ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 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) szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
2) miejsce i rolę Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocników ochrony kierowników bezpośrednio nadrzędnych jednostek organizacyjnych w resortowym systemie ochrony informacji niejawnych;
3) rodzaje, szczegółowe cele oraz sposób organizacji szkoleń z zakresu ochrony informacji niejawnych;
4) zakres, tryb i sposób współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych ze Służbą Kontrwywiadu Wojskowego, zwaną dalej „SKW”;
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) ustawa – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
2) Ministerstwo – Ministerstwo Obrony Narodowej;
3) 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;

4) jednostka organizacyjna – jednostkę nie wchodzącą w skład Ministerstwa, podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną, w tym przedsiębiorstwo państwowe, dla którego jest on organem założycielskim;

5) komórka organizacyjna – Sekretariat Ministra Obrony Narodowej, departament, zarząd, biuro - wchodzące w skład Ministerstwa;

6) kierownik jednostki organizacyjnej – dowódcę, szefa, dyrektora, komendanta, kierownika lub inną osobę, która kieruje całokształtem działalności tej jednostki, w tym również osobę czasowo pełniącą jego obowiązki;

7) kierownik komórki organizacyjnej – dyrektora, szefa, lub inną osobę kierującą całokształtem działalności tej komórki, w tym również osobę czasowo pełniącą jego obowiązki;

8) obszar chroniony – obszar objęty systemem kontroli dostępu lub systemem przepustkowym, znajdujący się poza strefami ochronnymi, w którym ruch osób i pojazdów odbywa się na podstawie dokumentów, o których mowa w § 17 niniejszego rozporządzenia;

9) pełnomocnik ochrony – pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych, w rozumieniu przepisu art. 14 ust. 2 ustawy;

10) pion ochrony – wyodrębnioną komórkę podległą pełnomocnikowi ochrony, wykonującą zadania określone w ustawie;

11) system ochrony informacji niejawnych - zespół przedsięwzięć organizacyjno-technicznych obejmujących: bezpieczeństwo osobowe, ochronę fizyczną i techniczną informacji niejawnych, obieg informacji niejawnych oraz bezpieczeństwo teleinformatyczne w jednostce organizacyjnej.

Rozdział 2
Szczegółowe zadania pełnomocników ochrony kierowników jednostek organizacyjnych

§ 3. 1. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych realizuje w Ministerstwie zadania określone w § 4 oraz koordynuje i nadzoruje realizację przedsięwzięć przez pełnomocników ochrony w zakresie ochrony informacji niejawnych, w celu zapewnienia jednolitego i skutecznego systemu ochrony informacji niejawnych w jednostkach organizacyjnych i jest uprawniony do:

1) określania, w porozumieniu z Szefem SKW, propozycji dotyczących kierunków działania i zasadniczych zadań dla pionów ochrony jednostek organizacyjnych oraz przedkładania ich do akceptacji Ministrowi Obrony Narodowej;

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

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

4) opiniowania projektów dokumentów decyzyjnych i rozkazodawczych regulujących problematykę ochrony informacji niejawnych, wydawanych przez kierowników jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa i kierownikom komórek organizacyjnych;

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

6) opracowywania, w porozumieniu z Szefem SKW, programów szkolenia specjalistycznego dla osób pełniących służbę lub zatrudnionych w kancelariach tajnych oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, a także kandydatów na te stanowiska;

7) organizowania szkolenia:

   a) określonego w art. 19 ust. 2 pkt 1 i 2 ustawy, prowadzonego przez SKW, dla osób z jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa oraz kierownikom komórek organizacyjnych, z wyłączeniem dowództw rodzajów Sił Zbrojnych (równorzędnych), Inspektoratu Wsparcia Sił Zbrojnych, Inspektoratu Uzbrojenia, Inspektoratu Wojskowej Służby Zdrowia, Komendy Głównej Żandarmerii Wojskowej, Dowództwa Garnizonu Warszawa i podległych im jednostek organizacyjnych, a także 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 jednostkach organizacyjnych, o których mowa w lit. a,

   c) specjalistycznego dla osób pełniących służbę lub zatrudnionych w kancelariach tajnych, tajnych zagranicznych (międzynarodowych) oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, a także kandydatów na te stanowiska z jednostek organizacyjnych, o których mowa w lit. a;

8) wydawania, stosownie do potrzeb, specjalistycznych wytycznych do działalności pionów ochrony jednostek organizacyjnych;

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

10) rozliczania funkcjonalnego pełnomocników ochrony kierowników jednostek organizacyjnych, o których mowa w pkt 4;

11) uzgadniania rocznych planów zasadniczych przedsięwzięć jednostek organizacyjnych, o których mowa w pkt 4, w zakresie zamierzeń realizowanych przez piony ochrony tych jednostek;

12) 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 4;

13) wydawania opinii w sprawach dotyczących ochrony informacji niejawnych;

14) 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 uprawnieni 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 dowódców rodzajów Sił Zbrojnych, Inspektoratu Wsparcia Sił Zbrojnych, Inspektoratu Uzbrojenia, Inspektoratu Wojskowej Służby Zdrowia, Dowódcy Garnizonu Warszawa, Komendanta Głównego Żandarmerii Wojskowej, niezależnie od przedsięwzięć wyszczególnionych w ust. 2, organizują szkolenie:

1) określone w art. 19 ust. 2 pkt 1 i 2 ustawy, prowadzone przez SKW, wobec osób z podporządkowanych jednostek organizacyjnych;

2) specjalistyczne z zakresu bezpieczeństwa teleinformatycznego, prowadzonego przez SKW dla inspektorów bezpieczeństwa

teleinformatycznego i administratorów systemu teleinformatycznego pełniących służbę lub zatrudnionych w jednostkach organizacyjnych, o których mowa pkt 1;

3) specjalistyczne dla osób pełniących służbę lub zatrudnionych w kancelariach tajnych, tajnych zagranicznych (międzynarodowych) oraz innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, a także kandydatów na te stanowiska z jednostek organizacyjnych, o których mowa w pkt 1.

