AKADEMIA OBRONY NARODOWEJ

KANCELARIA TAJNA

St. chor. szt. mgr Arkadiusz STRZELCZYK

ZBIÓR PRZEPISÓW NORMUJĄCYCH ZASADY OCHRONY INFORMACJI NIEJAWNYCH W RESORCIE OBRONY NARODOWEJ

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Akademii Obrony Narodowej
Nr ewid. II
62672

WARSZAWA 2007

AKADEMIA OBRONY NARODOWEJ

KANCELARIA TAJNA

AON 5810/07

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 62672
II
Akademii Obrony Narodowej

St. chor. szt. mgr Arkadiusz STRZELCZYK

ZBIÓR PRZEPISÓW NORMUJĄCYCH ZASADY OCHRONY INFORMACJI NIEJAWNYCH W RESORCIE OBRONY NARODOWEJ

Warszawa **2007**

Druk i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy, zam. nr 320/2007

SPIS TREŚCI

USTAWA z dnia 22 stycznia 1999 r.
o ochronie informacji niejawnych (Tekst ujednolicony po zmianie
z 15 kwietnia 2005 r z późn. zm.) 5

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 sierpnia 2005 r.
w sprawie szczegółowego trybu przygotowania i prowadzenia przez służby ochrony, państwa kontroli w zakresie ochrony informacji niejawnych 52

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 sierpnia 2005 r.
w sprawie wzorów poświadczenia bezpieczeństwa, decyzji o odmowie wydania poświadczenia bezpieczeństwa oraz decyzji o cofnięciu poświadczenia bezpieczeństwa 66

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 sierpnia 2005 r.
w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego 79

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 29 września 2005 r.
w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne 106

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 5 października 2005 r.
w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzuli tajności, a także zmiany nadanej klauzuli tajności 114

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 18 października 2005 r.
w sprawie organizacji i funkcjonowania kancelarii tajnych 118

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ
z dnia 13 września 2002 r. **w sprawie przechowywania i rejestrowania dokumentacji postępowań dyscyplinarnych oraz prowadzenia ewidencji ukarań żołnierzy** 132

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** 137

DECYZJA NR 336/MON MINISTRA OBRONY NARODOWEJ
z dnia 10 października 2005 r. **w sprawie wprowadzenia do użytku „Instrukcji o pieczęciach używanych w resorcie obrony narodowej"** 147

DECYZJA NR 20/MON MINISTRA OBRONY NARODOWEJ
z dnia 31 stycznia 2006 r. **w sprawie powołania pełnomocników, zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz inspektorów bezpieczeństwa teleinformatycznego w Ministerstwie Obrony Narodowej lub przez niego nadzorowanych** 179

DECYZJA NR 21/MON MINISTRA OBRONY NARODOWEJ
z dnia 31 stycznia 2006 r. **w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej** 183

DECYZJA NR 22/MON MINISTRA OBRONY NARODOWEJ
z dnia 31 stycznia 2006 r. **w sprawie szczegółowych zasad i trybu prowadzenia i dokumentowania postępowań sprawdzających oraz wydawania poświadczeń i certyfikatów bezpieczeństwa** 202

DECYZJA NR 23/MON MINISTRA OBRONY NARODOWEJ
z dnia 31 stycznia 2006 r. **w sprawie szkolenia w zakresie ochrony informacji niejawnych**..... 257

DECYZJA NR 24/MON MINISTRA OBRONY NARODOWEJ
z dnia 31 stycznia 2006 r. **w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej**..... 264

DECYZJA NR 25/MON MINISTRA OBRONY NARODOWEJ
z dnia 31 stycznia 2006 r. **w sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach i komórkach organizacyjnych resortu obrony narodowej**..... 276

ZARZĄDZENIE NR 25/MON MINISTRA OBRONY NARODOWEJ
z dnia 17 listopada 2005 r. **w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych** 283

ZARZĄDZENIE 3/MON MINISTRA OBRONY NARODOWEJ
z dnia 2 lutego 2005 r. **w sprawie zasad i trybu postępowania z materiałami archiwalnymi i inną dokumentacją w resorcie Obrony Narodowej** 340

DECYZJA Nr 390/MON MINISTRA OBRONY NARODOWEJ z dnia 28 września 2006 r. **w sprawie ograniczeń w używaniu urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w komórkach i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych** 365

DECYZJA Nr 488/MON MINISTRA OBRONY NARODOWEJ z dnia 30 listopada 2006 r. **w sprawie wprowadzenia do użytku w resorcie obrony narodowej „Tymczasowej instrukcji organizacji obiegu informacji niejawnych o klauzuli zastrzeżone w resortowej sieci teleinformatycznej MIL-WAN"**..... 367

WYTYCZNE MINISTRA OBRONY NARODOWEJ z dnia 23 stycznia 2007 r. **w sprawie ochrony informacji niejawnych oraz obiektów wojskowych w jednostkach organizacyjnych podporządkowanych Ministrowi Obrony Narodowej lub przez niego nadzorowanych w 2007 r.** 379

INNE PODSTAWY PRAWNE..... 384

Dz.U.1999.11.95
tekst jednolity:
Dz.U. 2005.196.1631
akty zmieniające:
Dz.U. 2006.104.708
Dz.U. 2006.104.711 - obowiązuje od 01.10.2006r, dotyczy zmian Wojskowych Służb Informacyjnych na Służby Kontrwywiadu Wojskowego

USTAWA

z dnia 22 stycznia 1999 r.

o ochronie informacji niejawnych

Tekst ujednolicony po zmianie z 15 kwietnia 2005 r.

Rozdział 1
Przepisy ogólne

Art. 1.

1. Ustawa określa zasady ochrony informacji, które wymagają ochrony przed nieuprawnionym ujawnieniem, jako stanowiące tajemnicę państwową lub służbową, niezależnie od formy i sposobu ich wyrażania, także w trakcie ich opracowania, zwanych dalej „informacjami niejawnymi", a w szczególności:

1) organizowania ochrony informacji niejawnych;
2) klasyfikowania informacji niejawnych;
3) udostępniania informacji niejawnych;
4) postępowania sprawdzającego, w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej „postępowaniem sprawdzającym";
5) szkolenia w zakresie ochrony informacji niejawnych;
6) ewidencjonowania, przechowywania, przetwarzania i udostępniania danych uzyskiwanych w związku z prowadzonymi postępowaniami o ustalenie rękojmi zachowania tajemnicy, w zakresie określonym w ankiecie bezpieczeństwa osobowego oraz w kwestionariuszu bezpieczeństwa przemysłowego;
7) organizacji kontroli przestrzegania zasad ochrony informacji niejawnych;
8) ochrony informacji niejawnych w systemach i sieciach teleinformatycznych;
9) stosowania środków fizycznej ochrony informacji niejawnych.

2. Przepisy ustawy mają zastosowanie do:

1) organów władzy publicznej, w szczególności:

a) Sejmu i Senatu Rzeczypospolitej Polskiej,
b) Prezydenta Rzeczypospolitej Polskiej,
c) organów administracji rządowej,
d) organów jednostek samorządu terytorialnego,
e) sądów i trybunałów,
f) organów kontroli państwowej i ochrony prawa;

2) Sił Zbrojnych Rzeczypospolitej Polskiej i ich jednostek organizacyjnych, zwanych dalej „Siłami Zbrojnymi", a także innych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
3) Narodowego Banku Polskiego i banków państwowych;

4) państwowych osób prawnych i innych niż wymienione w pkt 1-3 państwowych jednostek organizacyjnych;
5) przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych, zamierzających ubiegać się, ubiegających się o zawarcie lub wykonujących umowy związane z dostępem do informacji niejawnych albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

3. Przepisy ustawy nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych.

4. W zakresie nieuregulowanym w ustawie do postępowania sprawdzającego, postępowania odwoławczego oraz postępowania bezpieczeństwa przemysłowego stosuje się przepisy art. 6-8, art. 12, art. 14-16, art. 24 § 1 pkt 1-6 i § 2-4, art. 26 § 1, art. 28, art. 29, art. 30 § 1-3, art. 35 § 1, art. 39, art. 41-47, art. 57-60, art. 61 § 3 i 4, art. 63 § 4, art. 64, art. 97 § 1 pkt 4 i § 2, art. 98, art. 101, art. 104, art. 105, art. 107, art. 112, art. 113, art. 156-158 oraz art. 217 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.1)).

Art. 2.

W rozumieniu ustawy:
1) tajemnicą państwową - jest informacja określona w wykazie rodzajów informacji, stanowiącym załącznik
nr 1, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa;
2) tajemnicą służbową - jest informacja niejawna niebędąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej;
3) służbami ochrony państwa — są Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego;
4) rękojmia zachowania tajemnicy - oznacza spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem;
5) dokumentem - jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na elektronicznych nośnikach danych;
6) materiałem - jest dokument, jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia;
7) jednostką organizacyjną - jest podmiot wymieniony w art. 1 ust. 2;
7a) jednostką naukową - jest jednostka naukowa w rozumieniu przepisów o zasadach finansowania nauki;
8) systemem teleinformatycznym - jest system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji;
9) siecią teleinformatyczną - jest organizacyjne i techniczne połączenie systemów teleinformatycznych;
10) akredytacją bezpieczeństwa teleinformatycznego - jest dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie;
11) dokumentacją bezpieczeństwa systemu lub sieci informatycznej - są Szczególne Wymagania

Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie.

Art. 3.

Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy.

Art. 4.

1. Zasady zwalniania od obowiązku zachowania tajemnicy państwowej i służbowej oraz sposób postępowania z aktami spraw zawierających tajemnicę państwową i służbową w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw.

2. Jeżeli przepisy odrębnych ustaw uprawniają organy, służby lub instytucje państwowe albo ich upoważnionych pracowników do dokonywania kontroli, a w szczególności swobodnego dostępu do pomieszczeń i materiałów, jeżeli jej zakres dotyczy informacji niejawnych, uprawnienia te są realizowane z zachowaniem przepisów niniejszej ustawy.

Rozdział 2
uchylony

Rozdział 3
Organizacja ochrony informacji niejawnych

Art. 14.

1. Służby ochrony państwa są właściwe do:

1) kontroli ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie, z uwzględnieniem prawidłowości postępowań sprawdzających prowadzonych przez pełnomocników ochrony, z wyłączeniem postępowań, o których mowa w art. 30;
2) realizacji zadań w zakresie bezpieczeństwa systemów i sieci teleinformatycznych;
3) prowadzenia postępowania sprawdzającego według zasad określonych w ustawie;
4) ochrony informacji niejawnych wymienianych przez Rzeczpospolitą Polską z innymi państwami i organizacjami międzynarodowymi;
5) szkolenia i doradztwa w zakresie ochrony informacji niejawnych;
6) wykonywania innych zadań, w zakresie ochrony informacji niejawnych, określonych odrębnymi przepisami.

2. Służby ochrony państwa, w zakresie koniecznym do wykonywania swoich zadań, w celu ochrony informacji niejawnych mogą korzystać z informacji uzyskanych przez Centralne Biuro Antykorupcyjne, Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej, a także zwracać się do tych służb i organów o udzielenie niezbędnej pomocy przy wykonywaniu czynności w ramach prowadzonych postępowań sprawdzających.

3. Kierownicy jednostek organizacyjnych współdziałają ze służbami ochrony państwa w toku przeprowadzanych przez nie postępowań sprawdzających, a w szczególności udostępniają funkcjonariuszom albo żołnierzom, po przedstawieniu przez nich pisemnego upoważnienia, pozostające w ich dyspozycji informacje i dokumenty niezbędne do stwierdzenia, czy osoba objęta postępowaniem sprawdzającym daje rękojmię zachowania tajemnicy. Organy i służby, o których mowa w art. 30, udostępniają pozostające w ich dyspozycji informacje i dokumenty wyłącznie

w przypadku, gdy w ich opinii osoba ta nie daje rękojmi zachowania tajemnicy; w przeciwnym przypadku informują, że nie posiadają informacji i dokumentów świadczących, że osoba objęta postępowaniem sprawdzającym nie daje tej rękojmi.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, szczegółowy zakres, warunki i tryb:

1) przekazywania służbom ochrony państwa informacji i udostępniania dokumentów, o których mowa w ust. 3;
2) udzielania służbom ochrony państwa pomocy, o której mowa w ust. 2.

5. W rozporządzeniu, o którym mowa w ust. 4, określa się w szczególności:

1) szczegółowy zakres, warunki i tryb przekazywania przez kierowników jednostek organizacyjnych służbom ochrony państwa informacji oraz udostępniania im dokumentów niezbędnych do stwierdzenia, czy osoba objęta postępowaniem sprawdzającym daje rękojmię zachowania tajemnicy;
2) zakres, warunki i tryb udzielania przez Centralne Biuro Antykorupcyjne, Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej niezbędnej pomocy przy wykonywaniu czynności w ramach prowadzonych postępowań sprawdzających.

Art. 15.

W stosunkach międzynarodowych Szef Agencji Bezpieczeństwa Wewnętrznego i Szef Służby Kontrwywiadu Wojskowego pełnią funkcję krajowej władzy bezpieczeństwa.

Art. 16.

W zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych stanowiących tajemnicę państwową upoważnieni pisemnie funkcjonariusze lub żołnierze służb ochrony państwa mają prawo do:

1) swobodnego wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są wytwarzane, przetwarzane, przechowywane lub przekazywane;
2) wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej;
3) żądania udostępnienia do kontroli sieci lub systemów teleinformatycznych służących do wytwarzania, przechowywania, przetwarzania lub przekazywania tych informacji;
4) przeprowadzania oględzin obiektów, składników majątkowych i sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;
5) żądania od kierowników i pracowników kontrolowanych jednostek organizacyjnych udzielania ustnych i pisemnych wyjaśnień oraz posiadanych przez nich informacji dotyczących działalności wywiadowczej albo terrorystycznej skierowanej przeciwko Rzeczypospolitej Polskiej, jej Siłom Zbrojnym, przedsiębiorcom, jednostkom naukowym lub badawczo-rozwojowym, w odniesieniu do prowadzonej produkcji albo usług stanowiących tajemnicę państwową ze względu na bezpieczeństwo lub obronność państwa, a także na potrzeby Sił Zbrojnych;
6) zasięgania, w związku z przeprowadzaną kontrolą, informacji w jednostkach niekontrolowanych, jeżeli ich działalność pozostaje w związku z wytwarzaniem, przechowywaniem, przetwarzaniem, przekazywaniem lub ochroną informacji niejawnych stanowiących tajemnicę państwową, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek;
7) korzystania z pomocy biegłych i specjalistów, jeżeli stwierdzenie okoliczności ujawnionych w czasie przeprowadzania kontroli wymaga wiadomości specjalnych;
8) uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej.

Art. 17.

1. Do czynności, o których mowa w art. 16, dokonywanych przez służby ochrony państwa, mają odpowiednie zastosowanie przepisy art. 28, art. 29 pkt 1, art. 30-41 i art. 49-64 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.2)), z tym że przewidziane w tej ustawie uprawnienia i obowiązki:

1) Najwyższej Izby Kontroli - przysługują służbom ochrony państwa;
2) Prezesa, wiceprezesa i pracownika Najwyższej Izby Kontroli — przysługują odpowiednio Szefowi, zastępcy Szefa i upoważnionemu funkcjonariuszowi Agencji Bezpieczeństwa Wewnętrznego oraz Szefowi, zastępcy Szefa i upoważnionemu żołnierzowi albo funkcjonariuszowi Służby Kontrwywiadu Wojskowego.

1a. Czynności, o których mowa w art. 16 pkt 1-5 i 8, dokonywane przez służby ochrony państwa w stosunku do Sejmu Rzeczypospolitej Polskiej oraz Senatu Rzeczypospolitej Polskiej, wykonywane są w uzgodnieniu odpowiednio z Marszałkiem Sejmu Rzeczypospolitej Polskiej i Marszałkiem Senatu Rzeczypospolitej Polskiej. Uzgodnienia dokonuje Prezes Rady Ministrów, a w przypadku braku uzgodnienia czynność nie może być wykonana.

2. Prezes Rady Ministrów określi, w drodze rozporządzenia, szczegółowy tryb przygotowania i prowadzenia kontroli w zakresie ochrony informacji niejawnych, w tym uzgadniania kontroli w stosunku do Sejmu Rzeczypospolitej Polskiej i Senatu Rzeczypospolitej Polskiej, uwzględniając zadania funkcjonariuszy i żołnierzy służb ochrony państwa nadzorujących i wykonujących czynności kontrolne, dokumentowanie czynności kontrolnych oraz sporządzanie: protokołu kontroli, wystąpienia pokontrolnego i informacji o wynikach kontroli.

Art. 18.

1. Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej, w której takie informacje są wytwarzane, przetwarzane, przekazywane lub przechowywane.

2. Kierownikowi jednostki organizacyjnej podlega bezpośrednio pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony", który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

2a. Kierownik jednostki organizacyjnej może powołać zastępcę pełnomocnika ochrony.

3. Pełnomocnikiem ochrony w jednostce organizacyjnej może być osoba, która:

1) posiada obywatelstwo polskie;
2) posiada co najmniej średnie wykształcenie;
3) posiada odpowiednie poświadczenie bezpieczeństwa wydane przez służbę ochrony państwa po przeprowadzeniu postępowania sprawdzającego, o którym mowa w art. 36 ust. 1;
4) odbyła przeszkolenie w zakresie ochrony informacji niejawnych.

3a. Zastępcą pełnomocnika ochrony w jednostce organizacyjnej może być osoba, która spełnia warunki określone w ust. 3.

4. Pełnomocnik ochrony kieruje wyodrębnioną, wyspecjalizowaną komórką organizacyjną do spraw ochrony informacji niejawnych, zwaną dalej „pionem ochrony", do której zadań należy:

1) zapewnienie ochrony informacji niejawnych, w tym ich ochrony fizycznej;
2) zapewnienie ochrony systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne;

3) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji;
4) okresowa kontrola ewidencji, materiałów i obiegu dokumentów;
5) opracowywanie planu ochrony informacji niejawnych w jednostce organizacyjnej i nadzorowanie jego realizacji;
6) szkolenie pracowników w zakresie ochrony informacji niejawnych na zasadach określonych w rozdziale 8.

4a. Kierownik jednostki organizacyjnej może powierzyć pełnomocnikowi ochrony wykonywanie innych zadań, o ile ich realizacja nie naruszy prawidłowego wykonywania zadań, o których mowa w ust. 4.

5. Pracownikiem pionu ochrony w jednostce organizacyjnej może być osoba, która:

1) posiada obywatelstwo polskie;
2) posiada odpowiednie poświadczenie bezpieczeństwa wydane po przeprowadzeniu postępowania sprawdzającego, o którym mowa w art. 36 ust. 1;
3) odbyła przeszkolenie w zakresie ochrony informacji niejawnych.

6. Pełnomocnik ochrony, w zakresie realizacji swoich zadań, w razie wprowadzenia stanu nadzwyczajnego, ma prawo żądać od komórek organizacyjnych w swojej jednostce organizacyjnej udzielenia natychmiastowej pomocy.

7. W zakresie realizacji swoich zadań pełnomocnik ochrony współpracuje z właściwymi jednostkami i komórkami organizacyjnymi służb ochrony państwa. Pełnomocnik ochrony na bieżąco informuje kierownika jednostki organizacyjnej o przebiegu tej współpracy.

8. Pełnomocnik ochrony opracowuje plan postępowania z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego.

9. Pełnomocnik ochrony podejmuje działania zmierzające do wyjaśnienia okoliczności naruszenia przepisów o ochronie informacji niejawnych, zawiadamiając o tym kierownika jednostki organizacyjnej, a w przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne" lub wyższą, również właściwą służbę ochrony państwa.

Art. 18a.

1. W jednostkach organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2, pełnomocnik ochrony, oprócz realizacji zadań określonych w art. 18 ust. 4 i 4a, zapewnia również ochronę fizyczną tych jednostek.

2. Minister Obrony Narodowej określi, w drodze rozporządzenia, szczegółowe zadania pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych i przez niego nadzorowanych, szczególne wymagania w zakresie ochrony fizycznej informacji niejawnych, tryb opracowywania oraz niezbędne elementy planów ochrony tych jednostek, a także sposób nadzorowania ich realizacji.

3. Rozporządzenie, o którym mowa w ust. 2, określi w szczególności zadania dotyczące koordynowania oraz nadzorowania działalności pionów ochrony przez pełnomocników ochrony bezpośrednio nadrzędnych jednostek organizacyjnych, podstawowe wymagania, jakim powinny odpowiadać plany ochrony, podział stref bezpieczeństwa na rodzaje, a także warunki dostępu do tych stref.

Rozdział 4
Klasyfikowanie informacji niejawnych. Klauzule tajności

Art. 19.

1. Klasyfikowanie informacji niejawnej oznacza przyznanie tej informacji, w sposób wyraźny, przewidzianej w ustawie jednej z klauzul tajności, o których mowa w art. 23 i 24.

2. Klasyfikowanie informacji niejawnej zawartej w materiale, a zwłaszcza utrwalonej w dokumencie, polega na oznaczeniu tego materiału odpowiednią klauzulą tajności.

3. Informacjom niejawnym, materiałom, a zwłaszcza dokumentom lub ich zbiorom, przyznaje się klauzulę tajności co najmniej równą najwyżej zaklasyfikowanej informacji lub najwyższej klauzuli w zbiorze.

4. Dopuszczalne jest przyznawanie różnych klauzul tajności częściom dokumentu (rozdziałom, załącznikom, aneksom) lub poszczególnym dokumentom w zbiorze dokumentów, pod warunkiem wyraźnego ich oznaczenia i wskazania klauzuli tajności po odłączeniu dokumentu bądź jego części.

Art. 20.

1. Informacje niejawne, którym przyznano określoną klauzulę tajności, z zastrzeżeniem ust. 2, są chronione zgodnie z przepisami ustawy, które dotyczą informacji niejawnych oznaczonych daną klauzulą tajności. Oznacza to w szczególności, że informacje takie:

1) mogą być udostępnione wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli tajności;
2) muszą być wytwarzane, przetwarzane, przekazywane lub przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, obiegu i środków fizycznej ochrony informacji niejawnych, odpowiednich dla przyznanej im klauzuli tajności;
3) muszą być chronione, odpowiednio do przyznanej klauzuli tajności, przy zastosowaniu środków określonych w rozdziałach 9 i 10.

2. Kierownik jednostki organizacyjnej zatwierdza, opracowane przez pełnomocnika ochrony, szczegółowe wymagania w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone" w podległych komórkach organizacyjnych.

Art. 21.

1. Klauzulę tajności przyznaje osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

2. Uprawnienie do przyznawania, zmiany i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych.

3. Osoba, o której mowa w ust. 1, ponosi odpowiedzialność za przyznanie klauzuli tajności i bez jej zgody albo bez zgody jej przełożonego klauzula nie może być zmieniona lub zniesiona. Dotyczy to również osoby, która przekazała dane do dokumentu zbiorczego.

4. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.

5. Odbiorca materiału zgłasza osobie, o której mowa w ust. 1, albo jej przełożonemu fakt wyraźnego

zawyżenia lub zaniżenia klauzuli tajności. W przypadku gdy osoba ta lub jej przełożony zdecyduje o zmianie klauzuli, powinna poinformować o tym odbiorców tego materiału. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zmianie klauzuli.

Art. 22.

Kierownicy jednostek organizacyjnych zapewniają przeszkolenie podległych im pracowników w zakresie klasyfikowania informacji niejawnych oraz stosowania właściwych klauzul tajności, a także procedur ich zmiany i znoszenia.

Art. 23.

1. Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę państwową oznacza się klauzulą:

1) „ściśle tajne" - zgodnie z wykazem stanowiącym załącznik nr 1 do ustawy (część I);
2) „tajne" - zgodnie z wykazem stanowiącym załącznik nr 1 do ustawy (część II).

2. Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę służbową oznacza się klauzulą:

1) „poufne" - w przypadku gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli;
2) „zastrzeżone" - w przypadku gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

3. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób oznaczania materiałów, umieszczania na nich klauzul tajności, a także sposób zmiany nadanej klauzuli, uwzględniając, że materiały powinny być oznaczone w sposób zapewniający ich odróżnienie od materiałów jawnych oraz mając na uwadze rodzaje klauzul tajności i materiałów.

4. Prezes Rady Ministrów może określić, w drodze rozporządzenia, dodatkowe oznaczenia materiałów, które:

1) mogą poprzedzać klauzule wymienione w ust. 1 i 2, oraz wynikający z tych oznaczeń szczególny sposób postępowania z tak oznaczonymi materiałami; rozporządzenie powinno określać w szczególności: rodzaje oznaczeń, sposób ich nanoszenia na materiały oraz tryb wytwarzania, przetwarzania, przekazywania, udostępniania i przechowywania tak oznaczonych informacji niejawnych, a także krąg upoważnionych adresatów ze względu na wymóg wyższego stopnia ochrony tych materiałów,
2) mogą poprzedzać lub następować bezpośrednio po klauzulach wymienionych w ust. 1 i 2 lub ich zagranicznych odpowiednikach, oraz wynikający z umów międzynarodowych, których Rzeczpospolita Polska jest stroną, szczególny sposób postępowania z tak oznaczonymi materiałami; rozporządzenie powinno określać w szczególności: rodzaje oznaczeń, sposób ich nanoszenia na materiały oraz tryb wytwarzania, przetwarzania, przekazywania, udostępniania i przechowywania tak oznaczonych informacji niejawnych, a także sposób oceny spełnienia warunków dostępu do tych informacji przez osoby fizyczne, przedsiębiorców, jednostki naukowe i badawczo-rozwojowe.

Art. 24.

Materiały otrzymywane z zagranicy oraz wysyłane za granicę, w celu wykonania umów międzynarodowych, oznacza się odpowiednią do ich treści klauzulą tajności określoną w ustawie oraz jej zagranicznym odpowiednikiem.

Art. 25.

1. Informacje niejawne stanowiące tajemnicę państwową podlegają ochronie, w sposób określony ustawą, przez okres 50 lat od daty ich wytworzenia.

2. Chronione bez względu na upływ czasu pozostają:

1) dane identyfikujące funkcjonariuszy i żołnierzy Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego oraz byłego Urzędu Ochrony Państwa i byłych Wojskowych Służb Informacyjnych wykonujących czynności operacyjno-rozpoznawcze;
2) dane identyfikujące osoby, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych organom, służbom i instytucjom państwowym uprawnionym do ich wykonywania na podstawie ustawy;
3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia.

3. Informacje niejawne stanowiące tajemnicę służbową podlegają ochronie w sposób określony ustawą przez okres:

1) 5 lat od daty wytworzenia - oznaczone klauzulą „poufne";
2) 2 lat od daty wytworzenia - oznaczone klauzulą „zastrzeżone".

4. Osoba, o której mowa w art. 21 ust. 1, może:

1) określić krótszy okres ochrony informacji niejawnych stanowiących tajemnicę służbową;
2) po dokonaniu przeglądu materiałów zawierających informacje niejawne stanowiące tajemnicę służbową przedłużać okres ochrony tych informacji na kolejne okresy nie dłuższe niż 5 lat - dla oznaczonych klauzulą „poufne" i 2 lat - dla oznaczonych klauzulą „zastrzeżone", nie dłużej jednak niż na okres do 20 lat od daty wytworzenia tych informacji.

5. Rada Ministrów może określić, w drodze rozporządzenia, które spośród informacji niejawnych oznaczonych klauzulą „tajne" przestały stanowić tajemnicę państwową, jeżeli od ich powstania upłynęło co najmniej 20 lat, biorąc pod uwagę interesy obronności i bezpieczeństwa państwa oraz inne istotne interesy państwa.

6. Uprawnienia osoby, o której mowa w art. 21 ust. 1, w zakresie przyznawania, zmiany lub znoszenia klauzuli tajności materiału oraz określania okresu, przez jaki informacja niejawna podlega ochronie, przechodzą, w przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji dotyczących stanowiska lub funkcji tej osoby, na jej następcę prawnego. W razie braku następcy prawnego uprawnienia w tym zakresie przechodzą na właściwą służbę ochrony państwa.

Rozdział 5
Dostęp do informacji niejawnych. Postępowania sprawdzające

Art. 26.

1. Kierownik jednostki organizacyjnej określi stanowiska oraz rodzaje prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych, odrębnie dla każdej klauzuli tajności.
2. (uchylony).

Art. 27.

1. Dopuszczenie do pracy lub pełnienia służby na stanowisku albo zlecenie pracy, o której mowa w art. 26, z zastrzeżeniem ust. 2, 3 i 6-8, może nastąpić po:

1) przeprowadzeniu postępowania sprawdzającego;
2) przeszkoleniu tej osoby w zakresie ochrony informacji niejawnych.

2. Postępowania sprawdzającego nie przeprowadza się wobec osób sprawujących urzędy: Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu Rzeczypospolitej Polskiej, Marszałka Senatu Rzeczypospolitej Polskiej i Prezesa Rady Ministrów.

2a. Postępowania sprawdzającego nie przeprowadza się wobec kandydatów na członków Rady Ministrów powoływanych w trybie art. 154, 155 lub 161 Konstytucji Rzeczypospolitej Polskiej.

3. Postępowania sprawdzającego nie przeprowadza się, z zastrzeżeniem ust. 4, wobec posłów i senatorów.

4. Marszałek Sejmu lub Marszałek Senatu zwracają się, za zgodą osoby sprawdzanej, do służb ochrony państwa o przeprowadzenie postępowania sprawdzającego wobec posłów lub senatorów, których obowiązki poselskie bądź senatorskie wymagają dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne".

5. W przypadku odmowy wydania poświadczenia bezpieczeństwa osobie, o której mowa w ust. 4 - za jej zgodą - Prezes Rady Ministrów przedstawia informację o powodach tej odmowy Marszałkowi Sejmu, jeżeli odmowa dotyczy posła, albo Marszałkowi Senatu, jeżeli odmowa dotyczy senatora.

6. Postępowania sprawdzającego nie przeprowadza się wobec osób zajmujących stanowiska: Prezesa Rady Ministrów, członka Rady Ministrów, Pierwszego Prezesa Sądu Najwyższego, Prezesa Naczelnego Sądu Administracyjnego, Prezesa Trybunału Konstytucyjnego, Prezesa Narodowego Banku Polskiego, Prezesa Najwyższej Izby Kontroli, Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych, Rzecznika Interesu Publicznego, członków Rady Polityki Pieniężnej, członków Krajowej Rady Radiofonii i Telewizji, Prezesa Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz Szefów Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu i Prezesa Rady Ministrów.

7. W stosunku do kandydatów na stanowiska, o których mowa w ust. 6, z wyłączeniem kandydatów powoływanych w trybie art. 154, 155 lub 161 Konstytucji Rzeczypospolitej Polskiej, postępowanie sprawdzające przeprowadza właściwa służba ochrony państwa na wniosek organu uprawnionego do powołania na to stanowisko. Jeżeli do powołania jest uprawniony Sejm albo Senat, z wnioskiem tym występuje odpowiednio Marszałek Sejmu albo Marszałek Senatu. Postępowanie powinno być zakończone przed upływem 14 dni od dnia złożenia wniosku o przeprowadzenie tego postępowania wraz z wypełnioną ankietą, przekazaniem opinii z uzasadnieniem właściwej służby ochrony państwa Prezydentowi Rzeczypospolitej Polskiej, Marszałkowi Sejmu albo Marszałkowi Senatu. Przekazanie opinii jest równoznaczne z zakończeniem postępowania sprawdzającego w rozumieniu art. 36 ust. 2.

8. W stanach nadzwyczajnych Prezydent Rzeczypospolitej Polskiej lub Prezes Rady Ministrów, każdy w swoim zakresie, może wyrazić zgodę na odstąpienie od przeprowadzenia postępowania sprawdzającego wobec osoby, o której mowa w ust. 1, chyba że istnieją przesłanki do stwierdzenia, że nie daje ona rękojmi zachowania tajemnicy.

9. Prezydent Rzeczypospolitej Polskiej oraz Marszałek Sejmu i Marszałek Senatu zapoznają się z przepisami o ochronie informacji niejawnych i składają oświadczenie o znajomości tych przepisów. Posłowie i senatorowie oraz osoby, o których mowa w ust. 6, składają takie oświadczenie po odbyciu szkolenia w zakresie ochrony informacji niejawnych.

10. Udostępnianie informacji niejawnych sędziom i asesorom sądowym pełniącym czynności sędziowskie oraz prokuratorom i asesorom prokuratury pełniącym czynności prokuratorskie regulują przepisy o ustroju sądów powszechnych, o ustroju sądów wojskowych oraz o prokuraturze.

Art. 28.

1. Nie mogą być dopuszczone do pracy lub pełnienia służby na stanowisku albo do wykonywania prac zleconych, z którymi łączy się dostęp do informacji niejawnych stanowiących tajemnicę państwową, z uwzględnieniem ust. 2, osoby:

1) nieposiadające obywatelstwa polskiego, chyba że przepisy ustawy stanowią inaczej;
2) skazane prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub
3) które nie posiadają poświadczenia bezpieczeństwa, z wyjątkiem osób, o których mowa w art. 27 ust. 2, 3, 6 i 8.

2. Jeżeli z zawartych przez Rzeczpospolitą Polską umów międzynarodowych wynika, na zasadzie wzajemności, obowiązek dopuszczenia do informacji niejawnych obywateli obcych państw mających wykonywać w Rzeczypospolitej Polskiej pracę w interesie innego państwa lub organizacji międzynarodowej, postępowania sprawdzającego nie przeprowadza się.

Art. 29.

Postępowania sprawdzające, o których mowa w art. 36 ust. 1 pkt 2 i 3, na pisemny wniosek osoby upoważnionej na podstawie odrębnych przepisów do obsady stanowiska lub zlecenia prac, w tym także kierownika jednostki organizacyjnej, zwanej dalej „osobą upoważnioną do obsady stanowiska", przeprowadzają:

1) Służba Kontrwywiadu Wojskowego — w przypadku ubiegania się osoby o zatrudnienie lub zlecenie prac związanych z obronnością państwa:

a) wobec żołnierzy pozostających w czynnej służbie wojskowej i pracowników wojska,
b) u przedsiębiorców, w jednostkach naukowych lub badawczo-rozwojowych, których organem założycielskim jest Minister Obrony Narodowej, a także w innych jednostkach organizacyjnych, w zakresie, w jakim realizują one produkcję lub usługi, stanowiące tajemnicę państwową ze względu na obronność państwa i na potrzeby Sił Zbrojnych,
c) u przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową ze względu na obronność państwa, jeżeli uczestnikami tego obrotu są Siły Zbrojne lub jednostki organizacyjne podległe Ministrowi Obrony Narodowej,
d) w wojskowych organach ochrony prawa i wojskowych organach porządkowych;

2) Agencja Bezpieczeństwa Wewnętrznego - w razie ubiegania się osoby o stanowisko, zatrudnienie lub zlecenie prac w innych przypadkach niż wymienione w pkt 1.

Art. 29a.

Służba ochrony państwa przeprowadza postępowanie sprawdzające, o którym mowa w art. 36 ust. 1, wobec osób, które na mocy umów międzynarodowych zawartych przez Rzeczpospolitą Polską mają obowiązek uzyskania poświadczeń bezpieczeństwa upoważniających do dostępu do informacji niejawnych oznaczonych klauzulą „poufne", „tajne" lub „ściśle tajne", z wyłączeniem osób sprawujących urzędy Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu, Marszałka Senatu i Prezesa Rady Ministrów.

Art. 30.

Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne oraz Policja, Żandarmeria Wojskowa, Straż Graniczna i Służba Więzienna przeprowadzają samodzielne postępowania sprawdzające wobec osób ubiegających się o przyjęcie do służby lub pracy w tych organach, stosując odpowiednio przepisy ustawy. Przepis stosuje się także w stosunku do osób pełniących służbę lub zatrudnionych w tych organach i służbach.

Art. 31.

1. Przeprowadzenie postępowania sprawdzającego wymaga pisemnej zgody osoby, której ma dotyczyć, zwanej dalej „osobą sprawdzaną".

2. Podanie osoby, o której mowa w art. 29, ubiegającej się o zatrudnienie lub przyjęcie do służby na stanowisku objętym z mocy przepisów ustawy wymogiem przeprowadzenia postępowania sprawdzającego, w przypadku braku zgody osoby sprawdzanej na przeprowadzenie tego postępowania, pozostawia się bez rozpatrzenia.

3. Nie przeprowadza się postępowania sprawdzającego, jeżeli osoba, o której mowa w ust. 1, przedstawi odpowiednie poświadczenie bezpieczeństwa. Kierownik jednostki organizacyjnej informuje w terminie 7 dni organ, który wydał poświadczenie bezpieczeństwa, o zatrudnieniu osoby przedstawiającej to poświadczenie.

Art. 32.

Ustawa zezwala w zakresie niezbędnym dla ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, na zbieranie i przetwarzanie informacji o osobach trzecich, określonych w ankiecie bezpieczeństwa osobowego, o której mowa w art. 37 ust. 2 pkt 1(1), bez wiedzy i zgody tych osób.

Art. 33.

1. Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych wyższą klauzulą tajności uprawnia do dostępu do informacji niejawnych oznaczonych niższą klauzulą tajności wyłącznie w zakresie określonym w art. 3.

2. Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne" uprawnia do dostępu do informacji niejawnych oznaczonych klauzulą:

1) „tajne" - przez okres 7 lat od daty wystawienia;
2) „poufne" albo „zastrzeżone" - przez okres 10 lat od daty wystawienia.

3. Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą „tajne" uprawnia do dostępu do informacji niejawnych oznaczonych klauzulą „poufne" albo „zastrzeżone" przez okres 10 lat od daty wystawienia.

Art. 34.

Służby ochrony państwa oraz pełnomocnik ochrony, kierując się zasadami bezstronności i obiektywizmu, są obowiązani do wykazania najwyższej staranności w toku prowadzonego postępowania sprawdzającego co do jego zgodności z przepisami ustawy.

Art. 35.

1. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

2. W toku postępowania sprawdzającego ustala się, czy istnieją wątpliwości dotyczące:

1) uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej;
2) ukrywania lub świadomego niezgodnego z prawdą podawania przez osobę sprawdzaną w postępowaniu sprawdzającym informacji mających znaczenie dla ochrony informacji niejawnych, a także występowania związanych z tą osobą okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji;
3) przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim, czy osoba sprawdzana uczestniczyła lub uczestniczy, współpracowała lub współpracuje z partiami politycznymi albo innymi organizacjami, o których mowa w art. 13 Konstytucji;
4) zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu, a zwłaszcza obawy o wywieranie w tym celu presji;
5) właściwego postępowania z informacjami niejawnymi.

3. W toku postępowania sprawdzającego, o którym mowa w art. 36 ust. 1 pkt 2 i 3, ponadto ustala się, czy istnieją wątpliwości:

1) związane z wyraźną różnicą między poziomem życia osoby sprawdzanej a uzyskiwanymi przez nią dochodami;
2) związane z ewentualnymi informacjami o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do zajmowania stanowiska albo wykonywania prac związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową;
3) związane z uzależnieniem od alkoholu lub narkotyków.

4. W celu dokonania ustaleń, o których mowa w ust. 3 pkt 2 i 3, służba ochrony państwa może zobowiązać osobę sprawdzaną do poddania się specjalistycznym badaniom oraz udostępnienia wyników tych badań.

5. W razie niedających się usunąć wątpliwości, o których mowa w ust. 2 lub 3, interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami.

Art. 36.

1. W zależności od stanowiska lub zleconej pracy, o które ubiega się dana osoba, przeprowadza się postępowanie sprawdzające:

1) zwykłe - przy stanowiskach i pracach związanych z dostępem do informacji niejawnych stanowiących tajemnicę służbową;
2) poszerzone - przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „tajne";
3) specjalne - przy stanowiskach i pracach związanych z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne".

2. Postępowanie sprawdzające kończy się wydaniem poświadczenia bezpieczeństwa lub odmową wydania takiego poświadczenia.

2a. Poświadczenie bezpieczeństwa wydaje się na okres:

1) 10 lat w przypadku dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone" lub „poufne";
2) 7 lat w przypadku dostępu do informacji niejawnych oznaczonych klauzulą „tajne";
3) 5 lat w przypadku dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne".

2b. Służba ochrony państwa lub pełnomocnik ochrony umarzają postępowanie sprawdzające w przypadku:

1) śmierci osoby sprawdzanej;
2) rezygnacji osoby sprawdzanej z ubiegania się albo zajmowania stanowiska lub wykonywania pracy, łączących się z dostępem do informacji niejawnych;
3) odstąpienia przez kierownika jednostki organizacyjnej od zamiaru obsadzenia osoby sprawdzanej na stanowisku lub zlecenia jej prac związanych z dostępem do informacji niejawnych.

2c. Służba ochrony państwa lub pełnomocnik ochrony mogą zawiesić postępowanie sprawdzające w przypadku:

1) długotrwałej choroby osoby sprawdzanej, uniemożliwiającej skuteczne przeprowadzenie postępowania sprawdzającego;
2) wyjazdu za granicę osoby sprawdzanej na okres przekraczający 30 dni;
3) wszczęcia przeciwko osobie sprawdzanej postępowania karnego w sprawie o przestępstwo lub przestępstwo skarbowe, umyślne, ścigane z oskarżenia publicznego.

2d. W przypadku umorzenia postępowania sprawdzającego służba ochrony państwa lub pełnomocnik ochrony zawiadamiają wnioskodawcę oraz, w przypadkach, o których mowa w ust. 2b pkt 2 i 3, osobę sprawdzaną. W przypadku zawieszenia postępowania służba ochrony państwa lub pełnomocnik ochrony zawiadamiają wnioskodawcę i osobę sprawdzaną.

2e. Zawieszone postępowanie podejmuje się po uzyskaniu informacji o zakończeniu choroby, powrocie z zagranicy lub prawomocnym zakończeniu postępowania karnego. O podjęciu postępowania służba ochrony państwa lub pełnomocnik ochrony zawiadamiają wnioskodawcę i osobę sprawdzaną.

3. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory:

1) poświadczenia bezpieczeństwa;
2) decyzji o odmowie wydania poświadczenia bezpieczeństwa;
3) decyzji o cofnięciu poświadczenia bezpieczeństwa.

4. Poświadczenie bezpieczeństwa, decyzja o odmowie wydania poświadczenia bezpieczeństwa oraz decyzja o cofnięciu poświadczenia bezpieczeństwa powinny zawierać odpowiednio:

1) podstawę prawną;
2) wskazanie wnioskodawcy postępowania sprawdzającego;
3) określenie służby ochrony państwa lub pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające;
4) datę i miejsce wystawienia;
5) imię, nazwisko i datę urodzenia osoby sprawdzanej;
6) rodzaj przeprowadzonego postępowania sprawdzającego ze wskazaniem klauzuli informacji niejawnych, do których osoba sprawdzana może mieć dostęp;
7) stwierdzenie wydania poświadczenia bezpieczeństwa lub odmowy jego wydania bądź cofnięcia;
8) termin ważności;
9) imienną pieczęć i czytelny podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa lub pełnomocnika ochrony.

4a. Decyzja o odmowie wydania poświadczenia bezpieczeństwa i decyzja o jego cofnięciu powinny zawierać także uzasadnienie faktyczne i prawne. Można odstąpić od uzasadnienia faktycznego lub je ograniczyć w zakresie, w jakim udostępnienie informacji osobie sprawdzanej mogłoby spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej, dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa.
5. (uchylony).

Art. 37.

1. Zwykłe postępowania sprawdzające przeprowadza, z zastrzeżeniem ust. 2 i 3 oraz art. 76 ust. 3, pełnomocnik ochrony na pisemne polecenie kierownika jednostki organizacyjnej.

2. Służba ochrony państwa przeprowadza zwykłe postępowania sprawdzające wobec kandydatów na pełnomocników ochrony i pełnomocników ochrony w jednostkach organizacyjnych na pisemny wniosek osoby upoważnionej do obsady stanowiska, zgodnie z właściwością określoną w art. 29.

3. Służba ochrony państwa przeprowadza zwykłe postępowania sprawdzające wobec osób innych niż wymienione w ust. 2, gdy obowiązek taki wynika z umowy międzynarodowej zawartej przez Rzeczpospolitą Polską.

4. Zwykłe postępowanie sprawdzające obejmuje:

1) sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, a w szczególności w Krajowym Rejestrze Karnym oraz Centralnym Zarządzie Służby Więziennej, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie bezpieczeństwa osobowego, zwanej dalej „ankietą", której wzór wraz z instrukcją jej wypełnienia stanowi załącznik nr 2; ankietę po wypełnieniu oznacza się odpowiednią klauzulą tajności;
2) sprawdzenie, na pisemny wniosek pełnomocnika ochrony, przez odpowiednie służby ochrony państwa, w ewidencjach i kartotekach niedostępnych powszechnie, zawartych w ankiecie danych dotyczących osoby kandydującej lub zajmującej stanowisko związane z dostępem do informacji niejawnych, oznaczonych klauzulą „poufne";
3) rozmowę z osobą sprawdzaną, jeżeli jest to konieczne na podstawie uzyskanych informacji;
4) sprawdzenie akt stanu cywilnego dotyczących osoby sprawdzanej.

5. W toku sprawdzeń, o których mowa w ust. 4 pkt 2, służby ochrony państwa mają prawo przeprowadzić rozmowę z osobą sprawdzaną w celu usunięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach.

6. Służby ochrony państwa przekazują pełnomocnikowi ochrony pisemną informację o wynikach czynności, o których mowa w ust. 4 pkt 2.

7. Po zakończeniu zwykłego postępowania sprawdzającego z wynikiem pozytywnym pełnomocnik ochrony lub służba ochrony państwa, w przypadkach postępowań określonych w ust. 2 i 3, wydają poświadczenie bezpieczeństwa i przekazują je osobie sprawdzanej, zawiadamiając o tym osobę upoważnioną do obsady stanowiska. W przypadku negatywnego wyniku zwykłego postępowania sprawdzającego pełnomocnik ochrony lub służba ochrony państwa, w przypadkach postępowań określonych w ust. 2 i 3, odmawiają wydania poświadczenia bezpieczeństwa i doręczają decyzję o odmowie wydania poświadczenia bezpieczeństwa osobie sprawdzanej, zawiadamiając o tym osobę upoważnioną do obsady stanowiska.

8. Pełnomocnik ochrony lub służba ochrony państwa, w przypadkach postępowań określonych w ust. 2 i 3, odmawiają wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana świadomie podała w ankiecie nieprawdziwe lub niepełne dane, albo gdy nie zostaną usunięte wątpliwości, o których mowa w art. 35 ust. 2.

9. Pełnomocnik ochrony lub służba ochrony państwa, w przypadkach postępowań określonych w ust. 2 i 3, mogą odmówić wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą.

Art. 38.

1. Poszerzone postępowanie sprawdzające prowadzi właściwa służba ochrony państwa na pisemny wniosek osoby upoważnionej do obsady stanowiska. Postępowanie to obejmuje:

1) czynności, o których mowa w art. 37 ust. 4 pkt 1 i 3;
2) sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie danych zawartych w ankiecie;
3) przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej, jeżeli jest to konieczne w celu potwierdzenia danych zawartych w ankiecie;
4) rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami, jeżeli jest to konieczne na podstawie uzyskanych informacji o osobie sprawdzanej;
5) w uzasadnionych przypadkach sprawdzenie stanu i obrotów na rachunku bankowym w trybie art. 105 ust. 1 pkt 2 lit. k ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665, z późn. zm.3)) oraz zadłużenia osoby sprawdzanej, a w szczególności wobec Skarbu Państwa, jeżeli jest to konieczne w celu sprawdzenia danych zawartych w ankiecie; przepisy art. 82 § 1 i 2 oraz art. 182 ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60, Nr 85, poz. 727, Nr 86, poz. 732 i Nr 143, poz. 1199) oraz art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65, z późn. zm.4)) stosuje się odpowiednio.

2. Wywiad, o którym mowa w ust. 1 pkt 3, przeprowadzają służby ochrony państwa i stosują w tym zakresie odpowiednio przepisy ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.5)) i wydane na jego podstawie przepisy dotyczące wywiadu środowiskowego.

Art. 39.

Specjalne postępowanie sprawdzające prowadzi właściwa służba ochrony państwa na pisemny wniosek osoby upoważnionej do obsady stanowiska. Postępowanie to obejmuje czynności, o których mowa w art. 37 ust. 4 pkt 1 i w art. 38 ust. 1 pkt 2-5, a ponadto:

1) rozmowę z osobą sprawdzaną;
2) rozmowę z trzema osobami wskazanymi przez osobę sprawdzaną w celu potwierdzenia tożsamości tej osoby oraz innych informacji o osobie sprawdzanej.

Art. 40.

1. Jeżeli w toku poszerzonego lub specjalnego postępowania sprawdzającego wystąpią wątpliwości niepozwalające na ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, służba ochrony państwa zapewnia osobie sprawdzanej możliwość osobistego ustosunkowania się, w toku wysłuchania, do przesłanek faktycznych stwarzających te wątpliwości. Osoba ta może stawić się na wysłuchanie ze swoim pełnomocnikiem. Do informacji uzyskanych w wyniku wysłuchania stosuje się przepisy art. 39 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. Nr 74, poz. 676, z późn. zm.6)).

2. Służby ochrony państwa odstępują od przeprowadzenia czynności, o której mowa w ust. 1, jeżeli jej przeprowadzenie mogłoby spowodować naruszenie zasad ochrony informacji niejawnych stanowiących tajemnicę państwową.

3. Do poszerzonego i specjalnego postępowania sprawdzającego przepisy art. 37 ust. 7 stosuje się odpowiednio.

4. Służba ochrony państwa odmawia wydania poświadczenia bezpieczeństwa, jeżeli osoba sprawdzana świadomie podała w ankiecie nieprawdziwe lub niepełne dane albo gdy nie zostaną usunięte wątpliwości, o których mowa w art. 35 ust. 2 i 3.

Art. 41.

1. Odmowa wydania poświadczenia bezpieczeństwa nie jest wiążąca dla osoby upoważnionej do obsady stanowiska, z którym wiąże się dostęp do informacji niejawnych stanowiących tajemnicę służbową.

2. W razie obsady stanowiska lub zlecenia pracy osobie, w stosunku do której odmówiono wydania poświadczenia bezpieczeństwa dotyczącego informacji niejawnych oznaczonych klauzulą „poufne", osoba upoważniona do obsady stanowiska informuje o tym niezwłocznie właściwą służbę ochrony państwa.

2a. Osoba upoważniona do obsady stanowiska jest obowiązana, niezwłocznie po otrzymaniu zawiadomienia o odmowie wydania poświadczenia bezpieczeństwa, uniemożliwić dostęp do informacji niejawnych osobie, której odmowa dotyczy.

3. Postępowanie sprawdzające wobec osoby, która nie uzyskała poświadczenia bezpieczeństwa, można przeprowadzić najwcześniej po roku od daty odmowy wydania poświadczenia bezpieczeństwa.

Art. 42.
1. Wszystkie czynności przeprowadzone w toku postępowań sprawdzających muszą być rzetelnie udokumentowane i powinny być zakończone przed upływem:

1) 2 miesięcy - od daty pisemnego polecenia przeprowadzenia zwykłego postępowania sprawdzającego lub złożenia wniosku o przeprowadzenie zwykłego postępowania sprawdzającego wraz z wypełnioną ankietą;
2) 2 miesięcy - od daty złożenia wniosku o przeprowadzenie poszerzonego postępowania sprawdzającego wraz z wypełnioną ankietą;
3) 3 miesięcy - od daty złożenia wniosku o przeprowadzenie specjalnego postępowania sprawdzającego wraz z wypełnioną ankietą.

2. Akta zakończonych postępowań sprawdzających są przechowywane jako wyodrębniona część w archiwach służb, które przeprowadziły te postępowania, i mogą być udostępniane wyłącznie na pisemne żądanie:

1) sądowi lub prokuratorowi dla celów postępowania karnego;
2) służbom ochrony państwa dla celów postępowania sprawdzającego oraz potwierdzenia faktu wydania poświadczenia bezpieczeństwa;
3) Prezesowi Rady Ministrów, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Służby Kontrwywiadu Wojskowego, Szefowi Służby Wywiadu Wojskowego, Szefowi Centralnego Biura Antykorupcyjnego, Komendantowi Głównemu Policji, Komendantowi Głównemu Żandarmerii Wojskowej, Komendantowi Głównemu Straży Granicznej lub Dyrektorowi Generalnemu Służby Więziennej w celu rozpatrzenia odwołania;
4) sądowi administracyjnemu w związku z rozpatrywaniem skargi.

3. Akta zakończonych postępowań sprawdzających, prowadzonych w odniesieniu do osób ubiegających się o stanowisko lub zlecenie pracy, z którymi łączy się dostęp do informacji niejawnych stanowiących tajemnicę służbową, są przechowywane przez pełnomocnika ochrony i są udostępniane do wglądu wyłącznie na pisemne żądanie:

1) osobie sprawdzanej;
2) sądowi lub prokuratorowi dla celów postępowania karnego;
3) Prezesowi Rady Ministrów, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Służby Kontrwywiadu Wojskowego, Szefowi Służby Wywiadu Wojskowego, Szefowi Centralnego Biura Antykorupcyjnego, Komendantowi Głównemu Policji, Komendantowi Głównemu Żandarmerii Wojskowej, Komendantowi Głównemu Straży Granicznej lub Dyrektorowi Generalnemu Służby Więziennej w celu rozpatrzenia odwołania;
4) sądowi administracyjnemu w związku z rozpatrywaniem skargi;
5) osobie upoważnionej do obsady stanowiska, pełnomocnikom ochrony lub właściwym służbom ochrony państwa dla celów postępowania sprawdzającego lub kontroli, o której mowa w art. 14 ust. 1 pkt 1.

4. W przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji jednostki organizacyjnej akta, o których mowa w ust. 3, przejmuje jej następca prawny, a w jego braku - właściwa służba ochrony państwa.

5. Służby ochrony państwa, każda w zakresie swojego działania, prowadzą ewidencje osób, które uzyskały poświadczenie bezpieczeństwa, a także osób, które zajmują stanowiska lub wykonują prace, z którymi łączy się dostęp do informacji niejawnych oznaczonych klauzulą „poufne" lub stanowiących tajemnicę państwową, oraz ewidencje osób, którym odmówiono wydania poświadczenia bezpieczeństwa, a także wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa.

6. Dane z ewidencji, o których mowa w ust. 5, mogą obejmować wyłącznie:

1) w odniesieniu do osoby - jej imię i nazwisko, numer PESEL, imię ojca, datę i miejsce urodzenia, adres miejsca zamieszkania lub pobytu, nazwę i adres jednostki organizacyjnej, w której osoba jest zatrudniona, nazwę komórki organizacyjnej i stanowiska oraz sygnaturę akt postępowania sprawdzającego;
2) w odniesieniu do stanowiska lub pracy zleconej - datę objęcia stanowiska lub rozpoczęcia pracy, określenie, z dostępem do jakich informacji niejawnych łączy się to stanowisko, datę wydania i numer poświadczenia bezpieczeństwa.

7. Dane z ewidencji, o których mowa w ust. 5, są udostępniane wyłącznie na pisemne żądanie:

1) sądowi lub prokuratorowi dla celów postępowania karnego;
2) służbom ochrony państwa dla celów postępowania sprawdzającego oraz potwierdzenia faktu wydania poświadczenia bezpieczeństwa;
3) Prezesowi Rady Ministrów, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Służby Kontrwywiadu Wojskowego, Szefowi Służby Wywiadu Wojskowego, Szefowi Centralnego Biura Antykorupcyjnego, Komendantowi Głównemu Policji, Komendantowi Głównemu Żandarmerii Wojskowej, Komendantowi Głównemu Straży Granicznej lub Dyrektorowi Generalnemu Służby Więziennej w celu rozpatrzenia odwołania;
4) sądowi administracyjnemu w związku z rozpatrywaniem skargi.
Dane udostępnia szef właściwej służby ochrony państwa bądź upoważniony przez niego funkcjonariusz lub żołnierz.

8. Udostępnianie akt umorzonych postępowań sprawdzających oraz danych zebranych w ich toku odbywa się odpowiednio na zasadach określonych w ust. 2, 3 i 7.

Art. 43. (uchylony).

Art. 44.

1. Na pisemny wniosek osoby upoważnionej do obsady stanowiska, złożony co najmniej na 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa, służba ochrony państwa, organy i służby wymienione w art. 30 oraz pełnomocnicy ochrony, w przypadkach postępowań sprawdzających wymienionych w art. 37 ust. 1, przeprowadzają kolejne postępowanie sprawdzające.

2. Kolejne postępowanie sprawdzające powinno być zakończone przed upływem terminu ważności poświadczenia bezpieczeństwa. W przypadku kolejnego postępowania sprawdzającego terminy, o których mowa w art. 42 ust. 1, nie mają zastosowania.

Art. 45.

1. W przypadku gdy w odniesieniu do osoby, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe fakty wskazujące, że nie daje ona rękojmi zachowania tajemnicy, służby ochrony państwa lub pełnomocnik ochrony przeprowadzają kontrolne postępowanie sprawdzające z pominięciem terminów, o których mowa w art. 36 ust. 2a, i obowiązku wypełnienia nowej ankiety przez osobę sprawdzaną.

2. O wszczęciu kontrolnego postępowania sprawdzającego, o którym mowa w ust. 1, służby ochrony państwa lub pełnomocnik ochrony zawiadamiają kierownika jednostki organizacyjnej lub osobę odpowiedzialną za obsadę stanowiska wraz z wnioskiem o ograniczenie lub wyłączenie dostępu do informacji niejawnych osobie sprawdzanej.

3. Po otrzymaniu zawiadomienia, o którym mowa w ust. 2, kierownik jednostki organizacyjnej lub osoba odpowiedzialna za obsadę stanowiska informują osobę sprawdzaną o wszczęciu kontrolnego postępowania sprawdzającego oraz ograniczają lub wyłączają jej dostęp do informacji niejawnych.

Art. 46.

Do kolejnego lub kontrolnego postępowania sprawdzającego stosuje się przepisy ustawy odnoszące się do właściwego postępowania sprawdzającego, z uwzględnieniem art. 47.

Art. 47.

1. Kontrolne postępowanie sprawdzające prowadzone przez służbę ochrony państwa lub pełnomocnika ochrony, wszczęte na podstawie art. 45 ust. 1, kończy się:

1) wydaniem decyzji o cofnięciu poświadczenia bezpieczeństwa albo
2) poinformowaniem osób, o których mowa w art. 45 ust. 2, i osoby sprawdzanej, o braku zastrzeżeń w stosunku do osoby, którą objęto kontrolnym postępowaniem sprawdzającym, z jednoczesnym potwierdzeniem jej dalszej zdolności do zachowania tajemnicy w zakresie określonym w posiadanym przez nią poświadczeniu bezpieczeństwa.

2. Do decyzji, o której mowa w ust. 1 pkt 1, stosuje się odpowiednio przepisy art. 41.

3. Do kontrolnego postępowania sprawdzającego przepisy art. 36 ust. 2b-2e stosuje się odpowiednio.

Art. 48.

1. Pełnomocnik ochrony prowadzi wykaz stanowisk i prac zleconych oraz osób dopuszczonych do pracy lub służby na stanowiskach, z którymi wiąże się dostęp do informacji niejawnych.

2. Pełnomocnik ochrony jest obowiązany przekazać właściwej służbie ochrony państwa dane wymagane do 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 do ewidencji osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa.

3. W sprawach, o których mowa w ust. 1 i 2, stosuje się odpowiednio przepisy art. 42 ust. 5 i 6 oraz przepisy wydane na podstawie art. 42 ust. 7.

Rozdział 5a
Postępowanie odwoławcze i skargowe

Art. 48a.

1. Od decyzji o odmowie wydania poświadczenia bezpieczeństwa lub decyzji o cofnięciu poświadczenia bezpieczeństwa służy osobie sprawdzanej odwołanie do Prezesa Rady Ministrów, z zastrzeżeniem art. 48i ust. 1.

2. Odwołanie nie wymaga uzasadnienia.

3. Odwołanie wnosi się w terminie 14 dni od dnia doręczenia osobie sprawdzanej decyzji o odmowie wydania poświadczenia bezpieczeństwa lub decyzji o cofnięciu poświadczenia bezpieczeństwa, za pośrednictwem właściwej służby ochrony państwa.

Art. 48b.

1. Służba ochrony państwa jest obowiązana przesłać odwołanie wraz z aktami postępowania sprawdzającego Prezesowi Rady Ministrów w terminie 14 dni od dnia, w którym otrzymała odwołanie.

2. Rozpatrzenie odwołania powinno nastąpić nie później niż w ciągu 3 miesięcy od dnia otrzymania odwołania.

3. Do postępowania odwoławczego przepisy art. 36 ust. 2d oraz 2e stosuje się odpowiednio.

Art. 48c.

1. Prezes Rady Ministrów stwierdza, w drodze postanowienia, niedopuszczalność odwołania oraz uchybienie terminu do wniesienia odwołania. Postanowienie w tej sprawie jest ostateczne.

2. Postanowienie powinno zawierać w szczególności datę jego wydania, oznaczenie osoby sprawdzanej, powołanie podstawy prawnej, rozstrzygnięcie, uzasadnienie faktyczne i prawne oraz pouczenie o dopuszczalności i terminie wniesienia skargi do sądu administracyjnego.

Art. 48d.

Prezes Rady Ministrów może na żądanie osoby sprawdzanej lub z urzędu zlecić służbie ochrony państwa przeprowadzenie dodatkowych czynności w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym.

Art. 48e.

1. Prezes Rady Ministrów umarza postępowanie odwoławcze w przypadku:

1) śmierci osoby sprawdzanej lub
2) cofnięcia odwołania przez osobę sprawdzaną przed wydaniem decyzji, o której mowa w art. 48f ust. 1.

2. Prezes Rady Ministrów nie uwzględnia cofnięcia odwołania, jeżeli prowadziłoby to do naruszającego prawo lub interes bezpieczeństwa państwa utrzymania w mocy decyzji o odmowie wydania poświadczenia bezpieczeństwa.

Art. 48f.

1. Prezes Rady Ministrów wydaje decyzję, w której:

1) utrzymuje w mocy decyzję o odmowie wydania poświadczenia bezpieczeństwa lub decyzję o cofnięciu poświadczenia bezpieczeństwa albo
2) uchyla decyzję o odmowie wydania poświadczenia bezpieczeństwa i nakazuje służbie ochrony państwa wydanie poświadczenia bezpieczeństwa, albo
3) uchyla decyzję o cofnięciu poświadczenia bezpieczeństwa.

2. Można odstąpić od uzasadnienia faktycznego decyzji lub je ograniczyć w zakresie, w jakim udostępnienie informacji osobie sprawdzanej mogłoby spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa.

Art. 48g.

Po wydaniu decyzji lub postanowienia Prezes Rady Ministrów niezwłocznie zwraca właściwej służbie ochrony państwa akta, o których mowa w art. 48b ust. 1.

Art. 48h.

Decyzje i postanowienia doręcza się na piśmie osobie sprawdzanej i właściwej służbie ochrony państwa, zawiadamiając o rozstrzygnięciu zawartym w decyzji lub postanowieniu osobę upoważnioną do obsady stanowiska.

Art. 48i.

1. Od wydanej przez pełnomocnika ochrony decyzji o odmowie wydania poświadczenia bezpieczeństwa lub decyzji o cofnięciu poświadczenia bezpieczeństwa – osobie sprawdzanej służy odwołanie odpowiednio do Szefa Agencji Bezpieczeństwa Wewnętrznego albo Szefa Służby Kontrwywiadu Wojskowego.

2. Do postępowania odwoławczego przed Szefem Agencji Bezpieczeństwa Wewnętrznego lub Szefem Służby Kontrwywiadu Wojskowego stosuje się odpowiednio przepisy ustawy dotyczące postępowania odwoławczego przed Prezesem Rady Ministrów, z zastrzeżeniem ust. 3.

3. Odwołanie do Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Służby Kontrwywiadu Wojskowego składa się za pośrednictwem pełnomocnika ochrony, który odmówił wydania poświadczenia bezpieczeństwa.

Art. 48j.

Osobie sprawdzanej przysługuje skarga do sądu administracyjnego na decyzję utrzymującą w mocy decyzję o odmowie wydania poświadczenia bezpieczeństwa lub decyzję o cofnięciu poświadczenia bezpieczeństwa oraz na postanowienie, o którym mowa w art. 48c ust. 1, w terminie określonym w art. 53 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1270, z 2004 r. Nr 162, poz. 1692 oraz z 2005 r. Nr 94, poz. 788 i Nr 169, poz. 1417).

Art. 48k.

1. Sąd administracyjny rozpoznaje skargę na posiedzeniu niejawnym.

2. Przepisów art. 55 § 2 i art. 106 § 2 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi nie stosuje się.

3. Wyrok wydany na posiedzeniu niejawnym uzasadnia się tylko w przypadku uwzględnienia skargi. Odpis wyroku z uzasadnieniem doręcza się tylko właściwej służbie ochrony państwa. Skarżącemu oraz osobie upoważnionej do obsady stanowiska doręcza się odpis wyroku.

Art. 48l.

Po wydaniu wyroku sąd administracyjny niezwłocznie zwraca właściwej służbie ochrony państwa akta postępowania sprawdzającego.

Art. 48ł.

