pod nadzorem upoważnionego przez niego żołnierza lub pracownika wojska, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie;

2) strefę bezpieczeństwa klasy II — jeżeli informacje niejawne stanowiące tajemnicę państwową lub służbową o klauzuli „poufne" są wytwarzane, przetwarzane, przechowywane albo przekazywane w taki sposób, że wejście do strefy nie jest równoznaczne z bezpośrednim dostępem do tych informacji; żołnierze i pracownicy wojska komórek organizacyjnych objętych strefą powinni posiadać poświadczenia bezpieczeństwa uprawniające co najmniej do dostępu do informacji niejawnych oznaczonych klauzulą „poufne"; osoby niebędące żołnierzami albo pracownikami jednostki lub komórki organizacyjnej (interesanci) mogą przebywać w tej strefie za zgodą kierownika komórki organizacyjnej objętej strefą lub upoważnionych przez niego osób i pod nadzorem żołnierza lub pracownika tej komórki, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie.

5. Personel sprzątający oraz techniczny wykonujący obowiązki służbowe w strefach bezpieczeństwa, o których mowa w ust. 4, powinien posiadać poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli co najmniej „poufne". Na czas sprzątania oraz wykonywania prac remontowych, użytkownicy pomieszczeń objętych strefą bezpieczeństwa mają obowiązek zabezpieczenia dokumentów niejawnych w sposób uniemożliwiający przypadkowe ujawnienie ich treści osobom nieuprawnionym; sprzątanie oraz wykonywanie prac remontowych w pomieszczeniach zaliczonych do strefy bezpieczeństwa klasy I może odbywać się jedynie w obecności użytkownika pomieszczenia.

6. W stosunku do osób pełniących służby wewnątrz strefy bezpieczeństwa klasy I przepis ust. 4 pkt 1 stosuje się odpowiednio.

7. Pomieszczenia i obiekty znajdujące się w strefie bezpieczeństwa klasy I zalicza się do pomieszczeń i obiektów podlegających szczególnej ochronie.

§ 10. 1. Dokumentami uprawniającymi do wejścia do strefy administracyjnej są: przepustki stałe, okresowe, jednorazowe, elektroniczne karty dostępu lub inne identyfikatory, imienne upoważnienia do wykonywania czynności kontrolnych, legitymacje służbowe pracowników Najwyższej Izby Kontroli, Państwowej Inspekcji Pracy, legitymacje poselskie lub senatorskie oraz zezwolenia stałe i jednorazowe wydawane przedstawicielom placówek dyplomatycznych państw obcych.

2. Dokumentami uprawniającymi do wjazdu na teren strefy administracyjnej są przepustki samochodowe lub rozkazy wyjazdu w odniesieniu do pojazdów pozostających na wyposażeniu danej jednostki organizacyjnej.

3. Dokumenty, o których mowa w ust. 1, uprawniają również do wejścia do strefy bezpieczeństwa klasy I i II, na zasadach określonych przez kierownika jednostki organizacyjnej.

4. Wejścia do strefy bezpieczeństwa oraz wyjścia z niej osób niebędących żołnierzami lub pracownikami jednostki albo komórki organizacyjnej (interesantów) powinny być rejestrowane, a ewidencja przechowywana przez co najmniej jeden rok.

§ 11. 1. Strefy bezpieczeństwa oznacza się w następujący sposób:

1) strefę bezpieczeństwa klasy I:

a) w przypadku pojedynczych pomieszczeń — tablicą w kształcie prostokąta o podstawie 19 cm i wysokości 13 cm z napisem koloru czarnego „Strefa bezpieczeństwa klasy I" o wysokości liter 1 cm na czerwonym tle,

b) w pozostałych przypadkach (obszar, obiekt, fragment budynku, kilka pomieszczeń) — linią ciągłą koloru czerwonego szerokości 10 cm oraz tablicą w kształcie prostokąta o podstawie 29,5 cm i wysokości 21 cm z napisem koloru czarnego „Strefa bezpieczeństwa klasy I" o wysokości liter 1,7 cm na czerwonym tle;