§ 4. 1. Do szczegółowych zadań pełnomocnika ochrony należy zapewnienie ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych w jednostce organizacyjnej, a zwłaszcza:

1) opracowywanie i przedstawianie do akceptacji kierownikowi jednostki organizacyjnej projektów dokumentów normujących ochronę informacji niejawnych w jednostce organizacyjnej, a w tym:

   a) sposobu i trybu 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,

   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 planu postępowania z tymi materiałami 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) współudział w realizacji zadań związanych z akredytacją bezpieczeństwa systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych;

4) prowadzenie kontroli stanu zabezpieczenia informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w jednostce organizacyjnej;

5) organizowanie i nadzorowanie przebiegu kontroli okresowych ewidencji, materiałów i obiegu dokumentów w jednostce organizacyjnej;

6) prowadzenie zwykłych i kontrolnych postępowań sprawdzających;

7) prowadzenie 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;

8) prowadzenie wykazu osób, które uzyskały pisemną zgodę na udostępnienie informacji niejawnych na podstawie art. 21 ust. 4 pkt 1, art. 34 ust. 5 i 9 oraz art. 54 ust. 7 i 8 ustawy;

9) opracowywanie planów szkolenia oraz organizacja szkolenia z zakresu ochrony informacji niejawnych dla osób pełniących służbę lub zatrudnionych w jednostce organizacyjnej;

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

11) zapewnienie obsługi kancelaryjnej w jednostce organizacyjnej;

12) sprawowanie nadzoru nad funkcjonowaniem kancelarii tajnej, kancelarii tajnej zagranicznej (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;

15) podejmowanie działań zmierzających do ograniczenia skutków naruszenia przepisów o ochronie informacji niejawnych;

16) zapewnienie bezpieczeństwa fizycznego informacji niejawnych w jednostce organizacyjnej, a 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;

17) zapewnienie właściwej ochrony informacji niejawnych podczas ćwiczeń, treningów sztabowych, narad, odpraw i szkoleń oraz ochrony pomieszczeń, w których są one prowadzone;

18) prowadzenie wykazu umów i zadań związanych z dostępem do informacji niejawnych realizowanych przez przedsiębiorców na rzecz jednostki organizacyjnej;

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

20) 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;

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

2. Ewidencję określoną w ust. 1 pkt 7, 8, 18 prowadzi się w formie papierowej lub elektronicznej.

3. Powierzenie pełnomocnikowi ochrony realizacji innych, niewynikających z przepisów ustawy zadań, pod warunkiem, że nie spowoduje naruszenia prawidłowego wykonywania przedsięwzięć, o których mowa w § 3 ust. 2 i 3 oraz § 4 ust. 1, wymaga uzyskania opinii Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

Rozdział 3
Zakres tryb i sposób współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych z właściwymi jednostkami organizacyjnymi SKW

§ 5. 1. Współdziałanie pełnomocników ochrony z właściwymi jednostkami i komórkami organizacyjnymi SKW dotyczy realizacji zadań określonych w ustawie oraz zadań wynikających z innych przepisów regulujących problematykę ochrony informacji niejawnych.

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

1) bezpośrednich albo korespondencyjnych kontaktów utrzymywanych przez pełnomocników ochrony z właściwymi kierownikami jednostek lub komórek organizacyjnych SKW;

2) bieżących konsultacji dotyczących wspólnych obszarów działania;

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

3. Współdziałanie pełnomocników ochrony z SKW jest realizowane poprzez:

1) udostępnianie pełnomocnikom ochrony przez właściwe jednostki SKW materiałów informacyjnych o zagrożeniach mogących mieć wpływ na bezpieczeństwo informacji niejawnych przetwarzanych w jednostkach organizacyjnych;

2) przekazywanie pełnomocnikom ochrony 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) przekazywanie przez SKW Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych wyników inspekcji przeprowadzonych przez przedstawicieli organów bezpieczeństwa NATO i UE w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

4) udostępnianie przez SKW pełnomocnikom ochrony dokumentów regulujących problematykę ochrony informacji niejawnych w NATO i UE oraz tłumaczeń tych dokumentów;

5) udostępnianie przez pełnomocników ochrony upoważnionym przedstawicielom SKW, pozostających w ich dyspozycji informacji i dokumentów niezbędnych do przeprowadzenia czynności realizowanych w ramach postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego;

6) wzajemne informowanie się o toczących się postępowaniach karnych przeciwko posiadającym poświadczenia bezpieczeństwa osobom pełniącym służbę lub zatrudnionym w jednostce organizacyjnej oraz osobom, w stosunku do których prowadzone są postępowania sprawdzające, w sprawach o przestępstwa umyślne ścigane z oskarżenia publicznego, a także o przypadkach skazania prawomocnym wyrokiem za wyżej wymienione przestępstwa;