Do skargi kasacyjnej stosuje się odpowiednio art. 48k ust. 1 i 3 oraz art. 48l ustawy.

Art. 48m.

W zakresie postępowania odwoławczego i skargowego, dotyczącego postępowania sprawdzającego przeprowadzonego w trybie art. 30, przepisy niniejszego rozdziału dotyczące:
1) służby ochrony państwa stosuje się do Policji, Żandarmerii Wojskowej, Straży Granicznej, Agencji Wywiadu lub Służby Więziennej;
2) Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Służby Kontrwywiadu Wojskowego stosuje się do Szefa Agencji Wywiadu, Szefa Służby Wywiadu Wojskowego, Szefa Centralnego Biura Antykorupcyjnego, Komendanta Głównego Policji, Komendanta Głównego Żandarmerii Wojskowej, Komendanta Głównego Straży Granicznej lub Dyrektora Generalnego Służby Więziennej.

Rozdział 6
Udostępnianie informacji niejawnych

Art. 49.

1. Szef Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu lub Prezesa Rady Ministrów albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku właściwa służba ochrony państwa, może wyrazić pisemną zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę państwową osobie lub jednostce organizacyjnej, wobec której wszczęto postępowanie sprawdzające. Odpis zgody przekazuje się właściwej służbie ochrony państwa.

2. Zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę służbową osobie, wobec której wszczęto zwykłe postępowanie sprawdzające, może wyrazić - w formie pisemnej - kierownik jednostki organizacyjnej, w której ta osoba jest zatrudniona lub wykonuje prace zlecone.

3. W wyjątkowych, szczególnie uzasadnionych przypadkach, z zastrzeżeniem art. 4 ust. 1, podmioty, o których mowa w ust. 1 i 2, mogą wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa lub jednostce organizacyjnej nieposiadającej świadectwa bezpieczeństwa przemysłowego.

4. Wyrażenie zgody na udostępnienie informacji niejawnych określa zakres podmiotowy i przedmiotowy udostępnienia oraz nie oznacza zmiany lub zniesienia ich klauzuli tajności.

Rozdział 7
Kancelarie tajne. Kontrola obiegu dokumentów

Art. 50.

1. Jednostka organizacyjna, w której są wytwarzane, przetwarzane, przekazywane lub przechowywane dokumenty zawierające informacje niejawne oznaczone klauzulą „poufne" lub stanowiące tajemnicę państwową, ma obowiązek zorganizowania kancelarii, zwanej dalej „kancelarią tajną". W przypadku uzasadnionym względami organizacyjnymi kierownik jednostki organizacyjnej może utworzyć więcej niż jedną kancelarię tajną.

2. Kancelaria tajna stanowi wyodrębnioną komórkę organizacyjną podległą bezpośrednio pełnomocnikowi ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie takich dokumentów uprawnionym osobom. Kancelaria tajna powinna być zorganizowana w wyodrębnionym pomieszczeniu, zabezpieczonym zgodnie z przepisami o środkach ochrony fizycznej informacji niejawnych i być obsługiwana przez pracowników pionu ochrony.

Art. 51.

W kancelarii tajnej dokumenty o różnych klauzulach powinny być fizycznie od siebie oddzielone i obsługiwane przez osobę posiadającą poświadczenie bezpieczeństwa odpowiednie do najwyższej klauzuli wytwarzanych, przetwarzanych, przekazywanych lub przechowywanych w kancelarii dokumentów.

Art. 52.

1. Organizacja pracy kancelarii tajnej musi zapewniać możliwość ustalenia w każdych okolicznościach, gdzie znajduje się dokument klasyfikowany pozostający w dyspozycji jednostki organizacyjnej.

2. Dokumenty oznaczone klauzulami: „ściśle tajne" i „tajne" mogą być wydawane poza kancelarię tajną jedynie w przypadku, gdy odbiorca zapewnia warunki ochrony takich dokumentów przed nieuprawnionym ujawnieniem. W razie wątpliwości co do zapewnienia warunków ochrony, dokument może być udostępniony wyłącznie w kancelarii tajnej.

3. Kancelaria tajna odmawia udostępnienia lub wydania dokumentu, o którym mowa w art. 50 ust. 1, osobie nieposiadającej stosownego poświadczenia bezpieczeństwa.

4. Fakt zapoznania się przez osobę uprawnioną z dokumentem zawierającym informacje niejawne stanowiące tajemnicę państwową podlega odnotowaniu w karcie zapoznania się z tym dokumentem.

Art. 52a.

1. W jednostkach organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2, dopuszcza się organizowanie innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych.

2. Do komórek organizacyjnych, o których mowa w ust. 1, przepisy art. 51 i 52 stosuje się odpowiednio.

Art. 53.

1. Rada Ministrów określi, w drodze rozporządzenia, wymagania w zakresie organizacji i funkcjonowania kancelarii tajnych. Rozporządzenie powinno określać:

1) strukturę organizacyjną kancelarii, z uwzględnieniem możliwości tworzenia jej oddziałów;
2) podstawowe zadania kierownika kancelarii;
3) zakres i warunki stosowania środków ochrony fizycznej, z uwzględnieniem klauzul tajności przechowywanych przez kancelarię dokumentów;
4) tryb obiegu informacji niejawnych;
5) wzór karty zapoznania z dokumentem.

2. Ministrowie właściwi do spraw: wewnętrznych, administracji publicznej, zagranicznych, finansów publicznych, budżetu i instytucji finansowych. Minister Sprawiedliwości, Prezes Narodowego Banku Polskiego, Prezes Najwyższej Izby Kontroli, Szefowie Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu oraz Prezesa Rady Ministrów, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego, Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef Biura Ochrony Rządu, a także Prezes Instytutu Pamięci Narodowej — Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu określą, w drodze zarządzenia, każdy w zakresie swojego działania, szczególny sposób organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.

3. Minister Obrony Narodowej określi, w drodze zarządzenia, szczególny sposób organizacji kancelarii tajnych oraz komórek organizacyjnych, o których mowa w art. 52a ust. 1, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb i sposób przyjmowania, przewożenia, wydawania i ochrony materiałów w celu ich zabezpieczenia przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

Rozdział 8
Szkolenie w zakresie ochrony informacji niejawnych

Art. 54.

1. Dopuszczenie do pracy lub służby, z którymi łączy się dostęp do informacji niejawnych, poprzedza szkolenie w zakresie ochrony informacji niejawnych prowadzone w celu zapoznania się z:

1) zagrożeniami ze strony obcych służb specjalnych działających przeciwko Rzeczypospolitej Polskiej i państwom sojuszniczym, a także z zagrożeniami ze strony organizacji terrorystycznych;
2) przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności za ich ujawnienie;
3) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby;
4) sposobami ochrony informacji niejawnych stanowiących tajemnicę państwową oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia;

5) odpowiedzialnością karną, dyscyplinarną i służbową za naruszenie przepisów o ochronie informacji niejawnych.

2. Szkolenie, o którym mowa w ust. 1, przeprowadzają:

1) funkcjonariusze i żołnierze służb ochrony państwa - w stosunku do osób, o których mowa w art. 27 ust. 3-8, a także w stosunku do pełnomocników ochrony i ich zastępców;
2) pełnomocnicy ochrony - w stosunku do osób zatrudnionych lub pełniących służbę w jednostkach organizacyjnych.

3. Koszty szkolenia pokrywa jednostka organizacyjna, w której osoba szkolona jest zatrudniona lub pełni służbę.
3a. Szkolenie uzupełniające pełnomocników ochrony i ich zastępców przeprowadza się nie rzadziej niż co 5 lat.

4. Wzajemne prawa i obowiązki organizatora i uczestnika szkolenia, o którym mowa w ust. 2 pkt 1, określa umowa zawarta między tymi stronami.

Art. 55.
Prezes Rady Ministrów określi, w drodze rozporządzenia, wzory zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych, z uwzględnieniem odrębności wynikających z wydawania zaświadczeń przez służby ochrony państwa i pełnomocników ochrony.

Rozdział 9
Środki ochrony fizycznej informacji niejawnych

Art. 56.

1. Jednostki organizacyjne, w których materiały zawierające informacje niejawne są wytwarzane, przetwarzane, przekazywane lub przechowywane, mają obowiązek stosowania środków ochrony fizycznej w celu uniemożliwienia osobom nieupoważnionym dostępu do takich informacji, a w szczególności przed:

1) działaniem obcych służb specjalnych;
2) zamachem terrorystycznym lub sabotażem;
3) kradzieżą lub zniszczeniem materiału;
4) próbą wejścia osób nieuprawnionych;
5) nieuprawnionym dostępem pracowników do materiałów oznaczonych wyższą klauzulą tajności.

2. Zakres stosowania środków ochrony fizycznej musi odpowiadać klauzuli tajności i ilości informacji niejawnych, liczbie oraz poziomowi dostępu do takich informacji zatrudnionych lub pełniących służbę osób oraz uwzględniać wskazania służb ochrony państwa dotyczące w szczególności ochrony przed zagrożeniami ze strony obcych służb specjalnych, także w stosunku do państwa sojuszniczego.

Art. 57

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych, należy w szczególności:
1) wydzielić części obiektów, które poddane są szczególnej kontroli wejść i wyjść oraz kontroli przebywania, zwane dalej „strefami bezpieczeństwa";
2) wydzielić wokół stref bezpieczeństwa strefy administracyjne służące do kontroli osób lub pojazdów;
3) wprowadzić system przepustek lub inny system określający uprawnienia do wejścia, przebywania i wyjścia ze strefy bezpieczeństwa, a także przechowywania kluczy do pomieszczeń chronionych, szaf

pancernych i innych pojemników służących do przechowywania informacji niejawnych stanowiących tajemnicę państwową;
4) zapewnić kontrolę stref bezpieczeństwa i stref administracyjnych przez przeszkolonych zgodnie z ustawą pracowników pionu ochrony;
5) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym na podstawie odrębnych przepisów przyznano certyfikaty lub świadectwa kwalifikacyjne.

Art. 58.

1. W uzasadnionych przypadkach dla zapewnienia ochrony informacji niejawnych stanowiących tajemnicę państwową, w szczególności rozmów i spotkań, których przedmiotem są takie informacje, wydziela się specjalne strefy bezpieczeństwa, które są poddawane stałej kontroli w zakresie stosowania środków ochrony fizycznej informacji niejawnych.

2. Urządzanie i wyposażanie pomieszczeń objętych specjalną strefą bezpieczeństwa uwzględnia zastosowanie środków zabezpieczających te pomieszczenia przed podsłuchem i podglądem.

3. Do specjalnej strefy bezpieczeństwa zakazuje się wnoszenia oraz wynoszenia przedmiotów i urządzeń bez uprzedniego ich sprawdzenia przez upoważnionych pracowników pionu ochrony.

Art. 59.

Pełnomocnicy ochrony są obowiązani do bieżącego nadzoru nad stosowaniem środków ochrony fizycznej.

Rozdział 10
Bezpieczeństwo systemów i sieci teleinformatycznych

Art. 60.

1. Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

2. Akredytacja, o której mowa w ust. 1, następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.

3. Urządzenia i narzędzia kryptograficzne, służące do ochrony informacji niejawnych stanowiących tajemnicę państwową lub tajemnicę służbową oznaczonych klauzulą „poufne", podlegają badaniom i certyfikacji prowadzonym przez służby ochrony państwa.

4. W wyniku badań i certyfikacji, o których mowa w ust. 3, służby ochrony państwa wydają wzajemnie uznawane certyfikaty ochrony kryptograficznej.

5. Wytwarzanie, przetwarzanie, przechowywanie lub przekazywanie informacji niejawnych stanowiących tajemnicę państwową, odpowiednio do ich klauzuli tajności, jest dopuszczalne po uzyskaniu certyfikatu akredytacji bezpieczeństwa teleinformatycznego dla systemu lub sieci teleinformatycznej, wydanego przez właściwą służbę ochrony państwa.

6. Certyfikat, o którym mowa w ust. 5, wydaje się na podstawie:

1) przeprowadzonych zgodnie z ustawą postępowań sprawdzających wobec osób mających dostęp do systemu lub sieci teleinformatycznej;

2) zatwierdzonych przez właściwą służbę ochrony państwa dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji;
3) audytu bezpieczeństwa systemu lub sieci teleinformatycznej, polegającego na weryfikacji poprawności realizacji wymagań i procedur, określonych w dokumentach szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.

7. Szef właściwej służby ochrony państwa po zapoznaniu się z wynikiem analizy ryzyka dla bezpieczeństwa informacji niejawnych może, bez spełnienia niektórych wymagań w zakresie ochrony fizycznej, elektromagnetycznej lub kryptograficznej, dokonać, na czas określony, nie dłuższy jednak niż na 2 lata, akredytacji bezpieczeństwa teleinformatycznego systemu lub sieci teleinformatycznej, którym przyznano określoną klauzulę tajności, w przypadku gdy brak możliwości ich eksploatacji powodowałby zagrożenie dla porządku publicznego, obronności, bezpieczeństwa albo interesów międzynarodowych państwa.

8. Kierownicy jednostek organizacyjnych organów uprawnionych do prowadzenia na mocy odrębnych przepisów czynności operacyjno-rozpoznawczych mogą podjąć decyzję o eksploatacji środków technicznych umożliwiających uzyskiwanie, przetwarzanie, przechowywanie i przekazywanie w sposób tajny informacji oraz utrwalanie dowodów, bez konieczności spełnienia wymagań określonych w ust. 1 i 3 oraz 5 i 6, w przypadkach gdy ich spełnienie uniemożliwiałoby lub w znacznym stopniu utrudniałoby realizację czynności operacyjnych.

Art. 61.

1. Dokumenty szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej powinny być kompletnym i wyczerpującym opisem ich budowy, zasad działania i eksploatacji. Dokumenty te opracowuje się w fazie projektowania, bieżąco uzupełnia w fazie wdrażania i modyfikuje w fazie eksploatacji przed dokonaniem zmian w systemie lub sieci teleinformatycznej.

2. Procedury bezpiecznej eksploatacji opracowuje się i uzupełnia w fazie wdrażania oraz modyfikuje w fazie eksploatacji przed dokonaniem zmian w systemie lub sieci teleinformatycznej.

3. Dokumenty, o których mowa w ust. 1, oraz procedury, o których mowa w ust. 2, opracowuje oraz przekazuje służbie ochrony państwa kierownik jednostki organizacyjnej, który jest także odpowiedzialny za eksploatację i bezpieczeństwo systemu lub sieci teleinformatycznej.

4. Dokumenty szczególnych wymagań bezpieczeństwa oraz procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę państwową, są w każdym przypadku indywidualnie zatwierdzane przez właściwą służbę ochrony państwa w terminie 30 dni od dnia ich otrzymania.

5. Dokumenty szczególnych wymagań bezpieczeństwa oraz procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę służbową, są przedstawiane właściwej służbie ochrony państwa. Niewniesienie zastrzeżeń przez służbę ochrony państwa do tych wymagań, w terminie 30 dni od dnia ich przedstawienia, uprawnia do przejścia do kolejnej fazy budowy systemu lub sieci teleinformatycznej, o której mowa w ust. 1.

Art. 62.

1. Prezes Rady Ministrów określi, w drodze rozporządzenia, podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy i sieci teleinformatyczne służące do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, oraz sposób

opracowywania dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji tych systemów i sieci.

2. W rozporządzeniu, o którym mowa w ust. 1, określa się w szczególności podstawowe wymagania bezpieczeństwa teleinformatycznego w zakresie ochrony fizycznej, elektromagnetycznej, kryptograficznej, niezawodności transmisji, kontroli dostępu w sieciach lub systemach teleinformatycznych służących do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych. W dokumentach szczególnych wymagań bezpieczeństwa określa się środki ochrony kryptograficznej, elektromagnetycznej, technicznej i organizacyjnej systemu lub sieci teleinformatycznej. Procedury bezpiecznej eksploatacji obejmują sposób i tryb postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych oraz określają zakres odpowiedzialności użytkowników systemu lub sieci teleinformatycznych i pracowników mających do nich dostęp.

Art. 63.

1. Za przeprowadzenie czynności, o których mowa w art. 60 ust. 3-6, pobiera się opłaty.

2. Z opłat, o których mowa w ust. 1, są zwolnione jednostki organizacyjne będące jednostkami budżetowymi.

3. Przedsiębiorcy obowiązani na podstawie odrębnych ustaw do wykonywania zadań publicznych na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego zwolnieni są z opłat za przeprowadzenie czynności, o których mowa w art. 60 ust. 5 i 6, w przypadku akredytacji bezpieczeństwa teleinformatycznego systemów i sieci teleinformatycznych niezbędnych do wykonania tych zadań.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość opłat, o których mowa w ust. 1, z uwzględnieniem kosztów ponoszonych na przeprowadzenie czynności, o których mowa w art. 60 ust. 3-6.

Art. 64.

1. Kierownik jednostki organizacyjnej wyznacza:

1) osobę lub zespół osób, odpowiedzialnych za funkcjonowanie systemów lub sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych, zwane dalej „administratorem systemu";
2) pracownika lub pracowników pionu ochrony pełniących funkcje inspektorów bezpieczeństwa teleinformatycznego, odpowiedzialnych za bieżącą kontrolę zgodności funkcjonowania sieci lub systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz za kontrolę przestrzegania procedur bezpiecznej eksploatacji, o których mowa w art. 61 ust. 2.

2. Służby ochrony państwa udzielają kierownikom jednostek organizacyjnych pomocy niezbędnej dla realizacji ich zadań, w szczególności wydając zalecenia w zakresie bezpieczeństwa teleinformatycznego.

3. Stanowiska lub funkcje administratora systemu albo inspektora bezpieczeństwa teleinformatycznego mogą zajmować lub pełnić osoby określone w art. 18 ust. 5, posiadające poświadczenia bezpieczeństwa odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemach lub sieciach teleinformatycznych, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez służby ochrony państwa.

Rozdział 11
Bezpieczeństwo przemysłowe

Art. 65.

Przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa, zamierzający ubiegać się, ubiegający się o zawarcie lub wykonujący umowę związaną z dostępem do informacji niejawnych, zwaną dalej „umową", albo wykonujący na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych, mają obowiązek zapewnienia warunków do ochrony informacji niejawnych.

Art. 66.

1. Dokumentem potwierdzającym zdolność przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej do ochrony informacji niejawnych stanowiących tajemnicę państwową jest świadectwo bezpieczeństwa przemysłowego wydane po przeprowadzeniu postępowania sprawdzającego, zwanego dalej „postępowaniem bezpieczeństwa przemysłowego".

2. Postępowanie bezpieczeństwa przemysłowego przeprowadzają:

1) Służba Kontrwywiadu Wojskowego, jeżeli:

a) zlecającym umowę lub zadanie mają być Siły Zbrojne oraz jednostki organizacyjne podległe lub nadzorowane przez Ministra Obrony Narodowej,
b) wykonawcami umowy lub zadania mają być jednostki organizacyjne wymienione w lit. a;

2) Agencja Bezpieczeństwa Wewnętrznego w innych przypadkach niż wymienione w pkt 1.

3. Podział kompetencji określony w ust. 2 odnosi się również do:

1) przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych będących podwykonawcami tych umów lub zadań;
2) postępowań sprawdzających, o których mowa w art. 37 ust. 2 i 3.

4. W zależności od stopnia zdolności do ochrony informacji niejawnych stanowiących tajemnicę państwową o określonej klauzuli wydaje się świadectwo bezpieczeństwa przemysłowego odpowiednio:

1) pierwszego stopnia - potwierdzające pełną zdolność przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej do ochrony tych informacji;
2) drugiego stopnia - potwierdzające zdolność przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej do ochrony tych informacji, z wyłączeniem możliwości ich wytwarzania, przechowywania, przekazywania lub przetwarzania we własnych systemach i sieciach teleinformatycznych;
3) trzeciego stopnia - potwierdzające zdolność przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej do ochrony tych informacji, z wyłączeniem możliwości ich wytwarzania, przechowywania, przekazywania lub przetwarzania w użytkowanych przez niego obiektach.

5. Właściwa służba ochrony państwa nie przeprowadza postępowania bezpieczeństwa przemysłowego, jeżeli przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa przedstawią odpowiednie świadectwo bezpieczeństwa przemysłowego wydane przez drugą służbę ochrony państwa.

Art. 67.

Służba ochrony państwa przeprowadza postępowanie wobec przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej, sprawdzające zdolność do ochrony informacji niejawnych stanowiących tajemnicę służbową, tylko wtedy, gdy z umów międzynarodowych zawartych przez Rzeczpospolitą Polską lub z prawa wewnętrznego strony zlecającej umowę wynika obowiązek uzyskania świadectwa bezpieczeństwa przemysłowego upoważniającego do wykonywania umów związanych z dostępem do informacji niejawnych oznaczonych klauzulą „poufne" lub jej zagranicznym odpowiednikiem.

Art. 68.

1. Właściwa służba ochrony państwa przeprowadza postępowanie bezpieczeństwa przemysłowego na wniosek przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej, o których mowa w art. 1 ust. 2 pkt 5.

2. We wniosku, o którym mowa w ust. 1, przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa określają stopień świadectwa bezpieczeństwa przemysłowego, o które ubiegają się, z uwzględnieniem klauzuli tajności.

3. Do wniosku, o którym mowa w ust. 1, dołącza się ankiety osób określonych w ust. 4 lub kopie posiadanych przez te osoby poświadczeń bezpieczeństwa wydanych przez służby ochrony państwa i kwestionariusz bezpieczeństwa przemysłowego, o którym mowa w art. 69.

4. W toku postępowania bezpieczeństwa przemysłowego przeprowadza się postępowanie sprawdzające wobec:

1) osoby lub osób, które u przedsiębiorcy, w jednostce naukowej lub badawczo-rozwojowej zajmują stanowisko kierownika jednostki organizacyjnej, o którym mowa w art. 18 ust. 1;
2) osób zatrudnionych w pionie ochrony;
3) administratora systemu, o ile podmiot wnioskujący będzie wytwarzał, przechowywał, przetwarzał lub przekazywał informacje niejawne stanowiące tajemnicę państwową we własnych systemach i sieciach teleinformatycznych;
4) osób wskazanych w kwestionariuszu bezpieczeństwa przemysłowego, mających kierować wykonaniem umowy lub zadania albo uczestniczyć w ich bezpośredniej realizacji u przedsiębiorcy, w jednostce naukowej lub badawczo-rozwojowej;
5) osób wskazanych w kwestionariuszu bezpieczeństwa przemysłowego, które w imieniu przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej uczestniczą w czynnościach zmierzających do zawarcia umowy.

5. Do osób, o których mowa w ust. 4, z wyjątkiem osób zajmujących stanowisko pełnomocnika ochrony, pracownika pionu ochrony oraz administratora systemu, nie stosuje się wymogu posiadania obywatelstwa polskiego, o którym mowa w art. 28 ust. 1 pkt 1.

6. W toku postępowania bezpieczeństwa przemysłowego sprawdzeniu podlegają:

1) struktura kapitału oraz powiązania kapitałowe przedsiębiorcy;
2) struktura organizacyjna przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej oraz ich władz i organów;
3) sytuacja finansowa i źródła pochodzenia środków finansowych pozostających w dyspozycji podmiotów określonych w pkt 2;
4) osoby zarządzające lub wchodzące w skład organów zarządzających albo kontrolnych przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej, a także osoby działające z ich upoważnienia - na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, w tym niedostępnych powszechnie;

5) system ochrony osób, materiałów i obiektów u przedsiębiorcy, w jednostce naukowej lub badawczo-rozwojowej, ze szczególnym uwzględnieniem elementów systemu ochrony informacji niejawnych.

7. Do sprawdzenia, o którym mowa w ust. 6, stosuje się odpowiednio art. 14 ust. 3, z tym że przez sprawdzenie rękojmi zachowania tajemnicy należy rozumieć sprawdzenie zdolności finansowej i organizacyjnej do zapewnienia ochrony informacji niejawnych.

Art. 69.

1. Sprawdzenie, o którym mowa w art. 68 ust. 6, prowadzi się na podstawie danych zawartych w wypełnionym przez przedsiębiorcę, jednostkę naukową lub badawczo-rozwojową kwestionariuszu bezpieczeństwa przemysłowego.

2. Kwestionariusz bezpieczeństwa przemysłowego zawiera w szczególności:

1) dane identyfikujące podmiot podlegający sprawdzeniu, w tym jego status prawny;
2) dane o strukturze kapitału i powiązaniach kapitałowych przedsiębiorcy;
3) dane o sytuacji finansowej przedsiębiorcy;
4) dane o strukturze organizacyjnej przedsiębiorcy;
5) dane dotyczące osób, o których mowa w art. 68 ust. 6 pkt 4;
6) dane o systemie ochrony przedsiębiorcy;
7) wykaz pracowników posiadających poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych stanowiących tajemnicę państwową;
8) wykaz pracowników, którzy powinni być poddani poszerzonemu lub specjalnemu postępowaniu sprawdzającemu;
9) wykaz osób, które ze strony przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej wykonują lub będą wykonywać funkcje związane z ochroną informacji niejawnych;
10) podpis osoby upoważnionej do składania oświadczeń woli w imieniu przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej.

Art. 69a.

Postępowanie bezpieczeństwa przemysłowego powinno być przeprowadzone bez zbędnej zwłoki i zakończone w terminie nie dłuższym niż 6 miesięcy od dnia przedłożenia wszystkich dokumentów niezbędnych do jego przeprowadzenia.

Art. 70.

1. W przypadku pozytywnego wyniku postępowania, o którym mowa w art. 68 ust. 1, służba ochrony państwa wydaje świadectwo bezpieczeństwa przemysłowego, które zachowuje ważność od daty wydania przez okres:

1) 5 lat - w przypadku umów lub zadań, związanych z dostępem do informacji niejawnych oznaczonych klauzulą „ściśle tajne";
2) 7 lat - w przypadku umów lub zadań, związanych z dostępem do informacji niejawnych oznaczonych klauzulą „tajne";
3) 10 lat - w przypadku świadectwa bezpieczeństwa przemysłowego, wydanego w wyniku postępowania, o którym mowa w art. 67.

2. W okresie ważności świadectwa bezpieczeństwa przemysłowego służba ochrony państwa może przeprowadzić z urzędu sprawdzenie, w zakresie określonym w art. 68 ust. 6 i 7, w celu ustalenia, czy przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa nie utracili zdolności do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem.

Art. 71.

1. Jednostka organizacyjna zlecająca wykonanie umowy lub zadania, związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową, jest odpowiedzialna za wprowadzenie do umowy lub decyzji o zleceniu zadania instrukcji bezpieczeństwa przemysłowego, określającej:

1) szczegółowe wymagania dotyczące ochrony informacji niejawnych stanowiących tajemnicę państwową, które zostaną przekazane przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej w związku z wykonywaniem umowy lub zadania, odpowiednie do ilości tych informacji, klauzuli tajności oraz liczby osób mających do nich dostęp;
2) skutki oraz zakres odpowiedzialności wykonawcy umowy lub zadania z tytułu niewykonania lub nienależytego wykonania obowiązków wynikających z ustawy, a także nieprzestrzegania wymagań określonych w instrukcji bezpieczeństwa przemysłowego.

2. W szczególności instrukcja bezpieczeństwa przemysłowego powinna określać:

1) klauzule tajności poszczególnych materiałów lub rodzajów materiałów niejawnych, które zostaną wytworzone przez przedsiębiorcę, jednostkę naukową lub badawczo-rozwojową w związku z wykonaniem umowy lub zadania;
2) sposób postępowania z materiałami niejawnymi, które zostaną przekazane przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej lub przez niego wytworzone w związku z wykonaniem umowy lub zadania.

3. Kierownik jednostki organizacyjnej, która zleca wykonanie umowy lub zadania, związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową, wyznacza osobę odpowiedzialną za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez przedsiębiorcę, jednostkę naukową lub badawczo-rozwojową obowiązku ochrony przekazanych im informacji niejawnych.

4. Jeżeli w związku z wykonaniem umowy lub zadania zostaną wytworzone informacje niejawne, odpowiednią klauzulę tajności nadaje osoba, o której mowa w art. 21 ust. 1, zgodnie ze wskazaniami zawartymi w instrukcji bezpieczeństwa przemysłowego, a w przypadku ich braku, po uzgodnieniu z osobą, o której mowa w ust. 3.

5. Jednostka organizacyjna zlecająca wykonanie umowy lub zadania, związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową, ma obowiązek:

1) niezwłocznego informowania właściwej służby ochrony państwa o:

a) nazwie i adresie przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej, którym zleca wykonanie umowy lub zadania,
b) przedmiocie umowy lub zadania,
c) najwyższej koniecznej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem umowy lub zadania,
d) naruszeniu przepisów o ochronie informacji niejawnych u przedsiębiorcy, w jednostce naukowej lub badawczo-rozwojowej, którym zlecono wykonanie umowy lub zadania,
e) zakończeniu wykonania umowy lub zadania;

2) niezwłocznego przekazania właściwej służbie ochrony państwa:

a) kopii instrukcji bezpieczeństwa przemysłowego, o której mowa w ust. 1,
b) kopii świadectwa bezpieczeństwa przemysłowego przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej, którym zlecono wykonanie umowy lub zadania.

Art. 71a.

1. Przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa, w czasie trwania postępowania bezpieczeństwa przemysłowego, a także w okresie ważności świadectwa bezpieczeństwa przemysłowego, określonego w art. 70 ust. 1, mają obowiązek niezwłocznego informowania właściwej służby ochrony państwa o:

1) zmianach danych zawartych w kwestionariuszu bezpieczeństwa przemysłowego;
2) ogłoszeniu upadłości, likwidacji lub rozwiązaniu jednostki organizacyjnej albo zakończeniu przez nią działalności w innej formie;
3) potrzebie zawarcia lub zawarciu umowy z podwykonawcą, związanej z dostępem do informacji niejawnych;
4) wypowiedzeniu umowy;
5) zakończeniu wykonania umowy lub zadania;
6) zawarciu nowej umowy lub podjęciu wykonania nowego zadania związanych z dostępem do informacji niejawnych, ze szczególnym uwzględnieniem:

a) nazwy i adresu jednostki organizacyjnej zawierającej umowę lub zlecającej zadanie,
b) przedmiotu umowy lub zadania,
c) najwyższej klauzuli tajności informacji niejawnych, do których dostęp będzie wiązał się z wykonaniem umowy lub zadania.

2. Przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa, w czasie realizacji umowy albo zadania, mają obowiązek niezwłocznego informowania osoby, o której mowa w art. 71 ust. 3, o:

1) zmianach w systemie ochrony informacji niejawnych;
2) zmianach osób wykonujących umowę lub zadanie;
3) potrzebie zlecenia podwykonawcy wykonania umowy związanej z dostępem do informacji niejawnych.

Art. 72.

1. Świadome podanie nieprawdziwych danych lub zatajenie prawdziwych danych w kwestionariuszu bezpieczeństwa przemysłowego albo niewykonanie obowiązku wynikającego z art. 71a ust. 1 może stanowić podstawę do odmowy wydania świadectwa bezpieczeństwa przemysłowego.

2. Utrata zdolności do ochrony informacji niejawnych stwierdzona w toku sprawdzenia, o którym mowa w art. 70 ust. 2, lub kontroli, o których mowa w art. 14 ust. 1 i art. 16, stanowi podstawę do cofnięcia świadectwa bezpieczeństwa przemysłowego, a niewykonanie obowiązku wynikającego z art. 71a ust. 1 może stanowić podstawę do cofnięcia świadectwa bezpieczeństwa przemysłowego.

3. O cofnięciu świadectwa bezpieczeństwa przemysłowego służba ochrony państwa zawiadamia niezwłocznie jednostki organizacyjne, które zleciły przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej wykonanie umowy albo zadania.

4. Przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa mogą ponownie ubiegać się o wydanie świadectwa bezpieczeństwa przemysłowego w terminie nie krótszym niż rok od dnia doręczenia decyzji o jego cofnięciu.

Art. 72a.

1. Od decyzji o odmowie wydania lub decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej służy odwołanie do Prezesa Rady Ministrów.

2. Do odwołania, o którym mowa w ust. 1, stosuje się odpowiednio przepisy rozdziału 5a z wyłączeniem przepisów art. 48b ust. 3, art. 48e ust. 1 pkt 1, art. 48i oraz art. 48m.

3. W przypadku likwidacji przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej albo ogłoszenia upadłości przedsiębiorcy Prezes Rady Ministrów umarza postępowanie odwoławcze.

Art. 73.

1. Świadectwo bezpieczeństwa przemysłowego, decyzja o odmowie wydania oraz decyzja o cofnięciu świadectwa bezpieczeństwa przemysłowego powinny zawierać:

1) oznaczenie służby ochrony państwa, która wydała, odmówiła wydania bądź cofnęła świadectwo bezpieczeństwa przemysłowego;
2) miejsce i datę wystawienia;
3) nazwę podmiotu i adres jego siedziby;
4) podstawę prawną;
5) stwierdzenie wydania świadectwa bezpieczeństwa przemysłowego, odmowy wydania lub jego cofnięcia;
6) w przypadku wydania świadectwa bezpieczeństwa przemysłowego - jego stopień, klauzulę tajności oraz termin ważności;
7) imienną pieczęć i czytelny podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa.

2. Decyzja o odmowie wydania oraz decyzja o cofnięciu świadectwa bezpieczeństwa przemysłowego powinny zawierać uzasadnienie faktyczne i prawne oraz pouczenie o dopuszczalności i terminie wniesienia:

1) odwołania do Prezesa Rady Ministrów;
2) skargi do sądu administracyjnego.

3. Można odstąpić od uzasadnienia faktycznego decyzji lub je ograniczyć w zakresie, w jakim udostępnienie mogłoby spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa.

Art. 74.

Rada Ministrów określi, w drodze rozporządzenia, wzory:
1) kwestionariusza bezpieczeństwa przemysłowego;
2) świadectw bezpieczeństwa przemysłowego;
3) decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego;
4) decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego.

Art. 74a.

1. Służby ochrony państwa pobierają opłaty za:

1) przeprowadzenie postępowań bezpieczeństwa przemysłowego, o których mowa w art. 68 ust. 4;
2) przeprowadzenie sprawdzeń, o których mowa w art. 68 ust. 6;
3) przeprowadzenie postępowań sprawdzających, o których mowa w art. 37 ust. 2 i 3.

2. Prezes Rady Ministrów określi, w drodze rozporządzenia, wysokość i tryb pobierania opłat, o których mowa w ust. 1, z uwzględnieniem kosztów ponoszonych na przeprowadzenie czynności, o których mowa w art. 37 ust. 2 i 3 oraz art. 68 ust. 4 i 6.

Art. 75.

1. Dane zgromadzone w postępowaniu, o którym mowa w art. 68 ust. 1, podlegają ochronie i mogą być wykorzystywane wyłącznie w celu określonym w ustawie, a ich przekazywanie i udostępnianie innym osobom jest zabronione.

2. Dane, o których mowa w ust. 1, mogą być udostępniane przez służby ochrony państwa wyłącznie na żądanie sądu lub prokuratora dla celów postępowania karnego albo Prezydentowi Rzeczypospolitej Polskiej lub Prezesowi Rady Ministrów, gdy wymaga tego istotny interes Rzeczypospolitej Polskiej.

3. Akta postępowań sprawdzających prowadzonych w odniesieniu do przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych są przechowywane jako wyodrębniona część w archiwach służb ochrony państwa.

Art. 76.

1. W przypadku gdy przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa zamierzają ubiegać się lub ubiegają się o wykonanie umowy albo zadań związanych z dostępem do informacji niejawnych stanowiących tajemnicę służbową, świadectwo bezpieczeństwa przemysłowego nie jest wymagane, z zastrzeżeniem art. 67. Przepisy art. 71 ust. 1-4 oraz art. 71a ust. 2 stosuje się odpowiednio.

2. Przedsiębiorca, jednostka naukowa lub badawczo-rozwojowa, o których mowa w ust. 1, są obowiązani powołać pełnomocnika ochrony oraz spełniać inne wymagania ustawy w zakresie ochrony informacji niejawnych, stosownie do ich klauzuli tajności.

3. Na wniosek przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej, o których mowa w ust. 1, zwykłe postępowanie sprawdzające wobec osób wymienionych w art. 68 ust. 4, z wyjątkiem osoby kandydata na pełnomocnika ochrony, może przeprowadzić pełnomocnik ochrony jednostki organizacyjnej zawierającej umowę lub zlecającej zadanie, o których mowa w ust. 1. Wniosek składa się do kierownika jednostki organizacyjnej, która zleca wykonanie takiej umowy lub zadania.

4. Szkolenie w zakresie ochrony informacji niejawnych osób, wobec których przeprowadzono postępowanie sprawdzające, o którym mowa w ust. 3, przeprowadza pełnomocnik ochrony jednostki organizacyjnej zawierającej umowę lub zlecającej zadanie, o których mowa w ust. 1.

Rozdział 12
Zmiany w przepisach obowiązujących

Art. 77- 84 pominięte. Wprowadzały zmiany do następujących ustaw: z 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa; z 28 września 1991 r. o kontroli skarbowej; z 19 sierpnia 1994 r. o ochronie zdrowia psychicznego; z 14 grudnia 1995 r. o urzędzie ministra obrony narodowej; z 8 sierpnia 1996 r. o organizacji i trybie pracy Rady Ministrów oraz o zakresie działania ministrów; z 22 sierpnia 1997 r. o ochronie osób i mienia; z 29 sierpnia 1997 r. - Ordynacja podatkowa; z 29 sierpnia 1997 r. - Prawo bankowe.

Rozdział 13
Przepisy przejściowe i końcowe

Art. 85.

1. Kierownicy jednostek organizacyjnych, w terminie 3 miesięcy od dnia wejścia w życie ustawy, powołają pełnomocników ochrony i zorganizują piony ochrony w podległych jednostkach oraz dostosują, w terminie 6 miesięcy od dnia wejścia w życie ustawy, pomieszczenia służbowe do wymogów ustawy.

2. Pełnomocnicy ochrony dokonają, w terminie 6 miesięcy od dnia wejścia w życie ustawy, przeglądu stanowisk oraz sporządzą wykazy stanowisk i osób dopuszczonych do informacji niejawnych.

Art. 86.

1. Dokumenty wytworzone w okresie od dnia 10 maja 1990 r. do dnia wejścia w życie ustawy, zawierające wiadomości stanowiące tajemnicę państwową lub służbową i oznaczone stosownie do przepisów obowiązujących do dnia wejścia w życie ustawy klauzulami: „Tajne specjalnego znaczenia", „Tajne" lub „Poufne", stają się w rozumieniu tej ustawy dokumentami oznaczonymi odpowiednio klauzulami: „ściśle tajne", „tajne" lub „poufne".

2. Osoby, o których mowa w art. 21 ust. 1, lub ich następcy prawni w odniesieniu do dokumentów zawierających wiadomości stanowiące tajemnicę państwową, wytworzonych przed dniem 10 maja 1990 r. - dokonają w terminie 36 miesięcy od dnia wejścia w życie ustawy ich przeglądu w celu dostosowania ich dotychczasowych klauzul do klauzul wynikających z ustawy. Do tego czasu dokumenty te uważa się za oznaczone odpowiednio do postanowień ust. 1, chyba że przepisy odrębne stanowią inaczej. Przepis art. 25 ust. 5 stosuje się odpowiednio.

3. Po upływie 36 miesięcy od dnia wejścia w życie ustawy dokumenty, o których mowa w ust. 2, w stosunku do których nie dokonano przeglądu, stają się jawne, z wyjątkiem dokumentów odpowiadających kryteriom określonym w art. 25 ust. 2 pkt 1 i 2, które stają się dokumentami oznaczonymi klauzulą „ściśle tajne", podlegającymi ochronie na podstawie powołanego przepisu.

4. Przepisy ust. 2 i 3 nie naruszają przepisów innych ustaw.

Art. 87.

1. Z zastrzeżeniem ust. 2, wydane na podstawie dotychczasowych przepisów upoważnienia do dostępu do wiadomości stanowiących tajemnicę państwową lub służbową:

1) osobom na stanowiskach objętych wymogiem przeprowadzenia specjalnego postępowania sprawdzającego - tracą ważność po 12 miesiącach od dnia wejścia w życie ustawy,
2) osobom na stanowiskach objętych wymogiem przeprowadzenia poszerzonego postępowania sprawdzającego - tracą ważność po 18 miesiącach od dnia wejścia w życie ustawy,
3) osobom na stanowiskach objętych wymogiem przeprowadzenia zwykłego postępowania sprawdzającego - tracą ważność po 24 miesiącach od dnia wejścia w życie ustawy.

2. Przepis art. 44 ust. 2 stosuje się odpowiednio do osób, o których mowa w ust. 1.

3. Decyzje zezwalające na ujawnienie wiadomości stanowiących tajemnicę państwową lub służbową, wydane na podstawie ustawy z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 40, poz. 271, z 1989 r. Nr 34, poz. 178, z 1990 r. Nr 34, poz. 198, z 1996 r. Nr 106, poz. 496 i z 1997 r. Nr 110, poz. 714), zachowują ważność nie dłużej niż do dnia 31 grudnia 1999 r.

4. Zezwolenia wydane na podstawie art. 16 ustawy, o której mowa w ust. 3, zachowują ważność nie dłużej niż do dnia 31 grudnia 1999 r.

Art. 88.

Działającym na podstawie odrębnych ustaw wewnętrznym służbom ochrony w jednostkach organizacyjnych kierownicy tych jednostek mogą powierzyć zadania i uprawnienia pionów ochrony zgodnie z przepisami ustawy.

Art. 89.

1. Przepisy dotyczące tajemnicy państwowej lub służbowej, wydane na podstawie ustawy, o której mowa w art. 90, o ile nie są sprzeczne z niniejszą ustawą, zachowują moc przez okres 12 miesięcy od dnia wejścia w życie ustawy.

2. Przepisy dotyczące tajemnicy państwowej lub służbowej wydane na podstawie innych ustaw należy dostosować do wymogów ustawy w okresie 12 miesięcy od dnia wejścia w życie ustawy.

Art. 90.

Traci moc ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 40, poz. 271, z 1989 r. Nr 34, poz. 178, z 1990 r. Nr 34, poz. 198, z 1996 r. Nr 106, poz. 496 oraz z 1997 r. Nr 110, poz. 714).

Art. 91.

Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

---

1) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 49, poz. 509, z 2002 r. Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 169, poz. 1387, z 2003 r. Nr 130, poz. 1188 i Nr 170, poz. 1660, z 2004 r. Nr 162, poz. 1692 oraz z 2005 r. Nr 64, poz. 565, Nr 78, poz. 682 i Nr 181, poz. 1524.

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 154, poz. 1800, z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 123, poz. 1291 oraz z 2005 r. Nr 10, poz. 71, Nr 14, poz. 114 i Nr 169, poz. 1417.

3) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 126, poz. 1070, Nr 141, poz. 1178, Nr 144, poz. 1208, Nr 153, poz. 1271, Nr 169, poz. 1385 i 1387 i Nr 241, poz. 2074, z 2003 r. Nr 50, poz. 424, Nr 60, poz. 535, Nr 65, poz. 594, Nr 228, poz. 2260 i Nr 229, poz. 2276, z 2004 r. Nr 64, poz. 594, Nr 68, poz. 623, Nr 91, poz. 870, Nr 96, poz. 959, Nr 121, poz. 1264, Nr 146, poz. 1546 i Nr 173, poz. 1808 oraz z 2005 r. Nr 83, poz. 719, Nr 85, poz. 727, Nr 167, poz. 1398 i Nr 183, poz. 1538.

4) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2004 r. Nr 64, poz. 594, Nr 91, poz. 868, Nr 171, poz. 1800 i Nr 173, poz. 1808.

5) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155, Nr 111, poz. 1061 i Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 626, Nr 93, poz. 889, Nr 240, poz. 2405 i Nr 264, poz. 2641 oraz z 2005 r. Nr 10, poz. 70, Nr 48, poz. 461, Nr 77, poz. 680, Nr 96, poz. 821, Nr 141, poz. 1181, Nr 143, poz. 1203, Nr 163, poz. 1363, Nr 169, poz. 1416 i Nr 178, poz. 1479.

6) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 90, poz. 844, Nr 113, poz. 1070, Nr 130, poz. 1188 i Nr 166, poz. 1609 oraz z 2004 r. Nr 109, poz. 1159, Nr 171, poz. 1800, Nr 267, poz. 2647 i Nr 273, poz. 2703.

U S T A W A

z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw[1] [Dz.U.2005.85.727]

Art. 6.

Banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe obowiązane są dostosować przetwarzanie informacji zgromadzonych przed dniem wejścia w życie niniejszej ustawy do wymagań w niej określonych, w terminie nie dłuższym niż 3 lata od wejścia w życie niniejszej ustawy.

Art. 7.

Do postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy stosuje się przepisy tej ustawy.

Art. 8.

Poświadczenia bezpieczeństwa wydane przed dniem wejścia w życie ustawy, ważne w tym dniu, zachowują ważność w zakresie i okresie określonym ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, w brzmieniu nadanym niniejszą ustawą.

Art. 9.

Świadectwa bezpieczeństwa przemysłowego wydane przedsiębiorcom, jednostkom naukowym lub badawczo-rozwojowym w związku z wykonaniem umowy lub zadania łączącego się z dostępem do informacji niejawnych stanowiących tajemnicę państwową zachowują ważność do czasu zakończenia danej umowy lub zadania, ale nie dłużej niż 2 lata od dnia wejścia w życie ustawy.

Art. 10.

Dotychczasowe przepisy wykonawcze, wydane na podstawie upoważnień ustawowych zmienianych niniejszą ustawą, zachowują moc do czasu ich zastąpienia przez przepisy wykonawcze wydane na podstawie upoważnień ustawowych w brzmieniu nadanym niniejszą ustawą, jednak nie dłużej niż 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 11.

Ogłoszenie tekstu jednolitego ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych nastąpi w terminie 6 miesięcy od dnia ogłoszenia niniejszej ustawy.

Art. 12.

Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

---

[1] Niniejszą ustawą zmienia się ustawy: ustawę z dnia 21 sierpnia 1997 r. - Prawo o publicznym obrocie papierami wartościowymi, ustawę z dnia 29 sierpnia 1997 r. - Prawo bankowe, ustawę z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa, ustawę z dnia 8 października 2004 r. o zasadach finansowania nauki.

[2] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2001 r, Nr 49, poz. 509, z 2002 r. Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 169, poz. 138, z 2003 r. Nr 130, poz. 1188 i Nr 170, poz. 1660 oraz z 2004 r. Nr 162, poz. 1692.
[3] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2002 r. Nr 126, poz. 1070, Nr 141, poz. 1178, Nr 144, poz. 1208, Nr 153, poz. 1271, Nr 169, poz. 1385 i 1387, Nr 241, poz. 2074, z 2003 r. Nr 50, poz. 424, Nr 60, poz. 535, Nr 65, poz. 594, Nr 228, poz. 2260, Nr 229, poz. 2276 oraz z 2004 r. Nr 64, poz. 594, Nr 68, poz. 623, Nr 96, poz. 959, Nr 121, poz. 1264, Nr 146, poz. 1546 i Nr 173, poz. 1808.
[4] Zmiany ustawy zostały ogłoszone w Dz.U. Nr 64, poz. 594, Nr 91, poz. 868, Nr 171, poz. 1800 i Nr 173, poz. 1808.
[5] Zmiany ustawy zostały ogłoszone w Dz.U. Nr z 1999 r. Nr 83, poz. 931, z 2000 r. Nr 50, poz. 580, Nr 62, poz. 717, Nr 73, poz. 852 i Nr 93, poz. 1027, z 2001 r. Nr 98, poz. 1071 i Nr 106, poz. 1149, z 2002 r. Nr 74, poz. 676, z 2003 r. Nr 17, poz. 155 i Nr 111, poz. 1061, Nr 130, poz. 1188, z 2004 r. Nr 51, poz. 514, Nr 69, poz. 626, Nr 93, poz. 889, Nr 240, poz. 2405, Nr 264, poz. 2641 oraz z 2005 r. Nr 10, poz. 70.
[6] Zmiany ustawy zostały ogłoszone w Dz.U. z 2002 r. Nr 240, poz. 2055, z 2003 r. Nr 50, poz. 424, Nr 84, poz. 774, Nr 124, poz. 1151, Nr 170, poz. 1651, Nr 223, poz. 2216 oraz z 2004 r. Nr 64, poz

Załącznik nr 1

WYKAZ RODZAJÓW INFORMACJI, KTÓRE MOGĄ STANOWIĆ TAJEMNICĘ PAŃSTWOWĄ

I. Informacje niejawne, które mogą być oznaczone klauzulą „ściśle tajne":

1. Informacje dotyczące zagrożeń zewnętrznych bezpieczeństwa państwa o charakterze militarnym, plany i prognozowanie obronne oraz wynikające z nich decyzje i zadania.

2. Szczegółowa struktura, organizacja i funkcjonowanie systemu kierowania państwem oraz dowodzenia Siłami Zbrojnymi w czasie zagrożenia państwa lub wojny.

3. Lokalizacja, wyposażenie, właściwości ochronne i organizacja obrony stanowisk kierowania państwem i stanowisk dowodzenia Siłami Zbrojnymi w czasie zagrożenia państwa lub wojny.

4. Szczegółowa organizacja, funkcjonowanie systemów łączności kierowania państwem i dowodzenia Siłami Zbrojnymi w czasie wyższych stanów gotowości bojowej lub wojny.

5. Centralny program mobilizacji gospodarki.

6. Informacje dotyczące planowania, organizacji i funkcjonowania mobilizacyjnego rozwinięcia Sił Zbrojnych.

7. Szczegółowa struktura Sił Zbrojnych, rodzajów Sił Zbrojnych oraz okręgów wojskowych i korpusów na czas wojny.

8. Informacje dotyczące możliwości bojowych Sił Zbrojnych, rodzajów Sił Zbrojnych i okręgów wojskowych oraz potencjalnego przeciwnika na przewidywanych obszarach i kierunkach działań wojennych.

9. Zadania bojowe Sił Zbrojnych i związków operacyjnych.

10. Organizacja i funkcjonowanie systemu obrony powietrznej i przeciwlotniczej kraju.

11. Organizacja, rozmieszczenie, zadania i możliwości działania systemu rozpoznania i walki radioelektronicznej.

12. Planowanie i realizacja przedsięwzięć w zakresie operacyjnego maskowania wojsk.

13. Planowanie, realizacja, wyniki badań naukowych i prac badawczo-rozwojowych o szczególnie ważnym znaczeniu dla obronności i bezpieczeństwa państwa.

14. Hasła i kody dostępu do urządzeń przechowujących, przetwarzających i przesyłających informacje oznaczone klauzulą „ściśle tajne".

15. Szczególne wymagania bezpieczeństwa i procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych służących do wytwarzania, przetwarzania, przekazywania lub przechowywania informacji oznaczonych klauzulą „ściśle tajne".

16. Szczegółowe informacje dotyczące organizacji, form i metod pracy operacyjnej Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu i Wojskowych Służb Informacyjnych oraz byłego Urzędu Ochrony Państwa, a także ich kierunki pracy operacyjnej i zainteresowań.

17. Szczegółowa struktura organizacyjna oraz etatowa jednostek i komórek organizacyjnych wykonujących czynności operacyjno-rozpoznawcze w służbach, o których mowa w pkt 16, a także systemy ewidencji danych o funkcjonariuszach i żołnierzach tych jednostek i komórek organizacyjnych.

18. Dane identyfikujące lub mogące doprowadzić do identyfikacji funkcjonariuszy i żołnierzy służb, o których mowa w pkt 16, realizujących czynności operacyjno-rozpoznawcze.

19. Dane identyfikujące lub mogące doprowadzić do identyfikacji osób niebędących funkcjonariuszami lub żołnierzami służb, o których mowa w pkt 16, a które udzieliły pomocy tym służbom w zakresie wykonywania czynności operacyjno-rozpoznawczych.

20. Dane identyfikujące lub mogące doprowadzić do identyfikacji świadków koronnych i osób dla nich najbliższych oraz świadków, o których mowa w art. 184 Kodeksu postępowania karnego.

21. Informacje dotyczące dokumentów uniemożliwiających ustalenie danych identyfikujących funkcjonariuszy, żołnierzy lub pracowników organów, służb i instytucji państwowych uprawnionych do wykonania czynności operacyjno-rozpoznawczych lub środków, którymi posługują się przy wykonywaniu czynności operacyjno-rozpoznawczych.

22. Informacje dotyczące dokumentów uniemożliwiających ustalenie danych identyfikujących osoby udzielające organom, służbom i instytucjom państwowym uprawnionym do wykonywania czynności operacyjno-ropoznawczych pomocy przy wykonywaniu tych czynności.

23. Plany i stan zaopatrzenia w sprzęt i materiały techniki specjalnej przeznaczone do wykonywania czynności operacyjno-rozpoznawczych przez służby, o których mowa w pkt 16.

24. Informacje dotyczące prowadzonych przez Agencję Bezpieczeństwa Wewnętrznego, Wojskowe Służby Informacyjne oraz były Urząd Ochrony Państwa kontroli operacyjnej, niejawnego nabycia lub przejęcia przedmiotów pochodzących z przestępstwa ulegających przepadkowi, albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także przyjęcia lub wręczenia korzyści majątkowej oraz niejawnego nadzorowania, wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa.

25. Informacje dotyczące planowanych, wykonywanych i zrealizowanych czynności operacyjno-rozpoznawczych przez służby, o których mowa w pkt 16, oraz informacje i przedmioty uzyskane w wyniku tych czynności, które pozwalają na identyfikację osób udzielających im pomocy w zakresie wykonywania czynności operacyjno-rozpoznawczych.

26. Informacje o szczegółowych zasadach tworzenia, ewidencjonowania, gospodarowania i wykorzystaniu funduszu operacyjnego i środków specjalnych w służbach, o których mowa w pkt 16.

27. Organizacja, funkcjonowanie i środki techniczne radiokontrwywiadowczej ochrony państwa.

28. Informacje niejawne wymieniane przez Rzeczpospolitą Polską z Organizacją Traktatu Północnoatlantyckiego, Unią Europejską i Unią Zachodnioeuropejską oraz z innymi organizacjami międzynarodowymi i państwami, oznaczone klauzulą „TOP SECRET" lub równorzędną, jeżeli wymagają tego umowy międzynarodowe, na zasadzie wzajemności.

29. Informacje określone w pkt 16-19 i 23-26, będące w posiadaniu organów, służb i instytucji państwowych, innych niż służby, o których mowa w pkt 16, uprawnionych na podstawie ustaw do wykonywania czynności operacyjno-rozpoznawczych, związane z działalnością tych organów, służb lub instytucji.

II. Informacje, które mogą być oznaczone klauzulą „tajne":

1. Planowanie, rozmieszczenie i stan rezerw państwowych.

2. Resortowe i wojewódzkie programy mobilizacji gospodarki.

3. Plany obrony cywilnej państwa oraz plany obrony cywilnej województw.

4. Szczegółowe założenia systemu finansowego państwa w czasie podwyższonej gotowości obronnej lub wojny.

5. Stan rozwinięcia, ukompletowania i wyposażenia jednostek wojskowych w zakresie nieobjętym postanowieniami Traktatu o konwencjonalnych siłach zbrojnych w Europie (CFE).

6. Szczegółowa struktura Sił Zbrojnych, rodzajów Sił Zbrojnych oraz okręgów wojskowych.

7. Plany i prognozy rozwoju organizacyjnego i technicznego Sił Zbrojnych oraz poszczególnych rodzajów wojsk.

8. Lokalizacja, rodzaj i przeznaczenie oraz właściwości techniczno-ochronne budownictwa specjalnego.

9. Organizacja kompleksowego przygotowania jednolitej sieci telekomunikacyjnej państwa dla potrzeb obronnych.

10. Informacje dotyczące przygotowania, budowy, zarządzania oraz funkcjonowania systemów i sieci telekomunikacyjnych, teleinformatycznych i pocztowych służących do przekazywania informacji niejawnych stanowiących tajemnicę państwową, wykorzystywanych dla potrzeb Sił Zbrojnych, służb ochrony państwa lub administracji publicznej w zakresie niezbędnym do zabezpieczenia tych systemów i sieci.

11. Zbiorcze informacje dotyczące produkcji specjalnej przemysłu obronnego, a także prognozy rozwojowe, plany i zdolności produkcyjne oraz usługowe przedsiębiorców, jednostek naukowych i badawczo-rozwojowych w zakresie realizacji zamówień na uzbrojenie i sprzęt wojskowy.

12. Wojskowe mapy specjalne i fotodokumenty przedstawiające uczytelnione obiekty inżynieryjnej rozbudowy terenu prognozowanych rejonów i kierunków działań wojennych.

13. Współrzędne określające położenie obiektów (budynków, budowli, urządzeń) usytuowanych na terenach zamkniętych, o których mowa w przepisach szczególnych, jeżeli informacjom dotyczącym tych obiektów organ zamykający teren przyznał klauzulę „tajne".

14. Fotogrametryczne zobrazowanie lotnicze lub naziemne zarejestrowane na dowolnym nośniku oraz wysokorozdzielcze zdjęcia satelitarne, zawierające obraz obiektów, o których mowa w pkt 13.

15. Materiały geodezyjne i kartograficzne zawierające informacje o położeniu, rodzaju, charakterze lub przeznaczeniu obiektów, o których mowa w pkt 13.

16. Materiały uzyskane w wyniku przetworzenia zobrazowań satelitarnych, zawierające dodaną informację o położeniu, rodzaju, charakterze lub przeznaczeniu obiektów, o których mowa w pkt 13.

17. Informacje dotyczące przestawienia gospodarki narodowej na rzecz obronności w czasie podwyższonej gotowości obronnej państwa lub wojny.

18. Informacje dotyczące przygotowania, organizacji oraz wykorzystywania transportu kolejowego, drogowego i wodnego oraz ochrony obiektów komunikacyjnych w czasie podwyższonej gotowości obronnej państwa lub wojny.

19. Organizacja i funkcjonowanie systemu alarmowania wojsk oraz zadania jednostek wojskowych i garnizonów w procesie osiągania wyższych stanów gotowości bojowej.

20. Zadania ministrów, centralnych organów administracji rządowej, wojewodów, a także innych konstytucyjnych organów władzy publicznej, związane z osiąganiem podwyższonej gotowości obronnej państwa.

21. Organizacja i funkcjonowanie systemu zaopatrywania Sił Zbrojnych w uzbrojenie, sprzęt wojskowy i amunicję w procesie osiągania wyższych stanów gotowości bojowej.

22. Dane oraz zasady funkcjonowania systemu ewidencji danych o osobach zajmujących stanowiska związane z obronnością kraju.

23. Informacje dotyczące systemu ochrony i obrony jednostek organizacyjnych Służby Więziennej na czas podwyższonej gotowości obronnej państwa lub wojny.

24. Organizacja ochrony, na wypadek wojny, dóbr kultury mających szczególne znaczenie dla dziedzictwa kulturalnego narodu.

25. Dane dotyczące tworzonych na wypadek wojny rezerw rzeczowych jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych.

26. Szczegółowe informacje dotyczące organizacji, metod i środków służących do ochrony informacji stanowiących tajemnicę państwową, których ujawnienie może spowodować brak ich skuteczności, chyba że zawierają informacje oznaczone wyższą klauzulą tajności.

27. Szczególne wymagania bezpieczeństwa i procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych służących do wytwarzania, przetwarzania, przekazywania lub przechowywania informacji oznaczonych klauzulą „tajne".

28. Informacje dotyczące planowania, rozmieszczenia, przeznaczenia i wyposażenia obiektów i nieruchomości specjalnych oraz plany ich obrony i ochrony.

29. Szczegółowe informacje dotyczące osób podejrzewanych o prowadzenie działalności godzącej w bezpieczeństwo, obronność, niezależność, całość lub międzynarodową pozycję państwa albo działalności terrorystycznej, uzyskane i przetwarzane przez służby, o których mowa w części I w pkt 16, chyba że zawierają informacje oznaczone wyższą klauzulą tajności.

30. Szczegółowa struktura organizacyjna i etatowa jednostek organizacyjnych służb, o których mowa w części I w pkt 16, chyba że zawiera informacje oznaczone wyższą klauzulą tajności.

31. System ewidencji danych o funkcjonariuszach, żołnierzach i pracownikach służb, o których mowa w części I w pkt 16, chyba że zawiera informacje oznaczone wyższą klauzulą tajności.

32. Informacje określone w części I w pkt 16-19 i 23-26, będące w posiadaniu organów, służb i instytucji państwowych, innych niż służby, o których mowa w części I w pkt 16, uprawnionych na podstawie ustaw do wykonywania czynności operacyjno-rozpoznawczych, związane z

działalnością tych organów, służb lub instytucji, chyba że zawierają informacje oznaczone wyższą klauzulą tajności.

33. Szczegółowe Informacje dotyczące systemu i sposobu ochrony granicy państwowej w tym działań antyterrorystycznych i antysabotażowych.

34. Informacje z ewidencji operacyjnej, dotyczące pracy operacyjnej służb, o których mowa w części I pkt 16, chyba że zawierają informacje oznaczone wyższą klauzulą tajności.

35. Szczegółowe informacje dotyczące ochrony i zabezpieczenia obiektów szczególnie ważnych dla gospodarki narodowej albo ze względu na obronność lub bezpieczeństwo państwa.

36. Szczegółowe informacje dotyczące planowanych, wykonywanych i zrealizowanych czynności dochodzeniowo-śledczych, jeżeli ujawnienie tych informacji mogłoby stanowić przeszkodę dla prawidłowego toku postępowania karnego.

37. Projekty wynalazcze uznane za tajne zgodnie z przepisami prawa o własności przemysłowej.

38. Informacje dla Rady Ministrów i jej organów, dotyczące potencjału strategicznego państwa oraz strategicznych zamówień rządowych i ich realizacji.

39. Instrukcje do negocjacji w sprawie zawierania umów finansowych o znaczeniu ogólnopaństwowym, których ujawnienie mogłoby mieć wpływ na dalszy tok negocjacji.

40. Wnioski o udzielenie poręczenia, umowy poręczenia oraz umowy o udzielenie poręczenia dotyczące producentów sprzętu obronnego.

41. Technologia produkcji i system zabezpieczeń znaków akcyzy w przedsiębiorstwach wytwarzających te znaki.

42. Informacje dotyczące zabezpieczeń przed podrabianiem i przerabianiem znaków pieniężnych, papierów wartościowych emitowanych przez Skarb Państwa i Narodowy Bank Polski oraz znaków akcyzy, na etapie ich projektowania i przygotowania do produkcji, z wyłączeniem monet przeznaczonych na cele kolekcjonerskie.

43. Informacje dotyczące technologii produkcji znaków pieniężnych, znaków akcyzy i papierów wartościowych emitowanych przez Skarb Państwa lub Narodowy Bank Polski.

44. Informacje dotyczące technologii produkcji oraz szczegółowych sposobów zabezpieczeń dokumentów tożsamości, a także innych zabezpieczonych dokumentów wydawanych przez organy władzy publicznej.

45. Decyzje o skokowych zmianach kursu złotego w stosunku do walut obcych (dewaluacja, rewaluacja) dokonywane przez Narodowy Bank Polski do czasu podania ich do publicznej wiadomości.

46. Wysokość stóp procentowych Narodowego Banku Polskiego - do czasu ich podania do publicznej wiadomości.

47. Przedział odchyleń kursu złotego od centralnego parytetu - do czasu podania ich do publicznej wiadomości.

48. Prace badawczo-rozwojowe o szczególnie istotnym znaczeniu dla interesu gospodarczego państwa, zlecone przez ministrów i inne centralne organy państwowe.

49. Informacje dotyczące rozwiązań technicznych, technologicznych i organizacyjnych, których ujawnienie naraziłoby na szkodę istotny interes gospodarczy państwa.

50. Informacje o sposobie działania urządzeń kontrolno-sygnalizacyjnych i systemów alarmowych zabezpieczających dostęp do miejsc składowania i stosowania materiałów jądrowych kategorii I i II.

51. Informacje dotyczące planów i zadań polityki zagranicznej, których ujawnienie naraziłoby na szkodę istotny interes państwa lub innego podmiotu stosunków międzynarodowych, do czasu oficjalnego ich ogłoszenia.

52. Materiały, dokumenty, sprawozdania z negocjacji i konsultacji międzynarodowych oraz umowy międzynarodowe lub ich części, które zostały uznane za odpowiadające informacjom oznaczonym klauzulą „tajne" na wniosek jednej ze stron.

53. Informacje polityczne, gospodarcze lub wojskowe dotyczące państw obcych, uzyskane pod warunkiem zapewnienia ich tajności.

54. Organizacja i funkcjonowanie poczty dyplomatycznej.

55. System ochrony polskich przedstawicielstw dyplomatycznych i urzędów konsularnych.

56. Zadania polskich przedstawicielstw dyplomatycznych i urzędów konsularnych na czas wojny.

57. Zadania w zakresie ochrony przedstawicielstw dyplomatycznych i urzędów konsularnych państw obcych w Rzeczypospolitej Polskiej w czasie wojny.

58. Plany, prognozy i informacje na temat rozwoju obrotu z zagranicą sprzętem specjalnym i uzbrojeniem oraz technologiami i usługami specjalnymi.