2) strefę bezpieczeństwa klasy II:

a) w przypadku pojedynczych pomieszczeń — tablicą w kształcie prostokąta o podstawie 19 cm i wysokości 13 cm z napisem koloru czarnego „Strefa bezpieczeństwa klasy II" o wysokości liter 1 cm na żółtym tle,

b) w pozostałych przypadkach (obszar, obiekt, fragment budynku, kilka pomieszczeń) — linią ciągłą koloru żółtego szerokości 10 cm oraz tablicą w kształcie prostokąta o podstawie 29,5 cm i wysokości 21 cm z napisem koloru czarnego „Strefa bezpieczeństwa klasy II" o wysokości liter 1,7 cm na żółtym tle.

2. Tablice, o których mowa w ust. 1, umieszcza się:

1) w przypadku pojedynczych pomieszczeń — na drzwiach wejściowych do tych pomieszczeń;

2) w pozostałych przypadkach (obszar, obiekt, fragment budynku, kilka pomieszczeń) — na drzwiach wejściowych do stref, na ścianach przy wejściu do stref lub na specjalnych stojakach.

3. Linie, o których mowa w ust. 1, maluje się przed wejściem do obszaru, obiektu lub fragmentu budynku na całej jego szerokości.

Rozdział 4

Planowanie ochrony jednostki organizacyjnej. Elementy planu ochrony

§ 12. 1. Ochrona jednostki organizacyjnej jest organizowana i realizowana na podstawie planu ochrony.

2. Plan ochrony jednostki organizacyjnej opracowuje pełnomocnik ochrony, w porozumieniu z kierownikami komórek organizacyjnych, a zatwierdza kierownik jednostki organizacyjnej. Planowi ochrony przyznaje się klauzulę tajności stosowną do treści zawartych w nim informacji.

§ 13. 1. Plan ochrony składa się z części graficznej i opisowej.

2. W części graficznej przedstawia się rozmieszczenie:

1) budynków służbowych i mieszkalnych, magazynów, garaży oraz innych urządzeń rozmieszczonych w ochranianym obiekcie; wszystkie budynki przedstawia się w formie rzutu płaskiego z góry i opisuje się je;

2) technicznych środków wspomagających ochronę obiektów, takich jak ogrodzenia, bramy, furtki, wieże wartownicze, oświetlenie zewnętrzne, umocnienia inżynieryjne, stanowiska ogniowe, urządzenia alarmowe i kontroli dostępu, kamery telewizyjne oraz środki łączności wykorzystywane przez siły ochronne i służby dyżurne;

3) posterunków wartowniczych, patroli i tras ich patrolowania oraz rejonów posterunków ochranianych przez psy wartownicze;

4) służb dyżurnych realizujących zadania ochronne;

5) stref: bezpieczeństwa i administracyjnej oraz pomieszczeń i obiektów (rejonów) podlegających szczególnej ochronie, a ponadto w formie tabeli przedstawia się podział sił i środków wydzielanych do ochrony jednostki organizacyjnej;

6) dróg oraz rejonów ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych, kancelariach tajnych-zagranicznych, kancelariach kryptograficznych, stacjach łączności kryptograficznej oraz pomieszczeniach wydzielonych.

3. Zestawienie podstawowych znaków umownych stosowanych w części graficznej planów ochrony zawiera załącznik do rozporządzenia.

4. Część graficzną planu ochrony wykonuje się w skali umożliwiającej naniesienie wszystkich elementów ochrony i urządzeń ją wspomagających. Z części graficznej musi jasno wynikać sposób ochrony jednostki organizacyjnej lub obiektów wchodzących w jej skład.