7) zapraszanie przedstawicieli SKW do udziału w prowadzonych przez pełnomocników ochrony szkoleniach oraz odprawach rozliczeniowo-zadaniowych dla pracowników pionów ochrony;

8) wzajemne przekazywanie danych osób, które w wyniku przeprowadzonych postępowań sprawdzających lub kontrolnych postępowań sprawdzających otrzymały:

   a) poświadczenie bezpieczeństwa,

   b) decyzję o odmowie wydania poświadczenia bezpieczeństwa,

   c) decyzję o cofnięciu posiadanego poświadczenia bezpieczeństwa;

9) 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;

10) informowanie SKW przez pełnomocników ochrony 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;

11) informowanie SKW przez pełnomocników ochrony o przypadkach naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych o klauzuli „poufne” lub wyższej;

12) przekazywanie Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych do zaopiniowania 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;

13) inicjowanie wspólnych działań zmierzających do poprawy bezpieczeństwa informacji niejawnych.

Rozdział 4
Szkolenie w zakresie ochrony informacji niejawnych

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

1) podstawowe;

2) uzupełniające;

3) specjalistyczne.

§ 7. 1. Celem szkolenia podstawowego jest zapoznanie żołnierzy zawodowych, członków korpusu służby cywilnej oraz pracowników wojska z tematyką określoną w art. 19 ust. 1 ustawy, instrukcją dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” oraz sposobem i trybem przetwarzania informacji niejawnych o klauzuli „poufne” w jednostce organizacyjnej. W przypadku przetwarzania w jednostce organizacyjnej niejawnych pochodzących z wymiany międzynarodowej szkolenie podstawowe powinno obejmować również zasady ochrony informacji niejawnych NATO i UE.

2. Szkolenie podstawowe organizuje i przeprowadza pełnomocnik ochrony lub inne wyznaczone przez niego osoby spośród personelu pionu ochrony.

3. Osoby zajmujące kierownicze stanowiska Ministerstwa, kierownicy komórek organizacyjnych oraz kierownicy jednostek organizacyjnych są zobowiązani kierować podległych sobie żołnierzy, pracowników korpusu służby cywilnej i pracowników wojska do pionów ochrony, w celu odbycia przez nich szkolenia podstawowego.

4. Szkolenie podstawowe kończy się wydaniem przez pełnomocnika ochrony zaświadczenia, którego wzór określa rozporządzenie Prezesa Rady Ministrów wydane na podstawie art. 20 ust. 2 pkt 1 ustawy.

5. Osoba przeszkolona składa pełnomocnikowi ochrony pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych oraz o odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie w szczególności za nieuprawnione ujawnienie informacji niejawnych; wzór oświadczenia określa załącznik Nr 1 do niniejszego rozporządzenia.

6. Pełnomocnik ochrony prowadzi ewidencję wydanych zaświadczeń, której wzór zawiera załącznik Nr 2 do niniejszego rozporządzenia oraz przechowuje oświadczenia, o których mowa w ust. 5.

7. Ewidencję, o której mowa w ust. 6, prowadzi się w cyklu rocznym, rozpoczynając każdego roku kalendarzowego numerowanie od liczby „1”, przy czym numer zaświadczenia odpowiada numerowi pozycji w ewidencji oddzielonej myślnikiem od oznaczenia cyfrowego miesiąca i roku kalendarzowego, w którym zostało wydane (przykładowo 21-04-2011, gdzie liczba 21 odpowiada numerowi pozycji w ewidencji, liczba 04 miesiącowi, natomiast liczba 2011 oznacza rok).

8. W przypadku zagubienia lub utraty zaświadczenia, o którym mowa w ust. 4, pełnomocnik ochrony na pisemny wniosek osoby zainteresowanej, wydaje jego wtórnik zachowując numer oryginału zaświadczenia. W dolnej części dokumentu pośrodku zamieszcza się napis „WTÓRNIK”.

9. W przypadku zmiany danych personalnych, pełnomocnik ochrony na pisemny wniosek osoby zainteresowanej, wydaje nowe zaświadczenie, zawierające zmienione dane personalne, zachowując jego dotychczasowy numer.

§ 8. 1. Celem szkolenia uzupełniającego jest podtrzymanie 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 zmiany 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 uzupełniające dla osób pełniących służbę lub zatrudnionych w komórkach organizacyjnych prowadzi, w przypadkach, o których mowa w ust. 2, w terminach zaplanowanych przez kierowników tych komórek, Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych lub wyznaczone przez niego osoby z Departamentu Ochrony Informacji Niejawnych.

§ 9. Za opracowanie planu szkolenia podstawowego i uzupełniającego oraz prowadzenie ewidencji wydanych zaświadczeń, o której mowa w § 7 ust. 6, odpowiada pełnomocnik ochrony.

§ 10. 1. Szkoleniem specjalistycznym obejmuje się osoby przewidziane do objęcia stanowiska lub pełnienia funkcji:

1) pełnomocnika ochrony i zastępcy pełnomocnika ochrony;
2) administratora systemu teleinformatycznego;
3) pracownika pionu ochrony pełniącego funkcję inspektora bezpieczeństwa teleinformatycznego;
4) kierownika, zastępcy kierownika i kancelisty kancelarii tajnej, tajnej zagranicznej (międzynarodowej) oraz innych niż kancelaria tajna komórek odpowiedzialnych za przetwarzanie informacji niejawnych.