59. Informacje niejawne wymieniane przez Rzeczpospolitą Polską z Organizacją Traktatu Północnoatlantyckiego, Unią Europejską i Unią Zachodnioeuropejską oraz z innymi organizacjami międzynarodowymi i państwami, oznaczone klauzulą „SECRET" lub równorzędną, jeżeli wymagają tego umowy międzynarodowe, na zasadzie wzajemności.

Załącznik nr 2

ANKIETA BEZPIECZEŃSTWA OSOBOWEGO

Szanowna Pani,
Szanowny Panie,

Rząd Rzeczypospolitej Polskiej, kierując się troską o bezpieczeństwo narodowe i mając powinność jego ochrony, przedstawia tę ankietę w przekonaniu, iż zostanie ona wypełniona zgodnie z Pana /Pani najlepszą wiedzą i wolą. Dziękując za współpracę, podkreślamy, że celem tej ankiety jest wyłącznie ochrona bezpieczeństwa narodowego przed zagrożeniami ze strony obcych służb specjalnych, ugrupowań terrorystycznych lub grup przestępczych. Prosimy uważnie przeczytać poniższą instrukcję, a w razie wątpliwości zwrócić się do pełnomocnika ochrony w Pana /Pani jednostce organizacyjnej lub do właściwej służby ochrony państwa o pomoc w wypełnieniu ankiety.

I N S T R U K C J A

1. Przed wypełnieniem ankiety proszę się z nią dokładnie zapoznać.

2. Proszę wypełniać ankietę własnoręcznie, pismem drukowanym. Cudzoziemcy, nie władający językiem polskim, składają własnoręcznie wypełnione ankiety w językach ojczystych, dołączając do nich tłumaczenie ich treści, wykonane przez tłumacza przysięgłego.

3. Jeśli ankieta zawiera zbyt mało miejsca na wpisanie danych, proszę je podać na osobnej karcie formatu A-4, którą należy dołączyć do ankiety.

4. W razie braku wiedzy umożliwiającej podanie danych, proszę wpisać sformułowanie: „nie wiem", z podaniem przyczyny.

5. Jeżeli dane w kolejnych punktach ankiety są identyczne z danymi podanymi w poprzednich punktach, można w kolejnych punktach wpisywać sformułowanie: „jak w pkt ... lit. ...".

6. Jeżeli któryś z członków rodziny zmarł, proszę ograniczać wypełnianie takiego fragmentu ankiety
wyłącznie do podania jego imienia, nazwiska, daty i miejsca urodzenia oraz sformułowania: „nie żyje".

7. Osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone" wypełniają ankietę stanowiącą załącznik nr 2a.

8. Osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą „poufne" wypełniają ankietę stanowiącą załącznik nr 2b.

9. Osoby objęte postępowaniem sprawdzającym w związku z dostępem do informacji niejawnych oznaczonych klauzulą „tajne" lub „ściśle tajne" wypełniają ankietę stanowiącą załącznik 2c - przy klauzuli „tajne" nie wypełnia się pkt 33 ankiety.

10. Przy kolejnym postępowaniu sprawdzającym, przeprowadzanym po upływie 10 lat w stosunku do osoby, która otrzymała poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą „poufne" - osobę tę prosi się o wypełnienie pkt: 17, 18, 19 i 23 z odniesieniem się wyłącznie do okresu począwszy od daty wypełnienia poprzedniej ankiety do dnia wypełnienia następnej ankiety. Jeżeli dane odnoszące się do wyżej wymienionych punktów nie uległy zmianie, należy przy nich wpisać sformułowanie: „bez zmian".

11. Przy kolejnym postępowaniu sprawdzającym, przeprowadzanym po upływie 5 lat w stosunku do osoby, która otrzymała poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne", a po upływie 7 lat w stosunku do osoby, która otrzymała poświadczenie bezpieczeństwa upoważniające do dostępu do informacji oznaczonych klauzulą „tajne" - osoby te nie wypełniają punktów: 1j oraz 1k. Ponadto przy wypełnianiu punktów: 10, 19, 24-26 i 30-32 należy odnieść się wyłącznie do okresu począwszy od daty wypełnienia poprzedniej ankiety do dnia wypełnienia następnej ankiety. Jeżeli dane odnoszące się do wyżej wymienionych punktów nie uległy zmianie, należy przy nich wpisać sformułowanie: „bez zmian".

(Wzory ankiet ze względów objętościowych nie opublikowano – dostępne są u pełnomocnika ds. ochrony informacji niejawnych)

Dz.U.05.171.1430

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia 25 sierpnia 2005 r.

w sprawie szczegółowego trybu przygotowania i prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych

(Dz. U. z dnia 8 września 2005 r.)

Na podstawie art. 17 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa szczegółowy tryb przygotowania i prowadzenia kontroli w zakresie ochrony informacji niejawnych, w tym uzgadniania kontroli w stosunku do Sejmu Rzeczypospolitej Polskiej i Senatu Rzeczypospolitej Polskiej.
2. Kontrola obejmuje badanie:
1) stanu zabezpieczenia informacji niejawnych;
2) przestrzegania przepisów w zakresie ochrony informacji niejawnych;
3) prawidłowości prowadzenia postępowań sprawdzających, z wyłączeniem postępowań, o których mowa w art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, zwanej dalej „ustawą";
4) stanu zabezpieczenia sieci lub systemów teleinformatycznych, służących do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych.

§ 2. Szef właściwej służby ochrony państwa w postępowaniu kontrolnym w szczególności:
1) opracowuje ogólne założenia prowadzenia kontroli i sprawuje ogólny nadzór nad jej realizacją;
2) reprezentuje służbę ochrony państwa wobec innych organów, instytucji i podmiotów w sprawach objętych działaniami kontrolnymi;
3) wykonuje czynności związane z rozpatrywaniem zastrzeżeń;
4) kieruje opracowaniem informacji o wynikach kontroli;
5) podejmuje działania zmierzające do wykorzystania uwag i wniosków przez adresatów wystąpień pokontrolnych.

§ 3. Upoważniony do przeprowadzania kontroli funkcjonariusz albo żołnierz służby ochrony państwa, zwany dalej „kontrolerem", wykonując czynności kontrolne:
1) przeprowadza kontrolę w jednostce kontrolowanej, zgodnie z przepisami ustawy, trybem określonym w rozporządzeniu oraz programem kontroli;
2) dokonuje w sposób wnikliwy i obiektywny ustaleń kontroli oraz rzetelnie je dokumentuje;
3) sporządza dokumenty określone w przepisach rozporządzenia;
4) bierze udział w postępowaniu w sprawie rozpatrywania zastrzeżeń;
5) wykonuje inne zadania w zakresie postępowania kontrolnego, zlecone przez szefa właściwej służby ochrony państwa.

§ 4. 1. Służba ochrony państwa prowadzi kontrole na podstawie rocznego planu kontroli, zatwierdzonego przez szefa właściwej służby ochrony państwa, po uzyskaniu opinii Kolegium do Spraw Służb Specjalnych.
2. Szef właściwej służby ochrony państwa może zarządzić doraźną kontrolę, nieujętą w planie, jeżeli uzyska informacje wskazujące na występowanie istotnych zagrożeń dla systemu zabezpieczenia informacji niejawnych lub nieprawidłowości dotyczących postępowań sprawdzających.

§ 5. Kontrolę przeprowadza się na podstawie opracowanego programu kontroli. Program kontroli wykonuje się w jednym egzemplarzu.

§ 6. Przy opracowywaniu programu kontroli uwzględnia się w szczególności:
1) wyniki wcześniejszych kontroli;
2) wyniki analiz określonych problemów z zakresu ochrony informacji niejawnych;
3) informacje pochodzące od organów państwowych i samorządowych, jednostek organizacyjnych i podmiotów, o których mowa w art. 1 ust. 2 ustawy;
4) opinie, wnioski oraz inne ustalenia w zakresie ochrony informacji niejawnych, dokonane przez Kolegium do Spraw Służb Specjalnych.

§ 7. W programie kontroli zamieszcza się w szczególności:
1) nazwę kontrolowanej jednostki organizacyjnej oraz jej dokładny adres;
2) oznaczenie i temat kontroli;
3) określenie kierunku badań kontrolnych i problemów wymagających oceny;
4) szczegółowe określenie zakresu przedmiotowego i podmiotowego kontroli;
5) wskazówki metodyczne, w odniesieniu do określenia sposobu i technik przeprowadzania kontroli, zwłaszcza problemów, na które należy zwrócić szczególną uwagę w badaniach kontrolnych, dowodów niezbędnych do dokonania ustaleń i sposobu ich badania, powiązania tematyki z aktami normatywnymi, wskazówek o charakterze techniczno-organizacyjnym, wzorów wykazów i zestawień;
6) ewentualne wskazanie potrzeby zasięgnięcia opinii biegłego lub powołania specjalisty;
7) szczegółowe założenia organizacyjne kontroli, w tym wskazanie kontrolera mającego ją przeprowadzić.

§ 8. 1. Program kontroli zatwierdza, z zastrzeżeniem kontroli, o której mowa w ust. 2, szef właściwej służby ochrony państwa.
2. Program kontroli w stosunku do Sejmu Rzeczypospolitej Polskiej lub Senatu Rzeczypospolitej Polskiej zatwierdza Prezes Rady Ministrów, po uprzednim uzgodnieniu, określonych w tym programie czynności, odpowiednio z Marszałkiem Sejmu Rzeczypospolitej Polskiej lub Marszałkiem Senatu Rzeczypospolitej Polskiej.

§ 9. 1. Kontrolę przeprowadza kontroler na podstawie imiennego upoważnienia określającego jednostkę kontrolowaną i podstawę prawną do podjęcia kontroli.
2. Upoważnienie sporządza się w jednym egzemplarzu, który załącza się do akt kontroli.
3. Upoważnienie podlega ścisłemu ewidencjonowaniu.
4. Wzór upoważnienia stanowi załącznik nr 1 do rozporządzenia.

§ 10. 1. Kontroler dokumentuje przebieg i wyniki czynności kontrolnych, zakładając i prowadząc w tym celu akta kontroli.
2. Akta kontroli obejmują w szczególności materiały dowodowe oraz inne dokumenty wymienione w rozporządzeniu, które oznacza się klauzulą tajności, zgodnie z wymogami określonymi w ustawie.
3. Akta kontroli prowadzi się zgodnie z tokiem dokonywanych czynności, włączając do nich materiały dowodowe oraz protokół kontroli, wystąpienie pokontrolne, informację o wykorzystaniu uwag i wykonaniu wniosków zawartych w wystąpieniu. Strony akt powinny być ponumerowane, ponadto akta muszą być zszyte i umieszczone w teczce. Całość klasyfikuje się według dokumentu o najwyższej klauzuli tajności. Akta kontroli rejestruje się w ewidencji kontroli.
4. Na początku każdego tomu akt zamieszcza się wykaz dokumentacji zawartej w danym tomie, wymieniając nazwy dokumentów i wskazując odpowiednie strony akt.
5. Akta kontroli przechowuje służba ochrony państwa w swoim archiwum.

§ 11. 1. Zabezpieczenie materiału dowodowego zebranego w toku postępowania kontrolnego w postaci dokumentu lub rzeczy potwierdza się protokołem zabezpieczenia dokumentu lub rzeczy stanowiących materiał dowodowy, a ich zwrot potwierdza się pokwitowaniem.
2. Wzór protokołu zabezpieczenia dokumentu lub rzeczy stanowiących materiał dowodowy stanowi załącznik nr 2 do rozporządzenia.

§ 12. 1. Załączniki do protokołu oględzin utrwalone za pomocą aparatury i środków technicznych służących do utrwalania obrazu lub dźwięku zabezpiecza się w sposób uniemożliwiający ich zamianę na inne.
2. Wzór protokołu oględzin stanowi załącznik nr 3 do rozporządzenia.

§ 13. 1. Warunkiem przyjęcia przez kontrolera wyjaśnienia lub oświadczenia jest wskazanie osoby składającej to wyjaśnienie lub oświadczenie oraz jej podpis. Warunkiem przyjęcia wyjaśnienia jest ponadto wskazanie stanowiska służbowego osoby go składającej.
2. Wzór protokołu przyjęcia ustnych wyjaśnień stanowi załącznik nr 4 do rozporządzenia.
3. Wzór protokołu przyjęcia ustnego oświadczenia stanowi załącznik nr 5 do rozporządzania.

§ 14. W razie zasięgania przez kontrolera informacji lub uzyskiwania wyjaśnień na podstawie art. 16 pkt 6 ustawy, informacje lub wyjaśnienia powinny być utrwalone na piśmie i podpisane przez osobę, która je złożyła.

§ 15. 1. Postanowienie o powołaniu biegłego wydaje upoważniony przez szefa właściwej służby ochrony państwa funkcjonariusz albo żołnierz.
2. Wzór postanowienia o powołaniu biegłego stanowi załącznik nr 6 do rozporządzenia.

§ 16. W przypadku powołania biegłego podstawą wydania przez niego opinii oraz sporządzenia szczegółowego sprawozdania z badań mających wpływ na ustalenia kontroli jest umowa zawarta między biegłym a upoważnionym przez szefa właściwej służby ochrony państwa funkcjonariuszem albo żołnierzem, określająca wzajemne prawa i obowiązki stron, a w szczególności przedmiot badań, ich zakres, termin sporządzenia opinii i sprawozdania oraz wysokość wynagrodzenia.

§ 17. 1. Dokumenty sporządzone przez kontrolera, utrwalające przebieg czynności dokonanych przy udziale specjalisty, podpisują kontroler oraz specjalista.
2. Postanowienie o powołaniu specjalisty wydaje kontroler.
3. Przepis § 16 stosuje się odpowiednio do specjalisty.
4. Wzór postanowienia o powołaniu specjalisty stanowi załącznik nr 7 do rozporządzenia.

§ 18. 1. Dokonane w toku kontroli ustalenia kontroler opisuje w protokole kontroli.
2. Protokół kontroli oprócz danych zawartych w art. 53 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.[2)]) powinien zawierać:
1) oznaczenie jednostki kontrolowanej, jej adres, imię i nazwisko kierownika oraz oznaczenie i adres jednostki nadrzędnej nad jednostką kontrolowaną, z uwzględnieniem zmian w okresie objętym kontrolą;
2) stopień, imię i nazwisko kontrolera, nazwę służby ochrony państwa prowadzącej kontrolę oraz numer i datę upoważnienia do kontroli;
3) datę rozpoczęcia i zakończenia czynności kontrolnych, z wymienieniem dni przerw w kontroli;
4) określenie zakresu i przedmiotu kontroli oraz okresu objętego kontrolą;
5) wzmiankę o prawie, sposobie i terminie zgłoszenia zastrzeżeń co do ustaleń zawartych w protokole oraz o prawie odmowy podpisania protokołu, a także o prawie złożenia wyjaśnień, o których mowa w art. 59 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli;
6) wzmiankę o zgłoszeniu zastrzeżeń oraz o stanowisku zajętym wobec nich przez kontrolera;
7) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;
8) wzmiankę o doręczeniu egzemplarza protokołu kierownikowi jednostki kontrolowanej;
9) adnotację o dokonaniu wpisu do księgi ewidencji kontroli, jeżeli taka księga jest prowadzona przez jednostkę kontrolowaną;
10) oznaczenie miejsca i daty podpisania protokołu;
11) parafy kontrolera i kierownika jednostki kontrolowanej na każdej stronie protokołu;
12) w razie odmowy podpisania protokołu wzmiankę o tym fakcie i przyczynach odmowy podpisania protokołu.
3. Protokół kontroli sporządza się w dwóch egzemplarzach. Jeden egzemplarz protokołu otrzymuje kierownik jednostki kontrolowanej, a drugi załącza się do akt kontroli.

§ 19. 1. Po podpisaniu protokołu kontroli kontroler opracowuje projekt wystąpienia pokontrolnego do kierownika jednostki kontrolowanej zawierającego ocenę kontrolowanej działalności, w tym osób odpowiedzialnych za tę działalność, a w razie stwierdzenia nieprawidłowości, także uwagi i wnioski w sprawie ich usunięcia. W projekcie wystąpienia zawarta jest ponadto informacja o prawie kierownika jednostki kontrolowanej do złożenia zastrzeżeń, a także o terminie nadesłania informacji o sposobie wykorzystania ocen, uwag i wniosków zawartych w wystąpieniu oraz o terminie ponownej kontroli.
2. Jeżeli wyniki kontroli wskazują na konieczność podjęcia określonych czynności przez kierownika jednostki nadrzędnej nad jednostką kontrolowaną, kontroler opracowuje projekt wystąpienia pokontrolnego zawierającego ocenę kontrolowanej działalności oraz uwagi i wnioski dla jednostki nadrzędnej.
3. Jeżeli stwierdzone w wyniku kontroli nieprawidłowości wskazują na konieczność podjęcia działań przez właściwe organy państwowe lub samorządowe, w szczególności w celu zmiany obowiązującego prawa, kontroler opracowuje projekt wystąpienia pokontrolnego do tych organów.
4. Ocenę wskazującą na niezasadność zajmowania stanowiska lub pełnienia funkcji przez osobę odpowiedzialną za stwierdzone nieprawidłowości w jednostce kontrolowanej, wraz ze szczegółowym uzasadnieniem, kontroler przedstawia w projekcie wystąpienia pokontrolnego właściwej jednostce organizacyjnej lub właściwemu organowi.

§ 20. 1. Wystąpienie pokontrolne skierowane do jednostki organizacyjnej podpisuje szef właściwej służby ochrony państwa lub upoważniony przez niego funkcjonariusz albo żołnierz.
2. Wystąpienie pokontrolne załącza się do akt kontroli.

§ 21. 1. Informacje o wynikach przeprowadzonych kontroli opracowuje się w przypadku kontroli uwzględnionych w planach kontroli. Szef właściwej służby ochrony państwa może zarządzić opracowanie informacji o wynikach kontroli doraźnej.
2. Informacje o wynikach przeprowadzonych kontroli szef właściwej służby ochrony państwa przekazuje Przewodniczącemu Kolegium do Spraw Służb Specjalnych, a w razie potrzeby innym właściwym organom.

§ 22. Informacja o wynikach przeprowadzonych kontroli zawiera w szczególności:
1) określenie jednostki kontrolowanej, celu kontroli, jej zakresu, czasu przeprowadzenia i okresu objętego kontrolą;
2) istotne ustalenia kontroli ukazujące skalę stwierdzonych zjawisk, przyczyny ich powstania, skutki, jakie wywołują lub mogą wywołać, w odniesieniu do stanu zabezpieczenia informacji niejawnych;
3) ogólną ocenę oraz wynikające z niej uwagi i wnioski, zwłaszcza co do stosowania lub dokonania zmian obowiązującego prawa bądź podjęcia określonych działań organizacyjnych.

§ 23. 1. Zastrzeżenia do ustaleń zawartych w protokole kontroli rozpatruje szef właściwej służby ochrony państwa lub upoważniony przez niego funkcjonariusz albo żołnierz.
2. Zastrzeżenia do ustaleń zawartych w protokole kontroli dotyczącym kontroli przeprowadzanej w Sejmie Rzeczypospolitej Polskiej lub Senacie Rzeczypospolitej Polskiej rozpatruje szef właściwej służby ochrony państwa.

§ 24. Zastrzeżenia do wystąpienia pokontrolnego rozpatruje szef właściwej służby ochrony państwa.

§ 25. Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową (Dz. U. Nr 18, poz. 160).

§ 26. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

ZAŁĄCZNIK Nr 1

..... dnia .....

.....
pieczęć nagłówkowa służby ochrony państwa z adresem

UPOWAŻNIENIE Nr.....

Na podstawie art. 16 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) upoważniam Pana/Panią

.....
stopień, imię i nazwisko kontrolera

do przeprowadzenia kontroli

.....
oznaczenie i temat kontroli

.....
nazwa i adres jednostki kontrolowanej

Wyżej wymieniony(a) jest upoważniony(a) do dostępu do informacji niejawnych stanowiących tajemnicę państwową do klauzuli „ściśle tajne".

Upoważnienie niniejsze ważne jest za okazaniem legitymacji służbowej.

Ważność upoważnienia upływa z dniem.....

mp.

.....
imienna pieczęć i podpis osoby wydającej upoważnienie

Ważność upoważnienia przedłuża się do dnia .....

mp.

.....
imienna pieczęć i podpis osoby wydającej upoważnienie

WZÓR

ZAŁĄCZNIK Nr 2

..... dnia .....

.....
pieczęć nagłówkowa służby ochrony państwa z adresem

Protokół zabezpieczenia dokumentu lub rzeczy stanowiących materiał dowodowy

Na podstawie art. 17 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) w związku z art. 38 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.)

.....
stopień, imię i nazwisko kontrolera

działając w obecności

.....,
imię, nazwisko i stanowisko służbowe osoby uczestniczącej w zabezpieczeniu dokumentu/rzeczy

dokonał(a) w dniu .....
zabezpieczenia dokumentu/rzeczy* w postaci

.....
dokładny opis zabezpieczonego dokumentu/rzeczy

.....

.....

Dokument/rzecz* został(a) zabezpieczony(a) poprzez

.....
sposób zabezpieczenia dokumentu/rzeczy, uniemożliwiający zastąpienie go/jej inną

.....

.....

WZÓR

..... dnia .....

.....
podpis osoby uczestniczącej w zabezpieczeniu dokumentu/rzeczy

.....
podpis kontrolera

* Niepotrzebne skreślić.

ZAŁĄCZNIK Nr 3

.....
pieczęć nagłówkowa służby ochrony
państwa z adresem

Protokół oględzin

Na podstawie art. 16 pkt 4 i art. 17 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) w związku z art. 39 ust. 3 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.)

.....
stopień, imię i nazwisko kontrolera

działając w obecności .....
imię, nazwisko i stanowisko służbowe osoby uczestniczącej w oględzinach

.....,

dokonał(a) w dniu .....

.....

.....,
określenie przedmiotu

w wyniku których ustalono, co następuje: .....

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

WZÓR

.....

.....

.....

.....
pieczęć nagłówkowa służby ochrony
państwa z adresem

Protokół przyjęcia ustnych wyjaśnień

Na podstawie art. 16 pkt 5 i art. 17 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) w związku z art. 40 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.)

.....
stopień, imię i nazwisko kontrolera

w dniu ..... uprzedził(a) .....
.....
imię, nazwisko i stanowisko służbowe składającego wyjaśnienia

.....

o treści art. 16 pkt 5 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych oraz art. 40 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli oraz przyjął od niego ustne wyjaśnienia w sprawie .....
.....
.....
.....
.....
.....
.....
.....

o następującej treści .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

WZÓR

.....

.....

.....

ZAŁĄCZNIK Nr 5

.....
pieczęć nagłówkowa służby ochrony
państwa z adresem

Protokół przyjęcia ustnego oświadczenia

Na podstawie art. 17 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) w związku z art. 41 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.)

.....
stopień, imię i nazwisko kontrolera

w dniu ..... przyjął (przyjęła) od .....
imię, nazwisko składającego oświadczenie

.....

ustne oświadczenie w sprawie .....
.....
.....
.....
.....

o następującej treści .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

WZÓR

.....

.....

.....

ZAŁĄCZNIK Nr 6

..... dnia .....

.....
pieczęć nagłówkowa służby ochrony
państwa z adresem

Postanowienie o powołaniu biegłego

Na podstawie art. 16 pkt 7 i art. 17 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) w związku z art. 49 ust. 1 i 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.) powołuję biegłego z dziedziny .....

.....

w osobie .....

dla zbadania .....
przedmiot i zakres badań

oraz sporządzenia szczegółowego sprawozdania z przeprowadzonych badań i wydania na ich podstawie opinii w terminie do dnia .....

.....
stopień, imię i nazwisko oraz
podpis upoważnionego przez szefa służby ochrony
państwa funkcjonariusza albo żołnierza

WZÓR

ZAŁĄCZNIK Nr 7

..... dnia .....

.....
pieczęć nagłówkowa służby ochrony
państwa z adresem

Postanowienie o powołaniu specjalisty do udziału w czynnościach badawczych

Na podstawie art. 16 pkt 7 i art. 17 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) w związku z art. 49 ust. 4 i 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2001 r. Nr 85, poz. 937, z późn. zm.) powołuję specjalistę w dziedzinie

w osobie .....

do uczestniczenia w dniu (dniach) .....

w .....

.....
miejsce i przedmiot czynności badawczych

.....
stopień, imię i nazwisko oraz
podpis kontrolera

WZÓR

Dz. U. Nr 171 poz.1431

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia 25 sierpnia 2005 r.

w sprawie wzorów poświadczenia bezpieczeństwa, decyzji o odmowie wydania poświadczenia bezpieczeństwa oraz decyzji o cofnięciu poświadczenia bezpieczeństwa

(Dz. U. z dnia 8 września 2005 r.)

Na podstawie art. 36 ust. 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Ustala się wzór:

1) poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych, wydawany przez:

a) pełnomocnika ochrony, stanowiący załącznik nr 1 do rozporządzenia,

b) służbę ochrony państwa, stanowiący załącznik nr 2 do rozporządzenia,

c) krajową władzę bezpieczeństwa, stanowiące załączniki nr 3, 4 i 5 do rozporządzenia,

d) podmiot przeprowadzający samodzielne postępowania sprawdzające, na podstawie art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, zwanej dalej „ustawą", stanowiący załącznik nr 6 do rozporządzenia;

2) decyzji o odmowie wydania poświadczenia bezpieczeństwa wydawanej przez:

a) pełnomocnika ochrony, stanowiący załącznik nr 7 do rozporządzenia,

b) służbę ochrony państwa albo podmiot przeprowadzający samodzielne postępowania sprawdzające, na podstawie art. 30 ustawy, stanowiący załącznik nr 8 do rozporządzenia,

c) krajową władzę bezpieczeństwa, stanowiący załącznik nr 9 do rozporządzenia;

3) decyzji o cofnięciu poświadczenia bezpieczeństwa wydawanej przez:

a) pełnomocnika ochrony, stanowiący załącznik nr 10 do rozporządzenia,

b) służbę ochrony państwa albo podmiot przeprowadzający samodzielne postępowania sprawdzające, na podstawie art. 30 ustawy, stanowiący załącznik nr 11 do rozporządzenia,

c) krajową władzę bezpieczeństwa, stanowiący załącznik nr 12 do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[2)]

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2000 r. Nr 12, poz. 136 i Nr 39, poz. 462, z 2001 r. Nr 22, poz. 247, Nr 27, poz. 298, Nr 56, poz. 580, Nr 110, poz. 1189, Nr 123, poz. 1353 i Nr 154, poz. 1800, z 2002 r. Nr 74, poz. 676, Nr 89, poz. 804 i Nr 153, poz. 1271, z 2003 r. Nr 17, poz. 155, z 2004 r. Nr 29, poz. 257 oraz z 2005 r. Nr 85, poz. 727.

[2)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 r. w sprawie wzoru poświadczenia bezpieczeństwa oraz wzoru odmowy wydania poświadczenia bezpieczeństwa (Dz. U. Nr 18, poz. 165 oraz z 2001 r. Nr 80, poz. 869).

ZAŁĄCZNIKI

ZAŁĄCZNIK Nr 1

pieczęć nagłówkowa jednostki organizacyjnej

POŚWIADCZENIE BEZPIECZEŃSTWA Nr

Na podstawie art. 36 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na polecenie

stanowisko osoby wydającej polecenie

zwykłego postępowania sprawdzającego stwierdzam, że Pan(i)

imię i nazwisko, data urodzenia

uzyskał(a) poświadczenie bezpieczeństwa

upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą **„zastrzeżone”/„poufne” ***

na okres do

termin ważności

(miejscowość i data)

imienna pieczęć i czytelny
podpis pełnomocnika ochrony

* niepotrzebne skreślić

ZAŁĄCZNIK Nr 2

.....
pieczęć nagłówkowa służby ochrony państwa

POŚWIADCZENIE BEZPIECZEŃSTWA Nr .....

Na podstawie art. 36 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na wniosek

.....
wnioskodawca

specjalnego/poszerzonego/zwykłego* postępowania sprawdzającego stwierdzam, że Pan (i)

.....
imię i nazwisko, data urodzenia

uzyskał(a) poświadczenie bezpieczeństwa

upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą:

ŚCIŚLE TAJNE* – na okres do .....
termin ważności

TAJNE* – na okres do .....
termin ważności

POUFNE/ZASTRZEŻONE* – na okres do .....
termin ważności

.....
miejscowość i data

mp.

.....
imienna pieczęć i czytelny podpis
upoważnionego funkcjonariusza albo
żołnierza służby ochrony państwa

* Niepotrzebne skreślić.

UWAGA: Poświadczenie bezpieczeństwa jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze zielonym i z tekstem o treści: „służba ochrony państwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „służba ochrony państwa".

WZÓR

.....
pieczęć krajowej władzy bezpieczeństwa

POŚWIADCZENIE BEZPIECZEŃSTWA Nr .....

Na podstawie art. 36 ust. 2 w zw. z art. 15 i art. 29a ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na wniosek

.....
wnioskodawca

przez .....
określenie służby ochrony państwa

zwykłego/poszerzonego/specjalnego* postępowania sprawdzającego stwierdzam, że Pan(i)

.....
imię i nazwisko, data urodzenia

uzyskał(a) poświadczenie bezpieczeństwa

upoważniające do dostępu do informacji niejawnych **NATO** oznaczonych klauzulą:

.....
nazwa klauzuli tajności

na okres do .....
termin ważności

.....
miejscowość i data

m.p.

.....
imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa lub jej
upoważnionego przedstawiciela

* Niepotrzebne skreślić.

UWAGA: Poświadczenie bezpieczeństwa jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i z tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

ZAŁĄCZNIK Nr 4

.....
pieczęć krajowej władzy bezpieczeństwa

POŚWIADCZENIE BEZPIECZEŃSTWA Nr .....

Na podstawie art. 36 ust. 2 w zw. z art. 15 i art. 29a ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na wniosek

.....
wnioskodawca

przez .....
określenie służby ochrony państwa

zwykłego/poszerzonego/specjalnego* postępowania sprawdzającego stwierdzam, że Pan(i)

.....
imię i nazwisko, data urodzenia

uzyskał(a) poświadczenie bezpieczeństwa

upoważniające do dostępu do informacji niejawnych **Unii Zachodnioeuropejskiej** oznaczonych klauzulą:

.....
nazwa klauzuli tajności

na okres do .....
termin ważności

.....
miejscowość i data

m.p.

.....
imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa lub jej
upoważnionego przedstawiciela

* Niepotrzebne skreślić.

UWAGA: Poświadczenie bezpieczeństwa jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i z tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

WZÓR

ZAŁĄCZNIK Nr 5

.....
pieczęć krajowej władzy bezpieczeństwa

POŚWIADCZENIE BEZPIECZEŃSTWA Nr .....

Na podstawie art. 36 ust. 2 w zw. z art. 15 i art. 29a ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na wniosek

.....
wnioskodawca

przez .....
określenie służby ochrony państwa

zwykłego/poszerzonego/specjalnego* postępowania sprawdzającego stwierdzam, że Pan(i)

.....
imię i nazwisko, data urodzenia

uzyskał(a) poświadczenie bezpieczeństwa

upoważniające do dostępu do informacji niejawnych Unii Europejskiej oznaczonych klauzulą:

.....
nazwa klauzuli tajności

na okres do .....
termin ważności

.....
miejscowość i data

mp.

.....
imienna pieczęć i czytelny podpis krajowej władzy bezpieczeństwa lub jej upoważnionego przedstawiciela

* Niepotrzebne skreślić.

UWAGA: Poświadczenie bezpieczeństwa jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i z tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

WZÓR

ZAŁĄCZNIK Nr 6

.....

pieczęć nagłówkowa podmiotu wymienionego w art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych

POŚWIADCZENIE BEZPIECZEŃSTWA Nr .....

Na podstawie art. 36 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na wniosek

.....

wnioskodawcy

specjalnego/poszerzonego/zwykłego* postępowania sprawdzającego stwierdzam, że Pan(i)

.....

imię i nazwisko, data urodzenia

uzyskał(a) poświadczenie bezpieczeństwa

upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą:

ŚCIŚLE TAJNE* – na okres do .....

termin ważności

TAJNE* – na okres do .....

termin ważności

POUFNE/ZASTRZEŻONE* – na okres do .....

termin ważności

.....

miejscowość i data

m.p.

.....

imienna pieczęć i czytelny podpis osoby upoważnionej

* Niepotrzebne skreślić.

UWAGA: Poświadczenie bezpieczeństwa jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze beżowym i z tekstem o treści odpowiednio: „ABW", „Agencja Wywiadu", „WSI", „Policja", „Żandarmeria Wojskowa", „Straż Graniczna", „Służba Więzienna" oraz wprowadzonym w miejsce linii odpowiednim mikrotekstem o treści jak wyżej.

WZÓR

.....
pieczęć nagłówkowa jednostki organizacyjnej

DECYZJA Nr .....

O ODMOWIE WYDANIA POŚWIADCZENIA BEZPIECZEŃSTWA

Na podstawie art. 36 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na polecenie

.....
stanowisko osoby wydającej polecenie

przez .....
imię i nazwisko pełnomocnika ochrony

zwykłego postępowania sprawdzającego stwierdzam, że Panu(i)

.....
imię i nazwisko, data urodzenia

odmówiono wydania poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone"/„poufne"*.

.....
miejscowość i data

.....
imienna pieczęć i czytelny
podpis pełnomocnika ochrony

Pouczenie:

Na decyzję o odmowie wydania poświadczenia bezpieczeństwa przysługuje prawo wniesienia odwołania do Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o odmowie wydania poświadczenia bezpieczeństwa, za pośrednictwem pełnomocnika ochrony.

Na decyzję utrzymującą w mocy decyzję o odmowie wydania poświadczenia bezpieczeństwa, osobie sprawdzanej przysługuje skarga do sądu administracyjnego, za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia.

* Niepotrzebne skreślić.

ZAŁĄCZNIK Nr 8

.....

pieczęć nagłówkowa służby ochrony państwa lub podmiotu wymienionego w art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych

DECYZJA Nr .....

O ODMOWIE WYDANIA POŚWIADCZENIA BEZPIECZEŃSTWA

Na podstawie art. 36 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na wniosek

.....

wnioskodawca

przez .....

określenie służby ochrony państwa lub podmiotu wymienionego w art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych

specjalnego/poszerzonego/zwykłego* postępowania sprawdzającego stwierdzam, że Panu(i)

.....

imię i nazwisko, data urodzenia

odmówiono wydania poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą:

.....

nazwa klauzuli tajności

.....

miejscowość i data

m.p.

.....

imienna pieczęć i czytelny podpis osoby upoważnionej

Pouczenie:

Na decyzję o odmowie wydania poświadczenia bezpieczeństwa przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów/Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Agencji Wywiadu/Szefa Wojskowych Służb Informacyjnych/Komendanta Głównego Policji/Komendanta Głównego Żandarmerii Wojskowej/Komendanta Głównego Straży Granicznej/Dyrektora Generalnego Służby Więziennej*. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o odmowie wydania poświadczenia bezpieczeństwa, za pośrednictwem podmiotu, który ją wydał.

Na decyzję utrzymującą w mocy decyzję o odmowie wydania poświadczenia bezpieczeństwa, osobie sprawdzanej przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia.

* Niepotrzebne skreślić.

WZÓR

ZAŁĄCZNIK Nr 9

.....
pieczęć krajowej władzy bezpieczeństwa

DECYZJA Nr .....

O ODMOWIE WYDANIA POŚWIADCZENIA BEZPIECZEŃSTWA

Na podstawie art. 36 ust. 2 w zw. z art. 15 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu na wniosek

.....
wnioskodawca

przez .....
określenie służby ochrony państwa

specjalnego/poszerzonego/zwykłego* postępowania sprawdzającego stwierdzam, że Panu(i)

.....
imię i nazwisko, data urodzenia

odmówiono wydania poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych NATO/UZE/UE* oznaczonych klauzulą:

.....
nazwa klauzuli tajności

.....
miejscowość i data

m.p.

.....
imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa lub
jej upoważnionego przedstawiciela

Pouczenie:

Na decyzję o odmowie wydania poświadczenia bezpieczeństwa przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o odmowie wydania poświadczenia bezpieczeństwa, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*.

Na decyzję utrzymującą w mocy decyzję o odmowie wydania poświadczenia bezpieczeństwa, osobie sprawdzanej przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia.

* Niepotrzebne skreślić.

ZAŁĄCZNIK Nr 10

.....
pieczęć nagłówkowa jednostki organizacyjnej

DECYZJA Nr .....

O COFNIĘCIU POŚWIADCZENIA BEZPIECZEŃSTWA

Na podstawie art. 47 ust. 1 pkt 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu przez

.....
imię i nazwisko pełnomocnika ochrony

kontrolnego postępowania sprawdzającego stwierdzam, że Panu(i)

.....
imię i nazwisko, data urodzenia

zostaje cofnięte poświadczenie bezpieczeństwa nr ..... upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone"/„poufne"*.

.....
miejscowość i data

.....
imienna pieczęć i czytelny
podpis pełnomocnika ochrony

Pouczenie:

Na decyzję o cofnięciu poświadczenia bezpieczeństwa przysługuje prawo wniesienia odwołania do Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o cofnięciu poświadczenia bezpieczeństwa, za pośrednictwem pełnomocnika ochrony.

Na decyzję utrzymującą w mocy decyzję o cofnięciu poświadczenia bezpieczeństwa, osobie sprawdzanej przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie w terminie 30 (trzydziestu) dni od dnia doręczenia.

* Niepotrzebne skreślić.

WZÓR

ZAŁĄCZNIK Nr 11

.....

pieczęć nagłówkowa służby ochrony państwa lub podmiotu wymienionego w art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych

DECYZJA Nr .....

O COFNIĘCIU POŚWIADCZENIA BEZPIECZEŃSTWA

Na podstawie art. 47 ust. 1 pkt 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu przez

.....

określenie służby ochrony państwa lub podmiotu wymienionego w art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych

kontrolnego postępowania sprawdzającego stwierdzam, że Panu(i)

.....

imię i nazwisko, data urodzenia

zostaje cofnięte poświadczenie bezpieczeństwa nr ..... upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą:

.....

nazwa klauzuli tajności

.....

miejscowość i data

m.p.

.....

imienna pieczęć i czytelny podpis osoby upoważnionej

Pouczenie:

Na decyzję o cofnięciu poświadczenia bezpieczeństwa przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów/Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Agencji Wywiadu/Szefa Wojskowych Służb Informacyjnych/Komendanta Głównego Policji/Komendanta Głównego Żandarmerii Wojskowej/Komendanta Głównego Straży Granicznej/Dyrektora Generalnego Służby Więziennej*. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o cofnięciu poświadczenia bezpieczeństwa, za pośrednictwem podmiotu, który ją wydał.

Na decyzję utrzymującą w mocy decyzję o cofnięciu poświadczenia bezpieczeństwa, osobie sprawdzanej przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia.

* Niepotrzebne skreślić.

WZÓR

.....
pieczęć krajowej władzy bezpieczeństwa

DECYZJA Nr .....

O COFNIĘCIU POŚWIADCZENIA BEZPIECZEŃSTWA

Na podstawie art. 47 ust. 1 pkt 1 w zw. z art. 15 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) po przeprowadzeniu przez

.....
określenie służby ochrony państwa

kontrolnego postępowania sprawdzającego stwierdzam, że Panu(i)

.....
imię i nazwisko, data urodzenia

zostaje cofnięte poświadczenie bezpieczeństwa nr ..... upoważniające do dostępu do informacji niejawnych NATO/UZE/UE* oznaczonych klauzulą:

.....
nazwa klauzuli tajności

.....
miejscowość i data

m.p.

.....
imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa lub jej
upoważnionego przedstawiciela

Pouczenie:

Na decyzję o cofnięciu poświadczenia bezpieczeństwa przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o cofnięciu poświadczenia bezpieczeństwa, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*.

Na decyzję utrzymującą w mocy decyzję o cofnięciu poświadczenia bezpieczeństwa, osobie sprawdzanej przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia.

* Niepotrzebne skreślić.

Dz. U. Nr 171 poz. 1433

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia 25 sierpnia 2005 r.

w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

(Dz. U. z dnia 8 września 2005 r.)

Na podstawie art. 62 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:
1) podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy i sieci teleinformatyczne służące do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych;
2) sposób opracowywania dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji systemów lub sieci teleinformatycznych.

§ 2. Ilekroć w rozporządzeniu jest mowa o:
1) incydencie bezpieczeństwa teleinformatycznego - należy przez to rozumieć każde zdarzenie naruszające bezpieczeństwo teleinformatyczne spowodowane w szczególności awarią systemu lub sieci teleinformatycznej, działaniem osób uprawnionych lub nieuprawnionych do pracy w tym systemie lub sieci albo zaniechaniem osób uprawnionych;
2) przekazywaniu informacji niejawnych - należy przez to rozumieć zarówno transmisję informacji niejawnych, jak i przekazywanie elektronicznego nośnika danych, na którym zostały one utrwalone;
3) przetwarzaniu informacji niejawnych - należy przez to rozumieć także wytwarzanie, przechowywanie lub przekazywanie informacji niejawnych.

Rozdział 2

Podstawowe wymagania bezpieczeństwa teleinformatycznego

§ 3. 1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.
2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.

§ 4. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada kierownik jednostki organizacyjnej, który w szczególności:
1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego;
2) realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu lub sieci teleinformatycznej;

3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej;
4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;
6) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne".

§ 5. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:
1) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie bezpieczeństwa, strefie administracyjnej lub specjalnej strefie bezpieczeństwa, zwanych dalej „strefą kontrolowanego dostępu" w zależności od:
a) klauzuli tajności,
b) ilości,
c) zagrożeń dla poufności, integralności lub dostępności
- informacji niejawnych;
2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
a) nieuprawnionym dostępem,
b) podglądem,
c) podsłuchem.

§ 6. 1. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.
2. Utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń.
3. Utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.
4. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji niejawnych, o którym mowa w § 12, lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

§ 7. 1. Ochrona kryptograficzna informacji niejawnych przetwarzanych w systemie lub sieci teleinformatycznej polega na zastosowaniu mechanizmów gwarantujących ich poufność, integralność oraz uwierzytelnienie.
2. Ochronę kryptograficzną stosuje się przy przekazywaniu informacji niejawnych w formie transmisji poza strefę kontrolowanego dostępu.
3. Przekazywanie informacji niejawnych utrwalonych na elektronicznych nośnikach danych poza strefę kontrolowanego dostępu odbywa się z zapewnieniem, odpowiedniej do klauzuli tajności tych informacji, ochrony kryptograficznej lub po spełnieniu wymagań, o których mowa w przepisach w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów, w celu ich zabezpieczenia przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

§ 8. Niezawodność transmisji polega na zapewnieniu integralności i dostępności informacji niejawnych przekazywanych w systemach lub sieciach teleinformatycznych. Zapewnia się ją w szczególności przez wykorzystywanie zapasowych łączy telekomunikacyjnych.

§ 9. 1. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej:
1) kierownik jednostki organizacyjnej lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;

2) administrator systemów określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.
2. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.

§ 10. Projektowanie, organizacja i eksploatacja systemu lub sieci teleinformatycznej służącej do przetwarzania informacji niejawnych stanowiących tajemnicę państwową odbywa się w sposób uniemożliwiający niekontrolowany dostęp jednej osoby do wszystkich zasobów systemu lub sieci, w szczególności danych, informacji, oprogramowania, narzędzi lub urządzeń teleinformatycznych.

§ 11. Służby ochrony państwa mogą dopuścić do stosowania w systemie lub sieci teleinformatycznej urządzenia lub narzędzia, które spełniają właściwe wymagania bezpieczeństwa, jeżeli otrzymały stosowny certyfikat krajowej władzy bezpieczeństwa w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego lub w państwie członkowskim Unii Europejskiej.

Rozdział 3

Sposób opracowywania dokumentacji bezpieczeństwa teleinformatycznego

§ 12. Dokumenty szczególnych wymagań bezpieczeństwa opracowuje się po przeprowadzeniu szacowania ryzyka dla informacji niejawnych, które mają być przetwarzane w danym systemie lub sieci teleinformatycznej, z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej.

§ 13. 1. Przy opracowaniu szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej uwzględnia się w szczególności dane o budowie oraz charakterystykę systemu lub sieci teleinformatycznej.
2. Dane o budowie systemu lub sieci teleinformatycznej obejmują dane dotyczące elementów wchodzących w skład tego systemu lub sieci w zakresie:
1) lokalizacji;
2) typu wykorzystywanych urządzeń oraz oprogramowania;
3) sposobu realizowania połączeń wewnętrznych oraz zewnętrznych;
4) konfiguracji sprzętowej i ustawień mechanizmów zabezpieczających;
5) środowiska eksploatacji.
3. Charakterystyka systemu lub sieci teleinformatycznej powinna określać:
1) klauzulę tajności informacji niejawnych, które będą w nich przetwarzane;
2) kategorie uprawnień osób uprawnionych do pracy w systemie lub sieci teleinformatycznej w zakresie dostępu do przetwarzanych w nich informacji niejawnych, w zależności od klauzuli tajności tych informacji;
3) tryb bezpieczeństwa pracy systemu lub sieci teleinformatycznej.

§ 14. Szczególne wymagania bezpieczeństwa określają co najmniej:
1) osoby odpowiedzialne za wdrożenie środków zapewniających bezpieczeństwo teleinformatyczne;
2) zadania osób odpowiedzialnych za bezpieczeństwo teleinformatyczne;
3) granice i lokalizację stref kontrolowanego dostępu oraz środki ich ochrony;
4) środki ochrony kryptograficznej, elektromagnetycznej, technicznej lub organizacyjnej systemu lub sieci teleinformatycznej;
5) inne zastosowane środki ochrony zapewniające bezpieczeństwo teleinformatyczne informacji niejawnych;
6) zasady zarządzania ryzykiem;
7) zasady szkolenia z zakresu bezpieczeństwa teleinformatycznego osób odpowiedzialnych za bezpieczeństwo teleinformatyczne oraz osób uprawnionych do pracy w systemie lub sieci teleinformatycznej.

§ 15. 1. Procedury bezpiecznej eksploatacji zawierają szczegółowy wykaz czynności wraz z dokładnym opisem sposobu ich wykonania, które powinny być realizowane przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie lub sieci teleinformatycznej.

2. Szczegółowy wykaz czynności powinien być ujęty w tematycznie wyodrębnione procedury bezpieczeństwa dotyczące w szczególności:

1) administrowania systemem lub siecią teleinformatyczną;
2) bezpieczeństwa osobowego;
3) bezpieczeństwa dokumentów i materiałów niejawnych, w tym procedur sporządzania kopii z tych dokumentów oraz niszczenia dokumentów i ich kopii;
4) ochrony kryptograficznej, elektromagnetycznej, fizycznej, niezawodności transmisji lub kontroli dostępu do urządzeń systemu lub sieci teleinformatycznej;
5) bezpieczeństwa urządzeń i oprogramowania;
6) zapewnienia ciągłości działania systemu lub sieci teleinformatycznej;
7) zarządzania konfiguracją;
8) audytu bezpieczeństwa.

§ 16. W procedurach, o których mowa w § 15, określa się tryb postępowania przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie lub sieci teleinformatycznej w sytuacji wystąpienia incydentu bezpieczeństwa teleinformatycznego.

Rozdział 4

Przepisy końcowe

§ 17. Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18, poz. 162).

§ 18. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Dz. U. 05.181.1504

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia 8 września 2005 r.

w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego

(Dz. U. z dnia 21 września 2005 r.)

Na podstawie art. 74 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Ustala się wzór:

1) kwestionariusza bezpieczeństwa przemysłowego, określony w załączniku nr 1 do rozporządzenia;

2) świadectwa bezpieczeństwa przemysłowego:

a) pierwszego stopnia, określony w załącznikach nr 2 i 3 do rozporządzenia,

b) drugiego stopnia, określony w załącznikach nr 4 i 5 do rozporządzenia,

c) trzeciego stopnia, określony w załącznikach nr 6 i 7 do rozporządzenia;

3) decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, określony w załącznikach nr 8 i 9 do rozporządzenia;

4) decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, określony w załącznikach nr 10 i 11 do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

ZAŁĄCZNIKI

ZAŁĄCZNIK Nr 1

WZÓR

.....
(pieczęć przedsiębiorcy, jednostki naukowej
lub badawczo-rozwojowej ubiegającej
się o świadectwo bezpieczeństwa przemysłowego)

KWESTIONARIUSZ BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Dane zawarte w niniejszym Kwestionariuszu Bezpieczeństwa Przemysłowego będą wykorzystane zgodnie z ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.), zwaną dalej „ustawą", w toku postępowania sprawdzającego mającego na celu ocenę zdolności przedsiębiorcy, jednostki naukowej lub badawczo-rozwojowej, zwanych dalej „przedsiębiorcą", do zapewnienia ochrony informacji niejawnych przed nieuprawnionym ujawnieniem.

1. Dane identyfikujące przedsiębiorcę podlegającego sprawdzeniu

a. Pełna nazwa .....
.....
b. Nazwa skrócona .....
c. Nazwa używana do celów marketingowych .....
d. Adres siedziby .....
(kod pocztowy, miasto, ulica, nr domu)
.....
(województwo, powiat, gmina)
.....
(nr telefonu, faksu, adres poczty elektronicznej)
e. Statystyczny numer identyfikacyjny (REGON) .....
f. Numer identyfikacji podatkowej (NIP) .....
g. Forma prawna .....
h. Rejestr działalności gospodarczej[1)] .....
.....
(nazwa i siedziba rejestru)
.....
(nr rejestru, data rejestracji)
i. Data rozpoczęcia działalności gospodarczej .....

2. Dane o strukturze kapitału i powiązaniach kapitałowych

a. Wartość kapitału zakładowego .....
b. Liczba akcji/udziałów .....
c. Wartość nominalna akcji/udziału .....
d. Struktura kapitału:

Imię i nazwisko właściciela lub pełna nazwa i adres posiadacza powyżej 10 % akcji/udziałów (a/u)[2)]	Liczba a/u	% a/u	Stosunek uprzywilejowania

e. Wykaz 10 największych umów wykonywanych w ciągu ostatnich 3 lat na rzecz kontrahentów krajowych:

Umowa dotyczyła	Dane kontrahenta	Wartość umowy	Okres realizacji

f. Wykaz 10 największych umów wykonywanych w ciągu ostatnich 3 lat na rzecz kontrahentów zagranicznych:

Umowa dotyczyła	Dane kontrahenta	Wartość umowy	Okres realizacji

g. Udział powyżej 10 % w kapitale innych podmiotów:

Nazwa podmiotu	Adres siedziby	% a/u	Wartość a/u

3. Dane o sytuacji finansowej

a. Zysk/strata netto za ostatnie trzy lata obrachunkowe[1)]:

- .....
- .....
- .....

b. Suma bilansowa za ostatnie trzy lata obrachunkowe[1)]:

- .....
- .....
- .....

c. Wykaz wierzycieli, wobec których zobowiązania podmiotu przekraczają 20 % wartości kapitału zakładowego:

Nazwa wierzyciela	Adres wierzyciela	Kwota zobowiązań

d. Czy przedsiębiorca ma zaległości podatkowe[1)]:

	TAK		NIE

e. Czy przedsiębiorca ma zaległości w wywiązywaniu się z podatków i opłat lokalnych[1)]:

	TAK		NIE

f. Czy przedsiębiorca ma zaległości w odprowadzaniu składek na rzecz ZUS[1)]:

	TAK		NIE

g. Czy przedsiębiorca jest w trakcie postępowania ugodowego z wierzycielami:

	TAK		NIE

h. Czy w odniesieniu do przedsiębiorcy prowadzone jest postępowanie w sprawie o przestępstwo skarbowe lub wykroczenie skarbowe:

	TAK		NIE

i. Czy wobec przedsiębiorcy prowadzone jest sądowo-komornicze lub administracyjne postępowanie egzekucyjne:

	TAK		NIE

j. Czy wobec przedsiębiorcy toczy się postępowanie z wniosku o ogłoszenie upadłości:

	TAK		NIE

k. Wykaz numerów rachunków bankowych przedsiębiorcy (na pierwszym miejscu numer rachunku podstawowego):

Nr rachunku bankowego	Nazwa i adres banku

4. Dane o strukturze organizacyjnej

a. Liczba oddziałów .....

b. Oddziały, w których będą wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne (dane jak w pkt 1 lit. d):

Nazwa oddziału	Adres oddziału

5. Dane osób zarządzających lub wchodzących w skład organów zarządzających albo kontrolnych przedsiębiorcy, a także osób działających z ich upoważnienia:

Imię i nazwisko	Nr PESEL[3)]	Adres zamieszkania	Funkcja

6. Dane o systemie ochrony:

a. Czy przedsiębiorca posiada wydzieloną strefę (strefy) administracyjną:

	TAK		NIE

b. Czy przedsiębiorca posiada wydzieloną strefę (strefy) bezpieczeństwa z systemem kontroli uprawnień do wejścia, wyjścia i przebywania (jeżeli tak, proszę podać adres):

	TAK		NIE

.....

.....

c. Czy przedsiębiorca posiada pomieszczenie kancelarii tajnej (jeżeli tak, proszę podać adres):

	TAK		NIE

.....

.....

d. Czy system fizycznej ochrony jest obsługiwany lub wspomagany przez:

- wewnętrzny pion ochrony:

	TAK		NIE

- podmiot prowadzący działalność w zakresie ochrony osób i mienia (jeżeli tak, proszę podać pełną nazwę, adres siedziby, nr telefonu, nr koncesji/zezwolenia, datę wydania koncesji/zezwolenia):

	TAK		NIE

.....

.....

e. Czy do ochrony informacji niejawnych zastosowano wyposażenie i urządzenia posiadające certyfikaty lub świadectwa kwalifikacyjne wydane na podstawie odrębnych przepisów:

	TAK		NIE

f. Czy podjęto działania mające na celu uzyskanie certyfikatu akredytacji bezpieczeństwa teleinformatycznego dla systemu lub sieci teleinformatycznej:

- do poziomu „tajne":

	TAK		NIE

• do poziomu „ściśle tajne":

	TAK		NIE

7. Wykazy pracowników (osób)

a. pracowników posiadających poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych stanowiących tajemnicę państwową[4)]:

Imię i nazwisko	Nr PESEL[3)]	Klauzula i nr poświad.	Organ wydający	Data ważności	Stanowisko

b. pracowników, którzy powinni być poddani poszerzonemu lub specjalnemu postępowaniu sprawdzającemu[5)]:

Imię i nazwisko	Nr PESEL[3)]	Klauzula	Stanowisko

c. osób, które wykonują lub będą wykonywać funkcje związane z ochroną informacji niejawnych (pion ochrony):

Imię i nazwisko	Nr PESEL	Klauzula	Stanowisko

Niemieszczące się w polach kwestionariusza dane należy wpisać na dodatkowych arkuszach, z przywołaniem punktu, i dołączyć do dokumentu.

.....

(podpis i imienna pieczęć osoby upoważnionej do składania oświadczeń woli w imieniu przedsiębiorcy)

Miejscowość .....

Data .....

---

[1] Dane powinny być potwierdzone stosownym dokumentem.

[2] W przypadku osób fizycznych: obywateli polskich należy podać nr PESEL, obcokrajowców należy podać: datę i miejsce urodzenia, imię ojca i matki oraz obywatelstwo i narodowość.

[3] W przypadku obcokrajowców należy podać: datę i miejsce urodzenia, imię ojca i matki oraz obywatelstwo i narodowość.

[4] Oraz poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych stanowiących tajemnicę służbową wydane przez służby ochrony państwa w przypadku prowadzenia postępowania, o którym mowa w art. 67 ustawy.

[5] Oraz zwykłemu postępowaniu sprawdzającemu w związku z prowadzeniem postępowania, o którym mowa w art. 67 ustawy.

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

PIERWSZEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 1 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) wydano **świadectwo bezpieczeństwa przemysłowego pierwszego stopnia,** stwierdzając, że jednostka ta posiada pełną zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą .....
(nazwa klauzuli tajności)

do .....
(data ważności)

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
upoważnionego funkcjonariusza
albo żołnierza służby ochrony państwa)

---

* Niepotrzebne skreślić.

.....
(pieczęć krajowej władzy bezpieczeństwa)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

PIERWSZEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 1 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) wydano **świadectwo bezpieczeństwa przemysłowego pierwszego stopnia**, stwierdzając, że jednostka ta posiada pełną zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą **NATO** ..... do ..... .
(nazwa klauzuli tajności) (data ważności)

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

---

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

.....
(pieczęć krajowej władzy bezpieczeństwa)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

PIERWSZEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 1 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) wydano **świadectwo bezpieczeństwa przemysłowego pierwszego stopnia,** stwierdzając, że jednostka ta posiada pełną zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą **EU/UE** ..... do .....
(nazwa klauzuli tajności) (data ważności)

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

DRUGIEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 2 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) wydano **świadectwo bezpieczeństwa przemysłowego drugiego stopnia**, stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą ..... do ..... ,
(nazwa klauzuli tajności) (data ważności)

z wyłączeniem uprawnień do wytwarzania, przechowywania, przekazywania lub przetwarzania tych informacji we własnych systemach i sieciach teleinformatycznych.

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)

---

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze zielonym i tekstem o treści: „służba ochrony państwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „służba ochrony państwa".

.....
(pieczęć krajowej władzy bezpieczeństwa)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

DRUGIEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 2 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) wydano **świadectwo bezpieczeństwa przemysłowego drugiego stopnia,** stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą **NATO** ..... do .....
(nazwa klauzuli tajności) (data ważności)

z wyłączeniem uprawnień do wytwarzania, przechowywania, przekazywania lub przetwarzania tych informacji we własnych systemach i sieciach teleinformatycznych.

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

---

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i tekstem o treści: „krajowa władza bezpieczeństwa" oraz *wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".*

.....
(pieczęć krajowej władzy bezpieczeństwa)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

DRUGIEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 2 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) wydano **świadectwo bezpieczeństwa przemysłowego drugiego stopnia,** stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą **EU/UE** ..... do .....
(nazwa klauzuli tajności) (data ważności)

z wyłączeniem uprawnień do wytwarzania, przechowywania, przekazywania lub przetwarzania tych informacji we własnych systemach i sieciach teleinformatycznych.

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

---

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

TRZECIEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 3 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) wydano **świadectwo bezpieczeństwa przemysłowego trzeciego stopnia**, stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą ..... do ..... ,
(nazwa klauzuli tajności) (data ważności)

z wyłączeniem uprawnień do wytwarzania, przechowywania, przekazywania lub przetwarzania tych informacji w użytkowanych przez nią obiektach.

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
upoważnionego funkcjonariusza
albo żołnierza służby ochrony państwa)

---

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze zielonym i tekstem o treści: „służba ochrony państwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „służba ochrony państwa".

.....
(pieczęć krajowej władzy bezpieczeństwa)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

TRZECIEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 3 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) wydano **świadectwo bezpieczeństwa przemysłowego trzeciego stopnia,** stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą **NATO** ..... do ..... ,
(nazwa klauzuli tajności) (data ważności)

z wyłączeniem uprawnień do wytwarzania, przechowywania, przekazywania lub przetwarzania tych informacji w użytkowanych przez nią obiektach.

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

---

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

.....
(pieczęć krajowej władzy bezpieczeństwa)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

TRZECIEGO STOPNIA NR .....

Zaświadcza się, że .....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

na podstawie art. 66 ust. 4 pkt 3 i art. 70 ust. 1 pkt 1, 2, 3* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) wydano **świadectwo bezpieczeństwa przemysłowego trzeciego stopnia,** stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą **EU/UE** ..... do .....,
(nazwa klauzuli tajności) (data ważności)

z wyłączeniem uprawnień do wytwarzania, przechowywania, przekazywania lub przetwarzania tych informacji w użytkowanych przez nią obiektach.

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

---

* Niepotrzebne skreślić.

UWAGA: Świadectwo bezpieczeństwa przemysłowego jest sporządzane na papierze offsetowym formatu A4 z tłem rastrowanym w kolorze niebieskim i tekstem o treści: „krajowa władza bezpieczeństwa" oraz wprowadzonym w miejsce linii mikrotekstem o treści: „krajowa władza bezpieczeństwa".

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem)

DECYZJA NR .....

O ODMOWIE WYDANIA

ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Na podstawie art. 65 i art. 72 ust. 1* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) odmawiam wydania świadectwa bezpieczeństwa przemysłowego ..... stopnia

.....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

..... ,

stwierdzając, że jednostka ta nie posiada zdolności do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą ..... .
(nazwa klauzuli tajności)

UZASADNIENIE

.....

.....

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)

Pouczenie:

Od decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*.
Na decyzję utrzymującą w mocy decyzję o odmowie wydania świadectwa bezpieczeństwa przemysłowego przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia*.

---

* Niepotrzebne skreślić.

.....
(pieczęć krajowej władzy bezpieczeństwa)

DECYZJA NR .....

O ODMOWIE WYDANIA

ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Na podstawie art. 65 i art. 72 ust. 1* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) odmawiam wydania świadectwa bezpieczeństwa przemysłowego ..... stopnia

.....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....,

stwierdzając, że jednostka ta nie posiada zdolności do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą NATO .....
(nazwa klauzuli tajności)

UZASADNIENIE

.....

.....

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

Pouczenie:

Od decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*.
Na decyzję utrzymującą w mocy decyzję o odmowie wydania świadectwa bezpieczeństwa przemysłowego przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia*.

---

* Niepotrzebne skreślić.

.....
(pieczęć krajowej władzy bezpieczeństwa)

DECYZJA NR .....

O ODMOWIE WYDANIA

ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Na podstawie art. 65 i art. 72 ust. 1* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) odmawiam wydania świadectwa bezpieczeństwa przemysłowego ..... stopnia

.....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....,

stwierdzając, że jednostka ta nie posiada zdolności do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą EU/UE .....
(nazwa klauzuli tajności)

UZASADNIENIE

.....

.....

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

Pouczenie:
Od decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego / Szefa Wojskowych Służb Informacyjnych*.
Na decyzję utrzymującą w mocy decyzję o odmowie wydania świadectwa bezpieczeństwa przemysłowego przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia*.

---

* Niepotrzebne skreślić.

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem)

DECYZJA NR .....

O COFNIĘCIU ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Na podstawie art. 72 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) cofam świadectwo bezpieczeństwa przemysłowego ..... stopnia nr ..... wydane w dniu .....

.....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....,

stwierdzając, że jednostka ta utraciła zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą .....
(nazwa klauzuli tajności)

UZASADNIENIE

.....

.....

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis upoważnionego funkcjonariusza albo żołnierza służby ochrony państwa)

Pouczenie:
Od decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*.
Na decyzję utrzymującą w mocy decyzję o cofnięciu świadectwa bezpieczeństwa przemysłowego przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia*.

---

* Niepotrzebne skreślić.

.....
(pieczęć krajowej władzy bezpieczeństwa)

DECYZJA NR .....

O COFNIĘCIU ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Na podstawie art. 72 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) cofam świadectwo bezpieczeństwa przemysłowego ..... stopnia nr ..... wydane w dniu .....

.....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

..... ,

stwierdzając, że jednostka ta utraciła zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą NATO .....
(nazwa klauzuli tajności)

UZASADNIENIE

.....

.....

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

Pouczenie:

Od decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego/Szefa Wojskowych Służb Informacyjnych*.
Na decyzję utrzymującą w mocy decyzję o cofnięciu świadectwa bezpieczeństwa przemysłowego przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia*.

---

* Niepotrzebne skreślić.

.....
(pieczęć krajowej władzy bezpieczeństwa)

DECYZJA NR .....

O COFNIĘCIU ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

Na podstawie art. 72 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) cofam świadectwo bezpieczeństwa przemysłowego ..... stopnia nr ..... wydane w dniu .....

.....
(nazwa przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....

z siedzibą w .....
(adres przedsiębiorcy, jednostki naukowej, jednostki badawczo-rozwojowej)

.....,

stwierdzając, że jednostka ta utraciła zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą EU/UE .....
(nazwa klauzuli tajności)

UZASADNIENIE

.....

.....

.....
(miejscowość i data)

mp.

.....
(imienna pieczęć i czytelny podpis
krajowej władzy bezpieczeństwa
lub jej upoważnionego przedstawiciela)

Pouczenie:
Od decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego przysługuje prawo wniesienia odwołania do Prezesa Rady Ministrów. Odwołanie wnosi się w terminie 14 (czternastu) dni od dnia doręczenia decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, za pośrednictwem Szefa Agencji Bezpieczeństwa Wewnętrznego / Szefa Wojskowych Służb Informacyjnych*.
Na decyzję utrzymującą w mocy decyzję o cofnięciu świadectwa bezpieczeństwa przemysłowego przysługuje skarga do sądu administracyjnego, którą wnosi się za pośrednictwem organu wydającego rozstrzygnięcie, w terminie 30 (trzydziestu) dni od dnia doręczenia*.

*Niepotrzebne skreślić.

Dz. U. 05.200.1650

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia 29 września 2005 r.

w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne

(Dz. U. z dnia 13 października 2005 r.)