5. W części opisowej zawiera się:

1) charakterystykę jednostki organizacyjnej, a w niej:
   a) pełną nazwę jednostki organizacyjnej i jej rodzaj,
   b) opis położenia jednostki organizacyjnej i zajmowanego przez nią kompleksu (obiektu),
   c) opis otoczenia jednostki organizacyjnej, poczynając od strony północnej i następnie wschodniej, południowej i zachodniej,
   d) zaszeregowanie jednostki organizacyjnej pod względem ochrony do odpowiedniej kategorii;

2) analizę bezpieczeństwa i zagrożeń jednostki organizacyjnej z uwzględnieniem:
   a) zagrożeń zewnętrznych, takich jak wywiadowcze, terrorystyczne, dywersyjne i sabotażowe oraz kryminalne — na podstawie informacji uzyskanych od właściwych jednostek służb ochrony państwa, Żandarmerii Wojskowej i Policji,
   b) zagrożeń wewnętrznych związanych z ochroną przechowywanych informacji niejawnych i zabezpieczeniem broni, amunicji, materiałów wybuchowych, sprzętu specjalnego, a także ujawnionymi negatywnymi zjawiskami związanymi z tą problematyką;

3) ocenę aktualnego stanu ochrony jednostki organizacyjnej;

4) rodzaj, ilość i skład służb dyżurnych oraz zasady organizacji i wykonywania przez nie ochrony terenów, obiektów i mienia wojskowego;

5) rodzaj, ilość i skład sił ochronnych oraz zasady organizacji i wykonywania przez nie ochrony terenów, obiektów i mienia wojskowego, w tym także zasady dokonywania kontroli osobistej oraz przeglądania zawartości bagażu osobistego osób wchodzących i wychodzących oraz sprawdzania ładunków w środkach transportu wjeżdżających do i wyjeżdżających z obiektów wojskowych;

6) rodzaj oraz ilość uzbrojenia i wyposażenia sił ochronnych i służb dyżurnych, a także wyposażenie posterunków, stanowisk ogniowych i innych ukryć wykorzystywanych przez siły ochronne;

7) sposób zabezpieczenia broni i amunicji sił ochronnych i służb dyżurnych;

8) rodzaje zabezpieczeń technicznych wykorzystywanych w ochronie terenów, obiektów, mienia wojskowego oraz materiałów niejawnych;

9) określenie stref: administracyjnej i bezpieczeństwa oraz pomieszczeń i obiektów (rejonów) podlegających szczególnej ochronie, a także sposobu ich ochrony;

10) organizację systemu przepustkowego lub kontroli dostępu do obiektów i do poszczególnych stref oraz sposób przechowywania i zabezpieczenia kluczy użytku bieżącego i zapasowych, kodów do zamków szyfrowych oraz kodów systemów alarmowych do pomieszczeń i obiektów podlegających szczególnej ochronie, a także znajdujących się w nich urządzeń do przechowywania dokumentów niejawnych;

11) organizację systemu ochrony w godzinach służbowych, po godzinach służbowych oraz w dniach wolnych od zajęć służbowych;

12) sposób postępowania służb dyżurnych i sił ochronnych w sytuacjach kryzysowych;

13) sposób i organizację wzmocnienia systemu ochrony w sytuacjach kryzysowych oraz w przypadkach niesprawności technicznych środków wspomagających ochronę;

14) sposób współdziałania sił ochronnych z Żandarmerią Wojskową, Policją, jednostkami organizacyjnymi stacjonującymi w danym kompleksie (obiekcie) wojskowym oraz innymi organami porządkowymi, w tym alternatywne środki komunikacji i łączności;

15) organizację współdziałania z wojskowymi i cywilnymi służbami w zakresie ewakuacji personelu oraz pomocy medycznej;

16) siły i środki wydzielone do ewakuacji i zabezpieczenia dróg ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych, tajnych-zagranicznych, kryptograficznych, stacjach łączności kryptograficznej oraz pomieszczeniach wydzielonych;

17) inne ustalenia związane z ochroną obiektów, terenów i mienia wojskowego oraz materiałów niejawnych.

§ 14. 1. Plan ochrony obejmujący wszystkie ochraniane obiekty jednostki organizacyjnej przechowują pełnomocnik ochrony i oficer dyżurny jednostki organizacyjnej.

2. Wyciągi z planów ochrony dotyczące ochrony poszczególnych obiektów przechowuje się w wartowniach wart oraz w pomieszczeniach sił ochronnych i służb dyżurnych ochraniających dany obiekt.