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

3. Programy szkolenia specjalistycznego osób, o których mowa w ust. 1 pkt 1-3, opracowuje SKW.

4. Program szkolenia specjalistycznego osób, o których mowa w ust.1 pkt 4, opracowuje Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych w porozumieniu z SKW i przekazuje go odpowiednio osobom, o których mowa w § 3 ust. 3.

5. Potrzeby w zakresie szkolenia osób, o których mowa w ust. 1 na rok następny, zgłaszają na wnioskach według wzoru zawartego w załącznikach Nr 3-5 do rozporządzenia corocznie do dnia 31 października:

1) Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych:
   a) kierownicy komórek organizacyjnych,

b) kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa 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.

6. Sporządzone na podstawie zapotrzebowań, zgodnie z wzorem zawartym w załączniku Nr 6 do niniejszego rozporządzenia, listy uczestników szkoleń, o których mowa w ust. 1 pkt 1-3, są przekazywane SKW celem ewidencji i weryfikacji.

7. Szkolenie specjalistyczne, o którym mowa w ust. 1 pkt 1-3, organizuje Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocnicy ochrony wymienieni w § 3 ust. 3, natomiast zajęcia szkoleniowe prowadzą żołnierze, funkcjonariusze lub pracownicy SKW.

8. Szkolenie specjalistyczne, o którym mowa w ust. 1 pkt 4 organizują i prowadzą Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocnicy ochrony wymienieni § 3 ust. 3.

9. Terminy szkoleń, o których mowa w ust. 1 ustala się do 30 listopada roku kalendarzowego na rok następny i przesyła do pełnomocników ochrony wymienionych w § 3 ust. 3.

10. W uzasadnionych przypadkach szkolenie specjalistyczne może być organizowane w trybie roboczym z pominięciem terminów wyszczególnionych w ust. 5 i 9.

11. SKW potwierdza odbycie szkolenia specjalistycznego przez osoby, o których mowa w ust. 1 pkt 1- 3, wydaniem zaświadczenia.

12. Ukończenie szkolenia specjalistycznego przez osoby, o których mowa w ust. 1 pkt 4, pełnomocnicy ochrony dokumentują wydaniem zaświadczenia, według wzoru określonego w załączniku Nr 7 do rozporządzenia.

13. Do zaświadczeń, o których mowa w ust. 12, stosuje się odpowiednio przepisy § 7 ust. 6-9.

Rozdział 5
Szczególne wymagania w zakresie stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych

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

§ 12. 1. System ochrony informacji niejawnych w jednostce organizacyjnej realizuje się poprzez zastosowanie odpowiednich do poziomu zagrożeń środków bezpieczeństwa fizycznego oraz organizację systemu przepustkowego. Do środków bezpieczeństwa fizycznego zalicza się ochronę fizyczną i techniczne środki ją wspomagające.

2. Ochronę fizyczną stanowią warty wojskowe, oddziały wart cywilnych zwane dalej OWC, specjalistyczne uzbrojone formacje ochronne, zwane dalej SUFO, oraz służby dyżurne realizujące zadania ochronne w jednostce organizacyjnej lub w konwoju, a także portierzy i dozorcy.

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. Ochrona fizyczna informacji niejawnych powinna być wspomagana technicznymi środkami, które stanowią 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. Zakres stosowania środków bezpieczeństwa fizycznego powinien być dostosowany do poziomu zagrożenia nieuprawnionego dostępu do informacji niejawnych lub ich utraty, wynikającego z przeprowadzonej analizy.

3. Zastosowane w ochronie informacji niejawnych systemy powinny posiadać deklarację zgodności, natomiast urządzenia wykorzystane do ich budowy odpowiednie certyfikaty. Systemy i urządzenia alarmowe powinny spełniać wymagania określone w Normie Obronnej NO-04-A004 – Obiekty wojskowe. Systemy alarmowe.

4. Zainstalowane systemy i urządzenia alarmowe powinny być remontowane, konserwowane i poddawane 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 materiały niejawne, tworzy się strefy ochronne, które stanowią oznaczony obszar, obiekt, kompleks, budynek, a także fragment budynku, jedno lub kilka pomieszczeń, w których są przetwarzane informacje niejawne o klauzuli „poufne” lub wyższej, poddane kontroli wejść i wyjść oraz kontroli przebywania.

2. Organizuje się następujące strefy ochronne:

1) strefa I, w której przebywanie wiąże się z możliwością bezpośredniego dostępu do informacji niejawnych o klauzuli „ściśle tajne” lub „tajne”, 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) nie będących 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,

c) w strefie tej materiały niejawne oznaczone klauzulą „ściśle tajne" lub „tajne" można przechowywać poza szafami metalowymi;

2) strefa II, w której przebywanie nie wiąże się z bezpośrednim dostępem do informacji niejawnych o klauzuli „ściśle tajne" lub „tajne";

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) nie będących 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,

c) materiały niejawne należy przechowywać w urządzeniach odpowiedniej klasy, stosownie do klauzuli zawartych w tych materiałach informacji niejawnych;

3) strefa III, w której przebywanie nie wiąże się z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne" lub „tajne" oraz nie wiąże się z bezpośrednim dostępem do informacji niejawnych oznaczonych klauzulą „poufne", 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) nie będących 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,

c) materiały niejawne należy przechowywać w urządzeniach odpowiedniej klasy, stosownie do klauzuli zawartych w tych materiałach informacji niejawnych.