Na podstawie art. 53 ust. 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) zarządza się, co następuje:

§ 1. Rozporządzenie określa tryb i sposób przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne w celu ich zabezpieczenia przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

§ 2. 1. Materiały zawierające informacje niejawne są przekazywane przewoźnikom przez jednostki organizacyjne, o których mowa w art. 1 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, zwane dalej „nadawcą".
2. Nadawca składa zamówienie na wykonanie czynności i usług, o których mowa w § 1, kierując je do przewoźników spełniających wymagania w zakresie ochrony informacji niejawnych:
1) poczty specjalnej podlegającej ministrowi właściwemu do spraw wewnętrznych, działającej w jednostkach organizacyjnych Policji przy przesyłaniu materiałów zawierających informacje niejawne, stanowiące tajemnicę państwową, do adresatów zamiejscowych na terenie kraju;
2) właściwej komórki organizacyjnej Ministerstwa Spraw Zagranicznych zapewniającej przewóz materiałów zawierających informacje niejawne poza granicami Rzeczypospolitej Polskiej;
3) właściwych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej, zapewniających przewożenie materiałów zawierających informacje niejawne;
4) państwowego przedsiębiorstwa użyteczności publicznej „Poczta Polska" oraz innych podmiotów prowadzących działalność w zakresie usług pocztowych;
5) przedsiębiorców prowadzących działalność w zakresie ochrony osób i mienia.

§ 3. 1. Materiały zawierające informacje niejawne stanowiące tajemnicę państwową są przewożone przez przewoźników określonych w § 2 ust. 2 pkt 1-3.
2. W szczególnie uzasadnionych przypadkach decyzję o zamówieniu przewożenia materiałów stanowiących tajemnicę państwową przez przewoźników, o których mowa w § 2 ust. 2 pkt 4 i 5, podejmuje kierownik jednostki organizacyjnej.

§ 4. Materiały są przyjmowane przez przewoźników od nadawcy w postaci prawidłowo zapakowanych przesyłek listowych lub paczek, a w szczególności właściwie zaadresowanych, zabezpieczonych, opakowanych i oznaczonych, zwanych dalej „przesyłkami".

§ 5. 1. Materiały zawierające informacje niejawne stanowiące tajemnicę państwową, nadawane jako przesyłki listowe za pośrednictwem przewoźników, powinny być opakowane w dwie nieprzezroczyste i mocne koperty, przy czym na kopertach muszą być umieszczone:
1) na wewnętrznej:
a) klauzula tajności i ewentualne dodatkowe oznaczenie,
b) imienne określenie adresata,

c) imię, nazwisko i podpis osoby pakującej,
d) numer, pod którym dokument został zarejestrowany w dzienniku rejestracji dokumentów;
2) na zewnętrznej:
a) nazwa jednostki organizacyjnej adresata,
b) adres siedziby adresata,
c) numer wykazu i pozycji w wykazie przesyłek nadanych,
d) nazwa jednostki organizacyjnej nadawcy.

2. Miejsca sklejenia każdej koperty zabezpiecza się przez odciśnięcie pieczęci „do pakietów" i za pomocą przezroczystej taśmy samoprzylepnej, przy czym na kopercie zewnętrznej, zamiast tej taśmy, może być stosowana pieczęć odciśnięta w substancji zapewniającej jej trwały odcisk.
3. Materiały zawierające informacje niejawne stanowiące tajemnicę służbową nadawane są w postaci przesyłek listowych w dwóch nieprzezroczystych mocnych kopertach, oznaczonych tak jak w ust. 1, a w przypadku przewoźników, o których mowa w § 2 ust. 2 pkt 4, przekazuje się je jako przesyłki polecone lub z zadeklarowaną wartością.
4. Materiały zawierające informacje niejawne stanowiące tajemnicę państwową, nadawane w postaci paczek, przejęte przez przewoźnika do przemieszczenia i doręczenia, muszą być opakowane w dwie nieprzezroczyste warstwy mocnego papieru, oznaczone i zabezpieczone jak w ust. 1 i 2.
5. Materiały zawierające informacje niejawne stanowiące tajemnicę służbową, nadawane w postaci paczek, przekazuje się jako paczki z zadeklarowaną wartością opakowane w dwie warstwy nieprzezroczystego mocnego papieru, oznaczone i zabezpieczone jak w ust. 1.

§ 6. 1. Przesyłki przyjmowane przez przewoźników, o których mowa w § 2 ust. 2 pkt 1-3, nie powinny przekraczać następujących wymiarów i masy:
1) przesyłki listowe - wymiarów od 10 cm x 15 cm do 25 cm x 35 cm i masy do 0,5 kg;
2) paczki - wymiarów od 5 cm x 10 cm x 15 cm do 35 cm x 35 cm x 35 cm i masy do 5 kg.

2. Materiały, które przekraczają wymiary i masę określone w ust. 1, powinny być transportowane w zakrytych pojemnikach lub bezpiecznych opakowaniach, zaplombowanych albo zabezpieczonych w inny sposób uniemożliwiający identyfikację ich szczegółów, przy czym w czasie transportu powinny być one pod ciągłym dozorem uniemożliwiającym dostęp osób nieuprawnionych.

§ 7. 1. Przewoźnicy przyjmują przesyłki na podstawie wykazu przesyłek nadanych, sporządzonego przez nadawcę lub na podstawie dokumentów stosowanych przez operatora pocztowego.
2. Wykaz przesyłek nadanych sporządzany jest w dwóch egzemplarzach, po jednym egzemplarzu dla nadawcy przesyłki i przewoźnika.
3. Przyjęcie przesyłki potwierdza się podpisem, zapisem liczbowym i słownym ilości przyjętych przesyłek oraz odciskiem pieczęci przewoźnika na obu egzemplarzach wykazu przesyłek nadanych.
4. Przewoźnik nie przyjmuje przesyłki nieodpowiadającej wymaganiom określonym w § 6 ust. 1 lub może odmówić przyjęcia przesyłki nieodpowiadającej wymaganiom określonym w § 5.
5. W przypadku odmowy przyjęcia przesyłki, o której mowa w ust. 4, przewoźnik wykreśla ją na obu egzemplarzach wykazu przesyłek nadanych, potwierdzając to podpisem osoby odmawiającej przyjęcia przesyłki i odciskiem pieczęci przewoźnika.
6. W przypadku przekazania materiałów bez pośrednictwa przewoźników, o których mowa w § 2 ust. 2, adresat przesyłki potwierdza pisemnie nadawcy ich odbiór.

§ 8. Materiały zawierające informacje niejawne stanowiące tajemnicę państwową nie mogą być przewożone łącznie z przesyłkami zawierającymi przedmioty wartościowe, w szczególności z pieniędzmi, wyrobami z metalu lub kamieni szlachetnych albo mogącymi ulec uszkodzeniu w czasie transportu lub spowodować uszkodzenie pozostałych przesyłek, zwłaszcza z materiałami wybuchowymi, promieniotwórczymi, łatwo tłukącymi się, żrącymi, a także cuchnącymi.

§ 9. Przewóz przesyłek planuje się w taki sposób, aby dostarczane były w możliwie najkrótszym czasie do adresata.

§ 10. 1. Przesyłki przewozi się:

1) środkami publicznego transportu lądowego, pod warunkiem zarezerwowania pomieszczenia na potrzeby konwoju lub zarezerwowania miejsc w sposób gwarantujący ciągły dozór przesyłki;
2) specjalnie przystosowanymi pojazdami samochodowymi przewoźnika, które w przypadku przewożenia materiałów niejawnych stanowiących tajemnicę państwową muszą spełniać wymagania, o których mowa w załączniku nr 3 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 14 października 1998 r. w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne (Dz. U. Nr 129, poz. 858 oraz z 2000 r. Nr 17, poz. 221);
3) statkami powietrznymi, przy zapewnieniu wydzielonego miejsca ograniczającego dostęp osób nieuprawnionych do przesyłek lub wydzielenia miejsc gwarantujących ciągły dozór przesyłki przez konwojentów;
4) środkami transportu wodnego, przy zapewnieniu wydzielonego miejsca, ograniczającego dostęp osób nieuprawnionych do przesyłek i konwojentów.
2. Od warunków, o których mowa w ust. 1 pkt 2, można odstąpić wówczas, gdy przesyłka przekazywana jest bezpośrednio od nadawcy do odbiorcy własnymi środkami transportu nadawcy lub odbiorcy.

§ 11. 1. Przesyłki zawierające informacje niejawne stanowiące tajemnicę państwową przewożą i ochraniają konwoje złożone co najmniej z dwóch uzbrojonych w broń palną konwojentów posiadających odpowiednie poświadczenie bezpieczeństwa, przy zapewnieniu warunków, o których mowa w § 10.
2. Przesyłki zawierające informacje niejawne stanowiące tajemnicę służbową, oznaczone klauzulą „poufne", których utrata spowodowałaby szkodę dla interesu państwa, przewozi i ochrania co najmniej jeden uzbrojony w broń palną konwojent posiadający poświadczenie bezpieczeństwa.
3. Od warunku posiadania broni palnej można odstąpić w czasie przewozu przesyłek poza granicami lub za granicę Rzeczypospolitej Polskiej.
4. Konwojentów wyposaża się w środki łączności umożliwiające kontakt z nimi podczas przewozu oraz w instrukcję postępowania z ochranianymi i przewożonymi przesyłkami.
5. Odstępstwo od warunku posiadania broni palnej, o którym mowa w ust. 1, jest możliwe wówczas, gdy przesyłki przekazywane są bezpośrednio od nadawcy do odbiorcy na terenie tej samej miejscowości.

§ 12. 1. Przesyłki przewożone są w zamkniętych oraz zaplombowanych paczkach, workach lub innego rodzaju pojemnikach, zwanych dalej „pojemnikami".
2. Na każdym pojemniku umieszcza się informację zawierającą nazwę i adres nadawcy i odbiorcy oraz pouczenie o postępowaniu ze znalezionym pojemnikiem o następującej treści: „Znalazca niniejszego pojemnika proszony jest o niezwłoczne przekazanie go najbliższej jednostce Policji. Pojemnika nie rozplombowywać i nie otwierać".

§ 13. Trasa przewozu przesyłki zawierającej informacje niejawne może być uzgadniana z nadawcą.

§ 14. 1. W czasie przewożenia przesyłki niedopuszczalne jest pozostawienie jej bez nadzoru konwojentów, a w szczególności oddawanie do ogólnie dostępnych przechowalni bagażu lub magazynów.
2. Przesyłki czasowo składowane powinny być przechowywane w zamkniętych, chronionych miejscach, do których dostęp mogą mieć tylko osoby posiadające stosowne poświadczenie bezpieczeństwa.
3. Każdy przypadek składowania, o którym mowa w ust. 2, należy odnotować w wykazie przesyłek nadanych w rubryce „Uwagi".
4. Załadunek, przeładunek i wyładunek przesyłki musi odbywać się pod kontrolą konwojentów, przewoźnika lub pracowników nadawcy lub adresata przesyłki.

§ 15. Materiały zawierające informacje niejawne mogą być przekazywane także bez pośrednictwa przewoźników, o których mowa w § 2 ust. 2, po spełnieniu następujących warunków:

1) przewóz dokonywany jest przez nadawców lub odbiorców pod ochroną co najmniej dwóch uzbrojonych w broń palną konwojentów, jeżeli przewożą oni materiały stanowiące tajemnicę państwową, z zastrzeżeniem § 11 ust. 5;
2) przewozu dokonuje się za pomocą środków transportu drogowego, kolejowego, lotniczego lub wodnego, w których znajduje się zabezpieczone przed dostępem osób postronnych miejsce przystosowane i przeznaczone tylko do tego celu;
3) zabezpieczeniu przewożonych materiałów przed zniszczeniem oraz dostępem osób nieuprawnionych.

§ 16. 1. W przypadku uszkodzenia przesyłki przewoźnik zabezpiecza ją w celu niedopuszczenia do dalszych uszkodzeń oraz ujawnienia jej zawartości, sporządzając w tej sprawie protokół w trzech egzemplarzach, z których pierwszy wydaje się adresatowi, drugi wysyła do nadawcy, a trzeci pozostawia u przewoźnika.
2. Przesyłkę, o której mowa w ust. 1, wraz z protokołem sporządzonym w sprawie uszkodzenia przesyłki wydaje się adresatowi.
3. W przypadku odmowy przyjęcia przez adresata uszkodzonej przesyłki przewoźnik zwraca ją nadawcy wraz z protokołem, o którym mowa w ust. 1, i naniesioną na nim adnotacją o przyczynie odmowy przyjęcia przesyłki.
4. Zasady określone w ust. 1-3 stosuje się odpowiednio, w przypadkach gdy mogło dojść do ujawnienia lub doszło do ujawnienia treści przesyłki, wyjaśniając w protokole, komu jej treść mogła zostać ujawniona.
5. Wzór protokołu w sprawie uszkodzenia przesyłki określa załącznik nr 1 do rozporządzenia.

§ 17. 1. Przewoźnik wydaje przesyłki upoważnionemu przedstawicielowi adresata na podstawie wykazu przesyłek wydanych, sporządzonego przez przewoźnika.
2. Wzór wykazu przesyłek wydanych określa załącznik nr 2 do rozporządzenia.
3. Przedstawiciel adresata, przed odebraniem przesyłki, obowiązany jest przedstawić upoważnienie do jej odbioru.
4. Wzór upoważnienia do nadawania i odbioru przesyłek określa załącznik nr 3 do rozporządzenia.

§ 18. Przesyłkę nieodebraną w terminie trzech dni roboczych od daty zawiadomienia adresata o jej nadejściu odsyła się do nadawcy.

§ 19. 1. W przypadku nieotrzymania przez adresata od przewoźnika przesyłki ujętej w wykazie przesyłek nadanych, zawiadamia on niezwłocznie o tym nadawcę.
2. Nadawca występuje do przewoźnika z żądaniem podjęcia czynności wyjaśniających, których celem jest ustalenie osób odpowiedzialnych za utratę przesyłki, oraz okoliczności, w jakich to nastąpiło, informując o tym jednocześnie właściwą służbę ochrony państwa. Nie informuje się właściwej służby ochrony państwa, jeżeli doszło do utraty materiałów zawierających tajemnicę służbową, oznaczonych klauzulą „zastrzeżone".
3. Przewoźnik po dokonaniu ustaleń, o których mowa w ust. 2, udziela nadawcy odpowiedzi na piśmie, nie później niż w terminie 2 tygodni od otrzymania od nadawcy żądania, informując równocześnie właściwą służbę ochrony państwa.

§ 20. 1. Jeżeli zawarte umowy międzynarodowe nie stanowią inaczej, materiały zawierające informacje niejawne stanowiące tajemnicę państwową przekazywane są poza granice Rzeczypospolitej Polskiej za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 2 pkt 2.
2. Materiały niejawne stanowiące tajemnicę służbową mogą być przesyłane za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 2 pkt 4, z uwzględnieniem zasad zabezpieczenia i pakowania określonych w § 5 ust. 1-3 oraz ust. 5.

§ 21. 1. W przypadku gdy zachodzi konieczność pilnego wywozu za granicę materiałów w ramach wynikających z umów międzynarodowych rozmów, konferencji lub innych kontaktów i nie istnieje możliwość przekazania materiałów za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 2 pkt 2, kierownik jednostki delegującej może zezwolić na wywóz tych materiałów, jeżeli osoba wywożąca:

1) legitymuje się odpowiednim poświadczeniem bezpieczeństwa;
2) zapewnia stałą osobistą ochronę i bezpośrednią kontrolę w czasie podróży nad przewożonym materiałem;
3) ma zapewniony środek transportu umożliwiający bezpieczny przewóz materiałów do miejsca, w którym materiały będą wykorzystywane;
4) posiada środek łączności umożliwiający szybki kontakt z jednostką delegującą;
5) ma zapewnione miejsce gwarantujące bezpieczne przechowywanie tych materiałów.

2. Przed wydaniem zezwolenia, o którym mowa w ust. 1, kierownik jednostki delegującej, z wyjątkiem służb i organów, o których mowa w art. 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, jest obowiązany powiadomić o potrzebie wywozu materiałów stanowiących tajemnicę państwową właściwą służbę ochrony państwa. W przypadku konieczności zdeponowania tych materiałów informuje się Ministerstwo Spraw Zagranicznych lub właściwe polskie przedstawicielstwo dyplomatyczne.

3. Osobie wywożącej za granicę materiały stanowiące tajemnicę państwową wydaje się paszport dyplomatyczny oraz list kurierski.

4. Osoba wywożąca za granicę materiały musi być wyposażona w instrukcję określającą zasady postępowania z tymi materiałami, wydaną przez kierownika jednostki organizacyjnej.

5. Osoba, która po wykorzystaniu wywiezionych materiałów nie powraca z nimi bezpośrednio do kraju, jest obowiązana zdeponować je w kancelarii tajnej najbliższego polskiego przedstawicielstwa lub wskazanej przez Ministerstwo Spraw Zagranicznych placówce celem przesłania ich do kraju przy wykorzystaniu przewoźnika, o którym mowa w § 2 ust. 2 pkt 2.

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

[1)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów (Dz. U. Nr 18, poz. 168 oraz z 2005 r. Nr 39, poz. 375), utrzymanym w mocy na podstawie art. 10 ustawy z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 727), które utraciło moc z dniem wejścia w życie niniejszego rozporządzenia.

ZAŁĄCZNIKI

ZAŁĄCZNIK Nr 1

WZÓR

.....
(pieczęć nagłówkowa przewoźnika)

....., dnia ...-...-.....r.
(miejscowość)

Egz. nr .....

PROTOKÓŁ Nr .....
W SPRAWIE USZKODZENIA PRZESYŁKI

My niżej podpisani oświadczamy, że w dniu .....-.....-.....r.,

o godz. ....., przy rozpakowaniu pakietu, pojemnika* nr .....

nadanego przez ..... w .....

stwierdzono uszkodzenie ..... nr ..... adresowanego do .....
(określenie rodzaju przesyłki)

Uszkodzenie przesyłki nastąpiło w wyniku .....
(rodzaj i przyczyna uszkodzenia)

Wyżej wymieniona przesyłka została przepakowana i zabezpieczona celem niedopuszczenia do dalszych uszkodzeń i doręczona adresatowi wraz z egzemplarzem nr 1 niniejszego protokołu.
Uszkodzenie przesyłki wskazuje (nie wskazuje) na możliwość ujawnienia jej treści.

Podpis przewoźnika:

.....

.....

Przyczyny odmowy przyjęcia przesyłki przez adresata:

.....

.....
(imię i nazwisko)

Wyk. w 3 egz.
Egz. nr 1 - adresat przesyłki
Egz. nr 2 - nadawca
Egz. nr 3 - a/a

---

* Niepotrzebne skreślić.

ZAŁĄCZNIK Nr 2

WZÓR

..... (pieczęć nagłówkowa placówki przewoźnika)

....., dnia ...-...-.....r. (miejscowość)

WYKAZ Nr ...
PRZESYŁEK WYDANYCH

.....
(nazwa jednostki organizacyjnej odbierającej przesyłki)

.....
(nazwa przewoźnika)

Lp.	Numer i rodzaj przesyłki	Nadawca	Uwagi
1	2	3	4

Ogółem przesyłek .....
(liczbowo)

.....
(słownie)

.....
(podpis sporządzającego wykaz)

.....
(podpis wydającego przesyłki)

.....
(podpis przyjmującego przesyłki)

.....
(data przyjęcia)

.....
(pieczęć do pokwitowań adresata)

Pouczenie: Wykaz wypełnić maszynowo lub odręcznie w sposób czytelny. W kolumnie 2 wpisać literę symbolizującą rodzaj przesyłki: L - dla listu, P - dla paczki, I - inne.

ZAŁĄCZNIK Nr 3

WZÓR UPOWAŻNIENIA DO NADAWANIA I ODBIORU PRZESYŁEK

wzór

	..... Nr ..... **UPOWAŻNIENIE** **do nadawania i odbioru przesyłek**

Upoważniam Pana(ią) .... (imię i nazwisko) rodzaj i nr dowodu tożsamości .... wydanego przez .... do nadawania i odbioru przesyłek zawierających materiały niejawne w .... w ..... Upoważnienie ważne jest na rok ..... przy okazaniu dowodu tożsamości. pieczęć ..... (podpis wystawcy)	UWAGA Po wypełnieniu upoważnienie stanowi druk ścisłego zarachowania. W przypadku utraty upoważnienia kierownik jednostki organizacyjnej: 1) powiadamia natychmiast przewoźnika; 2) przeprowadza postępowanie wyjaśniające na okoliczność utraty upoważnienia. Ważność upoważnienia przedłuża się na rok: mp. mp. mp. mp. 20..... r. 20..... r. 20..... r. 20..... r.

Dz. U. 05.205.1696

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia 5 października 2005 r.

w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności

(Dz. U. z dnia 19 października 2005 r.)

Na podstawie art. 23 ust. 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) zarządza się, co następuje:

§ 1. 1. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzuli tajności.
2. Przyznaną klauzulę tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu.
3. Wprowadza się następujące oznaczenia klauzul tajności:
1) "00" - dla klauzuli „ściśle tajne";
2) "0" - dla klauzuli „tajne";
3) "Pf" - dla klauzuli „poufne";
4) "Z" - dla klauzuli „zastrzeżone".

§ 2. 1. Materiały zawierające informacje niejawne utrwalone na piśmie, dalej zwane „pismem", oznacza się w następujący sposób:
1) na pierwszej stronie pisma umieszcza się:
a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej,
b) w prawym górnym rogu, w kolejności pionowej:
– nazwę miejscowości i datę podpisania pisma,
– klauzulę tajności,
– numer egzemplarza pisma, a w przypadku gdy pismo sporządzono w jednym egzemplarzu napis „Egz. pojedynczy",
– napis o treści: „podlega ochronie do ...", jeżeli został określony krótszy niż wskazany w art. 25 ust. 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych okres ochrony informacji niejawnych stanowiących tajemnicę służbową,
c) w lewym dolnym rogu numer, pod jakim pismo zostało zarejestrowane w dzienniku ewidencji wykonanych dokumentów,
d) w prawym dolnym rogu klauzulę tajności oraz numer strony łamany przez liczbę stron całego pisma,
e) w przypadku pisma, któremu nadano bieg korespondencyjny dodatkowo:
– w lewym górnym rogu pod nazwą jednostki lub komórki organizacyjnej sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenia jednostki lub komórki organizacyjnej oraz numer, pod którym pismo zostało zarejestrowane w odpowiednim dzienniku, łamany przez rok lub dwie ostatnie cyfry roku, w którym pismo zostało sporządzone, poprzedzone cyframi: „00" - w przypadku pisma oznaczonego klauzulą „ściśle tajne", cyfrą „0" - w przypadku pisma oznaczonego klauzulą „tajne", literami „Pf" - w przypadku pisma oznaczonego klauzulą „poufne", literą „Z" - w przypadku pisma oznaczonego klauzulą „zastrzeżone", oddzielonymi od numeru rejestracyjnego myślnikiem, a także w zależności od potrzeb - inne oznaczenia ułatwiające ustalenie miejsca jego sporządzenia w jednostce lub komórce organizacyjnej nadawcy lub też przynależność pisma do określonej sprawy,

– w prawym górnym rogu pod numerem egzemplarza w kolejności pionowej: nazwę stanowiska adresata, imię i nazwisko oraz nazwę miejscowości, jednakże w przypadku wielu adresatów dopuszcza się umieszczenie jedynie adnotacji „adresaci według rozdzielnika”;

2) na kolejnych stronach pisma umieszcza się:

a) w prawym górnym rogu w kolejności pionowej:

– klauzulę tajności,

– numer egzemplarza pisma, a w przypadku sporządzenia go w jednym egzemplarzu napis „Egz. pojedynczy”,

b) w lewym dolnym rogu numer, pod jakim pismo zostało zarejestrowane w dzienniku ewidencji wykonanych dokumentów,

c) w prawym dolnym rogu klauzulę tajności, numer strony łamany przez liczbę stron całego pisma;

3) na ostatniej stronie pisma umieszcza się:

a) w prawym górnym rogu w kolejności pionowej:

– klauzulę tajności,

– numer egzemplarza pisma, a w przypadku sporządzenia go w jednym egzemplarzu napis „Egz. pojedynczy”,

b) z lewej strony pod treścią:

– liczbę załączników, jeżeli są dołączone do pisma,

– klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiednim dzienniku,

– liczbę stron każdego załącznika,

– w przypadku gdy adresatowi wysyła się inną liczbę załączników, niż pozostawia w aktach, dodatkowo napis „tylko adresat” - jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, oraz napis „do zwrotu” - jeżeli załączniki mają zostać zwrócone osobie podpisującej pismo,

c) z prawej strony pod treścią pisma i adnotacją o załącznikach w kolejności pionowej: stanowisko oraz imię i nazwisko osoby je podpisującej,

d) w lewym dolnym rogu w kolejności pionowej:

– liczbę wykonanych egzemplarzy,

– adresatów poszczególnych egzemplarzy pisma lub adnotację „Adresaci według rozdzielnika”,

– nazwisko lub inne dane identyfikujące sporządzającego i wykonawcę,

– numer, pod jakim pismo zostało zarejestrowane w dzienniku ewidencji wykonanych dokumentów,

e) w prawym dolnym rogu klauzulę tajności oraz numer strony łamany przez liczbę stron całego pisma.

2. W przypadku pisma, któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można zamieścić dyspozycję dla adresata o treści:

1) ”udzielanie informacji tylko za pisemną zgodą nadawcy”;

2) ”kopiowanie tylko za pisemną zgodą nadawcy”;

3) ”odpis tylko za pisemną zgodą nadawcy”;

4) ”kopiowanie stron ... tylko za pisemną zgodą nadawcy”;

5) ”odpis od ... do ... tylko za pisemną zgodą nadawcy”;

6) ”wypis (wyciąg) od ... do ... tylko za pisemną zgodą nadawcy”.

§ 3. 1. Na pismach stanowiących załączniki, na pierwszej stronie w prawym górnym rogu umieszcza się dodatkowo napis: „Załącznik nr ... do pisma nr ... z dnia ...”.

2. Napis, o którym mowa w ust. 1, zamieszcza się - w miarę możliwości - na innych niż pismo materiałach.

3. Jeżeli przy piśmie przewodnim przesyła się załączniki oznaczone różnymi klauzulami tajności, to:

1) klauzula pisma przewodniego lub dokumentu uwzględnia klauzulę załącznika o najwyższym stopniu tajności;

2) na piśmie przewodnim zamieszcza się dyspozycję co do klauzuli tajności pisma po trwałym odłączeniu załączników; na każdej stronie pod numerem egzemplarza zamieszcza się napis: „... (nazwa klauzuli tajności) po odłączeniu załączników” lub „jawne po odłączeniu załączników”.

4. Na piśmie przewodnim, o którym mowa w ust. 3, jeżeli jego treść jest jawna, nie umieszcza się numeru według dziennika ewidencji wykonanych dokumentów, a przy jego rejestracji, w rubryce „Informacje uzupełniające/Uwagi" dziennika korespondencyjnego, należy wpisać adnotację „pismo przewodnie jawne".

§ 4. 1. Na materiałach innych niż pismo, klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, bezpośrednio, a jeżeli to nie jest możliwe - na ich obudowie lub opakowaniu.
2. Utrwalanie informacji niejawnych w formie dźwięku lub obrazu powinno być poprzedzone i kończyć się informacją o nadanej klauzuli tajności, o ile istnieją takie możliwości techniczne.

§ 5. Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach klauzule tajności umieszcza się po prawej stronie na górze i dole zewnętrznych ścianek okładki oraz - jeżeli jest - na stronie tytułowej.

§ 6. 1. Na pismach zawierających informacje niejawne, wobec których zniesiono przyznaną klauzulę tajności lub minął ustawowy okres ochrony lub ustanowiony przez osobę, o której mowa w art. 21 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych:
1) skreśla się klauzulę tajności na każdej stronie w prawym górnym i dolnym rogu;
2) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się dodatkowo napis „Jawne" oraz datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.
2. Na pismach zawierających informacje niejawne, wobec których zmieniono przyznaną klauzulę tajności:
1) na każdej stronie w prawym górnym i dolnym rogu skreśla się dotychczasowe klauzule tajności;
2) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności;
3) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.
3. Na pismach zawierających informacje niejawne, których okres ochrony uległ skróceniu lub przedłużeniu, na pierwszej stronie w prawym górnym rogu nad klauzulą tajności umieszcza się odpowiednio napis: „Skrócono okres ochrony do dnia ..." albo „Przedłużono okres ochrony do dnia ...", a także datę, imię i nazwisko oraz podpis osoby dokonującej tych adnotacji.
4. Skreśleń i adnotacji, o których mowa w ust. 1-3, dokonuje odpowiednio kierownik kancelarii lub kierownik archiwum lub inne upoważnione osoby.
5. Skreślenia klauzul tajności oraz adnotacji, o których mowa w ust. 1 i 2, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.
6. W stosunku do pism znajdujących się w zbiorach dokumentów zawierających informacje niejawne, wobec których minął ustanowiony okres ochrony, czynności, o których mowa w ust. 1-5, można dokonać najpóźniej w przypadku ich udostępniania lub przekazywania osobom spoza jednostki lub komórki organizacyjnej.
7. W stosunku do materiałów, o których mowa w § 4 i 5, przepisy ust. 1-5 stosuje się odpowiednio, uwzględniając sposób oznakowania tych materiałów.

§ 7. 1. Na kopiach, odpisach, wypisach, wyciągach lub tłumaczeniach pism umieszcza się:
1) na wszystkich stronach w prawym górnym rogu odpowiednio napis: „Kopia", „Odpis", „Wypis", „Wyciąg" lub „Tłumaczenie z języka - (nazwa języka) - (imię i nazwisko tłumacza)";
2) na pierwszej stronie dodatkowo numer, pod jakim zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów, numer egzemplarza wykonanej kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
3) na ostatniej stronie dodatkowo napis „Za zgodność" i odcisk tuszowej pieczęci urzędowej z nazwą jednostki lub komórki organizacyjnej (numerem jednostki wojskowej), w której sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie.

2. Zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza podpisem kierownik jednostki lub komórki organizacyjnej albo inna osoba przez niego upoważniona, a tłumaczenia - osoba dokonująca tłumaczenia.
3. Fakt sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia odnotowuje się na dokumencie, z którego sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie, przez odcisk pieczęci lub umieszczenie adnotacji informującej o:
1) nazwie jednostki lub komórki organizacyjnej, w której sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie;
2) liczbie egzemplarzy sporządzonych kopii, odpisów, wypisów, wyciągów lub tłumaczeń;
3) dacie sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
4) numerze, pod jakim kopia, odpis, wypis, wyciąg lub tłumaczenie zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów.
4. Adnotacje, o których mowa w ust. 3 pkt 1-3, wpisuje się przed wykonaniem kopii, odpisu, wypisu, wyciągu lub tłumaczenia, natomiast numer, pod jakim zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów, nanosi się po wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia.
5. W przypadku wykonywania kopii, odpisu, wypisu, wyciągu lub tłumaczenia materiałów archiwalnych zgromadzonych w archiwach państwowych oraz archiwach państwowych wyodrębnionych, nie dokonuje się czynności, o których mowa w ust. 3, z tym że do materiałów dołącza się kartę informacyjną, na której każdorazowo umieszcza się informację o wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia. Napis na karcie powinien zawierać adnotacje, o których mowa w ust. 3.

§ 8. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Dz. U. 05.208.1741

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia 18 października 2005 r.

w sprawie organizacji i funkcjonowania kancelarii tajnych

(Dz. U. z dnia 25 października 2005 r.)

Na podstawie art. 53 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa:
1) strukturę organizacyjną kancelarii tajnych;
2) podstawowe zadania kierownika kancelarii;
3) zakres i warunki stosowania środków ochrony fizycznej, z uwzględnieniem klauzul tajności przechowywanych przez kancelarię dokumentów;
4) tryb obiegu informacji niejawnych;
5) wzór karty zapoznania się z dokumentem.

2. Postanowień, o których mowa w ust. 1 pkt 1-4, nie stosuje się w jednostkach organizacyjnych organów wymienionych w art. 53 ust. 2 i 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

§ 2. 1. Kancelarię tajną, zwaną dalej „kancelarią", tworzy kierownik jednostki organizacyjnej.
2. Kancelaria, ze względów organizacyjnych, może mieć swoje oddziały tworzone i funkcjonujące zgodnie z zasadami i na warunkach przewidzianych dla kancelarii.
3. Kancelarią kieruje kierownik kancelarii, wyznaczany przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony.
4. Oddziałem kancelarii kieruje wyznaczony przez pełnomocnika ochrony pracownik pionu ochrony.

§ 3. 1. Do podstawowych zadań kierownika kancelarii należy:
1) bezpośredni nadzór nad obiegiem dokumentów;
2) udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym;
3) egzekwowanie zwrotu dokumentów;
4) kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii oraz jednostce organizacyjnej;
5) prowadzenie bieżącej kontroli postępowania z dokumentami;
6) wykonywanie poleceń pełnomocnika ochrony;
7) nadzór nad pracą oddziałów kancelarii.

2. Pracownik pionu ochrony, o którym mowa w § 2 ust. 4, wykonuje obowiązki kierownika kancelarii określone w ust. 1 pkt 1-6.

§ 4. 1. W przypadku zmiany na stanowisku kierownika kancelarii sporządza się protokół zdawczo-odbiorczy.
2. Protokół, o którym mowa w ust. 1, sporządza się w obecności kierownika zdającego obowiązki, osoby przejmującej obowiązki kierownika oraz pełnomocnika ochrony. Protokół sporządza się w

dwóch egzemplarzach; pierwszy egzemplarz przechowywany jest w kancelarii, drugi - u pełnomocnika ochrony.
3. W przypadku czasowej nieobecności kierownika kancelarii jego obowiązki przejmuje upoważniony pracownik kancelarii lub inny pracownik pionu ochrony. W razie ich braku kancelarię przejmuje protokolarnie inny pracownik wyznaczony przez kierownika jednostki na wniosek pełnomocnika ochrony.

§ 5. 1. Kancelaria powinna spełniać następujące wymagania:
1) być zlokalizowana w strefie bezpieczeństwa;
2) ściany i stropy pomieszczeń kancelarii powinny być wykonane z materiałów niepalnych, spełniających wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej o grubości 250 mm;
3) drzwi do kancelarii wyposażone w zamek drzwiowy wielopunktowy powinny spełniać co najmniej wymagania, o których mowa w Polskiej Normie PN-90/B-92270; w przypadku gdy w kancelarii będą przechowywane dokumenty lub materiały zawierające informacje niejawne stanowiące tajemnicę państwową, drzwi należy wyposażyć w zamek drzwiowy dodatkowy, o którym mowa w Polskiej Normie PN-90/B-92270;
4) okna kancelarii w pomieszczeniach o architekturze umożliwiającej dostęp do nich, w szczególności gdy dolna krawędź okna znajduje się na wysokości poniżej 5 m od poziomu otaczającego terenu lub górna krawędź 3 m od poziomu dachu - powinny być zabezpieczone stalowymi kratami zewnętrznymi lub wewnętrznymi z prętów o przekroju co najmniej 16 mm, o oczkach nie większych niż 150 mm na 150 mm; dopuszcza się inne zabezpieczenia posiadające odporność na włamanie nie mniejszą niż krata;
5) okna powinny być zabezpieczone przed obserwacją z zewnątrz.
2. Kraty, o których mowa w ust. 1 pkt 4, mogą być rozsuwane lub otwierane pod warunkiem ich zabezpieczenia co najmniej jedną kłódką klasy 5 według Polskiej Normy PN-EN-12320.
3. W przypadku innego usytuowania okien niż określone w ust. 1 pkt 4, okna zabezpiecza się siatką wykonaną z drutu stalowego lub innego materiału o podobnych właściwościach, o grubości nie mniejszej niż 2 mm, o oczkach nie większych niż 20 mm na 20 mm lub innym zabezpieczeniem posiadającym odporność na włamanie nie mniejszą niż siatka.
4. W pomieszczeniach kancelarii, w których są przechowywane dokumenty oznaczone klauzulą „ściśle tajne" lub „tajne", powinny być ponadto zainstalowane co najmniej:
1) system sygnalizacji pożarowej;
2) system sygnalizacji włamania i napadu;
3) systemy nadzoru wizyjnego wraz z rejestracją obrazu, wyłącznie do obserwacji wejścia do pomieszczeń kancelarii - w przypadku przechowywania w kancelarii dokumentów oznaczonych klauzulą „ściśle tajne".
5. Instalowane systemy i urządzenia alarmowe powinny odpowiadać co najmniej klasie SA 3 według Polskiej Normy PN-93 E-08390/14.

§ 6. 1. W pomieszczeniach kancelarii można wydzielić miejsce, w którym osoby upoważnione mogą zapoznawać się z dokumentami - czytelnię.
2. Czytelnia powinna być zorganizowana w sposób umożliwiający stały nadzór ze strony pracowników kancelarii.
3. W czytelni zabrania się instalowania systemu nadzoru wizyjnego.

§ 7. 1. W zależności od nadanej klauzuli tajności, dokumenty lub materiały przechowywane są:
1) „poufne" - w szafach stalowych klasy A;
2) „tajne" - w szafach stalowych klasy B;
3) „ściśle tajne" - w szafach stalowych klasy C.
2. Dokumenty lub materiały mogą być przechowywane poza szafami stalowymi w znajdujących się wewnątrz kancelarii pomieszczeniach spełniających następujące wymagania, w zależności od nadanej tym dokumentom i materiałom klauzuli tajności:
1) „poufne" - odpowiadające co najmniej klasie 0 odporności na włamanie według Polskiej Normy PN-EN 1143-1;

2) „tajne" - odpowiadające co najmniej klasie I odporności na włamanie według Polskiej Normy PN-EN 1143-1;
3) „ściśle tajne" - odpowiadające co najmniej klasie I odporności na włamanie według Polskiej Normy PN-EN 1143-1.
3. Drzwi do pomieszczeń, o których mowa w ust. 2, zabezpiecza się dodatkowo odpowiednim zamkiem szyfrowym.
4. Klasyfikację i wymagania techniczne urządzeń do ochrony dokumentów i materiałów, o których mowa w ust. 1-3, określa załącznik nr 1 do rozporządzenia.

§ 8. 1. Dokumenty i materiały oznaczone różnymi klauzulami tajności są przechowywane w odrębnych szafach lub pomieszczeniach, chyba że wchodzą one w skład zbioru dokumentów.
2. Dokumenty i materiały, o których mowa w ust. 1, mogą być przechowywane w jednej szafie lub pomieszczeniu pod warunkiem ich fizycznego oddzielenia w sposób umożliwiający osobne zamknięcie. W takim przypadku szafa lub pomieszczenie musi spełniać wymagania określone w § 7, odpowiednie dla najwyższej klauzuli tajności przechowywanych w nich dokumentów lub materiałów.
3. Kierownik jednostki organizacyjnej lub inna upoważniona przez niego osoba mogą wyrazić pisemną zgodę na przechowywanie dokumentów poza pomieszczeniami kancelarii, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do ich klauzul tajności, na czas niezbędny do realizacji zadań związanych z dostępem do tych dokumentów.

§ 9. 1. Po zakończeniu pracy kierownik kancelarii lub upoważniony pracownik kancelarii jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń kancelarii.
2. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf kancelarii, a także zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych, określa plan ochrony informacji niejawnych.
3. Wszelkie nieprawidłowości związane z naruszeniem zasad, o których mowa w ust. 2, należy niezwłocznie zgłaszać pełnomocnikowi ochrony.
4. Zasady określone w ust. 1-3 obowiązują odpowiednio w stosunku do innych pomieszczeń, w których są przechowywane dokumenty lub materiały, oraz osób za te pomieszczenia odpowiedzialnych.

§ 10. 1. W kancelarii przyjmuje się, rejestruje, przechowuje, przekazuje i wysyła dokumenty oraz prowadzi:
1) rejestr dzienników, książek ewidencyjnych i teczek, którego wzór określa załącznik nr 2 do rozporządzenia;
2) dziennik korespondencyjny, którego wzór określa załącznik nr 3 do rozporządzenia;
3) dziennik ewidencji wykonanych dokumentów, oznaczonych klauzulą „ściśle tajne", „tajne" i „poufne", którego wzór określa załącznik nr 4 do rozporządzenia;
4) karty zapoznania się z dokumentem zawierającym tajemnicę państwową, którego wzór określa załącznik nr 5 do rozporządzenia;
5) książkę doręczeń przesyłek miejscowych, której wzór określa załącznik nr 6 do rozporządzenia;
6) wykaz przesyłek nadanych, którego wzór określa załącznik nr 7 do rozporządzenia.
2. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych kancelaria może prowadzić także inne rejestry niż wymienione w ust. 1, w tym odrębne rejestry dla dokumentów oznaczonych różnymi klauzulami tajności.
3. Za zgodą kierownika jednostki organizacyjnej, w porozumieniu z pełnomocnikiem ochrony, w kancelarii mogą być przyjmowane, rejestrowane, przechowywane i wysyłane dokumenty i materiały oznaczone klauzulą „zastrzeżone".

§ 11. 1. Kierownik lub pracownik kancelarii przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.
2. Przyjmując przesyłkę, sprawdza się:
1) prawidłowość adresu;
2) całość pieczęci i opakowania;
3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy;

4) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie lub w książce doręczeń.
3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania kierownik albo pracownik kancelarii kwitujący odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik - kolejny egzemplarz protokołu przekazuje się także jemu.
4. Po otwarciu przesyłki kierownik lub pracownik kancelarii:
1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
2) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.
5. W przypadku stwierdzenia nieprawidłowości w wyniku czynności, o których mowa w ust. 4, kierownik kancelarii lub pracownik kancelarii sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.
6. Kierownik lub pracownik kancelarii odnotowuje fakt sporządzenia protokołu, o którym mowa w ust. 3 i 5, w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi".

§ 12. 1. Kierownik lub pracownik kancelarii rejestruje przyjęte dokumenty w odpowiednim dzienniku lub rejestrze.
2. Dla każdego dokumentu zawierającego tajemnicę państwową, z chwilą zarejestrowania, zakłada się kartę zapoznania się z dokumentem, którą dołącza się do dokumentu. Podobną kartę można załączyć do dokumentu zawierającego informacje oznaczone klauzulą „poufne".
3. Do zbioru dokumentów załącza się jedną kartę zapoznania się z dokumentem.
4. Zarejestrowane dokumenty kierownik lub pracownik kancelarii przekazuje albo udostępnia adresatowi lub upoważnionej osobie za pokwitowaniem.

§ 13. 1. W kancelarii nie otwiera się przesyłek oznaczonych „do rąk własnych". W odpowiednim dzienniku lub rejestrze wpisuje się nadawcę, numer i datę wpływu dokumentu; w rubryce „Informacje uzupełniające/Uwagi" odnotowuje się, że przesyłka była oznaczona „do rąk własnych".
2. Na opakowaniu przesyłek, o których mowa w ust. 1, wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się - za pokwitowaniem - bezpośrednio adresatowi, a w razie jego nieobecności - osobie przez niego upoważnionej do odbioru.
3. Zatrzymanie przez adresata dokumentu, adresowanego „do rąk własnych", odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".
4. Czynności, o których mowa w § 11 ust. 4, w stosunku do przesyłek, o których mowa w ust. 1, dokonuje adresat przesyłki.
5. W przypadku zwrotu do kancelarii przesyłki, o której mowa w ust. 1, kierownik lub pracownik kancelarii uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.
6. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych" w kancelarii w stanie zamkniętym, kierownik lub pracownik kancelarii dokonuje czynności, o których mowa w ust. 5, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

§ 14. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu odbioru tych przesyłek odnotowuje się godzinę doręczenia.

§ 15. 1. Otrzymaną i wysyłaną przesyłkę bądź wytworzony dokument rejestruje się odpowiednio w kolejności wytworzenia lub otrzymania.
2. Adnotacji, o których mowa w ust. 1, dokonuje się atramentem lub tuszem. Zmian dokonuje się kolorem czerwonym, umieszczając datę i czytelny podpis dokonującego zmiany.
3. Zabrania się wycierania i zamazywania adnotacji, o których mowa w ust. 1.

§ 16. 1. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w kancelarii nie dłużej niż 2 lata. Po upływie tego okresu przekazuje się je do

archiwum zakładowego lub składnicy akt, spełniających wymogi bezpieczeństwa odpowiednie dla ich klauzuli tajności, jeżeli jednostka organizacyjna takim dysponuje.
2. Jeżeli w jednostce organizacyjnej nie ma odpowiedniego archiwum zakładowego lub składnicy akt, dokumenty, materiały i zbiory tych dokumentów są przechowywane w kancelarii lub innym pomieszczeniu zapewniającym ich ochronę odpowiednio do przyznanej im klauzuli tajności.

§ 17. 1. Pomieszczenia kancelarii, utworzone przed wejściem w życie niniejszego rozporządzenia, należy dostosować do określonych w nim wymagań w terminie 3 lat od dnia jego wejścia w życie.
2. Dzienniki, księgi, wykazy i rejestry, o których mowa w § 8 rozporządzenia Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych (Dz. U. Nr 18, poz. 156 oraz z 2003 r. Nr 17, poz. 156), stosuje się do dnia 31 grudnia 2005 r.

§ 18. Traci moc rozporządzenie Rady Ministrów z dnia 9 lutego 1999 r. w sprawie organizacji kancelarii tajnych (Dz. U. Nr 18, poz. 156 oraz z 2003 r. Nr 17, poz. 156).

§ 19. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

ZAŁĄCZNIKI

ZAŁĄCZNIK Nr 1

KLASYFIKACJA I WYMAGANIA TECHNICZNE URZĄDZEŃ DO OCHRONY DOKUMENTÓW I MATERIAŁÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

I. SZAFA STALOWA KLASY A

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 1 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe wyposażone w mechanizm dźwigniowy, blokujący je co najmniej na trzech krawędziach.
4. Szafa musi być wyposażona w zamek mechaniczny kluczowy wielozastawkowy z możliwością wyjęcia klucza tylko w pozycji zamkniętej, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem.
5. Podstawa szafy musi posiadać te same rozmiary co wierzch. W podstawie powinien znajdować się zaślepiony otwór umożliwiający zakotwiczenie jej do podłoża. Konstrukcja dna szafy musi wytrzymać siły minimum 50 kN.
6. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą, potwierdzający zgodność wyrobu z wymaganiami klasy A.
7. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:

a) nazwę wyrobu,
b) nazwę i kod identyfikacyjny producenta, typ i numer modelu,
c) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu,
d) masę.

II. SZAFA STALOWA KLASY B

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 3 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe wyposażone w mechanizm dźwigniowy, blokujący je co najmniej na czterech krawędziach.
4. Mechanizm dźwigniowy rygli w drzwiach musi być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglujący, w tym:

a) zamek mechaniczny kluczowy wielozastawkowy z możliwością wyjęcia klucza tylko w pozycji zamkniętej, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem,
b) zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skali nastawień nie większej niż półtorej działki i posiadający minimum 100 podziałek na pokrętle (minimum 1.000.000 kombinacji). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Z szafą powinny być dostarczone dwa komplety kluczy do zmiany kodu. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, pod warunkiem spełnienia przez niego takich samych wymagań odporności na włamanie co zamek mechaniczny szyfrowy.

5. Podstawa szafy musi posiadać te same rozmiary co wierzch. W podstawie powinien znajdować się zaślepiony otwór umożliwiający zakotwiczenie jej do podłoża. Konstrukcja dna szafy powinna wytrzymać siły minimum 50 kN.
6. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą, potwierdzający zgodność wyrobu z wymaganiami klasy B.
7. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:

a) nazwę wyrobu,
b) nazwę i kod identyfikacyjny producenta, typ i numer modelu,
c) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu,
d) masę.

III. SZAFA STALOWA KLASY C

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane ze stali konstrukcyjnej wyższej jakości, o grubości minimum 5 mm, a w przypadku konstrukcji wielopłaszczowej grubość płaszcza zewnętrznego powinna wynosić minimum 3 mm. Połączenia korpusu szafy powinny zapewnić dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe wyposażone w mechanizm dźwigniowy, blokujący je co najmniej na czterech krawędziach.
4. Mechanizm dźwigniowy rygli w drzwiach powinien być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglujący, w tym:
a) zamek mechaniczny kluczowy wielozastawkowy z możliwością wyjęcia klucza tylko w pozycji zamkniętej, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem,
b) zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skoku nastawień nie większym niż jedna działka i posiadający minimum 100 podziałek na pokrętle (minimum 1.000.000 kombinacji). Czas otwarcia zamka przez osobę nieuprawnioną drogą wybierania kolejnych kombinacji powinien wynosić nie mniej niż 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem radiologicznym (promieniowanie co najmniej 10 curie, Co-60 z odległości 760 mm). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy do ustawiania szyfru. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, pod warunkiem spełnienia przez niego takich samych wymagań odporności na włamanie co zamek mechaniczny szyfrowy.
5. Podstawa szafy musi posiadać te same rozmiary co wierzch. W podstawie powinien znajdować się zaślepiony otwór umożliwiający zakotwiczenie jej do podłoża. Konstrukcja dna szafy powinna wytrzymać siły minimum 50 kN.
6. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą, potwierdzający zgodność wyrobu z wymaganiami klasy C.
7. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:
a) nazwę wyrobu,
b) nazwę i kod identyfikacyjny producenta, typ i numer modelu,
c) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu,
d) masę.

IV. DODATKOWY ZAMEK DO DRZWI POMIESZCZEŃ, W KTÓRYCH PRZECHOWYWANE SĄ DOKUMENTY I MATERIAŁY ZAWIERAJĄCE INFORMACJE NIEJAWNE:

1. Stanowiące tajemnicę służbową o klauzuli „poufne" - zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skali nastawień nie większej niż półtorej działki i posiadający minimum 100 podziałek na pokrętle (minimum 1.000.000 kombinacji). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, pod warunkiem spełnienia przez niego takich samych wymagań odporności na włamanie co zamek mechaniczny szyfrowy.
2. Stanowiące tajemnicę państwową - zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skoku nastawień nie większym niż jedna działka i posiadający minimum 100 podziałek na pokrętle (minimum 1.000.000 kombinacji). Czas otwarcia zamka przez osobę nieuprawnioną drogą wybierania kolejnych kombinacji powinien wynosić

nie mniej niż 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem radiologicznym (promieniowanie co najmniej 10 curie, Co-60 z odległości 760 mm). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, pod warunkiem spełnienia przez niego takich samych wymagań odporności na włamanie co zamek mechaniczny szyfrowy.

ZAŁĄCZNIK Nr 2

WZÓR

REJESTR DZIENNIKÓW, KSIĄŻEK EWIDENCYJNYCH I TECZEK

Oznaczenie klauzuli tajności dziennika, rejestru, książki ewidencyjnej itp.	Numer kolejny dziennika, rejestru, książki ewidencyjnej itp.	Adnotacje dot. przedłużenia okresu ochrony, zniesienia bądź zmiany klauzuli tajności	Data rejestracji dziennika, rejestru, książki ewidencyjnej itp.	Nazwa teczki, dziennika, rejestru, książki ewidencyjnej itp.	Data		Liczba stron dziennika, rejestru, książki ewidencyjnej itp.	Komórka organizacyjna, odpowiedzialna za prowadzenie dziennika, rejestru, książki ewidencyjnej itp.	Pokwitowanie odbioru dziennika, rejestru, książki ewidencyjnej itp.			Informacje uzupełniające / Uwagi
					rozpoczęcia dziennika, rejestru, książki ewidencyjnej itp.	zakończenia dziennika, rejestru, książki ewidencyjnej itp.			imię i nazwisko	data oraz podpis osoby prowadzącej dziennik, rejestr, książkę ewidencyjną itp.	potwierdzenie zwrotu data i podpis	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**

(klauzula tajności) ...../.....

ZAŁĄCZNIK Nr 3

WZÓR

DZIENNIK KORESPONDENCYJNY

strona lewa

Oznaczenie klauzuli tajności	Numer kolejny zapisu	Adnotacje dot. przedłużenia okresu ochrony, zniesienia bądź zmiany klauzuli tajności	Data rejestracji dokumentu	Rodzaj dokumentu W- wychodzący P- przychodzący	Nazwa nadawcy/ adresata	Numer i data dokumentu otrzymanego	Nazwa dokumentu lub czego dotyczy	Liczba		
								stron dokumentu z załącznikami lub innych jednostek miary	załączników	stron załączników lub innych jednostek miary
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**

strona prawa

Nr pozycji z dziennika ewidencji wykonanych dokumentów	Imię i nazwisko osoby otrzymującej dokument, data i podpis	Potwierdzenie zwrotu dokumentu do kancelarii, data i podpis	Adnotacje o wysłaniu dokumentu lub załącznika (poz. ks. dor. przesyłek miejscowych/poz. wykazu przesyłek nadanych)	Informacje uzupełniające / Uwagi
12	**13**	**14**	**15**	**16**

...../.....

ZAŁĄCZNIK Nr 4

WZÓR

DZIENNIK EWIDENCJI WYKONANYCH DOKUMENTÓW

strona lewa

Oznaczenie klauzuli tajności	Numer kolejny zapisu	Data oddania brudnopisu do przepisania, dokumentu do reprodukcji	Adresat lub nazwa dokumentu	Nazwisko osoby oddającej brudnopis do przepisania, dokument do reprodukcji	Numer dokumentu kopiowanego	Nazwisko wykonującego
1	**2**	**3**	**4**	**5**	**6**	**7**

strona prawa

Liczba wykonanych		Pokwitowanie odbioru			Adnotacje		
egzemplarzy	stron jednego egzemplarza	imię i nazwisko	data	podpis	o wysłaniu (nr z dz. koresp./poz. ks. dor. przesyłek miejscowych)	o brakowaniu (nr protokołu)	Uwagi
8	**9**	**10**	**11**	**12**	**13**	**14**	**15**

WZÓR

KARTA ZAPOZNANIA SIĘ Z DOKUMENTEM OZNACZONYM KLAUZULĄ „ŚCIŚLE TAJNE"* / „TAJNE" *

nr .....

	UDOSTĘPNIENIE DOKUMENTU			ZWROT DOKUMENTU			
Lp.	imię i nazwisko osoby, której dokument udostępniono	data	Podpis	imię i nazwisko osoby, której dokument zwrócono	data	podpis	Uwagi

ZAŁĄCZNIK Nr 6

WZÓR

KSIĄŻKA DORĘCZEŃ PRZESYŁEK MIEJSCOWYCH

Numer kolejny zapisu	Data	Adresat	Numer pisma (rodzaj przesyłki)	Potwierdzenie odbioru
				podpis, pieczęć i data
1	2	3	4	5

strona ..... / .....

WZÓR

...., dnia ...-...-... r.
(pieczęć nagłówkowa jednostki organizacyjnej) (miejscowość)

WYKAZ Nr .....
PRZESYŁEK NADANYCH

przekazanych przez .....
(nazwa i adres jednostki organizacyjnej wysyłającego)

do wysłania ..... w .....
(nazwa przewoźnika lub nazwisko doręczyciela)

Lp.	Numer przesyłki	Rodzaj przesyłki (list, paczka itp.)	Do kogo adresowany	Uwagi
1	2	3	4	5

Ogółem przesyłek: ....
(liczbowo) (słownie)

.....
(podpis sporządzającego wykaz)
.....
(podpis doręczającego)
.....
(podpis przyjmującego)
.....
(data i godzina przyjęcia)

mp.

(pieczęć przewoźnika)

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 13 września 2002 r.

w sprawie przechowywania i rejestrowania dokumentacji postępowań dyscyplinarnych oraz prowadzenia ewidencji ukarań żołnierzy

Na podstawie art. 107 ustawy z dnia 4 września 1997 r. o dyscyplinie wojskowej (Dz.U. z 2002 r. Nr 42, poz. 370) zarządza się, co następuje:

§ 1. Rozporządzenie określa:
1) sposób i czas przechowywania dokumentacji postępowania dyscyplinarnego;
2) sposób rejestrowania postępowania dyscyplinarnego w komórce organizacyjnej Ministerstwa Obrony Narodowej, jednostce organizacyjnej podporządkowanej Ministrowi Obrony Narodowej lub przez niego nadzorowanej oraz przedsiębiorstwie państwowym, dla którego jest on organem założycielskim, zwanych dalej „jednostkami organizacyjnymi";
3) sposób prowadzenia ewidencji ukarań żołnierza.

§ 2.1. W toku postępowania dyscyplinarnego dokumentację dyscyplinarną przechowuje przełożony dyscyplinarny, z zastrzeżeniem ust. 2.
2. Rzecznik dyscyplinarny przechowuje dokumenty sporządzane:
1) w postępowaniu wyjaśniającym, jeżeli jest prowadzone, do czasu jego zakończenia;
2) w postępowaniu odwoławczym, jeżeli wyższy przełożony dyscyplinarny polecił uzupełnienie materiału dowodowego i przekazanie mu w wyznaczonym terminie.
3. Osoby, o których mowa w ust. 1i 2, przechowują dokumentację w kancelarii tajnej jednostki organizacyjnej lub w swoim pomieszczeniu służbowym, z uwzględnieniem wymogów ochrony danych zebranych w postępowaniu dyscyplinarnym przed ich nieuprawnionym ujawnieniem.

§ 3.1. Po zakończeniu postępowania dyscyplinarnego, w kancelarii tajnej jednostki organizacyjnej, w której wydane zostało orzeczenie w pierwszej instancji, a jeżeli organem orzekającym był sąd wojskowy, to w kancelarii tajnej jednostki organizacyjnej, w której postępowanie dyscyplinarne zostało wszczęte:
1) rejestruje się postępowanie dyscyplinarne w rejestrze postępowań dyscyplinarnych, zwanym dalej „rejestrem";
2) przechowuje się dokumentację przez kres jednego roku od dnia uprawomocnienia się orzeczenia.
2. Wzór rejestru określa załącznik nr 1 do rozporządzenia.
3. Dokumentacji nadaje się numer odpowiadający pozycji, pod którą postępowanie dyscyplinarne zostało zarejestrowane w rejestrze, wpisując po numerze liczbę oznaczającą bieżący rok kalendarzowy, poprzedzoną ukośną kreską.

§ 4.1. Po okresie, o którym mowa w § 3 ust. 1 pkt 2, do archiwum wojskowego przekazuje się dokumentację postępowania dyscyplinarnego:
1) prowadzonego w stosunku do żołnierza zasadniczej służby wojskowej, absolwenta szkoły wyższej odbywającego przeszkolenie wojskowe lub żołnierza rezerwy odbywającego ćwiczenia wojskowe –na przechowanie przez okres pięciu lat;
2) prowadzonego w stosunku do innego żołnierza niż wymieniony w pkt 1 – na przechowanie przez okres dziesięciu lat.
2. Rejestr przechowuje się w kancelarii tajnej jednostki organizacyjnej, w której ukarany żołnierz pełnił czynną służbę wojskową, przez okres piętnastu lat od dnia ostatniego wpisu w tym rejestrze.

§ 5.1. Przełożony dyscyplinarny prowadzi ewidencję ukarań żołnierza w kartach ukarań żołnierza, zwanych dalej „kartami".
2. Wzór karty określa załącznik nr 2 do rozporządzenia.
3. Jeżeli żołnierz ze względów służbowych lub wskutek ukarania karą dyscyplinarną wyznaczenia na niższe stanowisko służbowe został przeniesiony do innej jednostki organizacyjnej lub innego pododdziału albo został przeniesiony do rezerwy kadrowej lub dyspozycji organu wojskowego – ewidencję ukarań żołnierza przekazuje się właściwemu przełożonemu.

§ 6. Kartę:
1) przechowuje się do czasu zatarcia ukarania;
2) niszczy się w dniu zatarcia ukarania.

§ 7. W jednostkach organizacyjnych, w których żołnierze pełnią czynną służbę wojskową, prowadzi się statystykę ukarań żołnierzy w danym roku kalendarzowym.

§ 8. Rozporządzenie wchodzi w życie z dniem 1 października 2002r.[1]
Dz.U.2004.35.297

Minister Obrony Narodowej: *J. Szmajdziński*

[1] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Obrony Narodowej z dnia 29 marca 1999r. w sprawie dokumentowania postępowania dyscyplinarnego (Dz.U. Nr 35, poz.333), które traci moc z dniem 30 września 2002r. na podstawie art.8 ustawy z dnia 20 lipca 2001 r. o zmianie ustawy o dyscyplinie wojskowej oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 925)

Załącznik nr 1 do rozporządzenia Ministra Obrony Narodowej
z dnia 13 września 2002 r. (poz. 1294)

WZÓR

Lewa strona

REJESTR POSTĘPOWAŃ DYSCYPLINARNYCH

Pozycja rejestru	Data zarejestrowania	Dane o wszczęciu postępowania dyscyplinarnego				
		Stopień wojskowy, imię i nazwisko, imię ojca oraz data urodzenia żołnierza objętego postępowaniem dyscyplinarnym	Nazwa jednostki organizacyjnej Pododdział (komórka wewnętrzna)	Stopień wojskowy, imię i nazwisko, stanowisko służbowe przełożonego dyscyplinarnego, który wszczął postępowanie dyscyplinarne	Stopień wojskowy, imię i nazwisko rzecznika dyscyplinarnego	Nr i data rozkazu (decyzji) o wszczęciu postępowania dyscyplinarnego
1	2	3	4	5	6	7

Prawa strona

Sposób zakończenia postępowania dyscyplinarnego			Uwagi (wszelkie wpisy dodatkowe, w tym adnotacje o obiegu dokumentacji, przekazaniu dokumentacji do archiwum wojskowego itp.)
Organ orzekający, który wydał prawomocne orzeczenie	Data wydania prawomocnego orzeczenia	Treść orzeczenia (w tym określenie przewinienia, o które żołnierz został obwiniony, oraz sposobu ukarania, jeżeli orzeczenie stanowi o ukaraniu)	
8	9	10	11

WZÓR **Załącznik nr 2**

KARTA UKARANIA ŻOŁNIERZA

Jednostka organizacyjna	**Karta ukarania Żołnierza**	Stopień wojskowy, imię i nazwisko, imię ojca
Pododdział (komórka wewnętrzna)		Stanowisko służbowe

Organ orzekający	Data wydania orzeczenia	Rodzaj przewinienia dyscyplinarnego	Rodzaj wymierzonej kary dyscyplinarnej lub zastosowania środka dyscyplinarnego	Termin wykonania kary dyscyplinarnej lub środka dyscyplinarnego albo termin warunkowego zawieszenia wykonania wymierzonej kary dyscyplinarnej	Uwagi

Dz.U.2005.215.1821

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 Służby Kontrwywiadu Wojskowego 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 Służby Kontrwywiadu Wojskowego 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 Służb Kontrwywiadu Wojskowego o zleceniu przedsiębiorcy lub jednostce naukowej umowy albo zadania wiążącego się z dostępem do informacji niejawnych stanowiących tajemnicę państwową oraz przestanie 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 Służb Kontrwywiadu Wojskowego, 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 Służb Kontrwywiadu Wojskowego, 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 Służby Kontrwywiadu Wojskowego 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 Służb Kontrwywiadu Wojskowego oraz jednostek organizacyjnych podporządkowanych Szefowi Służb Kontrwywiadu Wojskowego;

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 Służby Kontrwywiadu Wojskowego 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.

DECYZJA Nr 336/MON

MINISTRA OBRONY NARODOWEJ

z dnia 10 października 2005 r.

w sprawie wprowadzenia do użytku „Instrukcji o pieczęciach używanych w resorcie obrony narodowej"

Na podstawie § 1 pkt 8 lit. a i c oraz § 2 pkt 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426) ustala się, co następuje:

1. Wprowadza się do użytku „Instrukcję o pieczęciach używanych w resorcie obrony narodowej", stanowiącą załącznik do decyzji.
2. Traci moc zarządzenie Nr Pf 1/MON Ministra Obrony Narodowej z dnia 20 marca 1995 r. w sprawie wprowadzenia do użytku „ I nstru kcj i o pieczęciach używanych w resorcie obrony narodowej" (sygn. Szt. Gen. 1439/95).
3. Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Obrony Narodowej: J. Szmajdziński

Załącznik do decyzji Nr 336/MON Ministra Obrony Narodowej z dnia 10 października 2005 r. (poz. 178)

INSTRUKCJA

o pieczęciach używanych w resorcie obrony narodowej

Rozdział 1

Postanowienia ogólne

§ 1. Instrukcja określa zasady prowadzenia gospodarki i postępowania z pieczęciami używanymi w resorcie obrony narodowej w czasie pokoju i wojny.

§ 2. 1. Do wyrobu pieczęci dla jednostek (komórek) organizacyjnych resortu obrony narodowej upoważniona jest wyłącznie Wojskowa Wytwórnia Pieczęci, z zastrzeżeniem ust. 2.
2. Do wyboru pieczęci, wymienionych w § 6 pkt 7, dla jednostek (komórek) organizacyjnych Wojskowych Służb Informacyjnych, upoważniona jest wyznaczona przez Szefa Wojskowych Służb Informacyjnych, podległa mu komórka organizacyjna.
3. Dowódca jednostki wojskowej w ramach posiadanych środków finansowych może zlecić wykonanie pieczęci pomocniczych, o których mowa w § 7 ust. 1, w dowolnym zakładzie wykonującym tego typu pieczęcie.
§ 3. Użyte w instrukcji określenia oznaczają:
1) jednostka wojskowa - jednostkę wojskową, o której mowa wart. 3 ust. 5 ustawy z dnia 21 listopada 1967r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2004 r. Nr 241, poz. 2416 i Nr 277, poz. 2742) oraz jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, a także komórki organizacyjne Ministerstwa Obrony Narodowej;

Dz U z 2005, Nr 4 poz 47

2) dowódca jednostki wojskowej - dowódcę, dyrektora, szefa, kierownika, komendanta (inną osobę funkcyjną stojącą na czele jednostki wojskowej), który kieruje całokształtem działalności tej jednostki;
3) pieczęć - przyrząd, którego matryca w wyniku odciśnięcia daje odbitkę, obraz tekstu, wyrazu, cyfry, symbolu, znaku lub rysunku;
4) cecha pieczęci - znak w postaci cyfry lub litery umieszczony w dolnej części pieczęci, świadczący o wykonaniu dodatkowych egzemplarzy pieczęci tego samego wzoru.