3. Plan ochrony może być udostępniony, w niezbędnym zakresie, służbom dyżurnym (ochronnym) i osobom realizującym zadania przewidziane dla nich w tym planie, a także osobom kontrolującym.

§ 15. Pełnomocnik ochrony nadzoruje realizację planu ochrony oraz na bieżąco go aktualizuje, stosownie do pojawiających się zagrożeń lub potrzeb.

§ 16. 1. Bieżący nadzór nad ochroną jednostki organizacyjnej sprawuje etatowy lub nieetatowy komendant ochrony, wyznaczony spośród pracowników pionu ochrony jednostki organizacyjnej.

2. W jednostkach organizacyjnych, w których nie ma możliwości powołania komendanta ochrony spośród pracowników pionu ochrony, kierownik jednostki organizacyjnej wyznacza rozkazem dziennym lub decyzją osobę z innej komórki organizacyjnej, podporządkowując ją pod względem merytorycznym pełnomocnikowi ochrony jednostki organizacyjnej.

Rozdział 5

Przepis końcowy

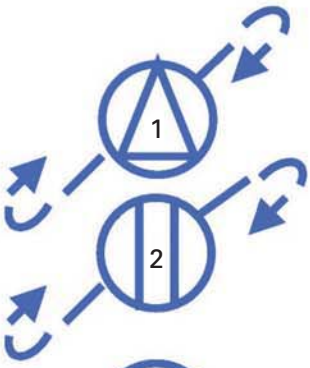
§ 17. Rozporządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Minister Obrony Narodowej: *J. Szmajdziński*

Załącznik do rozporządzenia Ministra Obrony Narodowej
z dnia 19 października 2005 r. (poz. 1821)

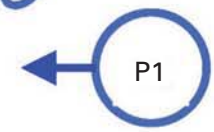
ZESTAWIENIE PODSTAWOWYCH ZNAKÓW UMOWNYCH STOSOWANYCH W CZĘŚCI GRAFICZNEJ PLANÓW OCHRONY

— **służby dyżurne** (**OD** — oficer dyżurny, **OP** — oficer dyżurny parku sprzętu technicznego, **DP** — dyżurny biura przepustek, **DT**— dyżurny punktu kontrolnego terenu technicznego, **PK** — podoficer dyżurny kompanii/baterii, **DS** — dowódca pogotowia ppoż.)

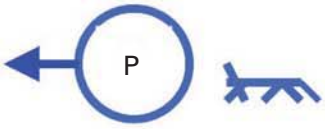


— rejon posterunku stałego trzyzmiennego — **nr 1**

— rejon posterunku stałego dwuzmiennego — **nr 2**

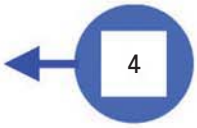


— posterunek ruchomy lub patrol **nr 1** (**P** — pieszy, **S** — na samochodzie, **M** — na motocyklu lub motorowerze, **R** — na rowerze)

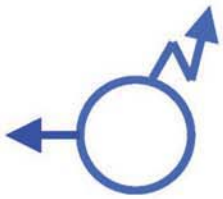


— patrol z psem wartowniczym

— rejon posterunku psa wartowniczego



— posterunek ruchomy lub patrol (**nr 4**) wystawiany doraźnie oraz podczas osiągania wyższych stanów gotowości bojowej



— posterunek ruchomy (patrol) z radiotelefonem lub z radiostacją

— ogrodzenie

— brama

— furtka

— wieża wartownicza

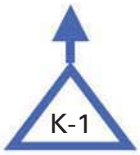
— punkt oświetlenia zewnętrznego

— chroniony budynek

— urządzenie alarmowe stosowane w ochronie zewnętrznej obiektu (budynku)

— urządzenie alarmowe stosowane w ochronie wewnętrznej obiektu (budynku)

— aparat telefoniczny lub miejsce do podłączenia urządzenia rozmównicze go



— radiotelefon bazowy dowódcy warty

— kamera telewizyjna

— zapory inżynieryjne (kozły)

— stanowisko ogniowe

— strefa bezpieczeństwa klasy I

— strefa bezpieczeństwa klasy II

— strefa administracyjna

— rejon szczególnej ochrony