3. Wejście do stref ochronnych, następuje wyłącznie z obszaru chronionego.

4. Na czas sprzątania i wykonywania prac remontowych użytkownicy pomieszczeń objętych strefą ochronną mają obowiązek zabezpieczenia dokumentów niejawnych 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.

5. W przypadku, gdy prace, o których mowa w ust. 4, wiążą się z bezpośrednim dostępem do informacji niejawnych, personel sprzątający lub techniczny powinien 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, powinien on posiadać stosowne świadectwo bezpieczeństwa przemysłowego.

6. W stosunku do osób pełniących służby dyżurne i ochronne wewnątrz strefy I i II, przepisy ust. 2 pkt 1 i 2 stosuje się odpowiednio, natomiast osoby pełniące służbę ochronną w strefie III powinny posiadać poświadczenia bezpieczeństwa uprawniające, co najmniej do dostępu do informacji niejawnych oznaczonych klauzulą „poufne” lub pisemne upoważnienie kierownika jednostki organizacyjnej, o którym mowa w art. 21 ust. 4 pkt 1 ustawy.

7. Kryteria tworzenia stref ochronnych określa załącznik Nr 8 do rozporządzenia.

8. Szczegółowe wymagania w zakresie stosowania środków bezpieczeństwa fizycznego oraz zabezpieczenia przed podsłuchem i podglądem w przypadku pomieszczeń przeznaczonych do omawiania informacji niejawnych oznaczonych klauzulami „ściśle tajne” i „tajne” określają odrębne przepisy.

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

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 1 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 1 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 1 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 poprzez 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 obszaru chronionego tworzy się system przepustkowy. Obejmuje on przepustki stałe, okresowe, jednorazowe, elektroniczne karty dostępu lub inne identyfikatory, imienne upoważnienia do wykonywania czynności kontrolnych, legitymacje poselskie lub senatorskie oraz 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.

2. Bieżący nadzór nad funkcjonowaniem systemu przepustkowego sprawuje dyżurny (obsada) biura przepustek.

3. W skład obsady biura przepustek mogą wchodzić żołnierze, pracownicy wojska, pracownicy ochrony OWC lub SUFO.

4. Wejście do obszaru chronionego może odbywać 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. 1;

4) zezwoleń stałych lub jednorazowych wydawanych cudzoziemcom.

5. Wjazd do obszaru chronionego może odbywać 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 wojskowej (kompleksu, obiektu) lub kierownik jednostki (komórki) organizacyjnej.

6. Zasady funkcjonowania systemu przepustkowego, a także wydawania i ewidencji wyżej wymienionych dokumentów określa Minister Obrony Narodowej.

7. Do wejścia lub wjazdu bez przepustki do obszaru chronionego 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, wodnokanalizacyjnych itp., a także funkcjonariusze Policji lub żołnierze Żandarmerii Wojskowej w przypadku wykonywania zadań związanych z bezpieczeństwem i ochroną porządku publicznego

8. W sytuacjach określonych w ust. 7 strażakom, pracownikom pogotowia, funkcjonariuszom Policji lub żołnierzom Żandarmerii Wojskowej powinny towarzyszyć służby dyżurne lub siły ochronne jednostek (komórek) organizacyjnych.

9. Dokumenty, o których w ust. 1, uprawniają również do wejścia do stref ochronnych na zasadach określonych przez kierownika jednostki organizacyjnej.

Rozdział 6
Planowanie ochrony informacji niejawnych. Elementy planu ochrony informacji niejawnych, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego

§ 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, zwanego dalej „planem ochrony informacji niejawnych”.

2. Plan ochrony informacji niejawnych opracowuje i aktualizuje na bieżąco pełnomocnik ochrony, w porozumieniu z kierownikami komórek wewnętrznych jednostki organizacyjnej.

3. Plan, o którym mowa w ust. 1, podlega zatwierdzeniu przez kierownika jednostki organizacyjnej.

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

2. W części graficznej przedstawia się w szczególności rozmieszczenie:

1) budynków (pomieszczeń), z wyróżnieniem tych, w których są przetwarzane materiały niejawne. Wszystkie budynki przedstawia się w formie rzutu płaskiego z góry i opisuje się je;

2) technicznych środków wspomagających ochronę fizyczną informacji niejawnych;

3) stref ochronnych;

4) dróg oraz rejonów ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych, tajnych zagranicznych (międzynarodowych) oraz innych komórek 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 zawiera załącznik Nr 9 do rozporządzenia.

4. Część graficzną planu ochrony informacji niejawnych wykonuje się w skali umożliwiającej naniesienie wszystkich elementów ochrony i urządzeń ją wspomagających. Z części graficznej musi jasno wynikać sposób ochrony informacji niejawnych w jednostce organizacyjnej.