Rozdział 2

Podział i przeznaczenie pieczęci

§ 4. Pieczęcie używane w resorcie obrony narodowej dzielą się na:
1) ze względu na stopień ważności:

a) urzędowe,
b) służbowe,
c) pomocnicze;

2) ze względu na sposób wykonania odcisku pieczęci:

a) do tłoczenia na sucho,
b) wypukłe do tuszu,
c) wklęsłe do laku;

3) ze względu na kształt:

a) okrągłe,
b) owalne,
c) prostokątne,
d) trójkątne;

4) ze względu na materiał z którego zostały wykonane:

a) metalowe,
b) kauczukowe,
c) z tworzywa.

§ 5. Pieczęcie urzędowe wykonywane są według następujących wzorów:
1) pieczęć okrągła o średnicy: 20, 30, 36, 39, 46 mm, wypukła do tuszu lub metalowa do tłoczenia na sucho, z wizerunkiem orła oraz numerem (nazwą) jednostki wojskowej, przeznaczona do nadawania świadectwa wiarygodności pisma lub dokumentu, na którym została umieszczona;
2) pieczęć okrągła o średnicy 30 mm, wklęsła do laku, z wizerunkiem orła oraz z numerem (nazwą) jednostki wojskowej, przeznaczona do zabezpieczania nienaruszalności opieczętowanego dokumentu, pakietu lub koperty;
3) pieczęć okrągła o średnicy 36 mm, wypukła do tuszu, z wizerunkiem orła, napisem „Do pieniężnych i gospodarczych dokumentów" oraz z numerem (nazwą) jednostki wojskowej, przeznaczona do poświadczania wiarygodności dokumentów o charakterze finansowym i gospodarczym;
4) pieczęć o średnicy 36 mm, wypukła do tuszu, z wizerunkiem orła oraz z napisem „SIŁY ZBROJNE RP", przeznaczona do opasek ze znakiem „Czerwonego Krzyża";
5) pieczęć okrągła o średnicy 20 mm, wypukła do tuszu, z wizerunkiem orła, napisem „SIŁY ZBROJNE RP" oraz z cechą identyfikacyjną w postaci dużej litery alfabetu łacińskiego i kolejnego numeru rozpoznawczego; przeznaczenie tej pieczęci określają przepisy „.instrukcji w sprawie kart i tabliczek tożsamości oraz prowadzenia w czasie wojny ewidencji strat bezpowrotnych i warunkowych".

§ 6. Pieczęcie służbowe wykonywane są według następujących wzorów:
1) pieczęć prostokątna o długości 54 mm i szerokości 33 mm, wychodząca, wypukła do tuszu, z

wizerunkiem orła, numerem (nazwą) jednostki wojskowej oraz numerem pisma i datą, przeznaczona do pieczętowania dokumentów lub pakietów wysyłanych z jednostki wojskowej;
2) pieczęć prostokątna o długości 54 mm i szerokości 27 mm, wypukła do tuszu, z numerem (nazwą) jednostki wojskowej oraz oznaczeniem wpływu pism (numer, data, ilość załączników, arkuszy/stron). przeznaczona do pieczętowania dokumentów wpływających do jednostki wojskowej;
3) pieczęć okrągła o średnicy 30 mm, wklęsła do laku, silikonu lub wypukła do tuszu z napisem „Do pakietów" oraz numerem (nazwą) jednostki wojskowej, przeznaczona:

a) wklęsła do laku - do pieczętowania dokumentów lub przesyłek o charakterze niejawnym lub jawnym,
b) wypukła do tuszu - do pieczętowania w szczególności arkuszy papieru, notatników wykorzystywanych przy pracach niejawnych, przesyłek o charakterze niejawnym lub jawnym oraz potwierdzania odbioru dokumentów przyjmowanych w jednostce wojskowej;

4) pieczęć okrągła do szyfrów o średnicy 30 mm, wklęsła do laku lub wypukła do tuszu, z napisem „Do szyfrów" lub literą „S" oraz numerem (nazwą) jednostki wojskowej, przeznaczona dla wojskowych organów kryptograficznych;
5) pieczęć owalna, biblioteczna o wymiarach 32 mm x 46 mm, wypukła do tuszu, z numerem (nazwą) jednostki wojskowej oraz numerem ewidencyjnym, przeznaczona do pieczętowania wydawnictw przyjmowanych i przechowywanych w bibliotece lub kancelarii jednostki wojskowej, a także do pieczętowania dokumentacji technicznej oraz materiałów filmowych;
6) pieczęć prostokątna firmująca, wypukła z godłem lub bez, z numerem (nazwą) jednostki wojskowej, znakiem firmowym lub fabrycznym, przeznaczona do oznakowania przedmiotów, kart lub dokumentów firmowych;
7) pieczęć prostokątna tytułowa (tytułowo-nazwiskowa). nie ograniczona wymiarami liniowymi, wypukła do tuszu, z nazwą stanowiska służbowego, pełnionej funkcji, z oznaczeniem identyfikacyjnym, stopniem wojskowym, tytułem (stopień naukowy albo tytuł zawodowy) oraz imieniem i nazwiskiem osoby uprawnionej do posługiwania się tą pieczęcią;
8) pieczęć prostokątna adresowa (wypukła do tuszu). z numerem (nazwą) jednostki wojskowej, numerem placówki pocztowo-telekomunikacyjnej, kodem pocztowym, w której jednostka wojskowa jest zarejestrowana, a także w razie potrzeby numerem konta bankowego, Numerem Identyfikacji Podatkowej (NIP) oraz numerem REGON;
9) pieczęć trójkątna o bokach 44 mm, wypukła do tuszu, z napisem „Jednostka Wojskowa – Do przepustek" oraz cechami literowymi i cyfrowymi, a także w razie potrzeby numerem (nazwą) jednostki wojskowej, przeznaczona do pieczętowania jednorazowych przepustek;
10) pieczęć okrągła, numerowa do teczek pracy, o średnicy 20 mm, metalowa, wklęsła, z napisem „Jednostka Wojskowa" lub skróconą nazwą jednostki wojskowej oraz cechą identyfikacyjną w postaci dużych liter alfabetu łacińskiego i kolejnym numerem rozpoznawczym, przeznaczona do zabezpieczenia teczek pracy, szaf, skrzyń lub pomieszczeń;
11) kamień do plombownicy, z oznaczeniem literowym (cyfrowym) jednostki wojskowej na jednej matrycy i wizerunkiem orła na drugiej, przeznaczony do zabezpieczenia pakietu lub pomieszczenia;
12) cecha identyfikacyjna o średnicy 10 mm, z wypukłym oznaczeniem literowym i cyfrowym, przeznaczona do oznakowania urządzeń technicznych lub ich elementów.

§ 7. 1. Pieczęcie pomocnicze wykonywane są według ustalonych, w odrębnych przepisach lub zamówieniu, wzorów; usprawniają pracę i zastępują wpisywanie do formularzy (pism, druków) często używanych, powtarzających się tekstów - nie podlegają ewidencji.
2. Do pieczęci pomocniczych zalicza się:

1) pieczęć uzupełniającą wypukłą do tuszu, przeznaczoną do uzupełniania niewypełnionych miejsc na drukach, formularzach i pismach;
2) pieczęć faksymilową wypukłą do tuszu, przeznaczoną do pieczętowania przez upoważnione osoby dokumentów w dużych nakładach, druków ścisłego zarachowania, w szczególności przepustek, skierowań, rozkazów wyjazdów;
3) pieczęć formularzową wypukłą do tuszu, której odciśnięty tekst wymaga uzupełniania ręcznego lub maszynowego;

4) pieczęć informacyjną wypukłą do tuszu, zawierającą pojedyncze wyrazy lub krótkie teksty np. „Tajne", „Ćwiczebne", „Zastrzeżone", ,Tu otwierać", „Pilne";
5) pieczęć znakową wypukłą do tuszu, zawierającą ustalone znaki w postaci liter, cyfr, rysunku.

Rozdział 3

Używanie i posługiwanie się pieczęciami

§ 8. Pieczęci urzędowych używają:
1) minister, sekretarz i podsekretarz stanu, szef Sztabu Generalnego WP, Naczelny Prokurator Wojskowy - o średnicy 46 mm i 20 mm;
2) attache wojskowy - o średnicy 39 mm;
3) Dowódca jednostki wojskowej (upoważnione osoby funkcyjne) - o średnicy 36 mm i 20 mm.

§ 9. Pieczęcie urzędowe do tłoczenia na sucho przydziela się jednostkom wojskowym, które zgodnie z obowiązującymi przepisami zobowiązane są do wystawiania dokumentów wymagających dla swej ważności odbitki suchej pieczęci.

§ 10. Pieczęcie służbowe, numerowe przysługują jednostkom wojskowym, w których żołnierze (pracownicy resortu obrony narodowej, słuchacze) przechowują materiały (dokumenty) wymagające, zgodnie z obowiązującymi przepisami, takiego zabezpieczenia.

§ 11. Do posługiwania się pieczęcią urzędową lub służbową upoważnia się wyłącznie jedną osobę.

§ 12. 1. Imienny wykaz osób upoważnionych do posługiwania się pieczęciami urzędowymi i służbowymi ustala dowódca jednostki wojskowej w rozkazie dziennym (decyzji).
2. Wykazu, o którym mowa w ust. 1, nie ustala się dla pieczęci tytułowo-nazwiskowych i pieczęci numerowych do teczek pracy.

§ 13. 1. Pieczęci urzędowych nie odciskuje się na nie wypełnionym formularzu, nie podpisanym piśmie lub innym dokumencie, z wyjątkiem blankietów jednorazowych przepustek upoważniających do opuszczenia terenu jednostki wojskowej. miejsca zakwaterowania przez żołnierzy pełniących tam służbę.
2. Nie wypełnione blankiety przepustek, na których odciśnięto pieczęć urzędową, przed przekazaniem do dyspozycji uprawnionych dowódców pododdziałów, ewidencjonuje się w kancelarii jednostki wojskowej, a po ich wykorzystaniu niszczy.
§ 14. 1. W czasie pokoju jednostka wojskowa posługuje się pieczęciami z numerem jednostki wojskowej.
2. Jednostki wojskowe, którym nie nadano numeru, posługują się pieczęciami z nazwą jednostki wojskowej, a w czasie wojny posługują się pieczęciami z nazwą jednostki wojskowej albo z numerem poczty polowej.
3. Przy posługiwaniu się pieczęciami, o których mowa w ust. 1, stosuje się zasady ustalone w czasie pokoju i wojny, zawarte w obowiązujących przepisach o wykonywaniu dokumentów i postępowaniu z nimi w wojsku.

Rozdział 4

Przechowywanie i wydawanie pieczęci

§ 15. 1. Pieczęcie urzędowe i służbowe przechowuje się na zasadach przewidzianych dla dokumentów niejawnych, w szczególności w metalowych szafach (skrzyniach) zamykanych po zakończeniu pracy i opieczętowanych pieczęciami numerowymi do teczek pracy.
2. Pieczęcie pomocnicze przechowuje się na zasadach przewidzianych dla dokumentów jawnych.

§ 16. 1. Pieczęcie urzędowe i pieczęcie służbowe przechowuje dowódca jednostki wojskowej lub

osoby, którym zostały one przydzielone decyzją lub rozkazem dziennym dowódcy.
2. Pieczęcie służbowe wykorzystywane do ewidencji materiałów w kancelarii tajnej przechowuje kierownik kancelarii, lub upoważnieni, etatowi jej pracownicy.

§ 17. Podczas pracy pieczęcie urzędowe i służbowe znajdują się w miejscu dostępnym tylko dla osoby upoważnionej do posługiwania się tymi pieczęciami.

§ 18. Za właściwe zabezpieczenie i przechowywanie pieczęci do przepustek odpowiedzialny jest oficer dyżurny lub osoba, której ta pieczęć została przydzielona.

§ 19. Przekazywanie, wydawanie i zwrot pieczęci urzędowych oraz pieczęci służbowych w jednostce wojskowej odbywa się tylko za pośrednictwem kancelarii i za pokwitowaniem w księdze ewidencji pieczęci, w obecności przekazującego i przyjmującego.

§ 20. Pieczęcie przeznaczone na czas wojny przechowuje się w jednostce wojskowej w pakiecie przesznurowanym i zaplombowanym przez Wojskową Wytwórnię Pieczęci.

§ 21. 1. Pakiety z pieczęciami na czas wojny ujmuje się w ewidencji przechowywanych pakietów, opracowanej według wzoru określonego w załączniku Nr 8.
2. Wydanie pakietu, o którym mowa w ust. 1, właściwej jednostce wojskowej następuje za pokwitowaniem wraz z innymi dokumentami mobilizacyjnymi zgodnie z przepisami o ochronie informacji niejawnych.

Rozdział 5

Ewidencja pieczęci

§ 22. Ewidencji podlegają wszystkie pieczęcie urzędowe i służbowe.

§ 23. Ewidencję pieczęci prowadzą:
1) kierownik Wojskowej Wytwórni Pieczęci;
2) szefowie sztabów dowództw: rodzajów Sił Zbrojnych, okręgów wojskowych oraz Dowództwa Garnizonu Warszawa;
3) dowódcy jednostek wojskowych.
§ 24. Kierownik Wojskowej Wytwórni Pieczęci odpowiada za:
1) ewidencję odbitek wszystkich pieczęci urzędowych oraz pieczęci służbowych, wymienionych w § 6 pkt 1-5, przeznaczonych do użytku w czasie pokoju (wojny);
2) ewidencję pakietów zawierających pieczęcie na czas wojny z numerem poczty polowej (pełną nazwą jednostki wojskowej);
3) wykazy pieczęci urzędowych do kart tożsamości i opasek ze znakiem „Czerwonego Krzyża", przydzielanych jednostkom wojskowym;
4) ewidencję zamówień pieczęci;
5) wykazy pieczęci do teczek pracy oraz wykazy pie częci do przepustek przydzielonych jednostkom wojskowym;
6) ewidencję pieczęci urzędowych oraz pieczęci służbowych utraconych w jednostkach wojskowych;
7) ewidencję pieczęci urzędowych oraz pieczęci służbowych zniszczonych w Wojskowej Wytwórni Pieczęci .

§ 25. Szef komórki wewnętrznej jednostki wojskowej właściwej w sprawach organizacyjno-etatowych (upoważniona osoba funkcyjna) odpowiada za:

1) ewidencję odbitek pieczęci urzędowych oraz pieczęci służbowych przeznaczonych do bieżącego użytku i znajdujących się w jednostkach wojskowych przez nie zaopatrywanych - według wzoru określonego w załączniku Nr 2;
2) ewidencję pakietów zawierających pieczęcie przeznaczone na czas wojny i przechowywanych w jednostkach wojskowych - według wzoru określonego w załączniku Nr 3;

3) wykazy pieczęci służbowych do teczek pracy oraz pieczęci do przepustek przydzielonych jednostkom wojskowym - według wzoru określonego w załączniku Nr 4;
4) ewidencję pieczęci służbowych utraconych według wzoru określonego w załączniku Nr 5;
5) ewidencję pieczęci służbowych zniszczonych według wzoru określonego w załączniku Nr 6.

§ 26. W jednostce wojskowej prowadzi się:
1) ewidencję wszystkich posiadanych pieczęci urzędowych oraz pieczęci służbowych - według wzoru określonego w załączniku Nr 7;
2) ewidencję pakietów zawierających pieczęcie przeznaczone na czas wojny - według wzoru określonego w załączniku Nr 8;
3) wykaz osób upoważnionych do posługiwania się pieczęciami urzędowymi i służbowymi - według wzoru określonego w załączniku Nr 9.

§ 27. Dowódca jednostki wojskowej wyznacza rozkazem osobę odpowiedzialną za prowadzenie ewidencji pieczęci w podległej mu jednostce, z tym że:
1) w przypadku gdy w jednostce wojskowej jest więcej niż jedna kancelaria - do prowadzenia ewidencji pieczęci wyznacza się kierownika kancelarii głównej;
2) w komórkach organizacyjnych Ministerstwa Obrony Narodowej, dowództwach rodzajów Sił Zbrojnych, dowództwach okręgów wojskowych oraz w Dowództwie Garnizonu Warszawa - do prowadzenia ewidencji pieczęci wyznacza się kierowników kancelarii tych komórek (jednostek) organizacyjnych, na terenie których działają te kancelarie.

§ 28. Osoba funkcyjna prowadząca ewidencję pieczęci obowiązana jest posiadać aktualny wykaz osób upoważnionych do posługiwania się pieczęciami urzędowymi i służbowymi.

§ 29. Książkę ewidencji pieczęci rejestruje się w „Rejestrze teczek dokumentów niejawnych, dzienników i książek ewidencyjnych" w kancelarii jednostki wojskowej i prowadzi się do całkowitego zapisania.
§ 30. Ewidencję pieczęci wypełnia się pismem czytelnym i wyraźnym; wpisów nie wolno wycierać lub wywabiać środkami chemicznymi.

§ 31. Dokumenty ewidencyjne dotyczące pieczęci posiadanych przez jednostkę wojskową oraz korespondencję w zakresie tych pieczęci klasyfikuje się zgodnie z rzeczowym wykazem akt.

§ 32. Dokumenty ewidencyjne dotyczące pakietów zawierających pieczęcie na czas wojny traktuje się jako dokumenty o charakterze mobilizacyjnym.

§ 33. Dowódcy jednostek wojskowych są odpowiedzialni za aktualność treści pieczęci, wynikającej z dokumentacji organizacyjno-etatowej i zgodność stanu ewidencyjnego pieczęci z ich stanem faktycznym.

§ 34. 1 Sprawdzenia zgodności stanu faktycznego posiadanych pieczęci ze stanem ewidencyjnym dokonuje się w czasie półrocznej i rocznej kontroli stanu ochrony informacji niejawnych w jednostce wojskowej.
2. Z czynności, o której mowa w ust. 1, przedstawia się dowódcy jednostki wojskowej (właściwemu przełożonemu) meldunek.

§ 35. Podstawę do prowadzenia ewidencji pieczęci przeznaczonych do użytku bieżącego oraz dokonywania w niej zmian stanowi:
1) dokument, przy którym doręczono jednostce wojskowej pieczęcie;
2) protokół przekazania pieczęci, opracowany według wzoru określonego w załączniku Nr 10;
3) wykaz nieaktualnych pieczęci przekazanych do zniszczenia, opracowany według wzoru określonego w załączniku Nr 11;
4) meldunek o utracie pieczęci służbowej.

§ 36. Podstawę do prowadzenia ewidencji pakietów zawierających pieczęcie do użytku w czasie wojny, oraz do dokonywania w niej zmian stanowi:

1) dokument, przy którym doręczono jednostce wojskowej pakiet;
2) dokument, przy którym wysłano (przekazano) pakiety poza jednostkę wojskową;
3) protokół zdawczo-odbiorczy pakietów zawierających pieczęcie na czas wojny;
4) pokwitowanie odbioru pakietu.

Rozdział 6

Zasady zamawiania i zaopatrywania w pieczęcie

§ 37. 1. Zamawianie i przekazywanie pieczęci oraz wszelka korespondencja z tym związana odbywa się za pośrednictwem dowództw rodzajów Sit Zbrojnych, okręgów wojskowych, Dowództwa Garnizonu Warszawa - zgodnie z obowiązującymi przepisami w zakresie zaopatrywania jednostek wojskowych i wykonywania dokumentów oraz postępowania z nimi w Sitach Zbrojnych.
2. Komórki (jednostki) organizacyjne centralnego podporządkowania zamawiają pieczęcie i rozliczają się z nich bezpośrednio w Wojskowej Wytwórni Pieczęci.

§ 38. Ustalenie należności i zasad zaopatrywania jednostek wojskowych w pieczęcie przeznaczone do użytku w czasie pokoju i wojny, należy do kompetencji Szefa ~~Generalne~~go Zarządu Zasobów Osobowych - P1

§ 39. Podstawę do zaopatrywania jednostek wojskowych w pieczęcie stanowią zarządzenia (decyzje) organizacyjne Ministra Obrony Narodowej oraz rozkazy organizacyjne (mobilizacyjne) Szefa Sztabu Generalnego Wojska Polskiego.
§ 40. Na podstawie zarządzenia (decyzji), o którym mowa w § 39, Wojskowa Wytwórnia Pieczęci wykonuje właściwe pieczęcie urzędowe oraz służbowe i przesyła je drogą służbową za pośrednictwem wojskowych organów pocztowych lub poczty specjalnej.

§ 41. W uzasadnionych przypadkach wykonane pieczęcie mogą być wydane przedstawicielowi jednostki wojskowej, posiadającemu pisemne upoważnienie dowódcy tej jednostki do ich odbioru.

§ 42. Pakiety zawierające pieczęcie urzędowe i pieczęcie służbowe przesyła się do rąk własnych dowódcom jednostek wojskowych.

§ 43. Zamawianie większej (dodatkowej) liczby egzemplarzy pieczęci urzędowych i pieczęci służbowych jest dopuszczalne w przypadkach uzasadnionych:
1) wielkością jednostki wojskowej;
2) warunkami rozmieszczenia pododdziałów jednostki wojskowej;
3) wymogami organizacji pracy.

§ 44. W celu zamówienia dodatkowej liczby egzemplarzy pieczęci tego samego rodzaju lub pieczęci, których treść jest inna niż wynika to z dokumentów organizacyjno-etatowych:
1) dowódca jednostki wojskowej występuje pisemnie, drogą służbową, poprzez właściwe dowództwo zaopatrujące, do kierownika Wojskowej Wytwórni Pieczęci;
2) komórki organizacyjne ministerstwa bezpośrednio do kierownika Wojskowej Wytwórni Pieczęci.

§ 45. Dodatkowe egzemplarze pieczęci urzędowych oraz pieczęci służbowych oznacza się odpowiednimi cechami identyfikacyjnymi (cyframi rzymskimi lub arabskimi), odróżniającymi je od egzemplarzy zasadniczych.

§ 46. Jednostki wojskowe otrzymują pieczęcie służbowe, numerowe do teczek pracy, do przepustek oraz pieczęcie pomocnicze z dowództw, przez które są zaopatrywane w wymienione pieczęcie.

§ 47. 1. Zamówienie pieczęci urzędowych i służbowych może być dokonane wyłącznie na piśmie podpisanym przez dowódcę jednostki wojskowej lub osobę upoważnioną przez dowódcę w rozkazie dziennym.

Dz. U. z 2007 r. Nr 4 poz. 47

2. Zamówienie, o którym mowa w ust. 1, powinno zawierać w szczególności następujące dane:

1) rodzaj, treść, cechę albo wzór pieczęci;
2) liczbę egzemplarzy pieczęci;
3) uzasadnienie ich zamawiania.

Rozdział 7

Postępowanie z pieczęciami w razie zmiany podporządkowania jednostki wojskowej

§ 48. W przypadku zmiany podporządkowania jednostki wojskowej, dowódca tej jednostki jest obwiązany:
1) sporządzić szczegółowy wykaz posiadanych pieczęci urzędowych i służbowych w czterech jednobrzmiących egzemplarzach, według wzoru określonego w załączniku Nr 1 i w terminie 7 dni od dnia przeniesienia jednostki przesłać (włączyć):

a) egz. nr 1 - do dowództwa jednostki nadrzędnej. w podporządkowanie którego jednostka wojskowa została przeniesiona,
b) egz. nr 2 - do dowództwa jednostki nadrzędnej, z którego jednostka wojskowa otrzymywała pieczęcie,
c) egz. nr 3 - do Wojskowej Wytwórni Pieczęci,
d) egz. nr 4 - do akt jednostki wojskowej zmieniającej podporządkowanie;

2) złożyć zapotrzebowanie na pieczęcie numerowe do teczek pracy oraz pieczęcie do przepustek do dowództwa, któremu jednostka wojskowa została podporządkowana;
3) przesłać dotychczas posiadane pieczęcie do dowództwa jednostki nadrzędnej, z podporządkowania której jednostka wojskowa wyszła, z chwilą otrzymania nowych pieczęci do teczek pracy i przepustek;
4) przekazać protokolarnie pakiety zawierające pieczęcie przeznaczone na czas wojny do dowództwa jednostki nadrzędnej. z którego podporządkowania jednostka wojskowa wyszła.

§ 49. Szef komórki wewnętrznej właściwej w sprawach organizacyjno-etatowych (upoważniona osoba funkcyjna):
1) przekazuje protokolarnie, po sprawdzeniu nadesłanych z jednostek wojskowych wykazów, karty ewidencyjne pieczęci na czas pokoju oraz pakiety zawierające pieczęcie na czas wojny do dowództwa rodzaju Sił Zbrojnych, Dowództwa Garnizonu Warszawa, któremu podporządkowano jednostkę wojskową;
2) przesyła do kierownika Wojskowej Wytwórni Pieczęci egzemplarz protokołu, o którym mowa w pkt 1.

Rozdział 8

Wymiana lub zwrot nieaktualnych pieczęci

§ 50. 1. Pieczęcie urzędowe oraz pieczęcie służbowe nieaktualne, zużyte lub uszkodzone podlegają wymianie w Wojskowej Wytwórni Pieczęci.
2. W celu wymiany pieczęci dowódca jednostki wojskowej przesyła do jednostki nadrzędnej, za pośrednictwem którego jednostka wojskowa jest zaopatrywana w pieczęcie, zapotrzebowanie, w którym należy:

1) odcisnąć pieczęć przeznaczoną do wymiany;
2) w przypadku nieczytelności odbitki pieczęci, opisać jej treść.

§ 51. 1. Pieczęcie nieaktualne, w szczególności z powodu zużycia (uszkodzenia). rozformowania (zmiany nazwy) jednostki wojskowej. dowódca jednostki wojskowej jest zobowiązany przekazać:

1) pieczęcie urzędowe oraz pieczęcie służbowe, o których mowa w § 6 pkt 1-5, wraz z odciskami - do Wojskowej Wytwórni Pieczęci, informując o tym fakcie dowództwo, z którego pieczęcie otrzymał;
2) pakiety z nieaktualnymi pieczęciami na czas wojny - do Wojskowej Wytwórni Pieczęci, za pośrednictwem właściwego dowództwa jednostki nadrzędnej, z którego jednostka wojskowa pakiety otrzymała;
3) pieczęcie służbowe - bezpośrednio do właściwego dowództwa jednostki nadrzędnej, z którego jednostka wojskowa pieczęcie otrzymała.

2. Pieczęcie służbowe, wymienione w § 6 pkt 6-10, używane przez komórki organizacyjne Ministerstwa Obrony Narodowej, dowództwa rodzajów Sił Zbrojnych, dowództwa okręgów wojskowych oraz Dowództwo Garnizonu Warszawa, nie podlegają przekazaniu do Wojskowej Wytwórni Pieczęci.

§ 52. 1. Jednostka wojskowa sporządza wykaz zwróconych, nieaktualnych, zużytych, uszkodzonych lub odnalezionych pieczęci urzędowych i służbowych w ilości:

1) trzech egzemplarzy - dla pieczęci, do zniszczenia których upoważniona jest wyłącznie Wojskowa Wytwórnia Pieczęci;
2) dwóch egzemplarzy - dla pieczęci, do zniszczenia których upoważnione są właściwe dowództwa.

2. Sporządzone egzemplarze wykazów, o których mowa w ust. 1 pkt 1, przesyła się (włącza) do:

1) kierownika Wojskowej Wytwórni Pieczęci egz. nr 1 wraz z pieczęciami;
2) właściwego dowództwa jednostki nadrzędnej za pośrednictwem którego jednostka wojskowa jest zaopatrywana w pieczęcie - egz. nr 2;
3) akt jednostki wojskowej - egz. nr 3.

3. Sporządzone egzemplarze wykazów, o których mowa w ust. 1 pkt 2, przesyła się (włącza) do:

1) właściwego dowództwa jednostki nadrzędnej, za pośrednictwem którego jednostka wojskowa jest zaopatrywana w pieczęcie - egz. nr 1 wraz z pieczęciami;
2) akt jednostki wojskowej - egz. nr 2.

Rozdział 9

Niszczenie pieczęci

§ 53. 1. Niszczenie nieaktualnych, zużytych lub uszkodzonych pieczęci, dokonuje komisja w składzie trzech osób, wyznaczona rozkazem właściwego przełożonego.
2. Wojskowa Wytwórnia Pieczęci niszczy pieczęcie urzędowe oraz pieczęcie służbowe wymienione w § 6 pkt 1-5.
3. Dowództwa: rodzajów Sit Zbrojnych i okręgów wojskowych, Dowództwo Garnizonu Warszawa oraz komórki organizacyjne Ministerstwa Obrony Narodowej dokonują niszczenia pieczęci służbowych wymienionych w § 6 pkt 6-10.
4. Pieczęcie pomocnicze jednostki wojskowe niszczą we własnym zakresie.

§ 54. Niszczenia pieczęci dokonuje się poprzez mechaniczne zniszczenie napisów i godła pieczęci metalowych oraz pocięcie i spalenie pieczęci z tworzyw sztucznych i z kauczuku.

§ 55. Z czynności zniszczenia pieczęci komisja, o której mowa w § 53 ust. 1, sporządza protokół, który podpisują członkowie komisji, a zatwierdza przełożony, który komisję wyznaczył.

§ 56. Zabrania się użytkownikom pieczęci samodzielnego niszczenia oraz dokonywania jakichkolwiek zmian w treści lub obrazie pieczęci.

Rozdział 10

Postępowanie z pieczęciami przeznaczonymi na czas wojny

§ 57. Jednostkom wojskowym formowanym na czas wojny przygotowuje się pakiety z pieczęciami, które mogą zawierać pieczęcie:

1) z nazwą jednostki wojskowej;
2) z numerem poczty polowej;
3) pomocnicze.

§ 58. Pieczęcie z nazwą jednostki wojskowej przydziela się:
1) jednostkom wojskowym formowanym w czasie mobilizacji;
2) jednostkom wojskowym, którym w czasie mobilizacji zostaje zmieniona nazwa.
§ 59. Pieczęcie z numerem poczty polowej przydziela się jednostkom wojskowym, którym takie numery zostały nadane.

§ 60. 1. Wojskowa Wytwórnia Pieczęci przekazuje pieczęcie przeznaczone do użytku w czasie wojny, w przesznurowanych i zaplombowanych pakietach, właściwym jednostkom wojskowym za pośrednictwem dowództw: rodzajów Sił Zbrojnych, okręgów wojskowych oraz Dowództwa Garnizonu Warszawa.
2. Pakiety, o których mowa w ust. 1, opatrzone są na zewnętrznej stronie odpowiednim numerem (cyframi arabskimi), według ewidencji prowadzonej w Wojskowej Wytwórni Pieczęci i posiadają na zewnętrznej, górnej części jednolicie ustalony tekst informacyjny o następującej treści:

U w a g a:
„Zabrania się dokonywania jakichkolwiek adnotacji na pakiecie. W czasie pokoju otwarcia pakietu, celem sprawdzenia jego zawartości, może dokonać tylko specjalnie upoważniona do tego komisja"

§ 61. 1. Pieczęcie przeznaczone dla jednostek wojskowych na czas wojny wprowadza się do użytku w ramach osiągania przez te jednostki gotowości do podjęcia działań lub z chwilą wybuchu wojny, na rozkaz Szefa Sztabu Generalnego Wojska Polskiego (Naczelnego Dowódcy Sił Zbrojnych).
2. Wszystkie dokumenty związane z okresem przejściowym, związanym z likwidacją spraw aktualnych w czasie pokoju, pieczętuje się pieczęciami używanymi w czasie pokoju, natomiast dokumenty dotyczące spraw czasu wojny pieczętuje się przeznaczonymi do użytku w czasie wojny.

§ 62. Pieczęcie, o których mowa w § 58, przechowuje się w jednostkach wojskowych, których dowódcy są odpowiedzialni za sformowanie tych jednostek, w miejscu zdeponowania dokumentacji mobilizacyjnej formowanych jednostek wojskowych.

§ 63. 1. W celu wprowadzenia do użytku pieczęci na czas wojny dowódca (szef sztabu) jednostki wojskowej uprawnionej do ich używania dokonuje komisyjnego otwarcia i sprawdzenia zawartości pakietu zawierającego te pieczęcie oraz kwituje odbiór pieczęci na formularzu pokwitowania odbioru znajdującym się wewnątrz pakietu, według wzoru określonego w załączniku Nr 16.
2. Pokwitowanie odbioru z odbitkami pieczęci, podpisane przez dowódcę (szefa sztabu) jednostki wojskowej, przesyła się jako przesyłkę niejawną oznaczoną właściwą klauzulą tajności, bezpośrednio do Wojskowej Wytwórni Pieczęci, natomiast drugą część formularza „Wykaz zawartości pakietu" pozostawia w aktach jednostki, co stanowi podstawę do ujęcia tych pieczęci w ewidencji jednostki wojskowej.

§ 64. 1. W przypadku uszkodzenia (naruszenia) plomby lub pakietu zawierającego pieczęcie przeznaczone na czas wojny, należy niezwłocznie sporządzić protokół - meldunek, według wzoru określonego w załączniku Nr 12, i wraz z zabezpieczonym pakietem przesłać do kierownika Wojskowej Wytwórni Pieczęci.

2. Jeżeli w wyniku uszkodzenia pakietu istniała możliwość użycia pieczęci lub wglądu w ich treść, należy dodatkowo powiadomić o tym fakcie bezpośredniego przełożonego, właściwą jednostkę organizacyjną Żandarmerii Wojskowej (prokuratora wojskowego).
3. W czasie pokoju obowiązuje bezwzględny zakaz używania pieczęci na czas wojny.

Rozdział 11

Postępowanie z pieczęciami w przypadkach szczególnych

§ 65. W przypadku otrzymania uszkodzonej przesyłki zawierającej pieczęcie do użytku bieżącego, w takim stopniu, że istniała realna możliwość ich użycia, należy niezwłocznie:

1) opakowanie zabezpieczyć i sporządzić protokół, według wzoru określonego w załączniku Nr 13;
2) powiadomić kierownika Wojskowej Wytwórni Pieczęci, poprzez właściwe dowództwo, z którego pakiet otrzymano;
3) powiadomić właściwą jednostkę organizacyjną Żandarmerii Wojskowej.

§ 66. 1. W przypadku utraty, zagubienia lub zniszczenia pieczęci urzędowej, dowódca jednostki wojskowej opracowuje meldunek, który przesyła do:

1) kierownika Wojskowej Wytwórni Pieczęci;
2) właściwego dowództwa rodzaju Sił Zbrojnych, dowództwa okręgu wojskowego, Dowództwa Garnizonu Warszawa;
3) bezpośredniego przełożonego;
4) właściwej jednostki organizacyjnej Żandarmerii Wojskowej (prokuratora wojskowego).

2. Kopię meldunku, o którym mowa w ust. 1, włącza się do akt jednostki wojskowej.

§ 67. 1. Unieważnienia utraconych pieczęci, o których mowa w § 5, dokonuje kierownik Wojskowej Wytwórni Pieczęci.
2. Fakt unieważnienia utraconych pieczęci urzędowych ogłasza się w Dzienniku Urzędowym Ministra Obrony Narodowej.

§ 68. 1. W przypadku utraty pieczęci służbowej, wymienionej w § 6 pkt 1-5, dowódca jednostki wojskowej opracowuje meldunek, który przesyła do:

1) kierownika Wojskowej Wytwórni Pieczęci;
2) szefa komórki wewnętrznej właściwej w spra
wach organizacyjno-etatowych dowództwa rodzaju Sit Zbrojnych, dowództwa okręgu wojskowego, Dowództwa Garnizonu Warszawa;
3) bezpośredniego przełożonego;
4) właściwej jednostki organizacyjnej Żandarmerii Wojskowej lub prokuratora wojskowego;

2. Kopię meldunku, o którym mowa w ust. 1, należy włączyć do akt jednostki wojskowej.

§ 69. 1. W przypadku utraty pieczęci służbowej, wymienionej w § 6 pkt 6-9, dowódca jednostki wojskowej opracowuje meldunek, który przesyła do:

1) szefa komórki wewnętrznej dowództwa rodzaju Sił Zbrojnych właściwej w sprawach organizacyjno-etatowych, dowództwa okręgu wojskowego, Dowództwa Garnizonu Warszawa;
2) bezpośredniego przełożonego;
3) właściwej jednostki organizacyjnej Żandarmerii Wojskowej lub prokuratora wojskowego.
2. Kopię meldunku, o którym mowa w ust. 1, włącza się do akt jednostki wojskowej.

§ 70. Meldunek, o którym mowa w §§ 66-69, opracowuje się według wzoru określonego w załączniku Nr 14.

§ 71. W przypadku utraty pieczęci służbowej, wymienionej w § 6 pkt 10, dowódca jednostki wojskowej przeprowadza postępowanie wyjaśniające i swoją decyzją unieważnia utraconą pieczęć.

§ 72. Każdą utraconą pieczęć służbową dowódca jednostki wojskowej unieważnia w rozkazie dziennym po zakończeniu postępowania wyjaśniającego prowadzonego przez właściwą jednostkę organizacyjną Żandarmerii Wojskowej lub prokuratura wojskowego.

§ 73. 1. W przypadku podrobienia pieczęci urzędowej (służbowej) albo wykonania jej w innym zakładzie niż Wojskowa Wytwórnia Pieczęci dowódca jednostki wojskowej obowiązany jest:

1) natychmiast wycofać pieczęć z użytku i ją zabezpieczyć;
2) wyznaczyć komisję, która przeprowadzi postępowanie wyjaśniające i sporządzi meldunek według wzoru określonego w załączniku Nr 15, który przesyła się do:

a) kierownika Wojskowej Wytwórni Pieczęci,
b) szefa komórki wewnętrznej dowództwa rodzaju Sił Zbrojnych właściwej w sprawach organizacyjno-etatowych, dowództwa okręgu wojskowego, Dowództwa Garnizonu Warszawa;
c) bezpośredniego przełożonego,
d) właściwej jednostki organizacyjnej Żandarmerii Wojskowej (prokuratora wojskowego).

2. Kopię meldunku należy włączyć do akt jednostki wojskowej.

§ 74. 1. Fakt unieważnienia pieczęci stanowi podstawę do skreślenia ich z ewidencji oraz wykonania nowych, w miejsce utraconych.
2. Odpowiedzialność za utratę pieczęci ponosi osoba, której pieczęć została przydzielona rozkazem dziennym, a także dowódca jednostki wojskowej w razie potwierdzenia braku odpowiedniego nadzoru.

§ 75. 1. Osoba, która stwierdziła brak pieczęci urzędowej lub służbowej, składa w trybie pilnym meldunek dowódcy jednostki wojskowej.
2. Osoba winna utraty pieczęci, o których mowa w § 5 i § 6, ponosi odpowiedzialność dyscyplinarną i materialną, według cen określonych w załączniku Nr 18.

§ 76. Zabrania się używać pieczęci urzędowych i służbowych, które zostały utracone, a następnie odnalezione. Pieczęcie te podlegają natychmiastowemu wycofaniu z użytku i odesłaniu do Wojskowej Wytwórni Pieczęci.

§ 77. Dowództwa rodzajów Sit Zbrojnych i okręgów wojskowych oraz Dowództwo Garnizonu Warszawa, na podstawie nadesłanych z poszczególnych jednostek wojskowych meldunków o utracie pieczęci do teczek pracy i pieczęci do przepustek, sporządzają raz w roku zbiorcze zestawienie ilościowe tych pieczęci, według wzoru określonego w załączniku Nr 17 i przesyłają je do Wojskowej Wytwórni Pieczęci, w terminie do dnia 31 stycznia za rok miniony.

Rozdział 12

Postępowanie z pieczęciami podczas ćwiczeń

§ 78. Jednostki wojskowe, wykonujące zadania w czasie ćwiczeń, zarówno w kraju jak i za granicą, używają wyłącznie pieczęci ćwiczebnych.

§ 79. Jednostki wojskowe biorące udział w ćwiczeniach, a nie posiadające pieczęci ćwiczebnych są zaopatrywane w pieczęcie ćwiczebne doraźnie przez właściwe dowództwa rodzajów Sit Zbrojnych, dowództwa okręgów wojskowych, Dowództwo Garnizonu Warszawa.
§ 80. Ewidencję pieczęci ćwiczebnych prowadzi tylko jednostka wojskowa, której pieczęcie te zostały przydzielone, na zasadach określonych dla pieczęci służbowych.

Rozdział 13

Zasady zaopatrywania jednostek wojskowych w plombownice

§ 81. 1. Decyzję w sprawie przydzielenia plombownicy, nie zawierającej numeru (nazwy) jednostki wojskowej podejmuje szef komórki organizacyjnej ministerstwa właściwej w sprawach logistyki.
2. Plombownica, o której mowa w ust. 1, przysługuje każdej osobie odpowiedzialnej materialnie za powierzone mienie.
3. W uzasadnionych przypadkach szef komórki organizacyjnej wymienionej w ust. 1 może dodatkowo przyznać plombownice niezależnie od należności zasadniczych.

§ 82. 1. Zaopatrywanie jednostek wojskowych w plombownice i kamienie do plombownic (godła i znaki - nie zawierające nazwy, numeru jednostki wojskowej lub numeru poczty polowej) oraz w plomby metalowe, należy do komórki organizacyjnej ministerstwa właściwej w sprawach logistyki.
2. Zaopatrywanie, o którym mowa w ust. 1, odbywa się poprzez organy logistyczne właściwych dowództw rodzaju Sil Zbrojnych, dowództw okręgów wojskowych oraz Dowództwa Garnizonu Warszawa.

§ 83. Koordynację i nadzór nad gospodarką w zakresie plombownic, kamieni do plombownic i plomb sprawuje w Sitach Zbrojnych RP szef komórki organizacyjnej ministerstwa właściwej w sprawach logistyki.

§ 84. W celu zaopatrzenia jednostek wojskowych w kamienie do plombownic, dowódca jednostki wojskowej przesyła pisemne zapotrzebowanie do komórki organizacyjnej właściwej w sprawach logistyki jednostki nadrzędnej.

§ 85. Wojskowe organy pocztowe są zaopatrywane w kamienie do plombownic (godła i znaki zawierające nazwy tych organów) przez Wojskową Wytwórnię Pieczęci według zapotrzebowania złożonego przez szefa komórki organizacyjnej właściwej w sprawach łączności, natomiast same plombownice (bez kamieni) organy te pobierają we właściwych oddziałach gospodarczych (zaopatrzenia).

§ 86. Niedozwolone jest samodzielne wykonywanie kamieni lub dokonywanie zmian na kamieniach (godłach i znakach) oraz używanie kamieni nietypowych, wykonanych poza Wojskową Wytwórnią Pieczęci.

§ 87. Właściwe organy zaopatrywania prowadzą we własnym zakresie ewidencję kamieni do plombownic, ich wymianę, niszczenie i postępowanie w przypadku ich utraty na zasadach ustalonych w rozdziale 5 instrukcji.

Rozdział 14

Kontrola w zakresie pieczęci

§ 88. Kontrolę przestrzegania przepisów instrukcji mają prawo zarządzić:
1) szef ~~Generalnego~~ Zarządu Zasobów Osobowych
- P1 - w zakresie wszystkich pieczęci;
2) szefowie sztabów w dowództwach rodzajów Sił Zbrojnych, dowództwach okręgów wojskowych oraz w Dowództwie Garnizonu Warszawa w podległych jednostkach wojskowych - w zakresie pieczęci przydzielonych przez te dowództwa;
3) szefowie sztabów związków taktycznych - w zakresie pieczęci w podległych jednostkach wojskowych;
4) dowódcy jednostek wojskowych - w zakresie pieczęci znajdujących się w podległej jednostce wojskowej;
5) inne organy - na podstawie odrębnych przepisów.

Dz U z 2003, Nr 4 poz. 47

§ 89. 1. Dowódca jednostki wojskowej jest obowiązany, podczas przeprowadzania rocznej kontroli stanu ochrony informacji niejawnych, dokonać komisyjnego sprawdzenia:

1) zgodności stanu faktycznego pieczęci urzędowych, pakietów z pieczęciami na czas wojny (bez ich otwierania) oraz pieczęci służbowych będących w jednostce wojskowej, ze stanem ewidencyjnym;
2) właściwego zaewidencjonowania w jednostce wojskowej pieczęci posiadanych i używanych przez użytkowników;
3) przestrzegania w jednostce wojskowej przepisów instrukcji.

2. Z przeprowadzonego sprawdzenia komisja sporządza protokół, który powinien zawierać opis stanu faktycznego stwierdzonego w toku sprawdzenia, w tym ustalone nieprawidłowości, ze wskazaniem przyczyn i skutków ich powstania oraz ewentualnie osób za nie odpowiedzialnych, a także wnioski i zalecenia pokontrolne.

ZAŁĄCZNIKI

Załączniki do „Instrukcji o pieczęciach używanych w resorcie obrony narodowej"

Załącznik Nr 1

WZÓR

WYKAZ PIECZĘCI

znajdujących się w .....
(nr lub nazwa jednostki wojskowej)

Lp.	Odcisk pieczęci	Opis pieczęci	Uwagi

.....
(data, stopień, imię i nazwisko dowódcy jednostki wojskowej)

Załącznik Nr 2

WZÓR

EWIDENCJA ODBITEK PIECZĘCI URZĘDOWYCH I SŁUŻBOWYCH

JW. Nr	
P	...../B

.....
(pełna nazwa instytucji, wojskowej jednostki organizacyjnej)

1	2	3	4	5	6	7	8	9	10 itd.
Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano .....
Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot .....
Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz .....
Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano .....
Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot .....
Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz .....
Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano .....
Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot .....
Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz .....
Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano .....
Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot .....
Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz .....
Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano	Wydano .....
Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot	Zwrot .....
Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz	Zniszcz .....

Załącznik Nr 3

WZÓR

EWIDENCJA PAKIETÓW ZAWIERAJĄCYCH PIECZĘCIE PRZEZNACZONE NA CZAS WOJNY

NUMER LUB NAZWA JEDNOSTKI WOJSKOWEJ	Nr poczty polowej (pakiety do kart tożsamości)	Nr ewid. pakietu z pełną nazwą jedn. wojskowej	PODSTAWA					Uwagi
			Ujęcia na ewidencji	Wydania do jednostki wojsk	Zwrotu z jednostki wojskowej	Przesunięcia wewnątrz RSZ OW	Zwrotu do WWP	
Przechowuje								
Przechowuje								
Przechowuje								
Przechowuje								

Załącznik Nr 4

WYKAZ PIECZĘCI SŁUŻBOWYCH DO TECZEK PRACY

.....
(cecha identyfikacyjna pieczęci)

.....
(numer pisma i data otrzymania pieczęci)

Numery rozpoznawcze pieczęci do teczek pracy																																							
1-100				101-200				201-300				301-400				401-500				501-600				601-700				701-800				801-900				900-999			
1	26	51	76	101	126	151	176	201	226	251	276	301	326	351	376	401	426	451	476	501	526	551	576	601	626	651	676	701	726	751	776	801	826	851	876	901	926	951	976
2	27	52	77	102	127	152	177	202	227	252	277	302	327	352	377	402	427	452	477	502	527	552	577	602	627	652	677	702	727	752	777	802	827	852	877	902	927	952	977
3	28	53	78	103	128	153	178	203	228	253	278	303	328	353	378	403	428	453	478	503	528	553	778	603	628	653	678	703	728	753	778	803	828	853	878	903	928	953	978
4	29	54	79	104	129	154	179	204	229	254	279	304	329	354	379	404	429	454	479	404	529	554	579	604	629	654	679	704	729	754	779	804	829	854	879	904	929	954	979
5	30	55	80	105	130	155	180	205	230	255	280	305	330	355	380	405	430	455	480	505	530	555	580	605	630	655	680	705	730	755	780	805	830	855	880	905	930	955	980
6	31	56	81	106	131	156	181	206	231	256	281	306	331	356	381	406	431	456	481	506	531	556	581	606	631	656	681	706	731	756	781	806	831	856	881	906	931	956	981
7	32	57	82	107	132	157	182	207	232	257	282	307	332	357	382	407	432	457	482	507	532	557	582	607	632	657	682	707	732	757	782	807	832	857	882	907	932	957	982
8	33	58	83	108	133	158	183	208	233	258	283	308	333	358	383	408	433	458	483	508	533	558	583	608	633	658	683	708	733	758	783	808	833	858	883	908	933	958	983
9	34	59	84	109	134	159	184	209	234	259	284	309	334	359	384	409	434	459	484	509	534	559	584	609	634	659	684	709	734	759	784	809	834	859	884	909	934	959	984
10	35	60	85	110	135	160	185	210	235	260	285	310	335	360	385	410	435	460	485	510	535	560	585	610	635	660	685	710	735	760	785	810	835	860	885	910	935	960	985
11	36	61	86	111	136	161	186	211	236	261	286	311	336	361	386	711	436	461	486	511	536	561	586	611	636	661	686	711	736	761	786	811	836	861	886	911	936	961	986
12	37	62	87	112	137	162	187	212	237	262	287	312	337	362	387	412	437	462	487	512	537	562	587	612	677	662	687	712	737	762	787	812	837	862	887	912	937	962	987
13	38	63	88	113	138	163	188	213	238	263	288	313	338	363	388	413	438	463	488	513	538	563	588	613	638	663	688	713	738	763	788	813	838	863	888	913	938	963	988
14	39	64	89	114	139	164	189	214	239	264	289	314	339	364	389	414	439	464	489	514	539	564	589	614	639	664	689	714	739	764	789	814	839	864	889	914	939	964	989
15	40	65	90	115	140	165	190	215	240	265	290	315	340	365	390	415	440	465	490	515	540	565	590	615	640	665	690	715	740	765	790	815	840	865	890	915	940	965	990
16	41	66	91	116	141	166	191	216	241	266	291	316	341	366	391	416	441	466	491	516	541	566	591	616	641	666	691	716	741	766	791	816	841	866	891	916	941	966	991
17	42	67	92	117	142	167	192	217	242	267	292	317	342	367	392	417	442	467	492	517	542	567	592	617	642	667	692	717	742	767	792	817	842	867	892	917	942	967	992
18	43	68	93	118	143	168	193	218	243	268	293	318	343	368	393	418	443	468	433	518	543	568	593	618	643	668	693	718	743	768	793	818	843	868	893	918	943	968	993
19	44	69	94	119	144	169	194	219	244	269	294	319	344	369	394	419	444	469	494	519	544	569	594	619	644	669	694	719	744	769	794	819	844	869	894	919	944	969	994
20	45	70	95	120	145	170	195	220	245	270	295	320	345	370	395	420	445	470	495	520	545	570	595	620	645	670	695	720	745	770	795	820	845	870	895	920	945	970	995
21	46	71	96	121	146	171	196	221	246	271	296	321	346	371	396	421	446	471	496	521	546	571	596	621	646	671	696	721	746	771	796	821	846	871	896	921	946	971	996
22	47	72	97	122	147	172	197	222	247	272	297	322	347	372	397	422	447	472	497	522	547	572	597	622	647	672	697	722	747	772	797	822	847	872	897	922	947	972	997
23	48	73	98	123	148	173	198	223	248	273	298	323	348	373	398	423	448	473	498	523	548	573	598	623	648	673	698	723	748	773	798	823	848	873	898	923	958	973	998
24	49	74	99	124	149	174	199	224	249	274	299	324	349	374	399	424	449	474	499	524	549	574	599	624	649	674	699	724	749	774	799	824	849	874	899	924	949	974	999
25	50	75	100	125	150	175	200	225	250	275	300	325	350	375	400	425	450	475	500	525	550	575	600	625	650	675	700	725	750	775	800	825	850	875	900	925	950	975	

Załącznik Nr 5

WZÓR

EWIDENCJA PIECZĘCI SŁUŻBOWYCH UTRACONYCH

Lp.	Podstawa	Treść utraconej pieczęci	Pieczęcie służbowe								Razem	Fakt utraty odnotowano w ewidencji	Do utraty pieczęci dopuścił:				Uwagi
			kauczukowe					metalowe									
	Nr wch. i data meldunku		tytułowo – nazwiskowe	firmujące	adresowe	do przepustek	inne	∅ 20 mm do teczek pracy	firmujące	inne			żołnierz zawodowy	żołnierz zasadniczej sł. wojsk.	pracownik wojska	nie ustalono	

Załącznik Nr 6

WZÓR

EWIDENCJA PIECZĘCI SŁUŻBOWYCH ZNISZCZONYCH

Lp.	Podstawa	Treść zniszczonych pieczęci	Pieczęcie służbowe								Razem	Fakt zniszczenia pieczęci odnotowano w ewidencji (nr kartoteki)	Data zniszczenia pieczęci	Uwagi
			kauczukowe					metalowe						
	Nr i data pisma wch. za którym otrzymano pieczęcie		tytułowo-nazwiskowe	firmujące	adresowe	do przepustek	inne	∅ 20 mm do teczek pracy	firmujące	inne				

Załącznik Nr 7

WZÓR

EWIDENCJA
pieczęci urzędowych i służbowych

w .....
(nr lub nazwa jednostki wojskowej)

Lp.	Od kogo otrzymano, numer i data pisma	Odbitka pieczęci	Odpis i nr fabryczny pieczęci metalowej	Data, stopień, imię i nazwisko oraz podpis otrzymującego pieczęć	Data i podpis prowadzącego ewidencję — przyjmującego pieczęć	Numer pisma, data i adresat, któremu wysłano — — przekazano pieczęcie	Uwagi Data i numer rozkazu unieważniającego zagubioną (utraconą) pieczęć
-1-	-2-	-3-	-4-	-5-	-6-	-7-	-8-

U w a g a:
W rubryce 5 w stosunku do każdej pozycji ujętej w ewidencji należy przewidzieć miejsce na pokwitowanie i datę otrzymania przez użytkownika pieczęci i w rubryce 6 na datę odbioru i podpis prowadzącego ewidencję w przypadku zwrotu pieczęci. Prowadzący ewidencję składa swój podpis w obecności zdającego pieczęć.

Załącznik Nr 8

WZÓR

EWIDENCJA
pakietów zawierających pieczęcie przeznaczone na czas wojny przechowywanych w .....
(nazwa lub nr jednostki wojskowej przechowującej pakiety)

Lp.	Wyszczególnienie jednostek wojskowych dla których przeznaczone są pakiety z pieczęciami na czas wojny	Numer ewidencyjny pakietu z pieczęciami na numer poczty polowej	Podstawa		Uwagi
		Numer ewidencyjny pakietu z pieczęciami na pełną nazwę jednostki	Ujęcie w ewidencji (numer i data pisma za którym doręczono pakiet do jednostki)	Skreślenie z ewidencji (numer i data pisma za którym wysłano — przekazano pakiet poza jednostkę)	
		P —			
		.....			

Załącznik Nr 9

WZÓR

WYKAZ
osób upoważnionych do posługiwania się pieczęciami urzędowymi i służbowymi

Lp.	Rodzaj i cecha pieczęci	Imię i nazwisko osoby upoważnionej	Nr rozkazu dziennego	Uwagi

„ZATWIERDZAM"

.....
(podpis dowódcy jednostki)

WZÓR

Załącznik Nr 10

PROTOKÓŁ
przekazania pieczęci do użytku bieżącego

dla .....
(nazwa lub numer jednostki wojskowej)

zgodnie z .....
(podstawa przekazania)

Lp.	Odbitki pieczęci	Opis pieczęci metalowej	Uwagi
-1-	-2-	-3-	-4-

Przekazał

.....
(stanowisko, stopień imię i nazwisko

.....
(podpis i data)

Przyjął:

.....
(stanowisko, stopień imię i nazwisko

.....
(podpis i data)

Załącznik Nr 11

WZÓR

.....
(nr lub nazwa jednostki wojskowej)

WYKAZ
nieaktualnych pieczęci przekazanych do zniszczenia

Lp.	Odbitka pieczęci	Opis pieczęci metalowej	Uwagi
-1-	-2-	-3-	-4-

.....
(data oraz podpis dowódcy)

Załącznik Nr 12

WZÓR

PROTOKÓŁ – MELDUNEK

dotyczący uszkodzenia (naruszenia) plomby lub pakietu zawierającego pieczęcie przeznaczone na czas wojny

Komisja w składzie:

Przewodniczący: .....

Członkowie: .....

.....

.....

stwierdziła uszkodzenie pakietu Nr ..... zawierającego pieczęcie na czas wojny (przechowywanego – doręczonego)*

.....
(nazwa lub nr jednostki przechowującej lub odbierającej pakiet)

Opis uszkodzenia pakietu: .....

Okoliczności uszkodzenia pakietu ustalone w toku postępowania wyjaśniającego: .....

.....

Osoba odpowiedzialna za przechowywanie pakietu: .....

Osoba, która dopuściła do uszkodzenia pakietu. .....

Wnioski komisji. .....

Pakiet zabezpieczono przez dodatkowe opakowanie, opieczętowanie pieczęcią do pakietów o treści ..... i przesłano do Wojskowej Wytwórni Pieczęci, wraz z jednym egzemplarzem protokołu.

Data i podpisy komisji:

.....

.....

.....

Rodzaj zastosowanych sankcji dyscyplinarnych i przedsięwzięć zapobiegających powtarzaniu się podobnych wypadków .....

.....
(data i podpis dowódcy wojskowej jednostki organizacyjnej)

---

* Niepotrzebne skreślić.

Załącznik Nr 13

WZÓR

PROTOKÓŁ
w sprawie uszkodzenia przesyłki zawierającej pieczęcie do użytku bieżącego

Komisja w składzie:

Przewodniczący: .....

Członkowie: .....

.....

.....

stwierdziła uszkodzenie doręczonej do .....
(nr lub nazwa jednostki wojskowej)

przesyłki zawierającej pieczęcie do użytku bieżącego nadanej przez .....

.....

Opis uszkodzenia: .....

Okoliczności uszkodzenia przesyłki ustalone w toku postępowania wyjaśniającego: .....

.....

Osoba, która dopuściła do uszkodzenia przesyłki: .....

Wnioski komisji: .....

Pakiet zabezpieczono i opieczętowano pieczęcią „do pakietów" o treści .....
i przesłano do Wojskowej Wytwórni Pieczęci wraz z jednym egzemplarzem protokołu.

Podpisy komisji:

.....

.....

.....

.....

Decyzja (rozkaz) dowódcy: .....

.....
(data i podpis)

Załącznik Nr 14

WZÓR

MELDUNEK
o utracie, zagubieniu lub zniszczeniu pieczęci urzędowej (służbowej)

Melduję, że w dniu ..... stwierdziłem brak pieczęci urzędowej (służbowej) o następującej treści ..... oznaczonej cechą .....

Okoliczności utraty pieczęci urzędowej ustalone w toku postępowania wyjaśniającego: .....

.....

.....

.....

Osoba upoważniona do posługiwania się utraconą pieczęcią urzędową (służbową): .....

.....
(stopień, imię i nazwisko oraz zajmowane stanowisko)

Osoba, która utraciła pieczęć: .....
(stopień, imię i nazwisko oraz zajmowane stanowisko)

Wynik postępowania wyjaśniającego: .....

.....

Zastosowane sankcje dyscyplinarne: .....

.....

Zastosowane przedsięwzięcia zapobiegające powtarzaniu się podobnych wypadków. .....

.....

Tytułem odpowiedzialności materialnej osoba winna utraty pieczęci wpłaciła do kasy jednostki wojskowej

..... kwotę ..... PLN, nr rachunku, (dowodu wpłaty)

.....

Pieczęć

.....
(podpis dowódcy jednostki)

Załącznik Nr 15

WZÓR

PROTOKÓŁ – MELDUNEK

w sprawie podrobienia lub wykonania w nieupoważnionym zakładzie pieczęci urzędowej lub służbowej

Melduję, że w dniu ..... stwierdzono w .....
(nazwa lub nr jednostki wojskowej)

użycie pieczęci podrobionej (wykonanej w nieupoważnionym zakładzie)

.....
(podać rodzaj i treść pieczęci)

w wyniku przeprowadzonego postępowania wyjaśniającego ustalono:

Pieczęć wykonano na zlecenie .....
(stopień, imię i nazwisko oraz stanowisko osoby zlecającej)

w zakładzie .....
(nazwa zakładu lub nazwa właściciela)

Pieczęć używana była do .....

.....

..... przez okres .....

Data i podpisy członków komisji:

.....

.....

.....

WZÓR

CZĘŚĆ I

Pieczęci urzędowych nie wolno odciskać na niewypełnionym formularzu i niepodpisanym piśmie lub dokumencie.

WYKAZ ZAWARTOŚCI PAKIETU

Nr .....

Niniejszy pakiet zawiera następujące pieczęcie przeznaczone na czas wojny dla:

1. .....

.....

2. .....

.....

3. .....

.....

4. .....

.....

Zawartość pakietu sprawdzono i pakiet opieczętowano w dniu .....

Wykonał: .....
(stopień, imię i nazwisko)

.....
(podpis)

Sprawdził: .....
(stopień, imię i nazwisko)

.....
(podpis)

U w a g i:

1. Pieczęcie zawarte w pakiecie należy odcisnąć w dalszej części niniejszego formularza przeznaczając na każdą odbitkę pieczęci jedną rubrykę. Przy odbitce pieczęci metalowej w rubryce „opis pieczęci" wpisać jej treść i cechę.
2. Po sprawdzeniu zawartości pakietu w jednostce wojskowej podpisane przez dowódcę lub szefa sztabu jednostki pokwitowanie odbioru pieczęci należy niezwłocznie przesłać jako przesyłkę niejawną bezpośrednio do Wojskowej Wytwórni Pieczęci.
3. Otrzymane pieczęcie należy ująć na ewidencję zgodnie z „Instrukcją o pieczęciach używanych w resorcie obrony narodowej".

CZĘŚĆ II

Załącznik Nr 16 (cd)

WOJSKOWA WYTWÓRNIA PIECZĘCI

POKWITOWANIE ODBIORU PIECZĘCI

przez .....
(nazwa lub numer wojskowej jednostki organizacyjnej)

Lp.	Odbitka pieczęci	Opis pieczęci metalowej	Uwagi

Zgodność zawartości pakietu
po jego otwarciu w jednostce
wojskowej komisyjnie sprawdzono.

Data .....

.....

.....

.....
(podpis członków komisji)

Pieczęcie znajdujące się

pakiet Nr .....

Przyjął:

.....
(data, stopień, imię i nazwisko oraz podpis dowódcy lub szefa sztabu jednostki wojskowej).

Załącznik Nr 17

ZESTAWIENIE ILOŚCIOWE

zniszczonych i zagubionych pieczęci służbowych do teczek pracy i do przepustek znajdujących się na ewidencji dowództw rodzajów sił zbrojnych, okręgów wojskowych oraz Dowództwa Garnizonu Warszawa

Lp.	Seria	Stan na dzień 31 grudnia roku poprzedniego	Rok rozliczany		Stan na dzień 31 grudnia roku rozliczanego	Uwagi
			Zagubiono szt.	Zniszczono szt.		

.....
(podpis sporządzającego)

DECYZJA Nr 20/MON

MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie powoływania pełnomocników, zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz inspektorów bezpieczeństwa teleinformatycznego w Ministerstwie Obrony Narodowej oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w związku z art. 18 i art. 64 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) zwanej dalej „ustawą", w celu realizacji zamierzeń związanych z powołaniem pełnomocników do spraw ochrony informacji niejawnych i ich zastępców, administratorów systemów i sieci teleinformatycznych oraz inspektorów bezpieczeństwa teleinformatycznego ustala się, co następuje:

1. Za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych w Ministerstwie Obrony Narodowej odpowiada Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz podległy mu pion ochrony.

2. Za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowych lub przez niego nadzorowanych odpowiadają pełnomocnicy kierowników tych jednostek organizacyjnych do spraw ochrony informacji niejawnych, zwani dalej „pełnomocnikami ochrony" oraz podległe im piony ochrony.

3. Struktury organizacyjne pionów ochrony jednostek organizacyjnych, o których mowa w pkt 2, określa etat danej jednostki.

4. Stanowisko służbowe pełnomocnika ochrony jest stanowiskiem etatowym. Pełnomocnik ochrony podlega bezpośrednio kierownikowi jednostki organizacyjnej (dowódcy, szefowi, dyrektorowi, kierownikowi, komendantowi instytucji wojskowej lub jednostki).

5. W jednostce organizacyjnej szczebla pułku (równorzędnego) i niższego dopuszcza się połączenie stanowiska pełnomocnika ochrony z innym stanowiskiem służbowym, usytuowanym w etacie jednostki wojskowej.

6. Osoby pełniące służbę lub zatrudnione na stanowisku, o którym mowa w pkt 5, wykonując zadania pełnomocnika ochrony podlegają bezpośrednio kierownikowi jednostki organizacyjnej (dowódcy, szefowi, dyrektorowi, kierownikowi, komendantowi instytucji wojskowej lub jednostki).