5. W części opisowej 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 „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 materiałów niejawnych;

4) opis granic obszaru chronionego, 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, w tym w razie wprowadzenia stanu nadzwyczajnego;

9) siły i środki wydzielone do ewakuacji i zabezpieczenia dróg ewakuacji materiałów niejawnych przechowywanych w kancelariach tajnych, tajnych zagranicznych (międzynarodowych) oraz innych komórek 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, a także w sytuacjach awaryjnych takich jak klęska żywiołowa, katastrofa naturalna lub awaria techniczna, a w tym:

   a) sposób postępowania sił ochronnych w poszczególnych stanach,

   b) sposób i organizację wzmocnienia systemu ochrony informacji niejawnych 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 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;

13) inne ustalenia związane z ochroną informacji niejawnych.

§ 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 odpowiada za realizację planu ochrony informacji niejawnych oraz na bieżąco go aktualizuje, stosownie do pojawiających się zagrożeń lub potrzeb.

2. Pełnomocnik ochrony, w zakresie realizacji zadań wynikających z planu ochrony informacji niejawnych, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego, ma prawo żądać od innych osób funkcyjnych udzielenia natychmiastowej pomocy.

Rozdział 7
Przepis końcowy

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

MINISTER OBRONY NARODOWEJ

Bogdan KLICH

[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).

UZASADNIENIE

Konieczność zmiany dotychczasowych przepisów jest konsekwencją wejścia w życie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228). Projekt rozporządzenia stanowi wykonanie przez Ministra Obrony Narodowej delegacji zawartej w art. 18 powołanej powyżej ustawy.

Zgodnie z art. 18 ust. 1 ustawy w przedłożonym projekcie uregulowano następującą problematykę:

1) w § 3 określono:

   a) zadania Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, wynikające z art. 18 ust. 2 ustawy, związane z koordynowaniem i nadzorowaniem realizacji przedsięwzięć dotyczących ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, osobom zajmującym kierownicze stanowiska Ministerstwa oraz kierownikom komórek organizacyjnych,

   b) zadania pełnomocników ochrony dowódców rodzajów Sił Zbrojnych (równorzędnych) i innych osób funkcyjnych, którym podporządkowano jednostki organizacyjne dotyczące koordynowania i nadzorowania realizacji przedsięwzięć w zakresie ochrony informacji niejawnych przez piony ochrony jednostek organizacyjnych podległych tym osobom.

2) w § 4 sprecyzowano szczegółowe zadania pełnomocników ochrony dowódców jednostek organizacyjnych związane z zapewnieniem w jednostkach organizacyjnych właściwego zabezpieczenia informacji niejawnych oraz przestrzegania przepisów w tym zakresie;

3) w § 5 określono zasady współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych w właściwymi jednostkami organizacyjnymi Służby Kontrwywiadu Wojskowego;

4) w § 6-10 określono rodzaje szkolenia w zakresie ochrony informacji niejawnych, a także zasady jego organizowania, prowadzenia i dokumentowania przez pełnomocników ochrony;

5) w § 11-15 sprecyzowano szczególne wymagania w zakresie stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych. Określono definicje stref ochronnych, sposoby oznaczania stref ochronnych, a także zasady wchodzenia i wjazdu na teren tych stref;

6) w § 15 ust. 8 wskazano, iż stosowanie środków bezpieczeństwa fizycznego oraz zabezpieczenia przed podsłuchem i podglądem w przypadku pomieszczeń przeznaczonych do omawiania informacji niejawnych oznaczonych klauzulami „ściśle tajne” i „tajne” określą odrębne przepisy. Regulacje takie zostaną opracowane przez SKW w postaci zaleceń;

7) w § 17 sprecyzowano oznaczenie stref ochronnych;

8) w § 16 zdefiniowano system przepustkowy;

9) w §18-21 określono 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.

W projekcie rozporządzenia, niezależnie od zmian wynikających z wprowadzenia przepisów nowej ustawy o ochronie informacji niejawnych, uwzględniono zmiany, które zaszły w ostatnim czasie w przepisach o ochronie obiektów wojskowych, a także przekształcenia wynikające z profesjonalizacji i restrukturyzacji Sił Zbrojnych.

Projekt rozporządzenia nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych, ponieważ nie zawiera przepisów technicznych.

Zakres projektu rozporządzenia nie jest objęty prawem Unii Europejskiej.

Projekt rozporządzenia nie podlega notyfikacji zgodnie z procedurą określoną w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039, z późn. zm.).

OCENA SKUTKÓW REGULACJI

1. **Podmioty, na które oddziałuje projekt aktu prawnego**
   Projekt dotyczy wyłącznie jednostek organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)

2. **Konsultacje społeczne**
   Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414, z późn. zm.) projekt zostanie udostępniony
   w Biuletynie Informacji Publicznej na stronie internetowej Ministerstwa Obrony Narodowej.

3. **Wpływ regulacji na dochody i wydatki budżetu oraz sektor finansów publicznych**
   Wejście w życie projektowanego rozporządzenia nie spowoduje dodatkowych skutków finansowych dla budżetu państwa.

4. **Wpływ regulacji na rynek pracy**
   Regulacja nie będzie miała wpływu na rynek pracy.

5. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw**
   Projektowane rozporządzenie nie będzie miało wypływu na konkurencyjność gospodarki i przedsiębiorczość.

6. **Wpływ regulacji na sytuację i rozwój regionów**
   Projektowane rozporządzenie nie będzie miało wpływu na sytuację i rozwój regionów.

Za zgodność pod względem
prawnym i redakcyjnym

Załącznik Nr 1 do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

.....
miejscowość, data

OŚWIADCZENIE

Oświadczam, że na podstawie art. 19 ust.1, w związku z art. 20 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) zostałem / zostałam***** zapoznany / zapoznana***** z przepisami:

- o ochronie informacji niejawnych**, ***
- o ochronie informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, *****
- o ochronie informacji niejawnych Unii Europejskiej, *****

oraz o odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, a w szczególności za nieuprawnione ujawnienie informacji niejawnych.

…….....
PESEL, czytelny podpis osoby przeszkolonej

Numer zaświadczenia o przeszkoleniu ……

*** - niepotrzebne skreślić**

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

REJESTR WYDANYCH ZAŚWIADCZEŃ

Układ strony lewej

Lp.	Stopień	Imię i nazwisko	Numer PESEL	Komórka organizacyjna
1	2	3	4	5

Układ strony prawej

Nr zaświadczenia	Data szkolenia	Rodzaj szkolenia	Uwagi
6	7	8	9

Załącznik Nr 3 do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

pieczęć nagłówkowa jednostki (komórki) organizacyjnej miejscowość, data.

WNIOSEK

o zakwalifikowanie na szkolenie specjalistyczne
dla administratora systemu / inspektora
bezpieczeństwa teleinformatycznego * Pana (Pani):

.....
stopień, imię i nazwisko

.....
PESEL, miejsce urodzenia, imię ojca

.....
aktualne miejsce pracy (służby)

.....
nr poświadczenia bezpieczeństwa, klauzula i data jego ważności

.....
obywatelstwo, wykształcenie

Niniejszym oświadczam, że kandydat jest przewidziany przez kierownika jednostki organizacyjnej do objęcia stanowiska lub pełnienia funkcji administratora systemu / inspektora bezpieczeństwa teleinformatycznego*.

.....
podpis kierownika jednostki (komórki) organizacyjnej

Załącznik: poświadczona za zgodność kserokopia poświadczenia bezpieczeństwa.

* - niepotrzebne skreślić

Załącznik Nr 4 do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

pieczęć nagłówkowa jednostki (komórki) organizacyjnej miejscowość, data.

WNIOSEK

o zakwalifikowanie na szkolenie specjalistyczne
dla kandydatów na pełnomocników do spraw ochrony informacji niejawnych Pana (Pani):

.....
stopień, imię i nazwisko

.....
PESEL, miejsce urodzenia, imię ojca

.....
aktualne miejsce pracy (służby)

.....
nr poświadczenia bezpieczeństwa, klauzula i data jego ważności

.....
obywatelstwo, wykształcenie

Niniejszym oświadczam, że kandydat:

1) jest przewidziany przez kierownika jednostki organizacyjnej do objęcia stanowiska lub pełnienia funkcji pełnomocnika / zastępcy pełnomocnika do spraw ochrony informacji niejawnych*.
2) pełni funkcję pełnomocnika / zastępcy pełnomocnika do spraw ochrony informacji niejawnych*

.....
podpis kierownika jednostki (komórki) organizacyjnej

Załącznik: poświadczona za zgodność kserokopia poświadczenia bezpieczeństwa wydanego przez SKW lub ABW.

* - niepotrzebne skreślić

Załącznik Nr 5 do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

pieczęć nagłówkowa jednostki (komórki) organizacyjnej miejscowość, data.

WNIOSEK

o zakwalifikowanie na szkolenie specjalistyczne
dla kierowników, zastępców kierowników i kancelistów kancelarii tajnych, tajnych zagranicznych (międzynarodowych) oraz innych niż kancelaria tajna komórek wewnętrznych lub organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i wydawanie materiałów niejawnych Pana (Pani):

.....
stopień, imię i nazwisko

.....
PESEL, miejsce urodzenia, imię ojca

.....
aktualne miejsce pracy (służby)

.....
nr poświadczenia bezpieczeństwa, klauzula i data jego ważności

.....
obywatelstwo, wykształcenie

Niniejszym oświadczam, że kandydat jest przewidziany przez kierownika jednostki organizacyjnej do objęcia stanowiska lub pełnienia funkcji kierownika / zastępcy kierownika / kancelisty kancelarii tajnej / tajnej zagranicznej (międzynarodowej) / innej niż kancelaria tajna komórki wewnętrznej lub organizacyjnej odpowiedzialnej za rejestrowanie, przechowywanie, obieg i wydawanie materiałów niejawnych*.

.....
podpis kierownika jednostki (komórki) organizacyjnej

Załącznik: poświadczona za zgodność kserokopia poświadczenia bezpieczeństwa.

* - niepotrzebne skreślić

Załącznik Nr 6 do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

LISTA UCZESTNIKÓW SZKOLENIA SPECJALISTYCZNEGO PROWADZONEGO PRZEZ SŁUŻBĘ KONTRWYWIADU WOJSKOWEGO

DLA .....

Termin : .....

Miejsce: .....

Lp.	Stopień	Imię	Nazwisko	Miejsce pełnienia służby (pracy)	PESEL, miejsce urodzenia, imię ojca	Nr poświadczenia bezpieczeństwa, klauzula, data ważności	Uwagi
1.							
2.							
3.							
4.							
5.							
6.							
KONIEC							

Załącznik Nr 7do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

pieczęć nagłówkowa jednostki (komórki) organizacyjnej

ZAŚWIADCZENIE Nr .....

stwierdzające odbycie szkolenia specjalistycznego w zakresie ochrony informacji niejawnych.