7. W Ministerstwie Obrony Narodowej, dowództwach rodzajów Sił Zbrojnych, okręgów wojskowych, korpusów, dywizji, brygad (równorzędnych), w Komendzie Głównej Żandarmerii Wojskowej oraz w Dowództwie Operacyjnym i Dowództwie Garnizonu Warszawa powołuje się zastępcę pełnomocnika ochrony.

8. W jednostkach organizacyjnych, nie wymienionych w pkt 7, kierownik tej jednostki może powołać zastępcę pełnomocnika ochrony.

9. Stanowisko zastępcy pełnomocnika ochrony może być stanowiskiem nieetatowym.

10. Zastępca pełnomocnika ochrony realizuje funkcję pełnomocnika ochrony podczas jego czasowej nieobecności, na podstawie decyzji (rozkazu) kierownika (dowódcy) jednostki organizacyjnej, o której mowa w pkt 1 i 2.

11. Kierownik jednostki organizacyjnej, o której mowa w pkt 1 i 2, może, uwzględniając potrzeby tej jednostki organizacyjnej, powierzyć pełnomocnikowi ochrony wykonywanie innych zadań, nie związanych bezpośrednio z ochroną informacji niejawnych, o ile ich realizacja nie naruszy prawidłowego wykonywania zadań, określonych w art. 18 ust. 4 ustawy.

12. Pełnomocnikiem ochrony i jego zastępcą nie może być kierownik kancelarii tajnej, kancelarii tajnej zagranicznej oraz innej komórki organizacyjnej odpowiedzialnej za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, a także osoba będąca pracownikiem tej komórki wewnętrznej.

13. Osobę lub zespół osób odpowiedzialnych za funkcjonowanie oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne w ramach danej jednostki organizacyjnej, o której mowa w pkt 1 i 2, zwane dalej „administratorem systemu", wyznacza kierownik (dowódca) tej jednostki organizacyjnej. Wzór decyzji (rozkazu) w sprawie wyznaczenia administratora systemu określa załącznik do decyzji.

14. Administratora systemu, w którym są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, obejmującego swoim zasięgiem komórkę organizacyjną Ministerstwa Obrony Narodowej, wyznacza kierownik tej komórki, natomiast administratora systemu obejmującego swoim zasięgiem co najmniej dwie komórki organizacyjne Ministerstwa Obrony Narodowej, wyznacza Dyrektor Generalny Ministerstwa Obrony Narodowej, na wspólny wniosek kierowników tych komórek organizacyjnych.

15. Administratora systemu, w którym są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, obejmującego swoim zasięgiem jednostki organizacyjne podległe dowódcom rodzajów Sił Zbrojnych, wyznaczają ci dowódcy na wniosek osoby odpowiedzialnej za organizację i funkcjonowanie systemu, zwanego dalej „organizatorem systemu".

16. Administratora systemu, w którym są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, wykraczającego swoim zasięgiem poza Ministerstwo Obrony Narodowej lub rodzaj Sił Zbrojnych, wyznacza Minister Obrony Narodowej na wniosek organizatora systemu.

17. O wyznaczeniu osoby na stanowisko lub do pełnienia funkcji (wykonywania zadań) administratora systemu, o których mowa w pkt. 14 i 15, informuje się właściwego pełnomocnika ochrony.

18. Administratorem systemu nie może być pracownik pionu ochrony, z zastrzeżeniem pkt 19.

19. Przepis pkt 18 nie dotyczy systemów i sieci teleinformatycznych eksploatowanych w pionach ochrony jednostek organizacyjnych, o których mowa w pkt 1 i 2.

20. Żołnierzom zawodowym wyznaczonym do pełnienia funkcji administratora systemu, za realizację powierzonych im czynności może być wypłacane dodatkowe wynagrodzenie na zasadach i w trybie określonych w przepisach o służbie wojskowej żołnierzy zawodowych, a pracownikom wyznaczonym do pełnienia tej funkcji – na zasadach określonych w przepisach o wynagrodzeniu pracowników.

21. Kierownik jednostki organizacyjnej, w której są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne w systemach lub sieciach teleinformatycznych, na wniosek pełnomocnika ochrony, wyznacza pracownika lub pracowników pionu ochrony do pełnienia funkcji inspektora lub inspektorów bezpieczeństwa teleinformatycznego, zwanego dalej „inspektorem

bezpieczeństwa teleinformatycznego", odpowiedzialnych za bieżącą kontrolę zgodności funkcjonowania tej sieci i systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

22. Inspektorów bezpieczeństwa teleinformatycznego w Ministerstwie Obrony Narodowej wyznacza Dyrektor Generalny Ministerstwa Obrony Narodowej na wniosek Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, spośród żołnierzy zawodowych i pracowników Biura Ochrony Informacji Niejawnych.

23. Inspektora bezpieczeństwa teleinformatycznego, koordynującego bieżącą działalność kontrolną w zakresie zgodności funkcjonowania systemów lub sieci teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji, obejmujących swoim zasięgiem jednostki organizacyjne podległe dowódcy rodzaju Sił Zbrojnych, wyznacza ten dowódca, na wniosek pełnomocnika ochrony dowódcy rodzaju Sił Zbrojnych, spośród żołnierzy zawodowych i pracowników pionu ochrony.

24. Inspektora bezpieczeństwa teleinformatycznego, koordynującego bieżącą działalność kontrolną w zakresie zgodności funkcjonowania systemów lub sieci teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzeganiem procedur bezpiecznej eksploatacji, obejmujących swoim zasięgiem jednostki organizacyjne, o których mowa w pkt 1 i 2, z zastrzeżeniem pkt 22 i 23, wyznacza Minister Obrony Narodowej na wniosek Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, spośród żołnierzy zawodowych i pracowników Biura Ochrony Informacji Niejawnych.

25. W przypadkach uzasadnionych względami etatowymi, funkcję inspektora bezpieczeństwa teleinformatycznego może pełnić pełnomocnik ochrony.

26. Żołnierzom zawodowym wyznaczonym do pełnienia funkcji inspektora bezpieczeństwa teleinformatycznego za realizację powierzonych im czynności może być wypłacane dodatkowe wynagrodzenie na zasadach i w trybie określonych w przepisach o służbie wojskowej żołnierzy zawodowych, a pracownikom wyznaczonym do pełnienia tej funkcji – na zasadach określonych w przepisach o wynagrodzeniu pracowników.

27. Traci moc decyzja Nr 30/MON Ministra Obrony Narodowej z dnia 8 marca 2000 r. w sprawie powołania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu Obrony Narodowej (Dz. Rozk. MON poz. 75, Dz. Urz. MON z 2001 r. Nr 6, poz. 57 i z 2003 r. Nr 19, poz. 205).

28. Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

ZAŁĄCZNIKI

*)KIEROWNIK JEDNOSTKI

(KOMÓRKI ORGANIZACYJNEJ *decyzja (rozkaz)

.....

(kierownika jednostki (komórki organizacyjnej)

z dnia .....

w sprawie wyznaczenia administratora systemu

***) w (obejmującego swoim zasięgiem)**

.....

(* nazwa jednostki (komórek organizacyjnej)

Na podstawie art. 64 ust. 1 pkt 1 ustawy z dnia 22 stycznia 1999r. o ochronie informacji niejawnych (Dz. U z 2005r. Nr 196, poz. 1631).

**) na wniosek

.....

(nazwy stanowisk kierowników komórek (jednostek) organizacyjnych)

wyznaczam

..... z .....

(stopień, imię nazwisko) (nazwa komórki organizacyjnej (wewnętrznej)

do pełnienia obowiązków administratora systemu i czynię go odpowiedzialnym za funkcjonowanie oraz przestrzeganie zasad i wymagań bezpieczeństwa systemu (sieci) teleinformatycznego .....

(nazwa systemu (sieci))

przewidzianego do przetwarzania informacji niejawnych do klauzuli

.....

(klauzula tajności)

zlokalizowanego w .....

(nazwa kompleksu, nr bloku i pomieszczenia)

.....

(podpis kierownika jednostki organizacyjnej)

*) - wpisać właściwy

*) – niepotrzebne skreślić

DECYZJA Nr 21/MON

MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej

Na podstawie § 2 pkt 6, 13 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w celu realizacji zamierzeń związanych ze sprawowaniem nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej, ustala się, co następuje:

1. Nadzór nad ochroną informacji niejawnych w komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych realizuje się w formie :

1) kontroli stanu ochrony informacji niejawnych;
2) oceny stanu ochrony informacji niejawnych;
3) decyzji wynikających z oceny , o której mowa w ppkt 2.

2. Kontrole stanu ochrony informacji niejawnych w jednostkach (komórkach) organizacyjnych, o których mowa w pkt 1, przeprowadza się w celu:

1) ustalenia stanu faktycznego realizacji zadań w zakresie ochrony informacji niejawnych oraz oceny przestrzegania przepisów wydanych w tym zakresie;
2) określenia przyczyn i skutków ewentualnych naruszeń przepisów o ochronie informacji niejawnych oraz wskazania osób za to odpowiedzialnych;
3) wskazania sposobów umożliwiających usunięcie stwierdzonych nieprawidłowości;
4) sformułowania i przedłożenia przełożonym wniosków oraz zaleceń dotyczących doskonalenia systemu ochrony informacji niejawnych.

3. Kontrole, o których mowa w pkt 2, przeprowadza się jako:

1) kontrole bieżące;
2) kontrole wyrywkowe;
3) kontrole półroczne;
4) kontrole roczne;
5) kontrole problemowe.

4. Do przeprowadzenia kontroli, o których mowa w pkt 3 ppkt 5, uprawnia imienne upoważnienie wystawione przez zarządzającego kontrolę, wraz z legitymacją służbową lub dowodem osobistym. Wzór upoważnienia określa załącznik Nr 1 do decyzji.

5. Kontrolę bieżącą stanu ochrony informacji niejawnych prowadzi się w celu dokonania oceny przestrzegania przez wykonawców i wykonawców technicznych zasad wykonywania, oznaczania, ewidencjonowania, przechowywania i udostępniania materiałów zawierających informacje niejawne.

6. Kontrole bieżące prowadzi pion ochrony jednostki organizacyjnej oraz bezpośredni przełożeni wykonawców.

7. Fakt przeprowadzenia kontroli bieżącej kontrolujący odnotowuje w „Dzienniku wykonawcy" kontrolowanego w postaci wpisu, który powinien zawierać datę kontroli, stopień imię i nazwisko osoby kontrolującej oraz wynik kontroli i zalecenia.

8. O wynikach kontroli bieżących przeprowadzonych przez pion ochrony powiadamia się przełożonych osób kontrolowanych.

9. Kontrolę wyrywkową stanu ochrony informacji niejawnych prowadzi się w celu sprawdzenia:

1) zgodności stanu faktycznego materiałów niejawnych posiadanych przez wykonawców ze stanem ewidencyjnym;
2) stanu przestrzegania przepisów o ochronie informacji niejawnych w zakresie wytwarzania, przetwarzania, ewidencjonowania, przechowywania i udostępniania dokumentów niejawnych stanowiących tajemnicę państwową i służbową.

10. Kontrolę wyrywkową, o której mowa w pkt 3, w komórkach wewnętrznych jednostki (komórki), o której mowa w pkt 1, przeprowadza pion ochrony, według planu zatwierdzonego przez kierownika tej jednostki (komórki).

11. Z kontroli wyrywkowej sporządza się notatkę, której wzór zawiera załącznik Nr 2 do decyzji.

12. Kontrolę półroczną stanu ochrony informacji niejawnych prowadzi się w celu dokonania oceny:

1) zgodności stanu faktycznego materiałów niejawnych, posiadanych przez wykonawców, ze stanem ewidencyjnym;
2) stanu przestrzegania przepisów o ochronie informacji niejawnych w zakresie wytwarzania, ewidencjonowania, przechowywania i niszczenia materiałów niejawnych;
3) wykonania zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli stanu ochrony informacji niejawnych.

13. Kontrolę półroczną prowadzą przełożeni w stosunku do bezpośrednio podległych im wykonawców.

14. Kierownicy kancelarii tajnych, tajnych - zagranicznych oraz innych komórek przechowujących i prowadzących ewidencję materiałów niejawnych, sporządzają dla osób, o których mowa w pkt 13, wykazy materiałów niejawnych pobranych przez wykonawców.

15. Kontrolę półroczną przeprowadza się corocznie, do dnia 30 czerwca, z zastrzeżeniem pkt 16. Termin rozpoczęcia kontroli podaje się w rozkazie dziennym (decyzji).

16. W uzasadnionych przypadkach kierownik jednostki (komórki), o której mowa w pkt 1, może przesunąć termin zakończenia kontroli, o którym mowa w pkt 15, nie więcej jednak niż o 30 dni.

17. W razie nieobecności wykonawcy w czasie trwania kontroli półrocznej, kontrolę w stosunku do tej osoby przeprowadza się bezpośrednio po jej powrocie do miejsca służby (pracy).

18. Wyniki kontroli półrocznej osoby kontrolujące dokumentują w notatce, której wzór zawiera załącznik Nr 3 do decyzji.

19. Notatkę zbiorczą o wynikach kontroli półrocznej przeprowadzonej w jednostce (komórce), o której mowa w pkt 1, na podstawie notatek, o których mowa w pkt 18, sporządza pełnomocnik ochrony i zapoznaje z jej treścią kierownika tej jednostki (komórki). Wzór notatki zawiera załącznik Nr 4 do decyzji.

20. Notatkę zbiorczą o wynikach kontroli półrocznej stanu ochrony informacji niejawnych przeprowadzonej w Ministerstwie Obrony Narodowej sporządza Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, na podstawie notatek zbiorczych otrzymanych od kierowników komórek organizacyjnych Ministerstwa Obrony Narodowej i przedkłada ją Dyrektorowi Generalnemu Ministerstwa Obrony Narodowej do zapoznania się, corocznie, w terminie do dnia 15 lipca.

21. Kontrola roczna jest podstawową formą sprawdzenia realizacji zadań w zakresie ochrony informacji niejawnych przez jednostkę (komórkę), o której mowa w pkt 1. Zakres przedmiotowy kontroli rocznej zawiera załącznik Nr 5 do decyzji.

22. W czasie trwania kontroli rocznej w jednostce organizacyjnej nie prowadzi się innych kontroli stanu ochrony informacji niejawnych.

23. Kontrolę roczną przeprowadza komisja wyznaczona rozkazem dziennym albo decyzją kierownika jednostki (komórki), o której mowa w pkt 1, z uwzględnieniem następujących zasad:

1) skład osobowy komisji powinien wynosić co najmniej trzy osoby;
2) osoby wchodzące w skład komisji powinny posiadać poświadczenia bezpieczeństwa, a w przypadku kontroli materiałów Unii Europejskiej także stosowne certyfikaty bezpieczeństwa, uprawniające do dostępu do informacji o klauzuli równej lub wyższej niż dokumenty podlegające kontroli;
3) termin ważności poświadczeń i certyfikatów nie może upływać przed zakończeniem kontroli rocznej stanu ochrony informacji niejawnych;
4) osoby wyznaczone do przeprowadzenia kontroli materiałów kryptograficznych dodatkowo powinny posiadać certyfikat upoważnienia kryptograficznego (CUK);
5) do składu komisji nie wyznacza się osób odpowiedzialnych za prowadzenie ewidencji materiałów niejawnych w jednostkach (komórkach), o których mowa w pkt 1, objętych kontrolą.

24. Kontrolę roczną w Ministerstwie Obrony Narodowej przeprowadza komisja wyznaczona decyzją Ministra Obrony Narodowej. Do składu komisji wyznacza się osoby pełniące służbę lub zatrudnione w komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych obsługiwanych przez kancelarie tajne i tajne zagraniczne Biura Ochrony Informacji Niejawnych.

25. Decyzja albo rozkaz, o których mowa w pkt 23 i 24, powinny zawierać w szczególności następujące dane:

1) imienny skład osobowy komisji z uwzględnieniem numerów poświadczeń i certyfikatów bezpieczeństwa, ich klauzul oraz terminów ważności;
2) termin rozliczenia wykonawców z materiałów niejawnych;
3) termin przygotowania do kontroli rocznej kancelarii tajnych, tajnych zagranicznych oraz innych komórek przechowujących i prowadzących ewidencję materiałów niejawnych;
4) termin rozpoczęcia i zakończenia kontroli rocznej.

26. Pełnomocnik do spraw ochrony informacji niejawnych odpowiada za organizację i przebieg kontroli rocznej w jednostce (komórce), o której mowa w pkt 1, w szczególności za:

1) opracowanie projektu rozkazu albo decyzji, o których mowa w pkt 23 i 24;
2) przeszkolenie członków komisji kontroli rocznej w zakresie metodyki prowadzenia kontroli;
3) przeszkolenie kierowników kancelarii tajnych, tajnych zagranicznych oraz innych komórek przechowujących i prowadzących ewidencję materiałów niejawnych w zakresie ich przygotowania do kontroli rocznej;
4) sprawowanie nadzoru służbowego nad realizacją czynności kontrolnych wykonywanych przez komisję.

27. Wyniki kontroli rocznej komisje, o których mowa w pkt 23 i 24, dokumentują w protokole, którego układ przedstawia załącznik Nr 6 do decyzji. Kierownik jednostki (komórki), o której mowa w pkt 1, potwierdza swoim podpisem na protokole fakt zapoznania się z jego treścią.

28. Wyniki kontroli rocznej stanu ochrony informacji niejawnych przeprowadzonej w jednostce (komórce), o której mowa w pkt 1, przedkłada jej kierownik swojemu bezpośredniemu przełożonemu w formie meldunku, corocznie, w terminie do dnia 15 marca. Wzór meldunku zawiera załącznik Nr 7.

29. Kierownicy jednostek (komórek), o których mowa w pkt 1, bezpośrednio podporządkowanych Ministrowi Obrony Narodowej oraz przewodniczący komisji, o której mowa w pkt 24, przedkładają Ministrowi Obrony Narodowej meldunki o wynikach kontroli rocznej stanu ochrony informacji niejawnych za pośrednictwem Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

30. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych przedkłada Ministrowi Obrony Narodowej meldunek zbiorczy o wynikach kontroli rocznej stanu ochrony informacji niejawnych przeprowadzonej w komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej – corocznie, w terminie do dnia 1 kwietnia.

31. Meldunki zbiorcze o wynikach kontroli rocznej stanu ochrony informacji niejawnych, według wzoru zawartego w załączniku Nr 8, przesyłają do Szefa Służby Kontrwywiadu Wojskowego, corocznie, w terminie do dnia 15 kwietnia.:

1) osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej – za podległe jednostki organizacyjne;
2) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych – za Ministerstwo Obrony Narodowej i jednostki organizacyjne bezpośrednio podporządkowane Ministrowi Obrony Narodowej;
3) dowódcy rodzajów Sił Zbrojnych Rzeczypospolitej Polskiej, zwanych dalej „Siłami Zbrojnymi" oraz kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej – za jednostki organizacyjnie bezpośrednio podporządkowane;
4) kierownicy komórek organizacyjnych Ministerstwa Obrony Narodowej – za bezpośrednio podporządkowane jednostki organizacyjne.

32. Kontrole problemowe są podstawową formą sprawdzania stanu ochrony informacji niejawnych w jednostkach (komórkach), o których mowa w pkt 1.

33. Minister Obrony Narodowej zarządza przeprowadzenie kontroli problemowych stanu ochrony informacji niejawnych w jednostkach (komórkach), o których mowa w pkt 1.
Do zarządzania i przeprowadzania kontroli problemowych są uprawnieni ponadto:

1) Sekretarz Stanu, podsekretarze stanu w Ministerstwie Obrony Narodowej – w podległych jednostkach organizacyjnych;
2) Szef Sztabu Generalnego WP – w komórkach organizacyjnych tworzących Sztab Generalny Wojska Polskiego oraz w jednostkach organizacyjnych podległych dowódcom rodzajów Sił Zbrojnych, Dowódcy Dowództwa Operacyjnego i Dowódcy Garnizonu Warszawa;
3) Dyrektor Generalny Ministerstwa Obrony Narodowej – w komórkach organizacyjnych Ministerstwa Obrony Narodowej;
4) dowódcy rodzajów Sił Zbrojnych, Dowódca Dowództwa Operacyjnego, Dowódca Garnizonu Warszawa, Szef Wojskowych Służb Informacyjnych, Komendant Główny Żandarmerii Wojskowej, dowódcy okręgów wojskowych, związków taktycznych – w podległych jednostkach organizacyjnych;
5) Szef Służby Kontrwywiadu Wojskowego – w jednostkach (komórkach), o których mowa w pkt 1;
6) kierownicy komórek organizacyjnych Ministerstwa Obrony Narodowej – w podległych jednostkach organizacyjnych.

34. Kontrole problemowe stanu ochrony informacji niejawnych przeprowadzają:

1) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych na zarządzenie Ministra Obrony Narodowej – w jednostkach (komórkach), o których mowa w pkt 1, a bez takiego zarządzenia - w jednostkach organizacyjnych podległych osobom, o których mowa w pkt 33 ppkt 1, 2, 3 i 6;

2) pełnomocnicy ochrony wyznaczeni przez osoby wymienione w pkt 33,
z zastrzeżeniem ppkt 1.

35. Kontrola problemowa stanu ochrony informacji niejawnych jest prowadzona w celu dokonania oceny:

1) stanu realizacji zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli stanu ochrony informacji niejawnych;
2) stanu zabezpieczenia informacji niejawnych;
3) przestrzegania przepisów o ochronie informacji niejawnych;
4) stanu zabezpieczenia systemów i sieci teleinformatycznych, w których są przetwarzane, wytwarzane, przechowywane lub przekazywane informacje niejawne;
5) ochrony fizycznej jednostki organizacyjnej.

36. Szczegółowy zakres przedmiotowy kontroli problemowej stanu ochrony informacji niejawnych zawiera załącznik Nr 9 do decyzji. W uzasadnionych przypadkach, osoby zarządzające kontrolę mogą ograniczyć jej zakres.

37. W przypadku wystąpienia istotnych zagrożeń w zakresie bezpieczeństwa informacji niejawnych, osoby wymienione w pkt 33, mogą zarządzić kontrolę nie ujętą w planie.

38. Planowanie kontroli problemowych stanu ochrony informacji niejawnych koordynuje Szef Służby Kontrwywiadu Wojskowego.

39. Szef Służby Kontrwywiadu Wojskowego, jako koordynator zamierzeń kontrolnych, ma prawo dokonywania zmian terminów planowanych przedsięwzięć kontrolnych, po uzgodnieniu z osobami, o których mowa w pkt 33.

40. Kontrole problemowe stanu ochrony informacji niejawnych w komórce (jednostce), o której mowa w pkt 1, powinny być prowadzone w miarę potrzeb.

41. Czas trwania kontroli problemowej ustala każdorazowo zarządzający kontrolę - w zależności od potrzeb.

42. Podstawę do przeprowadzenia kontroli problemowej stanu ochrony informacji niejawnych stanowi plan jej przeprowadzenia, zatwierdzony przez osoby, o których mowa w pkt 33.

43. Wyniki kontroli dokumentuje się w protokole, który powinien zawierać opis stanu faktycznego stwierdzonego w czasie kontroli, w tym ustalone nieprawidłowości i przyczyny ich powstania, osoby za to odpowiedzialne, wnioski oraz zalecenia pokontrolne.

44. Protokół, o którym mowa w pkt 43, sporządza się w trzech jednobrzmiących egzemplarzach, z przeznaczeniem dla:

1) zarządzającego kontrolę;
2) kierownika kontrolowanej komórki lub jednostki organizacyjnej;
3) przełożonego kierownika kontrolowanej jednostki lub komórki organizacyjnej.

45. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych przedkłada Ministrowi Obrony Narodowej protokoły z przeprowadzonych przez siebie kontroli problemowych stanu ochrony informacji niejawnych w jednostkach organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej. Protokoły z kontroli problemowych przeprowadzonych w Ministerstwie Obrony Narodowej pełnomocnik ten przedkłada Ministrowi Obrony Narodowej poprzez Dyrektora Generalnego Ministerstwa Obrony Narodowej.

46. W zakresie nieregulowanym w decyzji, do planowania, koordynowania, przeprowadzania i dokumentowania wyników kontroli problemowych stanu ochrony informacji niejawnych oraz postępowania pokontrolnego stosuje się przepisy decyzji Nr 149/MON Ministra Obrony Narodowej z dnia 12 maja 2005 r. w sprawie działalności kontrolnej w resorcie obrony narodowej (Dz. Urz. MON Nr 10, poz. 83).

47. Kierownicy jednostek, o których mowa w pkt 1, opracowują ocenę stanu ochrony informacji niejawnych, która stanowi kompleksową formę rozliczenia się z przestrzegania przepisów o ochronie informacji niejawnych oraz podstawę do doskonalenia systemu ochrony informacji niejawnych w tych jednostkach.

48. Ocenę stanu ochrony informacji niejawnych w komórkach organizacyjnych Ministerstwa Obrony Narodowej opracowuje Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

49. Ocenę, o której mowa w pkt 47 i 48, opracowuje się na podstawie:

1) wyników kontroli stanu ochrony informacji niejawnych przeprowadzonych w jednostce (komórce), o której mowa w pkt 1;
2) meldunków o naruszeniu przepisów o ochronie informacji niejawnych;
3) ocen stanu ochrony informacji niejawnych nadesłanych przez podległe jednostki organizacyjne;
4) wystąpień lub postanowień prokuratorów wojskowych oraz orzeczeń sądów wojskowych;
5) informacji uzyskanych od jednostek organizacyjnych Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej i Policji.

50. Ocena stanu ochrony informacji niejawnych powinna obejmować:

1) zagrożenia mogące mieć wpływ na bezpieczeństwo informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w jednostce (komórce), o której mowa w pkt 1;

a) ze strony obcych służb specjalnych,
b) ze strony przestępczości zorganizowanej i terroryzmu;

2) organizację systemu ochrony informacji niejawnych w jednostce (komórce), o której mowa w pkt 1, w szczególności:

a) działalność pionu ochrony,
b) wydawanie aktów prawnych regulujących problematykę ochrony informacji niejawnych,
c) sprawowanie nadzoru w zakresie ochrony informacji niejawnych,
d) działalność szkoleniową;

3) funkcjonowanie systemu ochrony informacji niejawnych w jednostce (komórce), o której mowa w pkt 1, a zwłaszcza:

a) przestrzeganie przepisów o ochronie informacji niejawnych,
b) ochronę fizyczną tej jednostki (komórki),
c) ochronę informacji niejawnych w systemach i sieciach teleinformatycznych,
d) ochronę informacji niejawnych podczas ćwiczeń i treningów sztabowych,
e) ochronę informacji niejawnych w kontaktach zagranicznych;

4) wnioski oraz zadania dla komórek organizacyjnych i osób funkcyjnych, których realizacja jest niezbędna do podniesienia poziomu ochrony informacji niejawnych w tej jednostce (komórce).

51. Ocenę stanu ochrony informacji niejawnych za dany rok kalendarzowy omawia się na posiedzeniu organu kolegialnego jednostki organizacyjnej oraz przesyła bezpośredniemu przełożonemu, do końca marca następnego roku kalendarzowego.

52. Kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej przedkładają ocenę, o której mowa w pkt 51, Ministrowi Obrony Narodowej za pośrednictwem Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, corocznie, w terminie do dnia 30 kwietnia.

53. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych przedkłada Ministrowi Obrony Narodowej, corocznie, w terminie do dnia 15 maja, ocenę stanu ochrony informacji niejawnych w Ministerstwie Obrony Narodowej.

54. Zbiorcze oceny stanu ochrony informacji niejawnych za podległe jednostki organizacyjne opracowują osoby wymienione w pkt 31, z wyłączeniem jednostki organizacyjnej wymienionej w pkt I poz. 9 wykazu jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych wraz z ich bezpośrednim podporządkowaniem, określonym w załączniku do decyzji Nr 53/MON Ministra Obrony Narodowej z dnia 3 marca 2005 r. w sprawie bezpośredniego podporządkowania jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. Urz. MON Nr 4, poz. 32) i przesyłają Szefowi Służby Kontrwywiadu Wojskowego, corocznie, w terminie do dnia 15 maja.

55. Szef Służb Kontrwywiadu Wojskowego przygotowuje zbiorczą ocenę stanu ochrony informacji niejawnych w resorcie obrony narodowej i przedkłada ją Ministrowi Obrony Narodowej, corocznie, w terminie do dnia 15 czerwca.

56. Traci moc decyzja Nr 182/MON Ministra Obrony Narodowej z dnia 6 października 2000 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie Obrony Narodowej (Dz. Rozk. MON, poz. 112 i Dz. Urz. MON z 2002 r. Nr 25, poz. 219).

57. Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Załącznik Nr 1

WZÓR

....dnia.....
(nazwa organu zarządzającego kontrolę)

Upoważnienie Nr.....

Na podstawie pkt 33 decyzji Nr...../MON Ministra Obrony Narodowej z dnia..... w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (Dz. Urz. MON Nr....., poz. .....)

upoważniam:

.....
(stopień, imię i nazwisko kontrolera)

do przeprowadzenia kontroli problemowej stanu ochrony informacji niejawnych w:.....

.....
(nazwa i adres kontrolowanej jednostki)

Upoważnienie ważne jest za okazaniem legitymacji służbowej (dowodu osobistego).
Ważność upoważnienia upływa z dniem .....

.....
(stanowisko, stopień, imię i nazwisko,
podpis osoby wydającej upoważnienie)

m.p.

(pieczęć okrągła organu
zarządzającego kontrolę)

Ważność upoważnienia przedłuża się do dnia .....

.....
(stanowisko, stopień, imię i nazwisko,
podpis osoby wydającej upoważnienie)

m.p.

(pieczęć okrągła organu
zarządzającego kontrolę)

Załącznik Nr 2

WZÓR

NOTATKA

o wynikach kontroli wyrywkowej stanu ochrony informacji niejawnych przeprowadzonej w dniach

.....w .....
(nazwa komórki organizacyjnej)

1. Zgodnie z planem kontroli wyrywkowych na rok ..... (Nr wych. ..... z dnia .....) zespół kontrolujący w składzie (ewentualnie stanowisko i nazwisko osoby kontrolującej):

   – .....

   – .....

   – .....

   przeprowadził w dniu ..... w .....
   (nazwa komórki organizacyjnej)

   kontrolę wyrywkową stanu ochrony informacji niejawnych. Kontrolą objęto następujące osoby (wyszczególnić stopnie wojskowe, imiona i nazwiska):

   – .....

   – .....

2. Na podstawie urządzeń ewidencyjnych (wymienić nazwy urządzeń) stwierdzono, iż stan faktyczny dokumentów niejawnych posiadanych przez skontrolowanych wykonawców jest zgodny (ewentualnie niezgodny) ze stanem ewidencyjnym (w razie stwierdzenia braku dokumentów podać ich klauzulę tajności, numery ewidencyjne, nazwy dokumentów lub czego dotyczą, przez kogo zostały pobrane oraz datę pobrania).
3. Podczas kontroli stwierdzono niedociągnięcia w zakresie przestrzegania przez wykonawców przepisów o ochronie informacji niejawnych (wymienić niedociągnięcia, przyczyny ich powstania, skutki oraz określić osoby odpowiedzialne).
4. Wnioski i zalecenia pokontrolne.

.....
(podpis kontrolującego)

Załącznik Nr 3

WZÓR

NOTATKA

o wynikach kontroli półrocznej stanu ochrony informacji niejawnych

Zgodnie z rozkazem dziennym (decyzją) Nr.....

..... z dnia.....
(nazwa stanowiska kierownika komórki (jednostki) organizacyjnej)

szef (dowódca, dyrektor, kierownik) .....
(nazwa stanowiska służbowego osoby funkcyjnej)

przeprowadził w dniach ..... kontrolę półroczną stanu ochrony informacji niejawnych w .....
(nazwa komórki (jednostki) organizacyjnej)

1. Kontrolą nie objęto następujących osób (wymienić nazwiska wykonawców, których nie skontrolowano, podać powód, określić termin kiedy zostaną skontrolowani oraz termin przedstawienia notatki uzupełniającej):
   - .....
   - .....
2. W wyniku przeprowadzonej kontroli na podstawie urządzeń ewidencyjnych (wymienić nazwy urządzeń) stwierdzono, iż stan faktyczny dokumentów niejawnych pobranych przez wykonawców jest zgodny ze stanem ewidencyjnym (w razie stwierdzenia braku dokumentów należy podać ich klauzulę, numery ewidencyjne, nazwy dokumentów lub czego dotyczą, przez kogo zostały pobrane, datę pobrania oraz okoliczności utraty).
3. U wykonawców stwierdzono niedociągnięcia w zakresie przestrzegania przepisów o ochronie informacji niejawnych dotyczących wytwarzania, ewidencjonowania, przechowywania i niszczenia materiałów niejawnych (wymienić niedociągnięcia, przyczyny ich powstania, skutki oraz określić osoby za to odpowiedzialne).
4. Stwierdzono, iż zalecenia z przeprowadzonych w bieżącym roku kontroli stanu ochrony informacji niejawnych zostały wykonane (ewentualnie wymienić zalecenia pokontrolne, które nie zostały zrealizowane, określić przyczyny oraz osoby odpowiedzialne).
5. Wnioski i zalecenia pokontrolne.

.....
(podpis osoby kontrolującej)

Załącznik Nr 4

WZÓR

NOTATKA

zbiorcza o wynikach kontroli półrocznej stanu ochrony informacji niejawnych przeprowadzonej

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

Zgodnie z rozkazem dziennym (decyzją) Nr.....

..... z dnia .....
(nazwa stanowiska kierownika jednostki (komórki) organizacyjnej)

w .....
(nazwa jednostki (komórki) organizacyjnej)

przeprowadzono kontrolę półroczną stanu ochrony informacji niejawnych. Skontrolowano następujące komórki (jednostki) organizacyjne oraz osoby zajmujące samodzielne stanowiska służbowe (wymienić nazwy kontrolowanych komórek (jednostek) organizacyjnych oraz samodzielnych stanowisk służbowych):

- .....
- .....

Kontrolą nie objęto następujących osób z powodu (podać stopnie wojskowe, nazwiska i imiona osób, których nie skontrolowano, przynależność do komórki (jednostki) organizacyjnej, powód nie poddania kontroli, termin, w jakim zostaną skontrolowane oraz termin złożenia notatki uzupełniającej):

- .....
- .....

Na podstawie wyników kontroli stwierdzono, iż:

1. Stan faktyczny dokumentów niejawnych pobranych przez wykonawców jest zgodny ze stanem ewidencyjnym (w razie stwierdzenia braku dokumentów należy podać ich klauzulę, numery ewidencyjne, nazwy dokumentów lub czego dotyczą, nazwę komórki (jednostki) organizacyjnej, na której ewidencji pozostawały, przez kogo zostały pobrane, datę pobrania oraz okoliczności ich utraty).
2. U wykonawców występują następujące niedociągnięcia w zakresie przestrzegania przepisów o ochronie informacji niejawnych dotyczących wytwarzania, ewidencjonowania, przechowywania i niszczenia materiałów niejawnych (wymienić niedociągnięcia, nazwy komórek (jednostek) organizacyjnych, w których występują, przyczyny ich powstania, skutki oraz określić osoby odpowiedzialne).
3. Zalecenia z przeprowadzonych w bieżącym roku kontroli stanu ochrony informacji niejawnych zostały (ewentualnie nie zostały) wykonane (wymienić jakie zalecenia nie zostały zrealizowane oraz odpowiedzialne za to komórki organizacyjne lub osoby funkcyjne).
5. Wnioski i zalecenia z kontroli.

.....
(podpis osoby funkcyjnej)

Załącznik Nr 5

ZAKRES

przedmiotowy kontroli rocznej stanu ochrony informacji niejawnych

1. Sprawdzenie stanu przestrzegania zasad postępowania z materiałami niejawnymi w kancelariach tajnych, tajnych-zagranicznych i innych komórkach, w których są przechowywane, ewidencjonowane i udostępniane materiały niejawne:

1) szczegółowe sprawdzenie stanu faktycznego materiałów niejawnych przechowywanych w kancelariach tajnych, tajnych-zagranicznych i innych komórkach, w których są przechowywane, ewidencjonowane i udostępniane materiały niejawne oraz porównanie ze stanem ewidencyjnym;
2) przestrzeganie zasad ewidencjonowania wytwarzanych i otrzymywanych materiałów niejawnych;
3) przestrzeganie zasad wytwarzania, przechowywania, udostępniania i niszczenia materiałów niejawnych;
4) przestrzeganie obowiązku dokumentowania faktu zapoznania się z informacjami niejawnymi stanowiącymi tajemnicę państwową.

2. Sprawdzenie stanu przestrzegania zasad postępowania z materiałami niejawnymi przez wykonawców:

1) szczegółowe sprawdzenie i porównanie ze stanem ewidencyjnym materiałów niejawnych pobranych przez wykonawców;
2) przestrzeganie zasad wytwarzania materiałów niejawnych, a zwłaszcza pism przewodnich, załączników, zbiorów materiałów, kopii, odpisów, wyciągów
i tłumaczeń;
3) przestrzeganie zasad przechowywania, przekazywania i niszczenia materiałów niejawnych.

3. Sprawdzenie realizacji zadań związanych z zapewnieniem bezpieczeństwa osobowego.

4. Sprawdzenie realizacji zadań związanych z ochroną fizyczną informacji niejawnych.

5. Sprawdzenie realizacji zadań związanych z zapewnieniem ochrony informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych.

6. Wybrakowanie materiałów niearchiwalnych kategorii B, Bc i Be.

Załącznik Nr 6

UKŁAD

protokołu z kontroli rocznej stanu ochrony informacji niejawnych

1. Część ogólna:

1) numer i data wydania rozkazu dziennego albo decyzji kierownika jednostki (komórki) organizacyjnej, będącego podstawą działania komisji kontroli rocznej;
2) stopnie wojskowe, imiona, nazwiska, numery, klauzule tajności oraz terminy ważności poświadczeń bezpieczeństwa członków komisji;
3) data rozpoczęcia i zakończenia kontroli rocznej;
4) wykaz komórek organizacyjnych (wewnętrznych) objętych kontrolą.

2. Część merytoryczna:

1) wyszczególnienie nazw urządzeń ewidencyjnych oraz pozycji zapisów w tych urządzeniach, na podstawie których sprawdzono stan faktyczny materiałów niejawnych wytworzonych, przechowywanych lub przekazanych przez jednostkę organizacyjną;
2) dane dotyczące stanu faktycznego materiałów niejawnych:

a) zgodność lub niezgodność stanu faktycznego materiałów niejawnych ze stanem ewidencyjnym,
b) w przypadku niezgodności stanu ewidencyjnego ze stanem faktycznym, wyszczególnienie brakujących materiałów (nie przedstawionych do kontroli, utraconych lub uznanych za utracone), z podaniem ich klauzuli tajności, tytułu lub czego dotyczą, numerów ewidencyjnych oraz nazwisk osób, które je pobrały ze wskazaniem przyczyn, okoliczności i skutków utraty oraz czynności podjętych przez komisję w celu ich odszukania,
c) wyszczególnienie numerów materiałów niejawnych, które nie zostały podszyte do właściwych teczek akt oraz przerejestrowane na rok następny;

3) przestrzeganie zasad ewidencjonowania, wytwarzania, przechowywania i niszczenia materiałów niejawnych;
4) przestrzeganie zasady selektywnego udostępniania informacji niejawnych oraz dokumentowania faktu zapoznania się z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową;
5) dokonywanie przeglądów materiałów niejawnych w celu aktualizacji ich klauzul tajności albo przedłużenia okresu ochrony;
6) przestrzeganie zasad przechowywania oraz przekazywania materiałów niejawnych przez wykonawców;
7) stan realizacji zadań związanych z ochroną fizyczną jednostki lub komórki organizacyjnej;
8) przestrzeganie zasad ochrony informacji niejawnych w systemach i sieciach teleinformatycznych;
9) ogólna ocena przestrzegania przepisów o ochronie informacji niejawnych w jednostce albo komórce organizacyjnej;
10) wnioski i zalecenia pokontrolne;
11) w załączniku - wykaz akt wybrakowanych oraz dokumentów niejawnych zniszczonych przez komisję kontroli rocznej;
12) podpisy członków komisji;
13) podpis kierownika jednostki lub komórki organizacyjnej, potwierdzający fakt zapoznania się z protokołem z kontroli rocznej stanu ochrony informacji niejawnych.

Załącznik Nr 7

WZÓR

MELDUNEK

o wynikach kontroli rocznej stanu ochrony informacji niejawnych za rok ..... przeprowadzonej w dniach..... w .....

(nazwa jednostki (komórki) organizacyjnej)

Zgodnie z decyzją Nr...../MON Ministra Obrony Narodowej z dnia..... w sprawie sprawowania nadzoru nad ochroną informacji niejawnych (Dz. Urz. MON poz. ...) oraz rozkazem dziennym (decyzją) Nr..... (podać nazwę stanowiska kierownika jednostki organizacyjnej) z dnia....., w dniach od ..... stycznia do ..... lutego ..... r.
w .....

(nazwa jednostki (komórki) organizacyjnej)

przeprowadzono kontrolę roczną stanu ochrony informacji niejawnych za ..... r. Skontrolowano następujące jednostki (komórki) organizacyjne:

- .....
- .....

Kontroli nie zakończono (nie przeprowadzono) w następujących jednostkach (komórkach) organizacyjnych:

- ..... z powodu.....
- ..... z powodu.....
- ..... z powodu.....

Kontrola wyżej wymienionych jednostek (komórek) zostanie zakończona do dnia .....

Meldunek uzupełniający w powyższej sprawie zostanie przedłożony w terminie do .....

Kontrola wykazała, iż:

1. Stan ochrony informacji niejawnych w .....

(nazwa jednostki (komórki) organizacyjnej)

kształtuje się na poziomie .....

(podać ocenę ogólną w skali : bardzo dobry, dobry, dostateczny, niedostateczny)

2. Stan faktyczny dokumentów niejawnych jest zgodny (niezgodny) ze stanem ewidencyjnym (w razie stwierdzenia braku dokumentów należy podać ich klauzulę, numery ewidencyjne, nazwy dokumentów lub czego dotyczą, nazwę jednostki (komórki) organizacyjnej, na której ewidencji pozostawały, przez kogo zostały pobrane, datę pobrania oraz okoliczności utraty).
3. Stwierdzono niedociągnięcia w zakresie przestrzegania przepisów o ochronie informacji niejawnych (wymienić niedociągnięcia, nazwy jednostek (komórek) organizacyjnych, w których wystąpiły, przyczyny powstania, skutki oraz określić osoby za to odpowiedzialne).
4. Wnioski.

.....

(data, stopień wojskowy, imię i nazwisko oraz podpis
przewodniczącego komisji (podkomisji) kontroli rocznej stanu ochrony informacji niejawnych)

Załącznik Nr 8

WZÓR

MELDUNEK ZBIORCZY

o wynikach kontroli rocznej stanu ochrony informacji niejawnych za rok ..... przeprowadzonej w dniach ..... w jednostkach (komórkach) organizacyjnych podległych.....
(stanowisko osoby funkcyjnej)

Zgodnie z decyzją Nr...../MON Ministra Obrony Narodowej z dnia..... w sprawie sprawowania nadzoru nad ochroną informacji niejawnych (Dz. Urz. MON poz. ...) w dniach od.....stycznia do.....lutego.....r. w jednostkach (komórkach) organizacyjnych podległych .....
(wpisać stanowisko osoby funkcyjnej)

przeprowadzono kontrolę roczną stanu ochrony informacji niejawnych za .....r.

Kontroli nie zakończono (nie przeprowadzono, nie zakończono) w następujących jednostkach (komórkach) organizacyjnych:

- ..... z powodu.....
- ..... z powodu.....

Kontrola wyżej wymienionych jednostek (komórek) zostanie zakończona do dnia.....

Meldunek uzupełniający o wynikach kontroli zostanie przedłożony w terminie do dnia.....

Kontrola roczna stanu ochrony informacji niejawnych wykazała, iż:

1. Stan ochrony informacji niejawnych w jednostkach (komórkach) organizacyjnych podległych.....
(wpisać nazwę stanowiska osoby funkcyjnej)

   kształtuje się na poziomie .....
(podać ocenę ogólną w skali : bardzo dobry, dobry, dostateczny, niedostateczny)

2. Stan faktyczny dokumentów niejawnych jest zgodny ze stanem ewidencyjnym (w przypadku stwierdzenia braku dokumentów należy podać ich klauzulę, numery ewidencyjne, nazwy dokumentów lub czego dotyczą, nazwę jednostki (komórki) organizacyjnej, na której ewidencji pozostawały, nazwiska osób które je pobrały, datę pobrania, okoliczności utraty).
3. Stwierdzono niedociągnięcia w zakresie przestrzegania przepisów o ochronie informacji niejawnych (wymienić niedociągnięcia, nazwy jednostek (komórek) organizacyjnych, w których wystąpiły, przyczyny ich powstania, skutki, osoby za to odpowiedzialne).
4. Wnioski.

.....
(data, stopień wojskowy, imię i nazwisko oraz podpis
przewodniczącego komisji kontroli rocznej stanu ochrony informacji niejawnych)

Załącznik Nr 9

SZCZEGÓŁOWY ZAKRES
przedmiotowy kontroli problemowej stanu ochrony informacji niejawnych

1. Działalność organizacyjna i normatywna:

1) kierownika jednostki organizacyjnej:

a) spójność dokumentów normatywnych wydanych przez kierownika kontrolowanej jednostki organizacyjnej z aktami prawnymi oraz normatywnymi szczebli nadrzędnych,

b) sprecyzowanie zadań, dotyczących ochrony informacji niejawnych, dla osób funkcyjnych w zakresach obowiązków,

c) prowadzenie nadzoru służbowego w zakresie ochrony informacji niejawnych oraz dokumentowanie jego wyników. Kontrole bieżące, wyrywkowe, roczne, półroczne oraz problemowe,

d) realizacja zaleceń pokontrolnych z kontroli stanu ochrony informacji niejawnych przeprowadzonych w jednostce organizacyjnej,

e) wartość merytoryczna przeprowadzonych w jednostce organizacyjnej ocen stanu ochrony informacji niejawnych,

f) reagowanie na fakty naruszania przepisów o ochronie informacji niejawnych, utraty dokumentów niejawnych oraz ujawnienia informacji niejawnych osobom nieupoważnionym,

g) przestrzeganie przepisów w zakresie upoważniania osób do dostępu do informacji niejawnych,

h) powołanie inspektora bezpieczeństwa teleinformatycznego oraz administratora systemu lub sieci teleinformatycznej,

i) prowadzenie przeglądów materiałów zawierających informacje niejawne stanowiących tajemnicę służbową, wytworzonych w jednostce organizacyjnej, w celu ewentualnego przedłużenia terminu ich ochrony;

2) pełnomocnika do spraw ochrony informacji niejawnych:

a) prowadzenie wykazu stanowisk i prac zleconych, z którymi wiąże się dostęp do informacji niejawnych oraz osób dopuszczonych do pracy lub służby na tych stanowiskach,

b) realizacja procedur sprawdzających w zakresie zwykłych postępowań sprawdzających, a zwłaszcza:

- podstawa wszczęcia postępowania sprawdzającego,
- sposób dokumentowania informacji uzyskanych w wyniku sprawdzeń,
- zgodność z przepisami podjętych decyzji o wydaniu lub odmowie wydania poświadczeń bezpieczeństwa,

- ewidencja akt postępowania sprawdzającego,
- przechowywanie i archiwizowanie akt postępowania sprawdzającego,

c) plan ochrony jednostki organizacyjnej, uaktualnianie planu oraz nadzorowanie jego realizacji,

d) organizacja obsługi kancelaryjnej w jednostce organizacyjnej,

e) szkolenie podstawowe i uzupełniające kadry i pracowników oraz specjalistyczne w zakresie ochrony informacji niejawnych. Programy szkolenia oraz prowadzenie ewidencji szkoleniowej,

f) szkolenie użytkowników systemów i sieci teleinformatycznych,

g) plan postępowania z materiałami zawierającymi informacje stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego,

h) szczegółowe wymagania w zakresie ochrony w jednostce organizacyjnej informacji oznaczonych klauzulą „Zastrzeżone",

i) dokumentacja inspektora bezpieczeństwa teleinformatycznego, planowanie oraz dokumentowanie wyników kontroli zgodności funkcjonowania systemów lub sieci teleinformatycznych z ich szczególnymi wymaganiami bezpieczeństwa oraz procedurami bezpiecznej eksploatacji,

j) wszczynanie, prowadzenie i dokumentowanie działań zmierzających do wyjaśnienia okoliczności naruszenia przepisów o ochronie informacji niejawnych.

2. Działalność kancelarii tajnej oraz tajnej-zagranicznej:

1) stan zabezpieczenia oraz wyposażenie pomieszczeń kancelaryjnych;
2) fizyczne oddzielenie materiałów o różnych klauzulach tajności oraz przestrzeganie zasady przechowywania dokumentów uzyskanych w ramach realizacji porozumień międzynarodowych odrębnie dla każdego państwa i organizacji międzynarodowej;
3) przygotowanie specjalistyczne kierownika, jego zastępcy oraz pracowników kancelarii tajnej;
4) organizacja pracy kancelarii, zakresy działania osób funkcyjnych;
5) przestrzeganie zasad ewidencjonowania dokumentów;
6) skuteczność nadzoru kierownika kancelarii nad wytwarzaniem i ewidencjonowaniem dokumentów niejawnych przez wykonawców technicznych;
7) przestrzeganie zasad wydawania, rozliczania i obiegu dokumentów niejawnych, a także adresowania, zabezpieczania i ekspedycji przesyłek;
8) prowadzenie kontroli bieżących wykonawców;
9) prowadzenie wykazu osób upoważnionych do dostępu do informacji niejawnych oraz jego bieżąca aktualizacja;
10) przestrzeganie zasad kompletowania i brakowania akt oraz niszczenia dokumentów niejawnych;

11) dokonywanie zmian klauzul tajności na materiałach niejawnych oraz w urządzeniach ewidencyjnych;
12) organizowanie kancelarii ćwiczebnej, ewidencjonowanie, obieg i rozliczanie dokumentów ćwiczebnych;
13) przygotowanie kancelarii tajnej do realizacji zadań na czas „W".

3. **Postępowanie z dokumentami niejawnymi w innych komórkach przechowujących oraz prowadzących ewidencję materiałów niejawnych:**
   1) zabezpieczenie i wyposażenie pomieszczeń, w których są przechowywane informacje niejawne;
   2) przeszkolenie specjalistyczne personelu;
   3) prowadzenie ewidencji materiałów niejawnych;
   4) prowadzenie oraz bieżąca aktualizacja wykazu osób upoważnionych do dostępu do informacji niejawnych;
   5) przestrzeganie zasad przechowywania, udostępniania i niszczenia materiałów niejawnych;
   6) kontrola bieżąca osób, które pobrały materiały niejawne;
   7) aktualizacja klauzul tajności na materiałach niejawnych oraz w urządzeniach ewidencyjnych;
   8) niszczenie materiałów niejawnych.

4. **Postępowanie wykonawców z informacjami niejawnymi:**
   1) znajomość przez wykonawców przepisów o ochronie informacji niejawnych;
   2) przestrzeganie zasad klasyfikowania informacji niejawnych oraz oznaczania dokumentów, w tym klauzulami tajności;
   3) przestrzeganie przepisów w zakresie przechowywania i przekazywania informacji niejawnych;
   4) terminowość rozliczania się wykonawców z pobranych materiałów niejawnych.

5. **Ochrona fizyczna jednostki organizacyjnej:**
   1) organizacja ochrony jednostki organizacyjnej;
   2) pełnienie służby wartowniczej (ochronnej) i dyżurnej oraz urządzenie i wyposażenie wartowni, posterunków i miejsc pełnienia służby;
   3) sprawność urządzeń alarmowych;
   4) stan ogrodzeń, sprawność oświetlenia i środków łączności służących ochronie, zabezpieczenie stref administracyjnej, bezpieczeństwa oraz pomieszczeń, w których jest przechowywany sprzęt i mienie wojskowe.

6. **Ochrona informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych:**
   1) posiadanie certyfikatów dla systemów, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę państwową;
   2) opracowanie i zatwierdzenie (akceptacja) przez Szefa Wojskowych Służb Informacyjnych Szczególnych Wymagań Bezpieczeństwa oraz Procedur Bezpiecznej Eksploatacji;
   3) zgodność elementów systemu lub sieci teleinformatycznej i realizowanych w nich czynności z ustaleniami Szczególnych Wymagań Bezpieczeństwa, w zakresie:
      a) oprogramowania systemowego, użytkowego i narzędziowego,
      b) konfiguracji sprzętu komputerowego,
      c) zabezpieczenia sprzętu przed nieuprawnionym dostępem,
      d) monitorowania i dokumentowania dostępu do systemu.
   4) zgodność ze Szczególnymi Wymaganiami Bezpieczeństwa zabezpieczeń oraz wyposażenia pomieszczenia wydzielonego;
   5) znajomość oraz przestrzeganie przez użytkowników postanowień Procedur Bezpiecznej Eksploatacji;
   6) przechowywanie, ewidencjonowanie, udostępnianie i niszczenie elektronicznych nośników informacji;
   7) wyznaczenie przez kierownika jednostki organizacyjnej administratora systemu lub sieci teleinformatycznej oraz inspektora bezpieczeństwa teleinformatycznego, jak też ukończenie przez niego szkolenia specjalistycznego.

DECYZJA Nr 22/MON

MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie szczegółowych zasad i trybu prowadzenia i dokumentowania postępowań sprawdzających oraz wydawania poświadczeń i certyfikatów bezpieczeństwa

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w związku z art. 29, 29a i 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631), zwanej dalej „ustawą", ustala się co następuje:

§ 1.
1. Dyrektorzy (szefowie) komórek organizacyjnych Ministerstwa Obrony Narodowej oraz kierownicy (dowódcy, komendanci) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych – zwani dalej odpowiednio „kierownikami komórek organizacyjnych MON" lub „kierownikami jednostek organizacyjnych" albo „kierownikami jednostek (komórek) organizacyjnych" – ustalają dla kierowanych jednostek organizacyjnych (komórek) „Wykaz stanowisk i prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych oraz osób dopuszczonych do pracy lub służby na tych stanowiskach", zwany dalej „wykazem stanowisk".
2. Wykaz stanowisk sporządza się na oddzielnych kartach dla każdego stanowiska (rodzaju pracy zleconej) oraz dla każdej klauzuli informacji niejawnej.
3. Wykaz stanowisk może być dodatkowo prowadzony w formie elektronicznej, a w przypadku znacznej liczby stanowisk – oddzielnie dla każdej komórki wewnętrznej w danej jednostce organizacyjnej, zgodnie z jej strukturą etatową.
4. Wzór wykazu stanowisk określa załącznik Nr 1 do decyzji.

§ 2.
1. Poszerzone lub specjalne postępowania sprawdzające wobec osób zajmujących kierownicze stanowiska Ministerstwa Obrony Narodowej oraz dowódców (szefów, komendantów) jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej – prowadzi Szef Służby Kontrwywiadu Wojskowego, na wniosek Ministra Obrony Narodowej.
2. Z wnioskami w sprawie przeprowadzenia poszerzonego lub specjalnego postępowania sprawdzającego, opracowanymi stosownie do wykazu stanowisk, występują:

1) do Szefa Służby Kontrwywiadu Wojskowego:

a) osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej - wobec kierowników bezpośrednio podporządkowanych komórek organizacyjnych MON,
b) Dyrektor Departamentu Kadr i Szkolnictwa Wojskowego – wobec żołnierzy zawodowych planowanych do wyznaczenia na stanowiska służbowe, o których mowa w art. 44 ust. 1 pkt 4-6 ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz. U. Nr 179, poz. 1750 z późn. zm.) –
w przypadku, gdy nie posiadają poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych o klauzuli wymaganej na danym stanowisku,
c) Szef Generalnego Zarządu Zasobów Osobowych – P 1 Sztabu Generalnego Wojska Polskiego - wobec żołnierzy zawodowych planowanych do wyznaczenia lub wyznaczonych na stanowiska służbowe poza granicami państwa, z wyjątkiem żołnierzy zawodowych planowanych do wyznaczenia lub wyznaczonych na stanowiska w ataszatach obrony,
d) Komendant Główny Żandarmerii Wojskowej – wobec pełnomocnika ochrony Komendy Głównej Żandarmerii Wojskowej oraz jego zastępcy
e) kierownicy przedsiębiorstw, jednostek naukowych lub badawczo – rozwojowych oraz innych

jednostek organizacyjnych spoza resortu obrony narodowej, zwani dalej „kierownikami przedsiębiorstw" – wobec pracowników wykonujących prace związane z realizacją produkcji lub usług stanowiących tajemnicę państwową ze względu na obronność państwa i potrzeby Sił Zbrojnych Rzeczypospolitej Polskiej albo prace związane z obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową ze względu na obronność państwa, jeżeli uczestnikami tego obrotu są jednostki organizacyjne Sił Zbrojnych lub inne jednostki organizacyjne resortu Obrony Narodowej.

2) do kierowników właściwych jednostek organizacyjnych Służby Kontrwywiadu Wojskowego, zwanych dalej „jednostkami organizacyjnymi SKW":

a) kierownicy komórek organizacyjnych MON wobec podległych żołnierzy i pracowników resortu obrony narodowej, zwanych dalej „pracownikami wojska", planowanych do wyznaczenia lub wyznaczonych na stanowiska służbowe albo do prac zleconych objętych wykazem stanowisk, w podporządkowanych (podległych) im komórkach organizacyjnych ministerstwa,
b) dowódcy (komendanci), o których mowa w art. 44 ust. 1 pkt 3-7 ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych, stosownie do przysługujących im uprawnień służbowych oraz kierownicy pozostałych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, wobec żołnierzy i pracowników wojska planowanych do wyznaczenia lub wyznaczonych w podległych albo kierowanych jednostkach organizacyjnych, na stanowiska lub do wykonania prac zleconych objętych wykazem stanowisk,
c) kierownicy komórek organizacyjnych MON oraz dowódcy (komendanci), o których mowa w lit. a i b – wobec pracowników wojska planowanych do wyznaczenia lub wyznaczonych na stanowiska poza granicami państwa, jeżeli ich zajmowanie wiąże się z dostępem do informacji niejawnych,

3. Z wnioskami w sprawie przeprowadzenia poszerzonego lub specjalnego postępowania sprawdzającego wobec żołnierzy (pracowników wojska), o których mowa w ust. 2 pkt 1 lit. a – c oraz pkt 2 lit. a i c, osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej oraz kierownicy komórek organizacyjnych MON występują poprzez Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

4. Kierownicy komórek organizacyjnych MON przesyłają wnioski o wszczęcie zwykłego postępowania sprawdzającego wraz z ankietami bezpieczeństwa osobowego Dyrektorowi Generalnemu Ministerstwa Obrony Narodowej, za pośrednictwem Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych. Polecenie wszczęcia postępowania sprawdzającego wydaje Dyrektor Generalny Ministerstwa Obrony Narodowej.

§ 3.
Z wnioskami o przeprowadzenie zwykłych postępowań sprawdzających wobec kandydatów na pełnomocników ochrony oraz ich zastępców, uprawnieni kierownicy jednostek organizacyjnych oraz kierownicy przedsiębiorstw, występują do kierowników właściwych jednostek organizacyjnych SKW.

§ 4.
W przypadkach, o których mowa w art. 44 ust. 1 ustawy, przepisy § 2 i § 3 stosuje się odpowiednio.

§ 5.
Wzór „Wniosku o wszczęcie postępowania sprawdzającego" i wzór „Polecenia wszczęcia postępowania sprawdzającego", określają odpowiednio załączniki Nr 2 i Nr 3 do decyzji.

§ 6.
1. Czynności postępowania sprawdzającego dokumentowane są w formie akt postępowania sprawdzającego.
2. Akta każdego postępowania sprawdzającego (nowego, kolejnego lub kontrolnego) są prowadzone i ewidencjonowane oddzielnie.
3. Wzory strony pierwszej i drugiej teczki akt postępowania sprawdzającego, spisu dokumentów, wykazu osób prowadzących postępowanie oraz wykazu osób zapoznanych z aktami, określa załącznik Nr 4 do decyzji.

4. W teczce akt postępowania sprawdzającego kompletuje się korespondencję i dokumenty sporządzone w toku tego postępowania, a w szczególności dokumenty, których wzór określają załączniki Nr 5-10 do decyzji.

§ 7.
1. W zakresie zwykłego postępowania sprawdzającego pełnomocnik ochrony w szczególności:

1) przed wszczęciem (zarejestrowaniem) postępowania:

a) wydaje ankietę bezpieczeństwa osobowego osobie planowanej do wyznaczenia (zatrudnienia) na stanowisku lub do wykonania prac zleconych objętych wykazem stanowisk albo osobie zajmującej takie stanowisko lub wykonującej prace zlecone objęte tym wykazem,
b) przyjmuje wypełnioną ankietę bezpieczeństwa osobowego i dokonuje jej sprawdzenia pod względem poprawności wypełnienia oraz podpisuje ankietę,
c) powoduje osobiste poprawienie lub uzupełnienie ankiety bezpieczeństwa osobowego przez osobę, której ankieta dotyczy, w przypadku wystąpienia uchybień formalnych albo potrzeby jej uzupełnienia; wszelkie zmiany nanoszone w ankiecie bezpieczeństwa osobowego muszą być potwierdzone wpisaniem daty dokonanej zmiany (uzupełnienia) i złożeniem podpisu przez osobę składającą ankietę,
d) przedstawia ankietę bezpieczeństwa osobowego uprawnionemu kierownikowi jednostki organizacyjnej, który po zapoznaniu się i złożeniu podpisu, wydaje pisemne polecenie przeprowadzenia zwykłego postępowania sprawdzającego,

2) w ramach postępowania sprawdzającego:

a) zakłada i rejestruje akta postępowania sprawdzającego w „Wykazie osób, wobec których przeprowadzono postępowanie sprawdzające", zwanym dalej „wykazem osób"; wzór wykazu określa załącznik Nr 11 do decyzji,
b) dokonuje sprawdzenia danych zawartych w ankiecie bezpieczeństwa osobowego poprzez wysłanie wniosków do:

- Krajowego Rejestru Karnego Ministerstwa Sprawiedliwości, na formularzu według wzoru określonego w załączniku Nr 5 do decyzji,
- Biura Informacji i Statystyki Centralnego Zarządu Służby Więziennej, na formularzu według wzoru określonego w załączniku Nr 6 do decyzji,
- właściwego Urzędu Stanu Cywilnego, na formularzu według wzoru określonego w załączniku Nr 7 do decyzji,
- właściwej jednostki organizacyjnej SKW (wyłącznie przy postępowaniu dotyczącym dostępu do informacji oznaczonych klauzulą POUFNE) o sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie; wzór wniosku określa załącznik Nr 8 do decyzji,

c) przeprowadza rozmowę z osobą sprawdzaną w przypadku konieczności wyjaśnienia wątpliwości wynikających z uzyskanych informacji i opracowuje notatkę z tej czynności, według układu merytorycznego określonego w załączniku Nr 9 do decyzji,
d) opracowuje notatkę dotyczącą wyników przeprowadzonego postępowania sprawdzającego, według układu merytorycznego określonego w załączniku Nr 10 do decyzji,
e) wydaje osobie sprawdzanej poświadczenie bezpieczeństwa lub decyzję o odmowie wydania poświadczenia bezpieczeństwa,
f) wydaje decyzję o cofnięciu poświadczenia bezpieczeństwa w wyniku kontrolnego postępowania sprawdzającego, albo informuje osobę sprawdzaną i kierownika jednostki organizacyjnej o braku zastrzeżeń w stosunku do osoby, którą objęto tym postępowaniem,
g) umarza postępowanie sprawdzające w sytuacjach określonych w art. 36 ust. 2b ustawy; wzór decyzji o umorzeniu postępowania określa załącznik Nr 12 do decyzji,
h) może zawiesić postępowanie sprawdzające w sytuacjach określonych w art. 36 ust. 2c ustawy; wzór postanowienia o zawieszeniu postępowania określa załącznik Nr 13 do decyzji,
i) podejmuje zawieszone postępowanie sprawdzające w przypadku ustania przyczyn tego zawieszenia; wzór postanowienia o podjęciu zawieszonego postępowania sprawdzającego określa załącznik Nr 14 do decyzji.

2. W zakresie postępowań sprawdzających, prowadzonych przez jednostki organizacyjne SKW, czynności o których mowa w ust. 1 pkt 1 lit. a-d realizują pełnomocnicy ochrony.

§ 8.
1. Poświadczenie bezpieczeństwa, decyzję o odmowie wydania poświadczenia bezpieczeństwa, decyzję o cofnięciu poświadczenia bezpieczeństwa, decyzję o umorzeniu postępowania sprawdzającego, postanowienie o zawieszeniu postępowania sprawdzającego oraz postanowienie o podjęciu zawieszonego postępowania sprawdzającego przekazuje się osobie sprawdzanej, za pokwitowaniem, na kopii poświadczenia lub na trzecim egzemplarzu decyzji bądź postanowienia. W przypadku braku możliwości przekazania wymienionych dokumentów bezpośrednio osobie sprawdzanej, należy:

1) doręczyć je osobie sprawdzanej za pośrednictwem poczty, a zwrotne potwierdzenie odbioru włączyć do akt postępowania sprawdzającego;
2) przesłać je kierownikowi jednostki (komórki) organizacyjnej, w której osoba sprawdzana pełni służbę (jest zatrudniona), a drugi egzemplarz pisma przewodniego, przy którym przesłano przedmiotowy dokument wraz z kopią, włączyć do akt postępowania sprawdzającego. Kierownik jednostki (komórki) organizacyjnej jest zobowiązany do pisemnego powiadomienia organu wydającego decyzję lub postanowienie o terminie wręczenia tych dokumentów osobie sprawdzanej.

2. O wyniku zakończonego postępowania sprawdzającego, jak również o zawieszeniu lub podjęciu zawieszonego postępowania sprawdzającego, należy zawiadomić pisemnie kierownika jednostki (komórki) organizacyjnej lub inną osobę funkcyjną, która wnioskowała albo poleciła jego przeprowadzenie. Do zawiadomienia dołącza się kopie poświadczenia bezpieczeństwa oraz decyzji, o których mowa w § 7 ust. 1 pkt. 2 lit. e-g, w celu włączenia do akt personalnych osoby sprawdzanej. Drugi egzemplarz pisemnego zawiadomienia włącza się do akt postępowania sprawdzającego.

3. Pełnomocnik ochrony, po wydaniu poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji oznaczonych klauzulą POUFNE, podjęciu decyzji o odmowie wydania poświadczenia bezpieczeństwa, o cofnięciu poświadczenia bezpieczeństwa bądź podjęciu decyzji o umorzeniu postępowania, przesyła w terminie 7 dni kartę ewidencyjną do właściwej jednostki organizacyjnej SKW; wzór karty ewidencyjnej określa załącznik Nr 15 do decyzji.

§ 9.
1. W przypadku zagubienia (utraty) poświadczenia bezpieczeństwa, jednostka organizacyjna SKW lub pełnomocnik ochrony, na pisemny wniosek osoby sprawdzonej, wydają jego duplikat. Duplikat poświadczenia bezpieczeństwa oznacza się dodatkowo napisem DUPLIKAT umieszczonym w środku dolnej części dokumentu, pod okrągłą pieczęcią urzędową pełnomocnika ochrony lub jednostki organizacyjnej SKW. Wniosek oraz kopię wydanego duplikatu poświadczenia włącza się do akt postępowania sprawdzającego.
Duplikat wydaje się z zachowaniem dotychczasowego numeru i daty ważności.

2. W przypadku zmiany danych personalnych zawartych w poświadczeniu bezpieczeństwa, jednostka organizacyjna SKW albo pełnomocnik ochrony, na pisemny wniosek osoby sprawdzonej, wydaje nowe poświadczenie bezpieczeństwa zawierające zmienione dane personalne z zachowaniem dotychczasowego numeru, oznaczenia klauzuli dostępu do informacji niejawnych i daty ważności.

3. Do wniosku, o którym mowa w ust. 2, zainteresowana osoba dołącza oryginał dokumentu potwierdzającego zmianę danych personalnych. Dokumenty te dołącza się do teczki akt postępowania sprawdzającego. Zmienione dane personalne aktualizuje się w wykazie osób i na okładce akt postępowania.

4. W przypadku wydania poświadczenia bezpieczeństwa, o którym mowa w ust. 2, dotyczącego dostępu do informacji niejawnych oznaczonych klauzulą POUFNE - pełnomocnik ochrony przesyła w terminie 7 dni kartę ewidencyjną do właściwej jednostki organizacyjnej SKW oraz zawiadamia

kierownika jednostki (komórki) organizacyjnej; przepis § 8 ust. 2 zdanie drugie – stosuje się odpowiednio.

§ 10.
1. Akta zakończonego zwykłego postępowania sprawdzającego przechowuje, przez okres 10 lat, pełnomocnik ochrony jednostki organizacyjnej, w której przeprowadzono postępowanie.

2. W przypadku zmiany miejsca służby (pracy) przez osobę, wobec której przeprowadzono bądź umorzono postępowanie sprawdzające, akta postępowania sprawdzającego przesyłane są do właściwego pełnomocnika ochrony na jego wniosek, z zastrzeżeniem ust. 3.

3. W przypadku ubycia osoby, o której mowa w ust. 2, poza resort obrony narodowej, akt postępowania sprawdzającego nie przesyła się; udostępnienie tych akt następuje na zasadach określonych w art. 42 ust. 3 ustawy.

4. O przekazaniu akt postępowania sprawdzającego do innej jednostki organizacyjnej, pełnomocnik ochrony informuje właściwą jednostkę SKW poprzez przesłanie w ciągu 7 dni karty ewidencyjnej oraz odnotowuje ten fakt w rubryce Nr 15 wykazu osób.

5. W przypadku przekazania akt postępowania sprawdzającego do jednostki organizacyjnej będącej nowym miejscem pełnienia służby (pracy) osoby sprawdzonej, pełnomocnik ochrony przyjmujący akta w terminie 7 dni przesyła kartę ewidencyjną do właściwej jednostki organizacyjnej SKW, podając w pkt. 9 karty aktualne miejsce przechowywania akt postępowania sprawdzającego. Karta ewidencyjna miejsca pełnienia służby (pracy) wymaga wypełnienia.

6. Po upływie okresu, o którym mowa w ust. 1, akta postępowania sprawdzającego archiwizuje się na zasadach, określonych w odrębnych przepisach.

§ 11.
1. Pełnomocnik ochrony prowadzi ewidencję osób, wobec których przeprowadził bądź umorzył postępowanie sprawdzające, przy wykorzystaniu kart ewidencyjnych oraz wykazu osób i wykazu stanowisk.

2. Wykaz osób stanowi książkę ewidencyjną akt postępowań sprawdzających i podlega zarejestrowaniu w rejestrze teczek dokumentów niejawnych, dzienników i książek ewidencyjnych w kancelarii tajnej.

3. W wykazie stanowisk pełnomocnik ochrony ewidencjonuje osoby, którym wydano poświadczenia i certyfikaty bezpieczeństwa, odmówiono wydania poświadczenia bezpieczeństwa bądź cofnięto poświadczenie bezpieczeństwa lub stwierdzono brak zastrzeżeń w wyniku kontrolnego postępowania sprawdzającego.

§ 12.
1. Komendanci akademii i szkół wojskowych oraz ośrodków szkolenia określają w wykazie stanowisk klauzule informacji niejawnych przekazywanych kandydatom na żołnierzy zawodowych (słuchaczom) w trakcie szkolenia.

2. Z chwilą zaliczenia kandydatów na żołnierzy zawodowych (słuchaczy) w poczet stanu zmiennego akademii (szkoły, ośrodka), komendanci, o których mowa w ust. 1, występują z pisemnym wnioskiem do właściwej jednostki organizacyjnej SKW lub polecają pełnomocnikom ochrony przeprowadzenie stosownego postępowania sprawdzającego, jeżeli kandydaci na żołnierzy zawodowych (słuchacze) nie posiadają odpowiedniego poświadczenia bezpieczeństwa.

§ 13.
1. Kierownicy jednostek organizacyjnych, przewidzianych do uzupełnienia żołnierzami rezerwy w drodze mobilizacji lub do mobilizacji nowych jednostek, w porozumieniu z terytorialnie właściwymi wojskowymi komendantami uzupełnień, określają w wykazach stanowisk – stanowiska związane z dostępem do informacji niejawnych, które są planowane do obsadzenia żołnierzami rezerwy.

2. Wykaz stanowisk, o którym mowa w ust. 1, opracowuje się oddzielnie dla nowo mobilizowanych jednostek.

3. O przeprowadzenie postępowań sprawdzających wobec żołnierzy rezerwy, o których mowa w ust. 1, wnioskuje (wydaje polecenie) kierownik mobilizującej jednostki organizacyjnej po otrzymaniu od wojskowego komendanta uzupełnień ankiet bezpieczeństwa osób, które nie posiadają aktualnego, odpowiedniego poświadczenia bezpieczeństwa.

4. W odniesieniu do żołnierzy rezerwy postępowania sprawdzające prowadzą:

1) zwykłe – pełnomocnicy ochrony mobilizujących jednostek organizacyjnych;
2) poszerzone i specjalne – właściwe jednostki organizacyjne SKW.

§ 14.
Kierownicy jednostek (komórek) organizacyjnych oraz inne osoby funkcyjne, uprawnione do występowania z wnioskami o przeprowadzenie postępowania sprawdzającego, występują do Szefa Służby Kontrwywiadu Wojskowego o wydanie:

1) certyfikatu bezpieczeństwa NATO (NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE) – osobom, o których mowa w art. 29 pkt. 1 oraz art. 29 a ustawy, do klauzuli nie wyższej niż posiadane poświadczenie bezpieczeństwa oraz na okres nie dłuższy niż termin ważności tego poświadczenia:

a) kierowanym do służby lub pracy w strukturach: Organizacji Traktatu Północnoatlantyckiego (NATO), Unii Europejskiej (UE) lub Unii Zachodnioeuropejskiej (UZE), zgodnie z etatem dla przedstawicieli Sił Zbrojnych Rzeczypospolitej Polskiej,
b) pełniącym służbę lub zatrudnionym w następujących komórkach, bezpośrednio dokonujących wymiany dokumentów i informacji niejawnych NATO, UE lub UZE:

- kancelariach zagranicznych,
- punktach obsługi dokumentów zagranicznych,
- kancelariach kryptograficznych (poświadczenie bezpieczeństwa oznaczone dodatkowo CRYPTO),
- stacjach łączności kryptograficznej (poświadczenie bezpieczeństwa oznaczone dodatkowo CRYPTO),
- w służbie kurierskiej;

c) uczestniczącym w pracach stałych zespołów i grup roboczych za granicą w strukturach NATO, UE lub UZE,
d) mającym dostęp do dokumentów niejawnych NATO oznaczonych dodatkowo ATOMAL,
e) posiadającym w opisie stanowiska „Job Description" wymóg dostępu do rozpoznania elektronicznego (certyfikat bezpieczeństwa oznaczony dodatkowo BOHEMIA) i po przeszkoleniu w Generalnym Zarządzie Rozpoznania Wojskowego – P2 Sztabu Generalnego WP;

2) certyfikatu potwierdzającego sprawdzenie osoby (CERTIFICATE OF SECURITY CLEARANCE) – osobom przewidzianym do uczestniczenia w konferencjach, ćwiczeniach wojskowych i wizytach międzynarodowych w instytucjach NATO, jeżeli takie wymogi zostaną określone przez partnera zagranicznego, do klauzuli zgodnej z posiadanym poświadczeniem bezpieczeństwa oraz na okres realizowanego przedsięwzięcia, jednak nie przekraczający daty ważności poświadczenia bezpieczeństwa.

§ 15.
1. Z wnioskami o przeprowadzenie zwykłych, poszerzonych lub specjalnych postępowań sprawdzających wobec osób, o których mowa w art. 29 a ustawy, Minister Obrony Narodowej, kierownicy jednostek (komórek) organizacyjnych oraz inne uprawnione osoby funkcyjne występują do Szefa Służby Kontrwywiadu Wojskowego.

2. Do wniosku, o którym mowa w ust. 1, dołącza się wypełnioną ankietę bezpieczeństwa osobowego. Wniosek wymaga uzasadnienia co do potrzeby posiadania certyfikatu.

3. Wzory wniosków o wydanie certyfikatów, o których mowa:

1) w § 14 pkt 1 – określają załączniki Nr 16, 16 a, 16 b;
2) w § 14 pkt 2 – określa załącznik Nr 17.

4. Szef Służby Kontrwywiadu Wojskowego wydaje, z zastrzeżeniem ust. 5, certyfikat bezpieczeństwa, niezwłocznie po zakończeniu postępowania sprawdzającego.

5. W przypadku wnioskowania o wydanie certyfikatu osobie posiadającej już właściwe poświadczenie bezpieczeństwa, Szef Służby Kontrwywiadu Wojskowego wydaje certyfikat, w terminie 30 dni od złożenia wniosku, po:

1) potwierdzeniu zasadności wniosku;
2) przeszkoleniu zainteresowanej osoby w zakresie przepisów bezpieczeństwa NATO, UE lub UZE i odebraniu oświadczenia o odbyciu przeszkolenia.

6. Wzory certyfikatów, o których mowa w:
1) w § 14 pkt 1 – określają załączniki Nr 18, 18 a, 18 b;
2) w § 14 pkt 2 – określa załącznik Nr 19.

7. W przypadku zagubienia (utraty) certyfikatu bezpieczeństwa lub zmiany danych personalnych, Szef Służby Kontrwywiadu Wojskowego wydaje jego duplikat, na pisemny wniosek osoby uprawnionej do występowania o przeprowadzenie postępowania sprawdzającego. Przepisy § 9 ust 1-3 stosuje się odpowiednio.

§ 16.
1. W przypadku zgłoszenia przez partnera zagranicznego wymogu potwierdzenia uprawnień do dostępu do informacji niejawnych w formie „Request for Visit" dla osób wyjeżdżających za granicę, pełnomocnik ochrony przekazuje Szefowi Służby Kontrwywiadu Wojskowego wniosek na formularzu, stanowiącym załącznik Nr 20 do decyzji. Zasady wypełniania formularza określa instrukcja stanowiąca załącznik Nr 21 do decyzji.
W przypadku partnera reprezentującego Republikę Federalną Niemiec obowiązuje formularz sporządzony również w języku niemieckim, którego wzór określają załączniki Nr 20 a, 20 b, 20 c do decyzji.

2. Wniosek, o którym mowa w ust. 1, przesyła się do Szefa Służby Kontrwywiadu Wojskowego, co najmniej na 5 dni roboczych przed upływem terminu złożenia wniosku do Krajowej Władzy Bezpieczeństwa wizytowanego kraju.

3. Zestawienie terminów składania wniosków „Request for Visit" określa załącznik Nr 22 do decyzji.

§ 17.
1. W przypadku wydania przez służby ochrony państwa decyzji o cofnięciu poświadczenia bezpieczeństwa lub poświadczenia bezpieczeństwa NATO, UE, UZE, certyfikat wydany na podstawie tych dokumentów traci ważność, o czym powiadamia się osobę, która utraciła certyfikat i osobę upoważnioną do obsady stanowiska.

2. W razie utraty ważności certyfikatu:

1) oznaczonego klauzulą ATOMAL – powiadamia się dodatkowo oficera CACO i kierownika głównej kancelarii ATOMAL;
2) oznaczonego klauzulą BOHEMIA – powiadamia się dodatkowo szefa Generalnego Zarządu Rozpoznania Wojskowego – P2 Sztabu Generalnego WP.

§ 18.
Przepisy decyzji stosuje się odpowiednio do postępowań sprawdzających prowadzonych przez Żandarmerię Wojskową, z wyłączeniem §13-17.

§ 19.
Traci moc decyzja Nr 40/MON Ministra Obrony Narodowej z dnia 9 lutego 2004r. w sprawie szczegółowych zasad i trybu przeprowadzania postępowań sprawdzających, wydawania certyfikatów bezpieczeństwa NATO i UE oraz ich dokumentowania (Dz. Urz. MON Nr 2 poz. 23).

§ 20.
Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Załącznik nr 1

.....

(klauzula tajności)

Egz. pojedynczy

WYKAZ STANOWISK I PRAC ZLECONYCH Z KTÓRYMI WIĄŻE SIĘ DOSTĘP DO INFORMACJI NIEJAWNYCH ORAZ OSÓB DOPUSZCZANYCH DO PRACY LUB SŁUŻBY NA TYCH STANOWISKACH

KLAUZULA TAJNOŚCI .....

NAZWA STANOWISKA /RODZAJ PRACY ZLECONEJ/ .....

Lp.	Stopień wojskowy	Imię i nazwisko numer PESEL	Okres pełnienia służby/pracy		Numer, data wydania i ważności		Klauzula tajności	Data szkolenia, numer zaświadczenia	Uwagi
			od	do	poświadczenia /odmowy, umorzenia/	certyfikatu			

Uwaga! Niniejszy wykaz należy prowadzić w oparciu o dołączony spis stanowisk (zleconych prac).

Załącznik nr 2

..... .

(nazwa jednostki organizacyjnej)

.....

(miejscowość i data)

.....

.....

(nazwa organu realizującego postępowanie sprawdzające)

WNIOSEK

o wszczęcie postępowania sprawdzającego

Na podstawie art. 29a, art. 37 ust. 2, art. 38 ust. 1, art. 39, art. 44 ust. 1* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631) wnoszę o wszczęcie postępowania sprawdzającego wobec:

.....

(stanowisko, stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia, PESEL)

Powód sprawdzenia**: .....

.....

.....

Wynik wcześniejszego postępowania sprawdzającego***: .....

.....

(nr poświadczenia bezpieczeństwa, data ważności)

Załącznik: 1 – Ankieta Bezpieczeństwa Osobowego – Nr ..... – tylko adresat.

Stanowisko, stopień, imię i nazwisko
kierownika jednostki organizacyjnej.

.....

(data i podpis)

* niepotrzebne skreślić

** w odniesieniu do osób przewidzianych do wyznaczenia na stanowiska lub zlecenia prac związanych z dostępem do informacji niejawnych podać nazwę stanowiska lub rodzaj pracy oraz klauzulę tajności i proponowany zakres uprawnień (NATO, UE, UZE)

*** wypełnić jeżeli postępowanie takie było prowadzone

Załącznik nr 3

..... .

(nazwa jednostki organizacyjnej)

.....

(miejscowość i data)

.....

.....

(nazwa organu realizującego postępowanie sprawdzające)

POLECENIE

wszczęcia postępowania sprawdzającego

Na podstawie art. 37 ust. 1, art. 44 ust. 1* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631.) polecam wszcząć postępowanie sprawdzające wobec:

.....

(stanowisko, stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia, PESEL)

Powód sprawdzenia**: .....

.....

Załącznik: 1 – Ankieta Bezpieczeństwa Osobowego – Nr ..... – tylko adresat.

Stanowisko, stopień, imię i nazwisko
kierownika jednostki organizacyjnej.

.....

(data i podpis)

* niepotrzebne skreślić

** w odniesieniu do osób przewidzianych do wyznaczenia na stanowiska lub zlecenia prac związanych z dostępem do informacji niejawnych podać nazwę stanowiska lub rodzaj pracy

Załącznik nr 4

.....

(nazwa organu realizującego postępowanie sprawdzające)

.....

(klauzula tajności)

Egzemplarz pojedynczy

AKTA

POSTĘPOWANIA SPRAWDZAJĄCEGO

.....

(nr akt / PS (Z, P lub S) / rok)

.....

(stopień wojskowy, nazwisko i imię, imię ojca, PESEL)

ROZPOCZĘTO .....

ZAKOŃCZONO .....

ILOŚĆ STRON .....

PRZECHOWYWAĆ LAT .....

KATEGORIA ARCHIWALNA .....

TECZKA AKT

POSTĘPOWANIA SPRAWDZAJĄCEGO

Zawiera:

1) Spis dokumentów;
2) Wykaz osób prowadzących teczkę;
3) Wykaz osób zapoznanych z dokumentami;
4) Wniosek o wszczęcie (polecenie wszczęcia) postępowania sprawdzającego;
5) Ankietę bezpieczeństwa osobowego (wg załącznika nr 2a, 2b, 2c ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych);
6) Wyniki sprawdzeń:

– w Krajowym Rejestrze Karnym,
– w Biurze Informacji i Statystyki Centralnego Zarządu Służby Więziennej,
– w Urzędzie Stanu Cywilnego,
– w ewidencjach i kartotekach niedostępnych powszechnie (wyłącznie w odniesieniu do osób kandydujących na stanowiska z dostępem do informacji niejawnych oznaczonych klauzulą „poufne"),

7) Inne dokumenty oraz korespondencję dotyczącą realizowanych czynności w ramach postępowania sprawdzającego;
8) Notatkę dotyczącą wyniku procedury sprawdzeniowej (wydanie poświadczenia bezpieczeństwa, odmowa wydania poświadczenia bezpieczeństwa, umorzenie postępowania sprawdzającego, zawieszenie postępowania sprawdzającego, podjęcia postępowania sprawdzającego);
9) Drugi egzemplarz informacji przesłanej do kierownika właściwej jednostki organizacyjnej dotyczącej sposobu zakończenia postępowania;
10) Kserokopie decyzji, postanowień, potwierdzeń odbioru.

(nr akt)

SPIS DOKUMENTÓW

Nr dokumentów		Skąd lub dokąd przesłany	Nazwa dokumentu	Numer strony	Uwagi
Wych.	Wch.				
1	2	3	4	5	6

(nr akt)

WYKAZ

osób prowadzących teczkę

Lp.	*Stanowisko, stopień, imię i nazwisko prowadzącego teczkę*	*Okres prowadzenia*		*Podpis i data*
		Od	*do*	
1	*2*	*3*	*4*	*5*

(nr akt)

WYKAZ

osób zapoznanych z dokumentami

Lp.	Stanowisko, stopień, imię i nazwisko	Podstawa (nr poświadczenia bezpieczeństwa)	Data zapoznania	Podpis
1	2	3	4	5

Załącznik nr 5

MINISTERSTWO SPRAWIEDLIWOŚCI
KRAJOWY REJESTR KARNY

Nazwa jednostki organizacyjnej

Data wpływu

znak opłaty

Data wystawienia .....

ZAPYTANIE O UDZIELENIE INFORMACJI O OSOBIE*)

Numer PESEL

1. Nazwisko rodowe .....
2. Nazwisko (w tym przybrane) .....
3. Imiona .....
4. Imię ojca ..... 5. Imię matki .....
6. Data urodzenia ..... 7. Nazwisko rodowe matki .....
8. Miejsce urodzenia ..... 9. Obywatelstwo .....
10. Miejsce zamieszkania .....
11. Wskazanie postępowania, o którym mowa w art. 6 pkt 4-6 i 8-10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. nr 50, poz. 580), w związku z którym zachodzi potrzeba uzyskania informacji o osobie**)

.....

12. Rodzaj danych, które mają być przedmiotem informacji o osobie***:

☐ 1. Kartoteka Karna ☐ 2. Kartoteka Nieletnich

☐ 3. Kartoteka Osób Pozbawionych Wolności oraz Poszukiwanych Listem Gończym)

13. Zakres danych, które mają być przedmiotem informacji o osobie .....

(pieczęć pełnomocnika ochrony
/żołnierza służby ochrony państwa****)

.....
(data i podpis)

*) Dane osobowe należy podać wyłącznie na podstawie dokumentów potwierdzających tożsamość.
**) W punkcie 11 należy wpisać podstawę prawną sprawdzenia:
SKW – art. 6 pkt. 7 ustawy o KRK;
Pełnomocnicy ochrony – art. 37 ust. 4 pkt. 1 ustawy o ochronie informacji niejawnych.
***) W punkcie 12 należy wpisać X w odpowiednim kwadracie.
****) Niepotrzebne skreślić.

Załącznik nr 6

.....
(nazwa jednostki organizacyjnej)

Centralny Zarząd Służby Więziennej

Biuro Informacji i Statystyki
ul. Rakowiecka 37 a
00-975 Warszawa 12 skr. poczt. 200

Na postawie art. 37 ust. 4 pkt. 1*/ art. 38 ust. 1 pkt. 1*/ art. 39* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz. 1631), w związku z prowadzonym postępowaniem sprawdzającym proszę o udzielenie informacji o:

PESEL .....
Nazwisko .....
Nazwisko rodowe .....
Imię .....
Imię ojca .....
Imię matki .....
Data urodzenia .....
Miejsce urodzenia .....

(pieczęć pełnomocnika ochrony
/żołnierza służby ochrony państwa*)

.....
(data i podpis)

*) Niepotrzebne skreślić.

.....
(nazwa jednostki organizacyjnej)

.....
(miejscowość, data)

KIEROWNIK
URZĘDU STANU CYWILNEGO
ul. .....
.....

WNIOSEK

Na podstawie art. 83 ust. 1 ustawy z dnia 29 września 1986 r. prawo o aktach stanu cywilnego *(Dz. U. nr 36 poz. 180 ze zm.)* w związku z art. 37 ust. 4 pkt 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz 1631) wnoszę o wydanie odpisu skróconego aktu urodzenia / małżeństwa*) niżej wymienionej osoby:

.....
(nazwisko, nazwisko rodowe i imiona)

.....
(imiona rodziców)

.....
(data i miejsce urodzenia, nr PESEL)

Wobec ww. prowadzone jest postępowanie sprawdzające przed wydaniem poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych stanowiących tajemnicę służbową.

pieczęć pełnomocnika ochrony

.....
(data i podpis)

* niepotrzebne skreślić

Załącznik 8

.....

(nazwa jednostki organizacyjnej)

.....

.....

(nazwa właściwej terytorialnie jednostki organizacyjnej realizującej sprawdzenia)

WNIOSEK

o przeprowadzenie sprawdzeń zgodnie z art. 37 ust. 4 pkt. 2 w związku z art. 18 ust. 7 ustawy z dnia 22 stycznia 1999 r. (Dz. U.z 2005r. nr 196 poz. 1631)

Proszę o dokonanie sprawdzeń w ewidencjach i kartotekach niedostępnych powszechnie wobec:

.....

(stopień, imię i nazwisko, imię ojca, imię i nazwisko panieńskie matki)

.....

.....

(data i miejsce urodzenia, dokładny adres zamieszkania, PESEL)

Podstawa sprawdzenia:.....

.....

(powód sprawdzenia, nr akt postępowania)

pieczęć pełnomocnika ochrony

.....

(data i podpis)

.....

(nazwa jednostki organizacyjnej)

.....

(miejscowość, data)

NOTATKA

w sprawie przeprowadzenia rozmowy z osobą sprawdzaną w ramach procedury postępowania sprawdzającego

.....

(stopień, imię, nazwisko osoby sprawdzanej, numer akt)

Dokument powinien zawierać następujące elementy:

1. Podstawę prawną, czas i miejsce rozmowy.

2. Powód przeprowadzenia rozmowy.

3. Cel rozmowy.

4. Zwięzły opis treści rozmowy oraz uzyskanych informacji od osoby sprawdzanej.

5. Ocena uzyskanych informacji w celu ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

6. Wnioski, podjęte decyzje, postanowienia, zamierzenia wraz z podstawą prawną.

(stanowisko, stopień, imię i nazwisko sporządzającego)

.....

(podpis)

Załącznik Nr 10

.....
(nazwa jednostki organizacyjnej)

.....
(miejscowość, data)

.....
(klauzula tajności)
Egz. pojedynczy

NOTATKA

w sprawie: ..... .
(wyników procedury sprawdzenia, akta nr)

Dokument powinien zawierać następujące elementy:

1. Podstawę, czas i miejsce zrealizowanych czynności i ustaleń oraz ich cel, w tym:
   - na czyje polecenie lub wniosek wszczęto postępowanie,
   - w jakim okresie realizowano postępowanie,
   - jakie czynności (sprawdzenia) zrealizowano, itp.

2. Zwięzły opis wykonanych czynności i uzyskanych rezultatów.

3. Ocena faktu (zdarzenia, zjawiska) lub uzyskanej informacji (zwłaszcza w sytuacji ustalenia wątpliwości, czy osoba sprawdzana daje rękojmię zachowania tajemnicy).

4. Wnioski i podjęte decyzje wraz z podstawą prawną.

(stanowisko, stopień, imię i nazwisko sporządzającego)

.....

(podpis)

Załącznik nr 11

WYKAZ OSÓB, WOBEC KTÓRYCH PRZEPROWADZONO POSTĘPOWANIA SPRAWDZAJĄCE*

Układ strony lewej

Lp. data wszczęcia	Stopień wojskowy	Dane personalne osoby		Miejsce zamieszkania (kod, miejscowość, ulica, nr domu i mieszkania	Miejsce pracy, służby, stanowisko	Sygnatura akt postępowania sprawdzającego (np.: nr koleiny akt/rodzaj postępowania/rok) ...../PS/...../.....
		Imię i nazwisko, imię ojca	Data i miejsce urodzenia			
1	2	3	4	5	6	7

Układ strony prawej

Miejsce przechowywania akt postępowania sprawdzającego**)	Data i numer				Klauzula tajności	Data wydania i nr zaświadczenia o przeszkoleniu	Data i właściwej stki SKW przesłano cyjną *
	Wydane poświadczenia bezpieczeństwa	Odmowy wydania poświadczenia bezpieczeństwa	umorzenia	Cofnięcia poświadczenia bezpieczeństwa			
8	9	10	11	12	13	14	15

Uwaga!

*) dopuszcza się prowadzenie wykazu oddzielnie dla każdej klauzuli tajności.

**) W pozycji nr 8 należy wpisywać nazwę jednostki organizacyjnej, w której realizowano postępowanie sprawdzające. Natomiast w pozycji nr 15 wpisuje się „Dowódca J.W. ....."

Załącznik Nr 12

.....
(pieczęć nagłówkowa jednostki organizacyjnej/
służby ochrony państwa)

DECYZJA Nr.....
z dnia.....
w sprawie umorzenia postępowania sprawdzającego

Na podstawie art. 36 ust. 2b pkt.....[1] ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631)
umarzam postępowanie sprawdzające prowadzone w stosunku do

.....
(imię i nazwisko osoby sprawdzanej, data urodzenia)

Uzasadnienie

Na polecenie/wniosek* .....,
(określenie osoby, na polecenie/wniosek której wszczęte zostało postępowanie sprawdzające)

w dniu.....zostało wszczęte zwykłe/poszerzone/specjalne* postępowanie sprawdzające

wobec.....,
(imię i nazwisko osoby sprawdzanej, data urodzenia)

w związku z zamiarem obsadzenia tej osoby na stanowisku.....
w....., z którym wiąże się dostęp do informacji niejawnych.
W toku prowadzonego postępowania sprawdzającego okazało się, że .....[2]
o czym *pełnomocnik do spraw ochrony informacji niejawnych/służba ochrony państwa** został poinformowany w piśmie..... z dnia .....
Wobec powyższego dalsze prowadzenie postępowania sprawdzającego stało się bezprzedmiotowe i dlatego – na podstawie art. 36 ust. 2b pkt .....[1] – postępowanie należy umorzyć.
Biorąc powyższe pod uwagę, orzeczono jak na wstępie.

Imienna pieczęć i podpis pełnomocnika
do spraw ochrony informacji niejawnych/
upoważnionego funkcjonariusza albo żołnierza służby
ochrony państwa

<u>Pouczenie:</u>

Od decyzji przysługuje zainteresowanemu odwołanie do Szefa Służby Kontrwywiadu Wojskowego /Prezesa Rady Ministrów * wniesione za pośrednictwem organu wydającego decyzję, w terminie 14 dni od dnia jej doręczenia.

Decyzję otrzymują:
1) osoba sprawdzana,
2) aa.

* Niepotrzebne skreślić.
[1] Wpisać odpowiedni punkt z art. 36 ust. 2 b ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.
[2] Wpisać okoliczności z odpowiedniego przepisu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

Załącznik Nr 13

.....
(pieczęć nagłówkowa jednostki organizacyjnej\
służby ochrony państwa)

POSTANOWIENIE Nr.....

z dnia.....
w sprawie zawieszenia postępowania sprawdzającego

Na podstawie art. 36 ust. 2c pkt.....[1] ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631)

postanawiam
zawiesić postępowanie sprawdzające prowadzone w stosunku do

.....
(imię i nazwisko osoby sprawdzanej, data urodzenia)

Uzasadnienie

Na polecenie/wniosek* .....,
(osoba, na polecenie/wniosek której wszczęte zostało postępowanie sprawdzające)

w dniu.....zostało wszczęte zwykłe/poszerzone/specjalne* postępowanie sprawdzające wobec....., w związku
(imię i nazwisko osoby sprawdzanej)

z zamiarem obsadzenia tej osoby na stanowisku ....., z którym wiąże się dostęp do informacji niejawnych.
W piśmie.....z dnia....., *pełnomocnik do spraw ochrony informacji niejawnych/służba ochrony państwa** został zawiadomiony o tym, że .....[2]
W świetle art. 36 ust. 2c pkt.....[1] ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, okoliczność powyższa uzasadnia zawieszenie postępowania sprawdzającego.
Mając powyższe na uwadze, postanowiono jak na wstępie.

Imienna pieczęć i podpis pełnomocnika
do spraw ochrony informacji niejawnych/
upoważnionego funkcjonariusza albo żołnierza służby ochrony
państwa

Pouczenie:
Od niniejszego postanowienia przysługuje zainteresowanemu zażalenie do Szefa Służby Kontrwywiadu Wojskowego /Prezesa Rady Ministrów* wniesione za pośrednictwem organu wydającego postanowienie, w terminie 7 dni od dnia doręczenia niniejszego postanowienia.

Decyzję otrzymują:
1) osoba sprawdzana,
2) aa.

* Niepotrzebne skreślić.
[1] Wpisać odpowiedni przepis ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.
[2] Wpisać okoliczności z odpowiedniego przepisu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

Załącznik Nr 14

.....
(pieczęć nagłówkowa jednostki organizacyjnej/
służby ochrony państwa)

POSTANOWIENIE Nr.....

z dnia.....
w sprawie podjęcia zawieszonego postępowania sprawdzającego

Na podstawie art. 36 ust. 2e ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005r. Nr 196, poz. 1631)

postanawiam
podjąć zawieszone postępowanie sprawdzające prowadzone w stosunku do

.....
(imię i nazwisko osoby sprawdzanej, data urodzenia)

Uzasadnienie

Na mocy postanowienia *pełnomocnika do spraw ochrony informacji niejawnych/służby ochrony państwa** Nr....., z dnia....., zwykłe/poszerzone/specjalne* postępowanie sprawdzające toczące się w stosunku do .....zostało, na podstawie art. 36 ust. 2c pkt.....[1] ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, zawieszone z powodu.....[2]
Przyczyna zawieszenia postępowania aktualnie ustąpiła, o czym *pełnomocnik do spraw ochrony informacji niejawnych/służba ochrony państwa** uzyskał informację w piśmie ..... z dnia.....
Na podstawie art. 36 ust. 2e ustawy o ochronie informacji niejawnych, *pełnomocnik ds. ochrony informacji niejawnych/służba ochrony państwa** podejmuje zawieszone postępowanie po ustaniu przyczyny zawieszenia.

Biorąc powyższe pod uwagę, postanowiono jak na wstępie.

Imienna pieczęć i podpis pełnomocnika
do spraw ochrony informacji niejawnych/
upoważnionego funkcjonariusza albo żołnierza służby ochrony
państwa

Postanowienie otrzymują:
3) osoba sprawdzana,
4) aa.

* Niepotrzebne skreślić.
[1] Wpisać odpowiedni przepis ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.
[2] Wpisać okoliczności z odpowiedniego przepisu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

Załącznik nr 15

KARTA EWIDENCYJNA

1. .....
Nazwisko (wypełnić drukowanymi literami)

2. .....
Nazwisko poprzednie (wypełnić drukowanymi literami)

3. .....
Imię, imiona (wypełnić drukowanymi literami)

4. .....
Imię ojca

5. .....
Nr PESEL, miejsce urodzenia

6. .....
Miejsce zamieszkania (kod i miejscowość, ulica, nr domu, nr mieszkania)

7. .....
Nazwa i adres jednostki organizacyjnej

8. .....
Nazwa komórki organizacyjnej zajmowane stanowisko(praca zlecona-data objęcia stanowiska/rozpoczęcia pracy

.....

9. .....
Sygnatura akt postępowania sprawdzającego i miejsce ich przechowywania

10. .....
Zakres dostępu do informacji (zastrzeżone poufne, tajne, ściśle tajne)*

11. .....
Data wydania poświadczenia bezpieczeństwa/odmowy/ umorzenia/cofnięcia/potwierdzenia*

12. .....
Data ważności poświadczenia bezpieczeństwa

13. .....
Numer poświadczenia bezpieczeństwa/odmowy umorzenia/ cofnięcia/potwierdzenia*

14. .....
Data wydania i numer zaświadczenia o przeszkoleniu w zakresie ochrony informacji niejawnych

.....
(imienna pieczęć i podpis upoważnionego żołnierza SKW lub pełnomocnika ochrony)

15. .....
Nazwa jednostki SKW (wypełnia właściwa jednostka terytorialna)

.....adnotacje .....

.....

.....

.....

.....

* Niepotrzebne skreślić

Załącznik nr 16

.....

(nazwa jednostki organizacyjnej)

.....

(miejscowość, data)

SZEF

SŁUŻBY KONTRWYWIADU WOJSKOWEGO

Warszawa

WNIOSEK

o wydanie certyfikatu bezpieczeństwa NATO

Wnoszę o wydanie certyfikatu bezpieczeństwa NATO (NATO PERSONEL SECURITY CLEARANCE CERTIFICATE) uprawniającego do dostępu do wiadomości oznaczonych klauzulą:

- COSMIC TOP SECRET,*
- NATO SECRET,*
- NATO CONFIDENTIAL,*

dodatkowo:

- ATOMAL,*
- CRYTO*
- BOHEMIA*

dla.....
.....

(stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia ,nr PESEL)

z datą ważności do ..... .

Nadmieniam, że ww. posiada poświadczenie bezpieczeństwa nr .....

ważne do dnia ....., upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą ..... .

Załączniki: potwierdzona kserokopia poświadczenia bezpieczeństwa i dokumentów dających podstawę wydania certyfikatu bezpieczeństwa NATO.

Stanowisko, stopień, imię i nazwisko

kierownika jednostki organizacyjnej
(wnioskodawcy)

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 16a

.....

(nazwa jednostki organizacyjnej)

.....
(miejscowość, data)

SZEF

SŁUŻBY KONTRWYWIADU WOJSKOWEGO

Warszawa

WNIOSEK

o wydanie certyfikatu bezpieczeństwa UE

Wnoszę o wydanie certyfikatu bezpieczeństwa UE (EU PERSONNEL SECURITY CLEARANCE CERTIFICATE) uprawniającego do dostępu do wiadomości oznaczonych klauzulą:

- TRÈS SECRET UE / EU TOP SECRET,*
- SECRET UE / EU SECRET,*
- CONFIDENTIEL UE / EU CONFIDENTIAL,*
- RESTREINT UE/ EU RESTRICTED.*

dla.....

(stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia, nr PESEL)

z datą ważności do ..... .

Nadmieniam, że ww. posiada poświadczenie bezpieczeństwa nr ..... ważne do dnia ....., upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą ..... .

Załączniki: potwierdzona kserokopia poświadczenia bezpieczeństwa i dokumentów dających podstawę wydania certyfikatu bezpieczeństwa UE.

Stanowisko, stopień, imię i nazwisko
kierownika jednostki organizacyjnej
(wnioskodawcy)

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 16b

.....

(nazwa jednostki organizacyjnej)

.....
(miejscowość, data)

SZEF

SŁUŻBY KONTRWYWIADU WOJSKOWEGO

Warszawa

WNIOSEK

o wydanie certyfikatu bezpieczeństwa UZE

Wnoszę o wydanie certyfikatu bezpieczeństwa UZE (WEU PERSONEL SECURITY CLEARANCE CERTIFICATE) uprawniającego do dostępu do wiadomości oznaczonych klauzulą:

- TRÈS SECRET UEO / WEU TOP SECRET,*
- SECRET UEO / WEU SECRET,*
- CONFIDENTIEL UEO / WEU CONFIDENTIAL,*
- RESTREINT UEO/ WEU RESTRICTED.*

dla.....

(stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia, nr PESEL)

z datą ważności do ..... .

Nadmieniam, że ww. posiada poświadczenie bezpieczeństwa nr ..... ważne do dnia ....., upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą ..... .

Załączniki: potwierdzona kserokopia poświadczenia bezpieczeństwa i dokumentów dających podstawę wydania certyfikatu bezpieczeństwa UZE.

Stanowisko, stopień, imię i nazwisko
kierownika jednostki organizacyjnej
(wnioskodawcy)

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 17

.....

(nazwa jednostki organizacyjnej)

.....

(miejscowość, data)

SZEF

SŁUŻBY KONTRWYWIADU WOJSKOWEGO

Warszawa

WNIOSEK

o wydanie certyfikatu potwierdzającego sprawdzenie osoby

Wnoszę o wydanie certyfikatu potwierdzającego sprawdzenie osoby (CERTIFICATE OF SECURITY CLEARENCE) uprawniającego do dostępu do wiadomości oznaczonych klauzulą:

- COSMIC TOP SECRET,*
- NATO SECRET,*
- NATO CONFIDENTIAL,*

dodatkowo:

- ATOMAL,*
- CRYTO*
- BOHEMIA*

dla .....

(stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia ,nr PESEL)

na okres od ..... do ..... .

Seria, numer, data i miejsce wydania paszportu .....

.....

Cel pobytu .....

Nadmieniam, że ww. posiada poświadczenie bezpieczeństwa nr .....

ważne do dnia ....., upoważniające do dostępu do informacji niejawnych

oznaczonych klauzulą ..... .

Załączniki: potwierdzona kserokopia poświadczenia bezpieczeństwa i dokumentów o udziale

osoby w konferencji, ćwiczeniu wojskowym, wizycie międzynarodowej.

Stanowisko, stopień, imię i nazwisko

kierownika jednostki organizacyjnej
(wnioskodawcy)

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 18

NATO PERSONEL SECURITY CLEARANCE CERTYIFICATE

1. Certification is herby given that:

Full Name:

.....

Date and Place of Birth:

.....

has been granted a personnel security clearance by the Government of:

.....

in accordance with current NATO regulations, including the Security Annex to C-M(64) 39 in the case of ATOMAL Information, and is, therefore, declared suitable to be entrusted with information classified up to and including:

.....

.....

2. The validity of this certificate will expire not later than

.....

Signed:

Title:
(Optional)

Official government stamp

Date:

Załącznik nr 18a

EU PERSONEL SECURITY CLEARANCE CERTYIFICATE

1. Certification is herby given that:

Full Name:

Date and Place of Birth:

Fulfils security requirements according to UE provision and has been cleared

For access to Information classified up to and including:

in accordance with performing his duties in the following institution:

2. The yalidity of this certificate will expire not later than

Signed:

Title: Official government stamp

Date:

Załącznik nr 18b

WEU SECURITY CERTYIFICATE

This is to certify that:

Surname and forenames: .....

Place and date of birth: .....

Is the holder of a security clearance astablished by the Government of:

.....

in conformity with current WUE regulations and may receive classified

information up to and including:

.....

.....

.....

.....

The present certificate expires on: ..... 20.....

Signed:

Title: Official Government Stamp

Date:

Załącznik nr 19

CERTYIFICATE OF SECURITY CLEARANCE

Issued by .....

(number nation or NATO civil or military body)

Date and Place of Issue

.....

.....

Valid until

.....

This is to certify that:

Full Name

.....

Date of Birth

.....

Place of Birth

.....

Nationality

.....

Were employed

.....

Purpose and Duration of Visit

.....

.....

.....

Holder of Passport/Identity Card No.

.....

Issued at

.....

Dated

.....

Military Rank and Number (where applicable)

.....

Hes been granted access to NATO information classified up to and including

.....

in accordance with current NATO security regulations, including the Security Annex to C-M(64) 39 in the case of ATOMAL information, and has been briefed accordingly by

.....

Signed:

Title: Official government stamp (Optional)

Date:

NOTE: This certificate must be handled in accordance with the provision of NATO

Security Policy and its supporting directives.

WNIOSEK O ZŁOŻENIE WIZYTY

Jednorazowa ( )
Wielokrotna ( )

Aneks(y)
( ) Tak
( ) Nie

1. DANE ADMINISTRACYJNE

WNIOSKUJĄCY: DATA:
DO: NR WIZYTY:

2. INSTYTUCJA RZĄDOWA LUB PODMIOT PRZEMYSŁOWY WYSTĘPUJĄCY Z WNIOSKIEM

NAZWA:
ADRES DO KORESPONDENCJI:

TELEX/FAX Nr: TELEFON Nr:
PUNKT KONTAKTOWY:

3. WIZYTOWANA INSTYTUCJA RZĄDOWA LUB PODMIOT PRZEMYSŁOWY

NAZWA :

ADRES DO KORESPONDENCJI:

TELEX/FAX Nr: TELEFON Nr:
PUNKT KONTAKTOWY:

4. DATA WIZYTY:

5. RODZAJ WIZYTY: (ZAZNACZ TYLKO JEDEN RODZAJ)

( ) INICJATYWA RZĄDOWA
( ) INICJATYWA ZAPRASZONEJ INSTYTUCJI LUB PODMIOTU RZEMYSŁOWEGO
( ) PRZEDSIĘWZIĘCIE HANDLOWE
( ) ZAPROSZENIE PODMIOTU, KTÓRY BĘDZIE ODWIEDZANY

6. TEMAT DO DYSKUSJI LUB UZASADNIENIE:

7. PRZEWIDYWANY STOPIEŃ TAJNOŚCI INFORMACJI:

8. CZY WIZYTA DOTYCZY: (TAK) ZAZNACZ

SZCZEGÓLNEGO WYPOSAŻENIA CZY SYSTEMU BRONI? SPRZEDAŻY SPRZĘTU ZA GRANICĘ CZY EKSPORTOWI LICENCJI? PROGRAMU CZY POROZUMIENIA? PRZYSWOJENIA PROCESU OBRONNEGO? INNE?

NATO JAWNE

WNIOSEK O ZŁOŻENIE WIZYTY (cd.)

9. DANE OSOBOWE SKŁADAJĄCEGO WIZYTĘ

NAZWISKO I IMIĘ:

DATA URODZENIA:

MIEJSCE URODZENIA:

OBECNY STOPIEŃ DOPUSZCZENIA DO TAJEMNICY:

NUMER PASZPORTU LUB DOWODU OSOBISTEGO:

NARODOWOŚĆ:

STANOWISKO:

PRZEDSIEBIORSTWO LUB INSTYTUCJA:

10. PEŁNOMOCNIK OCHRONY INSTYTUCJI SKŁADAJĄCEJ WNIOSEK

NAZWISKO I IMIĘ; TELEFON Nr:

PODPIS:

11. WYSTAWIENIE CERTYFIKATU (SPRAWDZENIE PRZEZ WŁAŚCIWE WŁADZE)

NAZWISKO:

ADRES: STEMPEL

TELEFON:

PODPIS:

12. KRAJOWE WŁADZE BEZPIECZEŃSTWA SKŁADAJĄCE WNIOSEK (KWB)

NAZWISKO:

ADRES: STEMPEL

TELEFON:

PODPIS:

13. UWAGI

NATO UNCLASSIFIED

One-time ( )
Recurring ( )

REQUEST FOR VISIT

Annex(es)
( ) Yes
( ) No

ADMINISTRATIVE DATA

1. REQUESTOR: DATE:
TO: VISIT ID:

REOUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY

2. NAME: POSTAL ADDRESS:

TELEX/FAX No.: TELEPHONE No .
POINT OF CONTACT:

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED

3. NAME: ADDRESS:

TELEX/FAX No.. TELEPHONE No.:
POINT OFCONTACT:

4. DATESOF VISIT:

5. TYPE OF VISIT: (SELECT ONE FROM EACH COLUMN)

( )GOVERNMENT INITIATIVE
( ) INITIATED BY REQUESTING AGENCY OR FACILITY
( ) COMMERCIAL iNITIATIVE
( ) BY INVITATION OF THE FACILITY TO BE VISITED

6. SUBJECT TO BE DISCUSSED/JUSTIFICATION:

7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED:

8. IS THE VISIT PERTINENT TO: (Y) SPECIFY

A SPECIFIC EOUIPMENT OR WEAPON SYSTEM
FOREIGN MILITARY SALES OR EXPORT LICENCE
A PROGRAMME OR AGREMENT
A DEFENCE ACQUISITION PROCESS
OTHER

REQUEST FOR VISIT (continuation)

9. PARTICULARS FOR VISITORS

NAME:
DATE OF BIRTH:
PLACE OF BIRTH:
SECURITY CLEARANCE:
ID/PP NUMBER:
NATIONALITY:
POSITION:
COMPANY/AGENCY:

10. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY

NAME: TELEPHONE No.:
SIGNATURE:

11. CERTIFICATION OF SECURITY CLEARANCE

NAME:

ADDRESS: STAMP

TELEPHONE:

SIGNATURE:

12. REQUESTING NATIONAL SECURITY AUTHORITY

NAME:

ADDRESS: STAMP

TELEPHONE

SIGNATURE:

13. REMARKS

WNIOSEK O ZŁOŻENIE WIZYTY (RFV) Odniesienie:

do pkt. 3 RFV

WIZYTOWANA INSTYTUCJA RZĄDOWA LUB PODMIOT PRZEMYSŁOWY

1. NAZWISKO

   ADRES:

   TELEX/FAX Nr: TELEFON Nr :

   PUNKT KONTAKTOWY

2. NAZWISKO

   ADRES:

   TELEX/FAX Nr: TELEFON Nr :

   PUNKT KONTAKTOWY

3. NAZWISKO

   ADRES:

   TELEX/FAX Nr : TELEFON Nr:

   PUNKT KONTAKTOWY

4 NAZWISKO

   ADRES

   TELEX/FAX Nr: TELEFON Nr:

   PUNKT KONTAKTOWY

5. NAZWISKO

   ADRES:

   TELEX/FAX Nr: TELEFON Nr:

   PUNKT KONTAKTOWY

Załacznik 20

REQUEST FOR VISIT

Refercnce: RFV- format, Item 3.

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED

1. NAME: .

ADDRESS:

TELEX/FAX No.: TELEPHONE No.:

POINT OFCONTACT:

2. NAME:

ADDRESS:

TELEX7FAXNo.: TELEPHONE No.:

POINT OFCONTACT:

3. NAME:

ADDRESS:

TELEX/FAX No.: TELEPHONE No. :

POINT OFCONTACT

4 NAME:

ADDRESS:

TELEX/FAX No.: TELEPHONE No.:

POINT OF CONTACT

5 NAME:

ADDRESS:

TELEX/FAX No.: TELEPHONE No.:

POINT OF CONTACT:

WNIOSEK O ZŁOŻENIE WIZYTY

Odniesienie: do pkt. 9 RFV.

DANE ODWIEDZAJĄCYCH

1. NAZWISKO i IMIĘ:

   DATA URODZENJA: ././. MIEJSCE URODZENIA:
   POSIADANY CERTYFIKAT: NARODOWOŚĆ:
   STANOWISKO: NR PASZPORTU:
   ZATRUDNIENIE:

2. NAZWISKO i IMIĘ:

   DATA URODZENIA: ././. MIEJSCE URODZENIA:
   POSIADANY CERTYFIKAT: NARODOWOŚĆ:
   STANOWISKO: NR PASZPORTU:
   ZATRUDNIENIE:

3 NAZWISKO i IMIĘ:

   DATA URODZENIA: ././. MIEJSCE URODZENIA:
   POSIADANY CERTYFIKAT: NARODOWOŚĆ:
   STANOWISKO: NR PASZPORTU:
   ZATRUDNIENIE:

4 NAZWISKO i IMIĘ:

   DATA URODZENIA: ././. MIEJSCE URODZENIA.
   POSIADANY CERTYFIKAT: NARODOWOŚĆ:
   STANOWISKO: NR PASZPORTU:
   ZATRUDNIENIE:

5. NAZWISKO i IMIĘ:

   DATA URODZENJA: ././. MIEJSCE URODZENIA:
   POSIADANY CERTYFIKAT: NARODOWOŚĆ:
   STANOWISKO: NR PASZPORTU:
   ZATRUDNIENIE:

6. NAZWISKO i IMIĘ:

   DATAURODZENJA: ././. MIEJSCE URODZENIA:
   POSIADANY CERTYFIKAT NARODOWOŚĆ:
   STANOWISKO: NR PASZPORTU:
   ZATRUDNIENIE:

REQUEST FOR VISIT

Reference: RFV - format, Item 9.

PARTICULARS OF VISITORS

1. NAME:

   DATE OF BIRTH: ././. PLACE OF BIRTH:
   SECURITY CLEARANCE: NATIONALITY:
   POSITION: ID/PP NUMBER:
   COMPANY/AGENCY:

2. NAME:

   DATE OF BIRTH: ././. PLACE OF BIRTH:
   SECURITY CLEARANCE: NATIONALITY:
   POSITION: ID/PP NUMBER:
   COMPANY/AGENCY:

3. NAME:

   DATE OF BIRTH: ././. PLACE OF BIRTH:
   SECURITY CLEARANCE: NATIONALITY:
   POSITION: ID/PP NUMBER:
   COMPANY/AGENCY:

4. NAME:

   DATE OF BIRTH: ././. PLACE OF BIRTH:
   SECURITY CLEARANCE: NATIONALITY:
   POSITION: ID/PP NUMBER:
   COMPANY/AGENCY:

5. NAME:

   DATE OF BIRTH: ././. PLACE OF BIRTH:
   SECURITY CLEARANCE: NATIONALITY:
   POSITION: ID/PP NUMBER:
   COMPANY/AGENCY:

6. NAME:

   DATE OF BIRTH: ././. PLACE OF BIRTH:
   SECURITY CLEARANCE: NATIONALITY:
   POSITION: ID/PP NUMBER:
   COMPANY/AGENCY:

Request for Visit (RFV)
Besuchsantrag

☐ One-time / Einmaliger Besuch

☐ Recurring / Wiederkehrender Besuch

☐ Emergency / Eiliger Besuch

Annex(es) / Anlage(n)

☐ Yes / Ja

☐ No / Nein

1	Administrative Data / Personendaten Requester / Antragsteller	Date / Datum
	to / an	Visit ID / Besuchsnummer
2	Requesting Government Agency or Industrial Facility / Antragstellende Dienststelle/Firma Name / Name	
	Postal Address / Postanschrift	
	Telex/Fax Nr.	Telephone Nr.
3	Government Agency or Industrial Facility to be visited / Zu besuchende Dienststelle/Firma Name / Name	
	Postal Address / Postanschrift	
	Telex/Fax Nr.	
	Point of contact / Ansprechpartner	Telephone Nr.
4	Dates of Visit / Besuchszeitraum von	to / bis
5	Type of Visit (Select one from each column) / Grund des Besuches (Kreuzen Sie bitte in jeder Spalte jeweils einen Punkt an) ☐ Government initiative / Regierungsinitiative/-auftrag ☐ Commercial initiative / Firmeninitiative/-intern ☐ Initiated by requesting agency or facility / von der antragstellenden Dienststelle/Firma gewünscht ☐ by invitation of the facility to be visited / auf Einladung der zu besuchenden Stelle	
6	Subject to be discussed/Justification / Besuchszweck (Angaben in Deutsch. Zusätzlich in der Landessprache oder in Englisch)	
7	Anticipated Level of classified Information to be involved / Zu erwartender Geheimhaltungsgrad	
8	Is the Visit pertinent to / Steht der Besuch in Zusammenhang mit ☐ a specific equipment or weapon system? / einem speziellen Waffensystem/Gerät?	Specify? / Mit welchem?
	☐ foreign military sales or export license? / einem Ausfuhrprojekt oder Export-Lizenz?	
	☐ a programme or agreement? / einem Programm oder Vereinbarung?	
	☐ a defence acquisition programme? / einem Beschaffungsprogramm?	
	☐ other? / Sonstigem?	

9	Particulars of Visitors / Daten der Besucher Name / Name		
	Date of birth / Geburtsdatum	Place of birth / Geburtsort	
	Security clearance / Sicherheitsermächtigung	ID/PP Number / Paß-/Ausweisnummer	Nationality / Staatsangehörigkeit
	Position / Funktion/Dienststellung		
	Company/Agency / Dienststelle/Firma		
	Name / Name		
	Date of birth / Geburtsdatum	Place of birth / Geburtsort	
	Security clearance / Sicherheitsermächtigung	ID/PP Number / Paß-/Ausweisnummer	Nationality / Staatsangehörigkeit
	Position / Funktion/Dienststellung		
	Company/Agency / Dienststelle/Firma		
10	The Security Officer of the requesting Government Agency or Industrial Facility / Siicherheitsbeauftragter/Sicherheitsbevollmächtigter Name / Name	Telephone Nr.	
	Signature / Unterschrift	Date / Datum	
11	Certification of Security Clearence / Bestätigung der Ermächtigung Name / Name	Telephone Nr.	
	Address / Anschrift		
	Signature / Unterschrift	(Stamp) Stempel	
12	Requesting National Security Authority / Antragstellende nationale Sicherheitsbehörde Name / Name	Telephone Nr.	
	Address / Anschrift		
	Signature / Unterschrift	(Stamp) Stempel	
13	Remarks / Bemerkungen		

Bitte geben Sie in Feld 9 zusätzlich den Vornamen und ggf. den Dienstgrad an

Załącznik 20b

Reguest for Visit (RFV)
Besuchstantrag

Visit ID – No:

Reference: RFV-format, para.3.

Annex 1/Anlage 1
to RFV – format

Govermment Agency or Industrial Facility to be visited/
Zu besuchende Dienststelle/Firma

1	Name/ Name	
	Postal address/ Postanschrift	
	Telex/Fax Nr.	
	Point of contact/ Ansprechpartner	Telephone Nr.
2	Name/ Name	
	Postal address/ Postanschrift	
	Telex/Fax Nr.	
	Point of contact/ Ansprechpartner	Telephone Nr.
3	Name/ Name	
	Postal address/ Postanschrift	
	Telex/Fax Nr.	
	Point of contact/ Ansprechpartner	Telephone Nr.
4	Name/ Name	
	Postal address/ Postanschrift	
	Telex/Fax Nr.	
	Point of contact/ Ansprechpartner	Telephone Nr.
5	Name/ Name	
	Postal address/ Postanschrift	
	Telex/Fax Nr.	
	Point of contact/ Ansprechpartner	Telephone Nr.
6	Name/ Name	
	Postal address/ Postanschrift	
	Telex/Fax Nr.	
	Point of contact/ Ansprechpartner	Telephone Nr.

Reguest for Visit (RFV)

Besuchstantrag

Visit ID – No:

Reference: RFV-format, para.9.

Annex 2/Anlage 2
to RFV – format

1	Name/Name	Date of birth, Place of birth/ Geburtsdatum, Geburtsort	Security clearance/ Sicherheitsermachtigung	ID/PP Number/ Paß-/Ausweisnummer
	Nationality/ Staatsangehörigkeit	Position/ Funktion/Dienststellung	Company/ Agency/ Dienststelle/Firma	
2	Name/Name	Date of birth, Place of birth/ Geburtsdatum, Geburtsort	Security clearance/ Sicherheitsermachtigung	ID/PP Number/ Paß-/Ausweisnummer
	Nationality/ Staatsangehörigkeit	Position/ Funktion/Dienststellung	Company/ Agency/ Dienststelle/Firma	
3	Name/Name	Date of birth, Place of birth/ Geburtsdatum, Geburtsort	Security clearance/ Sicherheitsermachtigung	ID/PP Number/ Paß-/Ausweisnummer
	Nationality/ Staatsangehörigkeit	Position/ Funktion/Dienststellung	Company/ Agency/ Dienststelle/Firma	
4	Name/Name	Date of birth, Place of birth/ Geburtsdatum, Geburtsort	Security clearance/ Sicherheitsermachtigung	ID/PP Number/ Paß-/Ausweisnummer
	Nationality/ Staatsangehörigkeit	Position/ Funktion/Dienststellung	Company/ Agency/ Dienststelle/Firma	
5	Name/Name	Date of birth, Place of birth/ Geburtsdatum, Geburtsort	Security clearance/ Sicherheitsermachtigung	ID/PP Number/ Paß-/Ausweisnummer
	Nationality/ Staatsangehörigkeit	Position/ Funktion/Dienststellung	Company/ Agency/ Dienststelle/Firma	
6	Name/Name	Date of birth, Place of birth/ Geburtsdatum, Geburtsort	Security clearance/ Sicherheitsermachtigung	ID/PP Number/ Paß-/Ausweisnummer
	Nationality/ Staatsangehörigkeit	Position/ Funktion/Dienststellung	Company/ Agency/ Dienststelle/Firma	
7	Name/Name	Date of birth, Place of birth/ Geburtsdatum, Geburtsort	Security clearance/ Sicherheitsermachtigung	ID/PP Number/ Paß-/Ausweisnummer
	Nationality/ Staatsangehörigkeit	Position/ Funktion/Dienststellung	Company/ Agency/ Dienststelle/Firma	

Załącznik nr 21

Zasady wypełniania formularza „Wniosek o Złożenie Wizyty" Request for Visit (RFV)

Wniosek o Złożenie Wizyty (RFV) należy wypełnić dokładnie, w języku angielskim, nie opuszczające żadnego z punktów. Niepodanie wszystkich wymaganych informacji opóźni prace nad wnioskiem.

RFV powinien być stosowany przy wizytach jednorazowych lub wielokrotnych, składanych w okresie nie przekraczającym jednego roku.

Wniosek wypełnić na maszynie lub komputerowo. Wytworzony w ten sposób dokument musi być zgodny z oryginalnym formularzem.

Niniejsze zalecenia są adresowane do osób, które wypełniają formularz RFV w związku z wizytą oraz do pełnomocników ds. ochrony informacji niejawnych instytucji lub podmiotu przemysłowego, posługujących się wnioskiem w związku z wizytami, składanymi w ramach przyjętych programów czy projektów NATO.

Dla ułatwienia wypełniania RFV w załączniku Nr 16 ujęto polskie tłumaczenie tego formularza.

1.	DANE ADMINISTRACYJNE	Nie wypełniać (wypełniają krajowe władze bezpieczeństwa /KWB/ występujące z wnioskiem).
2.	INSTYTUCJA RZĄDOWA lub PODMIOT PRZEMYSŁOWY WYSTĘPUJĄCY z WNIOSKIEM	Należy podać pełną nazwę i adres do korespondencji, wskazując miasta będące siedzibą jednostki organizacyjnej występującej z wnioskiem, region (stan, województwo, powiat itp., zgodnie z podziałem administracyjnym danego i kraju) i kod pocztowy.
3.	WIZYTOWANA INSTYTUCJA RZĄDOWA lub PODMIOT PRZEMYSŁOWY	Podać pełną nazwę i dokładny adres (miasta, region, kod pocztowy), numer teleksu lub telefaksu oraz dane dotyczące głównego punktu kontaktowego - nazwę komórki organizacyjnej lub nazwisko i numer telefonu osoby, z którą, omawiane były sprawy związane ze złożeniem wizyty. **Uwagi:** 1) Podanie właściwego kodu pocztowego jest bardzo ważne, ponieważ temu samemu przedsiębiorstwu lub instytucji może podlegać kilka jednostek organizacyjnych o różnej lokalizacji. 2) Przy wypełnianiu wniosku należy kierować się instrukcją. Gdy zachodzi potrzeba złożenia wizyty w dwóch lub kilku instytucjach w i związku z tą samą sprawą, należy posłużyć się formularzem zawartym na str. 6 załącznika nr 16, a w punkcie 3 zamieścić adnotację: „PATRZ ANEKS „LICZBA INSTYTUCJI/PODMIOTÓW PRZEMYSŁOWYCH". ... (podać liczbę odwiedzanych obiektów).
4.	DATA WIZYTY	Wskazać rzeczywistą datę wizyty lub czas jej trwania (od daty do daty), podając dzień, miesiąc i rok. Jeśli może dojść do zmiany terminu w nawiasach należy określić datę alternatywną.
5.	RODZAJ WIZYTY	Zaznaczyć, zgodnie ze wskazówką, jedną pozycję w każdej kolumnie.

6.	TEMAT do DYSKUSJI lub UZASADNIENIE	Krótko opisać temat (tematy), jaki będzie poruszany w czasie wizyty, określając jednocześnie powód odwiedzin. Nie należy posługiwać się skrótami nie opatrzonymi stosownym wyjaśnieniem. **Uwagi:** 1) W wypadku wizyt wielokrotnych trzeba to wyraźnie podkreślić stwierdzając: „wizyta wielokrotna" - muszą to być pierwsze słowa informacji zawartych w tym miejscu (np. *Wizyta wielokrotna w celu mówienia.....).* 2) Zaleca się powtórzenie tematu, który ma być omówiony lub uzasadnienie celu wizyty w języku kraju przyjmującego.
7.	PRZEWIDYWANY STOPIEŃ TAJNOŚCI INFORMACJI	Wskazać klauzulę odpowiadającą poziomowi sklasyfikowania informacji, które będą poruszane w czasie wizyty: NATO SECRET, NATO CONFIDENTIAL NATO RESTRICTED lub NATO UNCLASSFIED.
8.	CZY WIZYTA DOTYCZY:	Zaznaczyć w odpowiednim miejscu „tak" (Y) i - jeśli sprawa tego dotyczy - podać pełną nazwę projektu/programu lub posłużyć się powszechnie stosowanymi skrótami.
9.	DANE OSOBOWE SKŁADAJĄCEGO WIZYTĘ	NAZWISKO: nazwisko rodowe (przecinek, po nim pełne imię i pierwsza litera drugiego /ew. trzeciego/ imienia). DATA URODZENIA: dzień, miesiąc i rok. MIEJSCE URODZENIA: OBECNY STOPIEŃ DOPUSZCZENIA do TAJEMNICY: np. CTS (COSMIC TOP SECRET), NS (NATO SECRET), NC (NATO CONFIDENTIAL). D-P: numery dowodu osobistego lub paszportu, zgodnie z wymaganiami władz kraju przyjmującego. NAR: podać narodowość za pomocą kodu dwuliterowego. STANOWISKO: określić stanowisko zajmowane przez osobę wizytującą w instytucji, która ją zatrudnia (np. dyrektor, kierownik produkcji). PRZEDSIĘBIORSTWO lub INSTYTUCJA: nazwa jednostki organizacyjnej, którą reprezentuje osoba składająca wizytę (jeśli dane te są różne od ujętych w pozycji 2). **Uwaga:** Gdy wizytę składają więcej niż dwie osoby należy posłużyć się formularzem zawartym na str. 8 załącznika nr 16. Wówczas w pozycji 9 trzeba umieścić adnotację: „PATRZ ANEKS, LICZBA OSÓB SKŁADAJĄCYCH WIZYTĘ: ..." (podać tę liczbę).
10.	PEŁNOMOCNIK OCHRONY INSTYTUCJI SKŁADAJĄCEJ WNIOSEK.	W tym miejscu należy podać nazwisko, podpis i numer telefonu pełnomocnika ochrony instytucji lub podmiotu przemysłowego występujących z wnioskiem o złożenie wizyty.
11.	WYSTAWIENIE CERTYFIKATU (SPRAWDZENIE PRZEZ WŁAŚCIWE WŁADZE)	**Proszę nie wypełniać** (tę pozycję wypełnia przedstawiciel organu wystawiającego certyfikat). **Ważne:** - Podać nazwisko, adres i numer telefonu (może być wcześniej wydrukowany). - W tym punkcie złożyć podpis i ewentualnie przyłożyć stempel. - Jeśli organ wystawiający certyfikat koresponduje z krajowymi władzami bezpieczeństwa (KWB) składającymi wniosek, należy wpisać „Patrz pozycja 12". **Uwaga:** Pozycje 11 i 12 mogą być wypełnione przez właściwego urzędnika KWB kraju składającego wniosek.