Stwierdza się, że Pan(i):

- imię i nazwisko: .....
- data urodzenia: .....

odbył(a) w dniach ..... w .....
(nazwa jednostki organizacyjnej)

szkolenie specjalistyczne dla kierowników, zastępców kierowników i kancelistów kancelarii tajnych, tajnych zagranicznych (międzynarodowych) oraz innych niż kancelaria tajna komórek wewnętrznych lub organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i wydawanie materiałów niejawnych.

m.p.

…… ……
(miejscowość i data) *(pieczęć imienna i podpis pełnomocnika ochrony)*

Załącznik Nr 8 do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

KRYTERIA TWORZENIA STREF OCHRONNYCH

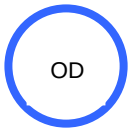
I	II	III
1. System kontroli dostępu lub książkowa ewidencja wejścia/ wyjścia. Dane z ewidencji przechowywane co najmniej przez 3 miesiące. 2. Telewizyjny system nadzoru rejestrujący wejście do strefy (w miarę potrzeb dla informacji oznaczonych klauzulą „ściśle tajne”). 3. System alarmowy co najmniej klasy SA3 wykonany wg Normy Obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe. 4. System sygnalizacji pożaru. 5. Zapis danych z ww. systemów musi być możliwy do odtworzenia po upływie, co najmniej trzech miesięcy. 6. Ściany i stropy stanowiące granice strefy powinny być wykonane z materiałów niepalnych o nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej o grubości 25 cm. Dopuszcza się inne zabezpieczenia posiadające właściwości nie mniejsze niż ściana o ww. konstrukcji lub czujki alarmowe sejsmiczne. 7. 1. Drzwi stalowe lub drewniane wykonane z litego drewna o grubości co najmniej 40 mm, obustronnie obite blachą stalową o grubości co najmniej 2 mm, blokowane na 4 krawędziach, zabezpieczone przed włamaniem od strony zawiasów, wyposażone w dwa zamki, w tym jeden mechaniczny o skomplikowanym mechanizmie, a drugi szyfrowy, o zmiennym nastawieniu, z tym że zamek szyfrowy powinien być co najmniej trzyzapadkowy, o cichym przesuwie skali nastawień nie większej niż jedna działka, posiadający co najmniej 100 podziałek na pokrętle, a zmiana kombinacji w zamku szyfrowym powinna być blokowana i uaktywniana kluczem od tyłu skrzynki zamka, zaś drzwi powinny posiadać element samozatrzaskowy	1. Kontrola wejścia/ wyjścia do/z obszaru chronionego. 2. Drzwi wykonane co najmniej z litego drewna wyposażone w jeden zamek. 3. Okna dodatkowo zabezpiecza się w sposób uniemożliwiający podgląd pomieszczenia z zewnątrz. 4. Miejsca, w których nie pracuje się 24 godz. na dobę muszą zostać sprawdzone przez użytkownika po zakończeniu normalnych godzin pracy, w celu upewnienia się, że informacje niejawne zostały należycie zabezpieczone.	1. Kontrola wejścia/ wyjścia do/z obszaru chronionego. 2. Drzwi zwykłe wyposażone w jeden zamek. 3. Okna jak w strefie II, w przypadku przetwarzania materiałów niejawnych o klauzuli „poufne”.

uniemożliwiający pozostawienie pomieszczenia otwartego. 7. 2. Drzwi o zwiększonej odporności na włamanie, które powinny spełniać, co najmniej wymagania klasy 3 lub 4, o których mowa w Polskiej Normie PN-ENV-1627 oraz wyposażone w zamek drzwiowy dodatkowy klasy 5 lub 7, o którym mowa w Polskiej Normie PN-EN-12209 (wymóg dotyczy nowobudowanych obiektów, budynków i pomieszczeń). 8. 1. Okna rozmieszczone na parterze oraz na ostatniej kondygnacji zabezpiecza się kratą lub innym zabezpieczeniem spełniającym wymagania, co najmniej w klasie 3, według Polskiej Normy PN-ENV-1627. 8. 2. Wszystkie okna dodatkowo zabezpiecza się przed podglądem z zewnątrz.		

Załącznik Nr 9 do rozporządzenia
Ministra Obrony Narodowej z dnia
2011 r. (poz.)

ZESTAWIENIE PODSTAWOWYCH ZNAKÓW UMOWNYCH

STOSOWANYCH W PLANACH OCHRONY INFORMACJI NIEJAWNYCH



- służby dyżurne (OD – oficer dyżurny, DP – dyżurny biura przepustek)

- ogrodzenie

- brama

- furtka

- szlaban (zapora)

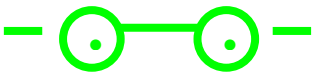
- drzwi

- 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

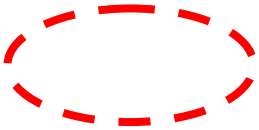
- kamera telewizyjna zewnętrzna z detektorem ruchu

- strefa ochronna klasy I

- strefa ochronna klasy II

- strefa ochronna klasy III

- droga ewakuacji materiałów niejawnych



- rejon ewakuacji materiałów niejawnych