12.	KRAJOWE WŁADZE BEZPIECZEŃSTWA SKŁADAJĄCE WNIOSEK (KWB)	**Nie wypełniać.** Uwagi dla KWB składającej wniosek: - Podać nazwisko, adres i numer telefonu (może być wcześniej wydrukowany). - W tym punkcie złożyć podpis i ewentualnie przyłożyć stempel.
13.	UWAGI	To miejsce jest przeznaczone na wpisanie różnego rodzaju uzupełnień dotyczących spraw administracyjnych (m. in. proponowanego przebiegu wizyty, wniosków w sprawie zarezerwowania hotelu lub przygotowania środków transportu). Można tu również przekazać uwagi przyjmującego organu KBW, np. w postaci stwierdzenia: *nie ma sprzeciwu z punktu widzenia bezpieczeństwa.* Ewentualnie skorygować numer dowodu tożsamości.

INSTRUCTION FOR THE USE AND COMPLETION OF A REQUEST FOR VISIT (RFV)

The Request for Visit (RFV) (Attachment 1) is an important document and must be completed without mis-statement or omission. Failure to provide all requested information will delay the processing of there quest.

The RFV should be used for a „one-time" visit and/or „recurring visits" during a certain period of time not to exceed one year.

This RFV should be typed-written or on a PC, provided that the original form and content are consistent.

These detailed instructions are guidance for the visitors who complete the RFV in the case of one-time visit or by the agency or facility Security Officer in case of recurring visits in the framework of approved programmes or projects.

B1.	ADMINISTRATIVE DATA	Do not fill in (to be completed by requesting NSA).
2.	REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY	Mention full name and postal address, include city, state, postal zone, as applicable.
3.	GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED	Mention full name and full address, include city, state, postal zone, telex or fax number. Mention the name and telephone number of your main point of contact or the person with whom you have made the appointment for the visit. **Remarks**: (1) Mentioning the correct postal zone (zip code) is very important because there can be different facilities of the same company. (2) During fulfill the RFV the instruction is useful. When two or more agencies or facilities have to be visited in the framework of the same subject, Attachment 2 will be used and item 3 should state : „SEE ANNEX, NUMBER OF AGENCIES/FAC. :. „ (state number of agencies / facilities).
4.	DATES OF VISIT	Mention the actual date or period (date-to-date) of the visit by „day-month-year". If applicable, place an alternative date or period in brackets.
5.	TYPE OF VISIT	Mark one item of each column as indicated.
6.	SUBJECT TO BE DISCUSSED or JUSTIFICATION	Give a brief description of the subject(s) stating the reason of your visit. Avoid the use of unexplained abbreviations. **Remarks** :

		(1) In case of a recurring visit, this item should state „Recurring Visits" as the first words in the data element (e.g., Recurring Visits to discuss...). (2) It is strongly advised to repeat the subject to be discussed and/or the justification of the visit in the language of the receiving country.
7.	ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	Mention NATO SECRET, NATO CONFIDENTIAL, NATO RESTRICTED or NATO UNCLASSIFIED as applicable.
8.	IS THE VISIT PERTINENT TO:	Mark the appropriate line yes (Y) and, if applicable, specify the full name of the project/programme, FMS-case, etc., using commonly-used abbreviations only.
9.	PARTICULARS OF VISITOR	NAME: Family name, (comma) followed by first name in full and middle initial(s). DOB: Date of birth (day-month-year). POB: Place of birth. Actual security clearance status, e. g., CTS, NS, NC. ID-PP: Enter the number of identification card or passport, as required by host government. NAT: Enter nationality in two-letter code. POSITION: Mention the position the visitor holds in the organization (e.g., director, product manager, etc.). COMPANY/AGENCY: Mention the name of the government agency or industrial facility that the visitor represents (if different from item 2.). **Remark :** When more than two visitors are involved in the visit, Attachment 3 should be used. In that case, Item No. 9 should state „SEE ANNEX, NUMBER OF VISITORS: ." (state the number of visitors).
10.	THE SECURITY OFFICER OF THE REQUESTING AGENCY	This item requires the name, signature and telephone number of the requesting Facility agency / facility Security Officer.
11.	CERTIFICATION OF	**Do not fill in** (to be completed by government certifying authority). Note for the certifying

	SECURITY CLEARANCE	authority: - Mention name, address and telephone number (can be pre-printed); - This item should be signed and eventually stamped, as applicable; - If the certifying authority corresponds with the requesting National Security Authority, enter „See item 12". **Remark** : Items 11 and 12 may be filled in by the appropriate official of the NSA of the requesting country.

Załącznik nr 22

CZAS PRZYGOTOWANIA WNIOSKU O ZŁOŻENIE WIZYTY MIĘDZYNARODOWEJ

W tabeli określono czas. w jakim właściwa KWB kraju wymienionego w kolumnie nr 1 ma rozpatrzyć wniosek o złożenie wizyty międzynarodowej (RFV). Czas ten liczony jest od dnia otrzymania dokumentu (RFV). W kolumnie nr 2 podano czas rozpatrzenia wniosku, a w kolumnie nr 3 podano minimalną liczbę dni poprzedzających wizytę, w trakcie których możliwe jest wprowadzenie zmian w RFV (np. w zakresie składu uczestników wizyty).

KRAJ CZŁONKOWSKI		LICZBA DNI ROBOCZYCH	
		WNIOSEK	ZMIANY
1		2	3
Belgia	BE	10	5
Kanada	CA	20	-
Czechy	CZ	-	-
Dania	DE	15	
Francja	FR	25	5
Niemcy	GE	20	7
Grecja	GR	20	10
Węgry	HU	-	-
Islandia	IC	-	-
Włochy	IT	20	7
Luxemburg	LU	10	5
Holandia	NL	14	-
Norwegia	NO	21	-
Polska	PL	25	10
Portugalia	PO	20	10
Hiszpania	SP	20	7
Turcja	TU	25	10
Wlk. Brytania	UK	15	7
Stany Zjednoczone	US	21	5

DECYZJA Nr 23/MON

MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie szkolenia w zakresie ochrony informacji niejawnych

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426) w związku z art. 18 ust. 4 pkt 6, art. 22, art. 54 ust. 1 i 2 i art. 64 ust. 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631), zwanej dalej „ustawą", w celu realizacji zamierzeń związanych ze szkoleniem
w zakresie ochrony informacji niejawnych ustala się, co następuje:

1. W zakresie ochrony informacji niejawnych w komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, prowadzi się następujące rodzaje szkolenia:

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

2. Szkoleniem podstawowym obejmuje się osoby po uzyskaniu przez nie po raz pierwszy poświadczenia bezpieczeństwa przed dopuszczeniem do pełnienia służby lub pracy na stanowisku, z którym łączy się lub może łączyć się dostęp do informacji niejawnych.

3. W uzasadnionych przypadkach szkoleniem podstawowym mogą być objęte osoby przed wydaniem poświadczenia bezpieczeństwa.

4. Szkolenie podstawowe osób, o których mowa w art. 49 ust. 1 – 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, zwanej dalej „ustawą" prowadzi się przed udostępnieniem im informacji niejawnych.

5. Celem szkolenia podstawowego jest zapoznanie osób, o których mowa w pkt. 2-4, z tematyką określoną w art. 54 ust. 1 ustawy, a ponadto z:

1) zagrożeniami dla informacji niejawnych, wynikającymi ze specyfiki komórki (jednostki), o której mowa w pkt. 1;

2) zasadami wytwarzania, przetwarzania, przechowywania, powielania, udostępniania i obiegu dokumentów niejawnych;

3) szczegółowymi wymaganiami ochrony w jednostce organizacyjnej informacji niejawnych oznaczonych klauzulą ZASTRZEŻONE;

4) zasadami klasyfikowania wytwarzanych w komórce (jednostce), o której mowa
w pkt. 1, dokumentów zawierających informacje niejawne, stosowania właściwych klauzul tajności, a także procedurami ich zmiany i znoszenia.

6. Szkolenie podstawowe przeprowadza pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony".

7. Pełnomocnik ochrony potwierdza odbycie szkolenia podstawowego wydaniem zaświadczenia według wzoru określonego w załączniku Nr 4, do rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych (Dz. U. Nr 171, poz.1432).

8. Pełnomocnik ochrony prowadzi ewidencję wydanych zaświadczeń, zgodnie ze wzorem zawartym w załączniku nr 1 do decyzji.

9. Ewidencję zaświadczeń prowadzi się w cyklu rocznym, rozpoczynając każdego roku kalendarzowego numerowanie od cyfry „1". Numer zaświadczenia odpowiada pozycji zapisu w ewidencji, łamanej przez oznaczenie roku kalendarzowego.

10. W przypadku zagubienia lub utraty zaświadczenia, o którym mowa w pkt. 6, pełnomocnik ochrony na pisemny wniosek osoby, która odbyła szkolenie podstawowe, wydaje jego duplikat. Duplikat zaświadczenia oznacza się napisem „DUPLIKAT" umieszczonym pośrodku w dolnej części dokumentu, poniżej odcisku pieczęci urzędowej komórki (jednostki), o której mowa w pkt. 1.

11. W przypadku zmiany danych personalnych, pełnomocnik ochrony, na pisemny wniosek osoby zainteresowanej, wydaje nowe zaświadczenie zawierające zmienione dane personalne, z zachowaniem dotychczasowego jego numeru.

12. Osoby, które uzyskały certyfikat bezpieczeństwa NATO (NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE), certyfikat potwierdzający sprawdzenie osoby (CERTIFICATE OF SECURITY CLEARANCE), certyfikat Unii Europejskiej (EU PERSONNEL SECURITY CLEARANCE CERTIFICATE), certyfikat Unii Zachodnioeuropejskiej (WEU PERSONNEL SECURITY CLEARANCE CERTIFICATE) przed ich wydaniem podlegają dodatkowo przeszkoleniu - w zależności od uzyskanego certyfikatu z przepisów bezpieczeństwa NATO lub Unii Europejskiej- przez żołnierzy lub pracowników Wojskowych Służb Informacyjnych. W przypadku wydania certyfikatu NATO o klauzuli BOHEMIA szkolenie prowadzą żołnierze Generalnego Zarządu Rozpoznania Wojskowego P-2 Sztabu Generalnego WP.

13. Dla osiągnięcia celu szkoleniowego, o którym mowa w pkt. 5 ppkt 4:

1) osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej oraz kierownicy jego komórek organizacyjnych bezpośrednio podległych Ministrowi Obrony Narodowej opracują wykazy typowych materiałów wytwarzanych w podległych komórkach organizacyjnych, które powinno się oznaczać odpowiednio klauzulami POUFNE lub ZASTRZEŻONE i przekażą je Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych;

2) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych opracuje i wyda w porozumieniu z osobami, o których mowa w ppkt. 1, zbiorczy wykaz typowych materiałów niejawnych wytwarzanych w komórkach, o których mowa w pkt. 1, które powinno się oznaczać odpowiednio klauzulami POUFNE lub ZASTRZEŻONE;

3) kierownicy jednostek, o których mowa w pkt. 1, w których są wytwarzane, przetwarzane, przekazywane lub przechowywane materiały zawierające informacje niejawne, opracują i wydadzą wykazy typowych materiałów niejawnych wytwarzanych w podległych im jednostkach organizacyjnych, które powinno się oznaczać odpowiednio klauzulami POUFNE lub ZASTRZEŻONE.

14. Szkoleniem uzupełniającym obejmuje się osoby pełniące służbę lub zatrudnione na stanowiskach, z którymi łączy się lub może łączyć się dostęp do informacji niejawnych.
15. Celem szkolenia uzupełniającego jest podtrzymanie i doskonalenie wiedzy uzyskanej podczas szkolenia podstawowego w zakresie ochrony informacji niejawnych.

16. Szkolenie uzupełniające dla osób zatrudnionych lub pełniących służbę w komórce (jednostce), o której mowa w pkt. 1, prowadzi pełnomocnik ochrony co najmniej raz w roku oraz każdorazowo po zmianie przepisów o ochronie informacji niejawnych, a także wtedy, gdy uzasadniają to negatywne wyniki kontroli przestrzegania przepisów o ochronie informacji niejawnych przeprowadzonej w tych komórkach (jednostkach).

17. Osoby przybyłe na stanowiska służbowe z innych komórek (jednostek), o których mowa w pkt. 1, w których odbyły szkolenie podstawowe, podlegają szkoleniu uzupełniającemu z problematyki, o której mowa w pkt. 5.

18. Szkolenie uzupełniające dla kierowników komórek organizacyjnych, o których mowa w pkt. 1, i ich zastępców oraz pełnomocników ochrony i ich zastępców z jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej oraz osób zajmujących kierownicze stanowiska Ministerstwa Obrony Narodowej, prowadzi Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, co najmniej raz na dwa lata oraz każdorazowo po zmianie przepisów o ochronie informacji niejawnych, a także wtedy, gdy uzasadniają to negatywne wyniki kontroli przestrzegania przepisów o ochronie informacji niejawnych przeprowadzonych w tych komórkach (jednostkach).

19. Pełnomocnicy ochrony dowódców rodzajów Sił Zbrojnych Rzeczypospolitej Polskiej, zwanych dalej „Siłami Zbrojnymi", okręgów wojskowych oraz związków taktycznych (równorzędnych) prowadzą co najmniej raz na dwa lata oraz każdorazowo po zmianie przepisów o ochronie informacji niejawnych, a także wtedy gdy uzasadniają to negatywne wyniki uzyskane przez jednostki organizacyjne podczas kontroli przestrzegania przepisów o ochronie informacji niejawnych, szkolenie uzupełniające dla kierowników jednostek organizacyjnych, pełnomocników ochrony i ich zastępców z jednostek organizacyjnych bezpośrednio podległych dowódcom tych szczebli dowodzenia.

20. Szef Zarządu Ochrony Informacji Niejawnych Inspektoratu Służby Kontrwywiadu Wojskowego przeprowadza szkolenie uzupełniające pełnomocników ochrony i ich zastępców z jednostek, o których mowa w pkt. 1, nie rzadziej niż raz na 5 lat.

21. Pełnomocnik ochrony odpowiada za:

1) opracowanie szczegółowych programów szkolenia uzupełniającego, uwzględniających specyfikę komórek (jednostek), o których mowa w pkt. 1, stanowiska służbowe oraz zakres dostępu do informacji niejawnych osób szkolonych;

2) prowadzenie dokumentacji szkoleniowej, w szczególności:

a) dzienników lekcyjnych,
b) dokumentowanie wyników przeprowadzonych sprawdzianów,
c) rejestru wydanych zaświadczeń.

22. Szkoleniem specjalistycznym obejmuje się osoby przewidziane do objęcia stanowiska lub pełnienia funkcji:

1) pełnomocnika ochrony i zastępcy pełnomocnika ochrony;
2) kierownika, zastępcy kierownika i kancelisty kancelarii tajnej, tajnej – zagranicznej oraz innych niż kancelaria tajna komórek wewnętrznych lub organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych;
3) kierownika i pracownika biblioteki, w której są przechowywane i ewidencjonowane niejawne wojskowe wydawnictwa specjalistyczne;
4) administratora systemu;
5) pracownika pionu ochrony pełniącego funkcję inspektora bezpieczeństwa teleinformatycznego.

23. Szkoleniem specjalistycznym mogą być objęte odpłatnie osoby wymienione w pkt.22 ppkt. 1, 4 i 5, zatrudnione u przedsiębiorcy, w jednostce naukowej lub badawczo-rozwojowej, zamierzającej ubiegać się, ubiegającej się lub wykonującej umowy na rzecz resortu obrony narodowej, z wykonaniem których łączy się dostęp do informacji niejawnych.

24. Celem szkolenia specjalistycznego jest przygotowanie osób, o których mowa w pkt. 22, do wykonywania obowiązków służbowych.

25. Program szkolenia specjalistycznego osób, o których mowa w pkt. 22 ppkt. 1, 4 i 5, opracowuje Szef Zarządu Ochrony Informacji Niejawnych Inspektoratu Służby Kontrwywiadu Wojskowego.

26. Program szkolenia specjalistycznego osób, o których mowa w pkt. 22 ppkt 2 i 3, opracowują odpowiednio Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocnicy ochrony dowódców rodzajów Sił Zbrojnych, w porozumieniu z Szefem Zarządu Ochrony Informacji Niejawnych Inspektoratu Służby Kontrwywiadu Wojskowego.

27. Potrzeby w zakresie szkolenia osób, o których mowa w pkt.22, zgłaszają do dnia 31 marca na następny rok kalendarzowy:

1) Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych – kierownicy komórek, o których mowa w pkt. 1, oraz jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej, z wyłączeniem dowództw rodzajów Sił Zbrojnych, a także kierownicy jednostek organizacyjnych podległych osobom zajmującym kierownicze stanowiska Ministerstwa Obrony Narodowej lub kierownikom komórek, o których mowa w pkt.1;
2) pełnomocnikom ochrony dowódców rodzajów Sił Zbrojnych – kierownicy komórek organizacyjnych dowództw rodzajów Sił Zbrojnych oraz kierownicy pozostałych jednostek organizacyjnych, nie wymienionych w pkt. 22.

28. Osoby, o których mowa w pkt. 26, na podstawie zgłoszonych potrzeb, organizują szkolenie specjalistyczne w ośrodkach szkoleniowych wytypowanych odpowiednio przez Szefa Służby Kontrwywiadu Wojskowego, dowódców rodzajów Sił Zbrojnych oraz Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, z zastrzeżeniem, iż:

1) szkolenie osób, o których mowa w pkt. 22 ppkt 1, 4 i 5, prowadzą żołnierze Służby Kontrwywiadu Wojskowego;
2) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocnicy ochrony dowódców rodzajów Sił Zbrojnych uzgadniają terminy szkoleń, o których mowa w ppkt 1, z Szefem Zarządu Ochrony Informacji Niejawnych Inspektoratu Służby Kontrwywiadu Wojskowego, w terminie do dnia 30 września;
3) wytypowane ośrodki szkoleniowe spełniają określone wymagania dotyczące lokalizacji, wielkości oraz wyposażenia w sprzęt informatyczny i audiowizualny.

29. Wydatki na szkolenie specjalistyczne planują osoby, o których mowa w pkt. 27, na podstawie potrzeb zgłoszonych przez kierowników komórek (jednostek), o których mowa w pkt. 1.

30. Szef Służby Kontrwywiadu Wojskowego lub upoważniona przez niego osoba potwierdza odbycie szkolenia specjalistycznego przez osoby, o których mowa w pkt. 22 ppkt. 1, 4 i 5, oraz szkolenia uzupełniającego dla pełnomocników i ich zastępców wydaniem zaświadczenia, według wzoru określonego w załącznikach nr 2, 3 i 11 do rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych.

31. Ukończenie szkolenia specjalistycznego przez osoby, o których mowa w pkt. 22 ppkt 2 i 3, Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz

pełnomocnicy ochrony dowódców rodzajów Sił Zbrojnych dokumentują odpowiednio wydaniem zaświadczenia, według wzoru określonego w załączniku Nr 2 do decyzji.

32. Do zaświadczeń, o których mowa w pkt. 30 i 31, stosuje się odpowiednio przepisy pkt. 8 – 11.

33. Wykazy, o których mowa w pkt 13 ppkt. 1 i 3, należy opracować w terminie do 3 miesięcy od daty wejścia w życie decyzji.

34. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych opracuje i wyda w terminie do 6 miesięcy od daty wejścia decyzji w życie, wykaz, o którym mowa w pkt. 13 ppkt 2.

35. Traci moc decyzja Nr 16/MON Ministra Obrony Narodowej z dnia 25 stycznia 2001 r. w sprawie szkolenia w zakresie ochrony informacji niejawnych (Dz. Urz. MON Nr 1, poz. 9).

36. Decyzja wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Załącznik Nr 1

REJESTR WYDANYCH ZAŚWIADCZEŃ

Układ strony lewej

Lp.	Stopień	Imię i nazwisko	Data urodzenia	Komórka organizacyjna
1	2	3	4	5

Układ strony prawej

Nr zaświadczenia	Data szkolenia	Rodzaj szkolenia	Uwagi
6	7	8	9

.....
(nazwa jednostki organizacyjnej
z adresem i numerem telefonu)

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 personelu kancelarii tajnych, tajnych – zagranicznych oraz innych niż kancelaria tajna komórek wewnętrznych lub organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych.

m.p.

.....
(miejscowość i data)

.....
(pieczęć imienna i podpis osoby wystawiającej)

DECYZJA Nr 24/MON

MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. z 1996 r., Nr 94, poz. 426), w celu poddania szczególnej ochronie systemów i sieci teleinformatycznych, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, ustala się, co następuje:

1. Użyte w decyzji określenia oznaczają:

1) ustawa - ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631);
2) jednostka organizacyjna:

a) Ministerstwo Obrony Narodowej jako urząd Ministra Obrony Narodowej,
b) jednostkę nie wchodzącą w skład ministerstwa, podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną,
c) przedsiębiorcę, jednostkę naukową lub badawczo-rozwojową, zamierzających ubiegać się o zawarcie lub wykonujących umowę związaną z dostępem do informacji niejawnych, albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych;

3) komórka organizacyjna - Sekretariat Ministra Obrony Narodowej, departament, generalny zarząd, samodzielny zarząd, szefostwo, biuro;

4) kierownik jednostki (komórki) organizacyjnej - dowódcę, dyrektora, szefa, komendanta, prezesa;

5) pełnomocnik ochrony - pełnomocnika do spraw ochrony informacji niejawnych;

6) system lub sieć teleinformatyczna- system lub sieć teleinformatyczną (w rozumieniu ustawy) przeznaczoną do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych;

7) bezpieczeństwo teleinformatyczne - całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych oraz ochrony informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w tych systemach i sieciach przed przypadkowym lub celowym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania poprzez zastosowanie w sposób kompleksowy technicznych, programowych, kryptograficznych oraz organizacyjnych środków i metod;

8) dokumentacja bezpieczeństwa teleinformatycznego - szczególne wymagania bezpieczeństwa i procedury bezpiecznej eksploatacji systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie;

9) wyroby o przeznaczeniu specjalnym, służące do ochrony informacji niejawnych - wszelkie wyroby zaprojektowane i wykonane do ochrony informacji niejawnych oraz technologie związane z produkcją lub używaniem tych wyrobów, w szczególności:
a) urządzenia i narzędzia kryptograficzne,

b) pomocniczy sprzęt kryptograficzny, nie będący urządzeniem kryptograficznym, wykorzystywany do zabezpieczenia funkcjonowania systemu kryptograficznego, który wymaga specjalnej obsługi lub kontroli, w celu ochrony specjalnych elementów i układów kontrolnych,
c) urządzenia w wykonaniu specjalnym, przeznaczone do zobrazowania, wytwarzania, przetwarzania, przechowywania i przekazywania informacji niejawnych,
d) urządzenia ochrony elektromagnetycznej, w tym kabiny ekranujące, indywidualne osłony ekranujące, urządzenia do maskowania emisji ujawniającej,
e) aparatownie łączności i informatyki, mobilne kancelarie kryptograficzne, zautomatyzowane wozy dowodzenia.

2. Zadania w zakresie ochrony systemów i sieci teleinformatycznych realizują:

1) w jednostce (komórce) organizacyjnej:

a) kierownik jednostki (komórki) organizacyjnej,
b) pełnomocnik ochrony,
c) administrator systemu,
d) inspektor bezpieczeństwa teleinformatycznego;

2) Centrum Bezpieczeństwa Teleinformacyjnego;

3) Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki;

4) organy bezpieczeństwa systemów łączności i informatyki jednostek organizacyjnych wszystkich szczebli dowodzenia;

5) Centrum Zarządzania Systemami Teleinformatycznymi;

6) Wojskowe Służby Informacyjne.

3. Kierownik komórki organizacyjnej odpowiada za organizację, eksploatację i bezpieczeństwo systemów i sieci teleinformatycznych, funkcjonujących w komórce organizacyjnej, w szczególności za:

1) wyznaczenie administratorów systemów lub sieci teleinformatycznych;
2) opracowanie i przekazanie do Służby Kontrwywiadu Wojskowego dokumentacji bezpieczeństwa teleinformatycznego, uzgodnionej w trybie określonym w pkt 5-7;
3) informowanie Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych o stanie realizacji prac związanych z opracowywaniem dokumentacji bezpieczeństwa teleinformatycznego oraz jej przygotowaniem do wdrożenia;
4) przekazanie Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych informacji o potrzebach w zakresie wyposażenia w sprzęt informatyczny i urządzenia, w tym wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, o których mowa w pkt 1 ppkt 9 lit. c i d;

5) występowanie do Służby Kontrwywiadu Wojskowego poprzez Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, z wnioskami o:

a) dokonanie pomiarów i określenie Poziomu Zabezpieczenia Miejsca oraz Poziomu Zabezpieczenia Urządzenia,
b) przeprowadzenie akredytacji bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych,
c) przeprowadzenie certyfikacji lub ponownej certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, wymienionych w pkt 1 ppkt 9 lit. c i d,
d) przeprowadzenie certyfikacji pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnych.

4. Kierownik jednostki organizacyjnej odpowiada za organizację, eksploatację i bezpieczeństwo systemów i sieci teleinformatycznych, funkcjonujących w jednostce organizacyjnej, w szczególności za:

1) wyznaczenie osób funkcyjnych, zgodnie z art. 64 ustawy;
2) opracowanie i przekazanie do Służby Kontrwywiadu Wojskowego dokumentacji bezpieczeństwa teleinformatycznego, uzgodnionej w trybie, o którym mowa w pkt 5-7;
3) określenie warunków i sposobu przydzielenia uprawnień użytkownikom systemów lub sieci teleinformatycznych;
4) występowanie do Służby Kontrwywiadu Wojskowego z wnioskami o:

a) dokonanie pomiarów i określenie Poziomu Zabezpieczenia Miejsca oraz Poziomu Zabezpieczenia Urządzenia,
b) przeprowadzenie akredytacji bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych,
c) przeprowadzenie certyfikacji lub ponownej certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, o których mowa w pkt 1 ppkt 9 lit. c i d,
d) przeprowadzenie certyfikacji lub ponownej certyfikacji: kancelarii kryptograficznych, stacji kryptograficznych, kabin kryptograficznych, pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnych, kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych.

5. Dokumentacja bezpieczeństwa teleinformatycznego przed przekazaniem do Służby Kontrwywiadu Wojskowego podlega uzgodnieniu z:

1) pełnomocnikiem ochrony jednostki organizacyjnej, w której będzie eksploatowany system lub sieć teleinformatyczna, oraz
2) Wojskowym Biurem Bezpieczeństwa Łączności i Informatyki lub organem bezpieczeństwa systemów łączności i informatyki dowództwa rodzaju Sił Zbrojnych, Dowództwa Garnizonu Warszawa, Dowództwa Operacyjnego, w przypadku gdy:

a) w systemie lub sieci teleinformatycznej jest planowane stosowanie środków ochrony kryptograficznej, lub
b) zasięg systemu lub sieci teleinformatycznej wykracza poza obręb strefy bezpieczeństwa jednostki (komórki) organizacyjnej.

6. Dokumentacja bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych, o których mowa w pkt 5 ppkt 2, podlega uzgodnieniu z:

1) Wojskowym Biurem Bezpieczeństwa Łączności i Informatyki w stosunku do systemów i sieci teleinformatycznych obejmujących swoim zasięgiem:

a) komórkę organizacyjną,
b) jednostkę organizacyjną, z zastrzeżeniem ppkt 2,
c) rodzaj Sił Zbrojnych lub dowództwo rodzaju Sił Zbrojnych, Dowództwo Garnizonu Warszawa, Dowództwo Operacyjne,
d) resort obrony narodowej lub wykraczających poza niego na podstawie umów, porozumień, aktów prawnych;

2) organem bezpieczeństwa systemów łączności i informatyki dowództwa rodzaju Sił Zbrojnych, Dowództwa Garnizonu Warszawa, Dowództwa Operacyjnego, w stosunku do systemów i sieci teleinformatycznych obejmujących swoim zasięgiem jednostkę organizacyjną podległą właściwemu dowódcy.

7. Do Służby Kontrwywiadu Wojskowego przekazuje dokumentację bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych, obejmujących swoim zasięgiem:

1) komórkę organizacyjną – jej kierownik;
2) jednostkę organizacyjną – jej kierownik, z zastrzeżeniem ppkt 3-6;
3) rodzaj Sił Zbrojnych lub dowództwo rodzaju Sił Zbrojnych – dowódca rodzaju Sił Zbrojnych;
4) Dowództwo Garnizonu Warszawa lub jednostki organizacyjne podległe dowódcy Garnizonu Warszawa – dowódca Garnizonu Warszawa;
5) Dowództwo Operacyjne lub jednostki organizacyjne podległe dowódcy Dowództwa Operacyjnego – dowódca Dowództwa Operacyjnego;
6) resort obrony narodowej lub wykraczających poza niego, na podstawie umów, porozumień, aktów prawnych, a także w innych przypadkach nie określonych w ppkt 3-5 – kierownik jednostki (komórki) organizacyjnej, będący organizatorem systemu lub sieci.

8. Pełnomocnik ochrony:

1) odpowiada za zapewnienie ochrony systemów i sieci teleinformatycznych funkcjonujących w jednostce organizacyjnej z wyłączeniem organizacyjnych, technicznych, programowych i eksploatacyjnych aspektów ochrony kryptograficznej, o których mowa w pkt 11-15, w szczególności za:

a) zapewnienie przestrzegania zasad ochrony informacji niejawnych w systemie lub sieci teleinformatycznej, w tym właściwego i bezpiecznego obiegu dokumentów oraz elektronicznych nośników informacji,
b) zapewnienie bezpieczeństwa fizycznego obszaru, w którym usytuowany jest system lub sieć teleinformatyczna,
c) planowanie potrzeb rzeczowo-finansowych na zabezpieczenie, zgodnie z wymaganymi standardami, funkcjonowania systemów i sieci teleinformatycznych,
d) zapewnienie dostępu do systemu lub sieci teleinformatycznej wyłącznie upoważnionym osobom, posiadającym odpowiednie i ważne poświadczenia bezpieczeństwa oraz uprawnienia,
e) organizację i prowadzenie szkolenia użytkowników w zakresie bezpieczeństwa systemów i sieci teleinformatycznych funkcjonujących w jednostce (komórce) organizacyjnej oraz ochrony informacji niejawnych w tych systemach i sieciach,
f) kontrolę znajomości i przestrzegania procedur bezpiecznej eksploatacji przez użytkowników systemu lub sieci teleinformatycznej,
g) nadzór nad konfiguracją systemu lub sieci teleinformatycznej oraz przemieszczaniem ich elementów składowych,
h) prowadzenie ewidencji systemów i sieci teleinformatycznych, w tym wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, o których mowa w pkt 1 ppkt 9 lit. c i d,
i) nadzór nad bezpieczną eksploatacją systemów i sieci teleinformatycznych oraz wyrobów o przeznaczeniu specjalnym, o których mowa w pkt 1 ppkt 9 lit. c i d;

2) uczestniczy w opracowywaniu projektów dokumentów normatywnych regulujących w jednostce (komórce) organizacyjnej problematykę ochrony informacji niejawnych wytwarzanych, przechowywanych, przetwarzanych lub przekazywanych w systemach i sieciach teleinformatycznych, w tym:

a) programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów i sieci teleinformatycznych,
b) dokumentacji bezpieczeństwa teleinformatycznego;

3) uzgadnia dokumentację bezpieczeństwa systemów i sieci teleinformatycznych:

a) w jednostce (komórce) organizacyjnej,
b) obejmujących swoim zasięgiem dwie albo więcej bezpośrednio podległe jednostki organizacyjne;

4) w przypadku stwierdzenia naruszeń bezpieczeństwa lub rozbieżności pomiędzy stanem faktycznym, a zapisami zawartymi w dokumentacji bezpieczeństwa teleinformatycznego, informuje o powyższym Szefa Wojskowych Służb Informacyjnych oraz właściwy organ bezpieczeństwa systemów łączności i informatyki, jeżeli uczestniczył w opiniowaniu dokumentacji bezpieczeństwa teleinformatycznego.

9. Administrator systemu realizuje zadania w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad bezpieczeństwa systemu lub sieci teleinformatycznej, w szczególności:

1) opracowuje dokumentację bezpieczeństwa teleinformatycznego oraz propozycje jej uaktualniania;
2) przechowuje oryginały zatwierdzonej (zaakceptowanej) dokumentacji bezpieczeństwa teleinformatycznego;
3) wdraża procedury bezpiecznej eksploatacji systemu lub sieci teleinformatycznej;
4) współuczestniczy w szkoleniu użytkowników systemu lub sieci teleinformatycznej z zakresu ich bezpiecznej eksploatacji;
5) utrzymuje zgodność konfiguracji i parametrów systemu lub sieci teleinformatycznej z dokumentacją bezpieczeństwa teleinformatycznego oraz innymi dokumentami normatywnymi;
6) systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń oraz poprawność działania systemu lub sieci teleinformatycznej;
7) informuje pełnomocnika ochrony oraz Centrum Wsparcia Technicznego funkcjonującego w Centrum Zarządzania Systemami Teleinformatycznymi resortu obrony narodowej o stwierdzonych naruszeniach bezpieczeństwa systemu lub sieci teleinformatycznej;
8) zgłasza pełnomocnikowi ochrony potrzeby w zakresie serwisowania i ponownej certyfikacji wyrobów o przeznaczeniu specjalnym, o których mowa w pkt 1 ppkt 9 lit. c i d;
9) analizuje i archiwizuje rejestr zdarzeń w systemie lub sieci teleinformatycznej, prawidłowość dokumentowania i archiwizowania zdarzeń;
10) prowadzi na bieżąco wykaz osób mających dostęp do systemu lub sieci teleinformatycznej oraz przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki (komórki) organizacyjnej.

10. Inspektor bezpieczeństwa teleinformatycznego realizuje zadania w zakresie bieżącej kontroli zgodności funkcjonowania systemu lub sieci teleinformatycznej z dokumentacją bezpieczeństwa teleinformatycznego z wyłączeniem organizacyjnych, technicznych, programowych i eksploatacyjnych aspektów ochrony kryptograficznej, o których mowa w pkt 11-15, w szczególności kontroluje:

1) przestrzeganie zasad ochrony informacji niejawnych w systemie lub sieci teleinformatycznej;
2) stan zabezpieczeń fizycznych, elektromagnetycznych i elektronicznych pomieszczeń lub obszarów, w których usytuowane są systemy lub sieci teleinformatyczne;
3) aktualność wykazów osób mających dostęp do systemu lub sieci teleinformatycznej, przydzielanie kont użytkownikom, zakres nadanych im uprawnień oraz prawidłowość zabezpieczeń zastosowanych w systemie lub sieci;
4) znajomość i przestrzeganie przez użytkowników procedur bezpiecznej eksploatacji systemu lub sieci teleinformatycznej;
5) przestrzeganie zasad i wymagań w zakresie oznaczania, ewidencjonowania, przechowywania i przekazywania wytworzonych dokumentów niejawnych oraz ich terminowe rozliczanie;
6) zgodność konfiguracji systemu lub sieci teleinformatycznej z dokumentacją bezpieczeństwa teleinformatycznego;
a ponadto:
7) analizuje rejestr zdarzeń w systemie lub sieci teleinformatycznej, prawidłowość dokumentowania i archiwizowania zdarzeń;
8) informuje pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu lub sieci teleinformatycznej;

9) prowadzi szkolenia użytkowników w zakresie ochrony informacji niejawnych oraz przestrzegania zasad bezpieczeństwa w systemie lub sieci teleinformatycznej;

10) uczestniczy w opracowywaniu:

a) programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów i sieci teleinformatycznych,
b) dokumentacji bezpieczeństwa teleinformatycznego.

11. Organy wymienione, o których mowa w pkt 2 ppkt 2- 4, odpowiadają za kryptograficzną ochronę informacji w systemach i sieciach teleinformatycznych oraz sprawowanie nadzoru nad eksploatacją technicznych i programowych środków ochrony tych systemów i sieci.

12. Centrum Bezpieczeństwa Teleinformacyjnego, podporządkowane Szefowi Służby Kontrwywiadu Wojskowego, jest właściwe do:

1) opracowywania projektów dokumentów normatywnych dotyczących zasad bezpieczeństwa teleinformatycznego;
2) opiniowania projektów dokumentów normatywnych dotyczących organizacji, funkcjonowania i bezpieczeństwa systemów łączności i informatyki, systemów ochrony kryptograficznej oraz systemów i sieci teleinformatycznych chronionych kryptograficznie;
3) opiniowania dokumentacji bezpieczeństwa teleinformatycznego systemów i sieci chronionych kryptograficznie;
4) opiniowania programów szkoleń dotyczących bezpieczeństwa teleinformatycznego, w tym również eksploatacji urządzeń ochrony kryptograficznej;
5) dokonywania rocznej i doraźnych ocen stanu bezpieczeństwa systemów i sieci chronionych kryptograficznie;
6) badania i oceny systemów ochrony kryptograficznej oraz systemów i sieci chronionych kryptograficznie, w ramach prowadzonego procesu certyfikacyjnego lub akredytacyjnego;
7) wykonywania funkcji centralnego organu dystrybucji narodowych materiałów kryptograficznych oraz materiałów kryptograficznych pochodzących z wymiany międzynarodowej w resorcie obrony narodowej;
8) generacji i wytwarzania dokumentów kryptograficznych dla potrzeb narodowych systemów ochrony kryptograficznej;
9) sprawowania nadzoru nad bezpieczeństwem narodowych materiałów kryptograficznych i materiałów kryptograficznych pochodzących z wymiany międzynarodowej, eksploatowanych i wykorzystywanych w jednostkach (komórkach) organizacyjnych resortu obrony narodowej;
10) prowadzenia kontroli w zakresie bezpieczeństwa teleinformatycznego, zarządzanych przez Szefa Służby Kontrwywiadu Wojskowego;
11) dokonywania sprawdzeń zgodności stanu faktycznego systemów i sieci chronionych kryptograficznie z dokumentacją bezpieczeństwa teleinformatycznego;
12) szkolenia z zakresu ochrony informacji niejawnych osób dokonujących odbioru technicznego lub serwisowania urządzeń ochrony kryptograficznej, kończonego egzaminem i wydaniem zaświadczenia o odbyciu przeszkolenia oraz prowadzenie ewidencji tych zaświadczeń (wzór zaświadczenia o odbyciu przeszkolenia z zakresu ochrony informacji niejawnych w przedmiocie odbioru technicznego lub serwisowania urządzeń ochrony kryptograficznej określa załącznik Nr 1 do decyzji);
13) wydawania pozwoleń na dostęp do systemów ochrony kryptograficznej osobom spoza organów bezpieczeństwa teleinformacyjnego oraz nie będącym pracownikami w jednostce organizacyjnej;
14) pełnienia funkcji Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe.

13. Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki jest właściwe do:

1) opracowywania projektów dokumentów normatywnych dotyczących:

a) organizacji, funkcjonowania i bezpieczeństwa systemów łączności specjalnej wykorzystujących materiały kryptograficzne (szyfrowe i kodowe),
b) organizacji, funkcjonowania i bezpieczeństwa systemów ochrony kryptograficznej stosowanych w systemach i sieciach teleinformatycznych resortu obrony narodowej,

c) gospodarki materiałowej i zasad eksploatacji urządzeń ochrony kryptograficznej;

2) koordynowania działalności organów bezpieczeństwa systemów łączności i informatyki rodzajów Sił Zbrojnych, Dowództwa Garnizonu Warszawa, Dowództwa Operacyjnego i Centrum Zarządzania Systemami Teleinformatycznymi;

3) planowania, organizowania, prognozowania rozwoju, eksploatacji i nadzoru nad funkcjonowaniem systemów łączności specjalnej, systemów ochrony kryptograficznej stosowanych w systemach i sieciach teleinformatycznych resortu obrony narodowej oraz podczas misji pokojowych i ćwiczeń, a także Wojennego Systemu Dowodzenia;

4) rozdziału, dystrybucji, ewidencji, wprowadzania, wycofywania oraz nadzoru nad niszczeniem materiałów kryptograficznych w Siłach Zbrojnych;

5) planowania i organizowania szkoleń i kursów specjalistycznych personelu stacji/aparatowni kryptograficznych i kancelarii kryptograficznych oraz żołnierzy i pracowników organów, o których mowa w pkt 2 ppkt 4, w zakresie organizacji, funkcjonowania i bezpieczeństwa systemów ochrony kryptograficznej, a także gospodarki materiałowej sprzętem ochrony kryptograficznej w Siłach Zbrojnych;

6) uzgadniania dokumentacji bezpieczeństwa teleinformatycznego;

7) opracowywania dokumentacji bezpieczeństwa teleinformatycznego dla systemów, o których mowa w ppkt 1 lit. a, oraz przekazywania jej do Służby Kontrwywiadu Wojskowego celem zatwierdzenia lub akceptacji;

8) współuczestniczenia w kontrolach systemów i sieci chronionych kryptograficznie;

9) prowadzenia kontroli problemowych, zarządzanych przez Szefa Generalnego Zarządu Dowodzenia i Łączności – P6, organów bezpieczeństwa, o których mowa w pkt 2 ppkt 4, w zakresie organizacji, funkcjonowania, bezpieczeństwa materiałów kryptograficznych oraz systemów i sieci chronionych kryptograficznie;

10) wydawania pozwoleń na eksploatację urządzeń ochrony kryptograficznej oraz prowadzenia ewidencji wydanych pozwoleń (wzory pozwoleń na eksploatację urządzeń określa załącznik Nr 2 do decyzji).

14. Organy bezpieczeństwa systemów łączności i informatyki danego szczebla organizacyjnego odpowiadają za realizację zadań, o których mowa w pkt 13 ppkt 1 i 3-8, stosownie do zakresu kompetencji na swoim szczeblu organizacyjnym, koordynują działalność organów bezpieczeństwa systemów łączności i informatyki jednostek podległych oraz uzgadniają dokumentację bezpieczeństwa teleinformatycznego, zgodnie z pkt 5 ppkt 2 i pkt 6 ppkt 2.

15. Personel organów bezpieczeństwa systemów łączności i informatyki, o których mowa w pkt 2 ppkt 4, współpracuje z pełnomocnikiem ochrony i inspektorem bezpieczeństwa teleinformatycznego w zakresie zapewnienia właściwej ochrony informacjom niejawnym w systemach i sieciach teleinformatycznych danej jednostki (komórki) organizacyjnej, a także udziela pełnomocnikowi ochrony niezbędnych konsultacji w zakresie opracowywania dokumentacji bezpieczeństwa teleinformatycznego oraz innych dokumentów dotyczących problematyki ochrony informacji niejawnych w systemach i sieciach teleinformatycznych.

16. Centrum Zarządzania Systemami Teleinformatycznymi realizuje zadania Centrum Wsparcia Technicznego Systemu Reagowania na Incydenty Komputerowe w stosunku do systemów i sieci teleinformatycznych w resorcie obrony narodowej.

17. Służby Kontrwywiadu Wojskowego są właściwe do:

1) określania ogólnych zasad bezpieczeństwa teleinformatycznego dla systemów i sieci teleinformatycznych w formie dyrektyw, wytycznych i instrukcji wydanych przez Szefa Służby Kontrwywiadu Wojskowego;
2) potwierdzania przydatności algorytmów kryptograficznych i środków gwarantujących ochronę tych algorytmów, kluczy kryptograficznych oraz innych istotnych parametrów zabezpieczenia, w szczególności haseł zabezpieczających, służących ochronie informacji niejawnych stanowiących tajemnicę państwową i służbową;
3) opiniowania przedstawianej do zatwierdzenia lub akceptacji dokumentacji bezpieczeństwa teleinformatycznego;
4) akceptowania dokumentacji bezpieczeństwa teleinformatycznego, opracowanej dla systemów lub sieci teleinformatycznych, dotyczących informacji niejawnych stanowiących tajemnicę służbową;
5) zatwierdzania dokumentacji bezpieczeństwa teleinformatycznego, opracowanej dla systemów lub sieci teleinformatycznych, dotyczących informacji niejawnych stanowiących tajemnicę państwową;

6) akredytacji systemów i sieci teleinformatycznych;
7) wydawania certyfikatów akredytacji bezpieczeństwa teleinformatycznego dla systemów i sieci teleinformatycznych, dotyczących informacji niejawnych stanowiących tajemnicę państwową;
8) prowadzenia badań i wydawania certyfikatów dla wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych;
9) określania Poziomu Zabezpieczenia Miejsca i Poziomu Zabezpieczenia Urządzenia;
10) planowania i prowadzenia specjalistycznych szkoleń administratorów systemów, zakończonych egzaminem i wydaniem zaświadczenia o odbyciu przeszkolenia (wzór zaświadczenia o odbyciu przeszkolenia z zakresu obowiązków administratora systemu określa załącznik Nr 3 do decyzji);
11) planowania i prowadzenia specjalistycznych szkoleń inspektorów bezpieczeństwa teleinformatycznego, zakończonych egzaminem i wydaniem zaświadczenia o odbyciu przeszkolenia (wzór zaświadczenia o odbyciu przeszkolenia z zakresu obowiązków pracownika pionu ochrony inspektora bezpieczeństwa teleinformatycznego określa załącznik Nr 4 do decyzji);
12) planowania i prowadzenia specjalistycznych szkoleń w zakresie serwisowania wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych;
13) kontroli systemów i sieci teleinformatycznych oraz przestrzegania obowiązujących w tym zakresie przepisów;
14) dokonywania rocznej i doraźnych ocen stanu ochrony informacji niejawnych w resorcie obrony narodowej, w zakresie bezpieczeństwa teleinformatycznego.

18. Traci moc decyzja Nr 181/MON Ministra Obrony Narodowej z dnia 6 października 2000 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej (Dz. Rozk. MON z 2000 r., poz. 111).

19. Decyzja wchodzi w życie po upływie 30 dni od dnia jej ogłoszenia.

Załącznik nr 1

.....
(pieczęć nagłówkowa
z adresem i nr telefonu)

ZAŚWIADCZENIE

o odbyciu przeszkolenia z zakresu ochrony informacji niejawnych w przedmiocie odbioru technicznego/serwisowania* urządzeń ochrony kryptograficznej

Nr .....

Stwierdza się, że Pan(i):

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

odbył(a) przeszkolenie z zakresu ochrony informacji niejawnych dla osób dokonujących odbioru technicznego/serwisowania* urządzeń ochrony kryptograficznej typu:

.....

.....

.....

przeprowadzone przez Służby Kontrwywiadu Wojskowego.

.....
(miejscowość i data)

m.p.

.....
(pieczęć imienna i podpis
upoważnionego przedstawiciela SKW)

* niepotrzebne skreślić

WZÓR

Wzory
pozwoleń na eksploatację urządzeń ochrony kryptograficznej

Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY
KRYPTOGRAFICZNEJ

Nr .....

Pan(i)
.....
.
(stopień, nazwisko i imię)

....
.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu

Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY
KRYPTOGRAFICZNEJ

Nr .....

Pan(i)
.....
.
(stopień, nazwisko i imię)

....
.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu

Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY
KRYPTOGRAFICZNEJ

Nr .....

Pan(i)
.....
.
(stopień, nazwisko i imię)

....
.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu

Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY
KRYPTOGRAFICZNEJ

Nr .....

Pan(i)
.....
..
(stopień, nazwisko i imię)

.....
.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu

Duże litery: **S, IFF, U, R** – są koloru żółtego:

S - kryptograficzne urządzenia szyfrujące
IFF - kryptograficzne urządzenia identyfikacji obiektów
U - kryptograficzne urządzenia utajniające
R - kryptograficzne radiowe urządzenia utajniające

Załącznik nr 3

.....
(pieczęć nagłówkowa
z adresem i nr telefonu)

ZAŚWIADCZENIE

o odbyciu przeszkolenia z zakresu obowiązków administratora systemu

Nr .....

Stwierdza się, że Pan(i):

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

odbył(a) specjalistyczne przeszkolenie z zakresu obowiązków „administratora systemu" w przedmiocie ochrony informacji niejawnych wymagane przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz. 1631), przeprowadzone przez Służby Kontrwywiadu Wojskowego.

.....
(miejscowość i data)

m.p.

.....
(pieczęć imienna i podpis
upoważnionego przedstawiciela SKW)

WZÓR

Załącznik nr 4

.....
(pieczęć nagłówkowa
z adresem i nr telefonu)

ZAŚWIADCZENIE

o odbyciu przeszkolenia z zakresu obowiązków inspektora bezpieczeństwa teleinformatycznego

Nr .....

Stwierdza się, że Pan(i):

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

odbył(a) specjalistyczne przeszkolenie z zakresu obowiązków „pracownika pionu ochrony informacji niejawnych - inspektora bezpieczeństwa teleinformatycznego" odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania systemu lub sieci teleinformatycznej ze szczególnymi wymaganiami bezpieczeństwa w przedmiocie ochrony informacji niejawnych, wymagane przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz. 1631), przeprowadzone przez Służby Kontrwywiadu Wojskowego.

.....
(miejscowość i data)

m.p.

.....
(pieczęć imienna i podpis
upoważnionego przedstawiciela SKW)

DECYZJA Nr 25/MON

MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach i komórkach organizacyjnych resortu obrony narodowej

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. z 1996 r., Nr 94, poz. 426), w związku z art. 14 ust. 1 pkt 1 i 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631), w celu zapewnienia szczególnej ochrony informacjom niejawnym pochodzącym z wymiany zagranicznej oraz materiałom i narzędziom kryptograficznym, stanowiącym tajemnicę państwową i służbową, przed ich nieuprawnionym ujawnieniem, ustala się, co następuje:

1. Ilekroć w decyzji jest mowa o:

1) pomieszczeniu wydzielonym - należy przez to rozumieć pomieszczenie, w którym:

a) zainstalowano serwery sieciowe, terminale sieci teleinformatycznych, autonomiczne stanowiska komputerowe, a także ich elementy aktywne lub pasywne, w szczególności routery, switche, modemy, panele światłowodowe, służące do ochrony informacji niejawnych wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w komórce organizacyjnej Ministerstwa Obrony Narodowej i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, z wykorzystaniem materiałów i narzędzi kryptograficznych,
b) prowadzi się projektowanie, produkcję, montaż, naprawę lub serwisowanie urządzeń ochrony kryptograficznej lub innych wyrobów o przeznaczeniu specjalnym służących do ochrony informacji niejawnych, wchodzące w skład zespołu pomieszczeń kancelarii kryptograficznej;

2) certyfikacie bezpieczeństwa dla pomieszczenia - należy przez to rozumieć formalny dokument, potwierdzający zdolność personelu i pomieszczenia lub zespołu pomieszczeń do zapewnienia wymaganej ochrony informacjom niejawnym pochodzącym z wymiany zagranicznej oraz materiałom i narzędziom kryptograficznym, stanowiącym tajemnicę państwową i służbową, wytwarzanym, przechowywanym, przetwarzanym lub przekazywanym w tych pomieszczeniach, przed ich nieuprawnionym ujawnieniem.

2. Szef Wojskowych Służb Informacyjnych powoła, ze składu osobowego podległych komórek i jednostek organizacyjnych, Stałą Komisję do Certyfikacji i Kontroli, zwaną dalej „Komisją".

3. W skład Komisji wchodzi:

1) przewodniczący;
2) sekretarz;
3) członkowie (audytorzy wiodący, audytorzy techniczni).

4. Komisja przeprowadza audyty certyfikacyjne, recertyfikacyjne oraz kontrole okresowe:

1) kancelarii zagranicznych;
2) punktów obsługi dokumentów zagranicznych, tworzonych na bazie kancelarii tajnych;
3) kancelarii kryptograficznych;

4) stacji łączności kryptograficznej;
5) kabin kryptograficznych;
6) pomieszczeń wydzielonych,
organizowanych lub funkcjonujących w komórkach organizacyjnych Ministerstwa Obrony Narodowej i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, innych jednostkach organizacyjnych realizujących produkcję lub usługi, stanowiące tajemnicę państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa i potrzeby Sił Zbrojnych Rzeczypospolitej Polskiej, zwanych dalej „Siłami Zbrojnymi" a także przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa, jeśli uczestnikami tego obrotu są jednostki organizacyjne Sil Zbrojnych lub inne jednostki podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.

5. Komisja przeprowadza audyty certyfikacyjne, recertyfikacyjne oraz kontrole okresowe pomieszczeń, o których mowa w pkt 4, na podstawie pisemnego upoważnienia, wydanego przez Szefa Służby Kontrwywiadu Wojskowego. Wzór upoważnienia określa załącznik nr 1 do decyzji.

6. Nadzór nad pracami Komisji, z upoważnienia i w imieniu Szefa Wojskowych Służb Informacyjnych, sprawuje Szef Zarządu Ochrony Informacji Niejawnych Inspektoratu Służby Kontrwywiadu Wojskowego.

7. Szef Służby Kontrwywiadu Wojskowego:

1) decyduje o przeprowadzeniu audytu certyfikacyjnego lub recertyfikacyjnego pomieszczeń, o których mowa w pkt 4, na podstawie wniosków w sprawie przeprowadzenia audytu certyfikacyjnego lub recertyfikacyjnego, złożonych przez właściwych kierowników komórek lub jednostek organizacyjnych;
2) wydaje certyfikaty bezpieczeństwa dla pomieszczeń, o których mowa w pkt 4, których wzór określa załącznik nr 2 do decyzji;
3) określi sposoby prowadzenia ewidencji i przechowywania certyfikatów bezpieczeństwa pomieszczeń, o których mowa w pkt 4;
4) wyda i wprowadzi do użytku służbowego, w resorcie obrony narodowej, wytyczne w zakresie stosowania środków bezpieczeństwa fizycznego i zasad organizacji pomieszczeń, wymienionych w pkt 4 ppkt 3-6.

8. Do podstawowych zadań i obowiązków Komisji należy:

1) sprawdzanie, w trakcie prowadzonego audytu certyfikacyjnego lub recertyfikacyjnego stanu zabezpieczeń pomieszczeń, o których mowa w pkt 4, w zakresie spełniania wymagań bezpieczeństwa osobowego, fizycznego, technicznego oraz zastosowanych procedur organizacyjnych i prawnych;
2) sporządzanie raportów z wykonanych szczegółowych czynności sprawdzających w ramach prowadzonych audytów certyfikacyjnych lub recertyfikacyjnych;
3) występowanie z wnioskami do Szefa Służby Kontrwywiadu Wojskowego o wydanie certyfikatów bezpieczeństwa dla pomieszczeń, o których mowa w pkt 4, które zostały sprawdzone, a stan ich zabezpieczeń został zweryfikowany z obowiązującymi wymaganiami i pozytywnie oceniony przez Komisję, w trakcie prowadzonego audytu certyfikacyjnego lub recertyfikacyjnego;
4) formułowanie zaleceń (dotyczy tylko przypadków negatywnej oceny pomieszczenia lub pomieszczeń, o których mowa w pkt 4) przedkładanych do realizacji właściwemu kierownikowi komórki lub jednostki organizacyjnej;
5) prowadzenie kontroli okresowych certyfikowanych pomieszczeń, o których mowa w pkt 4, w zakresie spełniania wymagań dla pomieszczeń certyfikowanych, zgodnie z planem kontroli, zatwierdzonym przez Szefa Służby Kontrwywiadu Wojskowego.

9. Terminy ważności dokumentów z przeprowadzonego audytu certyfikacyjnego lub recertyfikacyjnego pomieszczeń , o których mowa w pkt 4:

1) raporty z przeprowadzonych audytów – zachowują ważność na czas ważności certyfikatów bezpieczeństwa pomieszczeń wydanych na ich podstawie;
2) certyfikaty bezpieczeństwa:

a) 5 lat - dla pomieszczeń, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową o klauzuli ŚCIŚLE TAJNE,
b) 7 lat - dla pomieszczeń, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową o klauzuli TAJNE,
c) 10 lat - dla pomieszczeń, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę służbową o klauzuli POUFNE.

10. Dokumenty z przeprowadzonego audytu certyfikacyjnego lub recertyfikacyjnego, wykonane przez Komisję przechowuje:

1) raporty z przeprowadzonych audytów - Stała Komisja do Certyfikacji i Kontroli Służby Kontrwywiadu Wojskowego;

2) certyfikaty bezpieczeństwa kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych:

a) egz. nr 1 - Stała Komisja do Certyfikacji i Kontroli Służby Kontrwywiadu Wojskowego,
b) egz. nr 2 - Główna Kancelaria Zagraniczna Ministerstwa Obrony Narodowej,
c) egz. nr 3 - kancelaria zagraniczna lub punkt obsługi dokumentów zagranicznych, której dotyczył audyt certyfikacyjny lub recertyfikacyjny;

3) certyfikaty bezpieczeństwa kancelarii kryptograficznych i kabin kryptograficznych:

a) egz. nr 1 - Stała Komisja do Certyfikacji i Kontroli Służby Kontrwywiadu Wojskowego,
b) egz. nr 2 - Główna Kancelaria Kryptograficzna Centrum Bezpieczeństwa Teleinformacyjnego,
c) egz. nr 3 - kancelaria kryptograficzna lub kabina kryptograficzna, których dotyczył audyt certyfikacyjny lub recertyfikacyjny;

4) certyfikaty bezpieczeństwa stacji łączności kryptograficznej oraz pomieszczeń wydzielonych:

a) egz. nr 1 - Stała Komisja do Certyfikacji i Kontroli Służby Kontrwywiadu Wojskowego,
b) egz. nr 2 - Centrum Bezpieczeństwa Teleinformacyjnego,
c) egz. nr 3 - stacja łączności kryptograficznej lub pomieszczenie wydzielone, których dotyczył audyt certyfikacyjny lub recertyfikacyjny.

11. Dysponenci środków budżetowych, każdy w swoim zakresie, wydzielają środki finansowe na utworzenie pomieszczeń, o których mowa w pkt 4, ich zabezpieczenie i wyposażenie, w podległych sobie jednostkach i komórkach organizacyjnych.

12. Dyrektor Departamentu Administracyjnego, w porozumieniu z Dyrektorem Generalnym Ministerstwa Obrony Narodowej, zapewni wyposażenie w niezbędny sprzęt biurowy, kwaterunkowy i informatyczny oraz środki łączności tworzonych w komórkach organizacyjnych Ministerstwa Obrony Narodowej pomieszczeń, o których mowa w pkt 4.

13. Dyrektor Biura Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej zapewni:

1) prowadzenie w Głównej Kancelarii Zagranicznej Ministerstwa Obrony Narodowej szczegółowej ewidencji kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych tworzonych i certyfikowanych w:

a) komórkach organizacyjnych Ministerstwa Obrony Narodowej,
b) jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych,
c) innych jednostkach organizacyjnych realizujących produkcję lub usługi, stanowiące tajemnicę państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa i potrzeby Sił Zbrojnych, a także przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa, jeśli uczestnikami tego obrotu są Siły Zbrojne lub inne jednostki organizacyjne podległe Ministrowi Obrony Narodowej;

2) przechowywanie w Głównej Kancelarii Zagranicznej Ministerstwa Obrony Narodowej certyfikatów bezpieczeństwa, o których mowa w pkt 4 ppkt 1 i 2.

14. Kierownicy jednostek i komórek organizacyjnych resortu obrony narodowej, w których utworzono pomieszczenia, o których mowa w pkt 4 ppkt 1 i 2:

1) występują do Szefa Służby Kontrwywiadu Wojskowego z pisemnymi wnioskami o przeprowadzenie:

a) audytu certyfikacyjnego - w przypadkach nowo utworzonych kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych lub kancelarii tajnych, które mają pełnić funkcje punktów obsługi dokumentów zagranicznych (przed ich uruchomieniem),
b) audytu recertyfikacyjnego - w przypadkach wprowadzania w funkcjonujących kancelariach zagranicznych lub punktach obsługi dokumentów zagranicznych posiadających certyfikaty bezpieczeństwa, jakichkolwiek zmian w ich organizacji, funkcjonowaniu, zabezpieczeniu i wyposażeniu oraz na sześć miesięcy przed wygaśnięciem terminu obowiązywania certyfikatu bezpieczeństwa;

2) ogłaszają w rozkazie wewnętrznym fakt uruchomienia w jednostce lub komórce organizacyjnej resortu obrony narodowej, na podstawie certyfikatu bezpieczeństwa otrzymanego ze Służby Kontrwywiadu Wojskowego, kancelarii zagranicznej lub punktu obsługi dokumentów zagranicznych;

3) obejmują kancelarię zagraniczną lub punkt obsługi dokumentów zagranicznych kontrolą i stałym nadzorem służbowym, realizowanym przez podległy kierownikowi jednostki lub komórki organizacyjnej pion ochrony informacji niejawnych;

4) zapewniają im warunki funkcjonowania, zgodnie z przepisami o ochronie informacji niejawnych;

5) informują Szefa Służby Kontrwywiadu Wojskowego o przypadkach naruszenia przepisów o ochronie informacji niejawnych;

6) informują Dyrektora Biura Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej o uruchomieniu w jednostce lub komórce organizacyjnej resortu obrony narodowej kancelarii zagranicznej lub punktu obsługi dokumentów zagranicznych oraz o ich likwidacji – dla celów, określonych w pkt 13.

15. Kierownicy jednostek i komórek organizacyjnych resortu obrony narodowej, w których utworzono pomieszczenia, określone w pkt 4 ppkt 3-6, występują do Szefa Służby Kontrwywiadu Wojskowego z pisemnymi wnioskami o przeprowadzenie:

1) audytu certyfikacyjnego - w przypadkach nowo utworzonych specjalistycznych komórek lub pomieszczeń (przed ich uruchomieniem);

2) audytu recertyfikacyjnego - w przypadkach wprowadzania w funkcjonujących pomieszczeniach posiadających certyfikaty bezpieczeństwa, jakichkolwiek zmian w ich organizacji, funkcjonowaniu,

zabezpieczeniu i wyposażeniu oraz na sześć miesięcy przed wygaśnięciem terminu obowiązywania certyfikatu bezpieczeństwa.

16. Kierownicy jednostek i komórek organizacyjnych resortu obrony narodowej, jako zleceniodawcy, określają przedsiębiorcom, jednostkom naukowym lub badawczo-rozwojowym w „Instrukcji bezpieczeństwa przemysłowego", warunki do spełnienia wymagane niniejszą decyzją, w przypadkach realizacji umów na rzecz resortu obrony narodowej, związanych z dostępem do informacji niejawnych, pochodzących z wymiany zagranicznej lub materiałów i narzędzi kryptograficznych.

17. Pomieszczenia, o których mowa w pkt 4, którym kończy się okres ważności wydanego certyfikatu bezpieczeństwa, należy zgłaszać do audytu recertyfikacyjnego, nie później niż sześć miesięcy przed wygaśnięciem ważności certyfikatu bezpieczeństwa.

18. Traci moc decyzja Nr 29/MON Ministra Obrony Narodowej z dnia 22 lutego 2001 r. w sprawie trybu certyfikacji i kontroli kancelarii zagranicznych, kancelarii środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych (terminali) teleinformatycznych w jednostkach organizacyjnych resortu Obrony Narodowej (Dz. Urz. MON Nr 3, poz. 32).

19. Decyzja wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

ZAŁĄCZNIKI DO DECYZJI:

- Wzór CERTYFIKATU BEZPIECZEŃSTWA dla pomieszczenia / zespołu pomieszczeń

Załącznik nr 1

SZEF

Warszawa, ...

WOJSKOWYCH SŁUŻB INFORMACYJNYCH
00-909 Warszawa 60, tel. 6 841 664

UPOWAŻNIENIE NR ..... / ..... /SKCiK

Na podstawie pkt 5 decyzji nr ...../MON Ministra Obrony Narodowej z dnia ..... 2006 roku w sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach organizacyjnych resortu obrony narodowej, upoważniam:

Pana

.....

(stopień, imię i nazwisko)

do przeprowadzenia sprawdzenia pomieszczenia / zespołu pomieszczeń * .... w ramach audytu certyfikacyjnego / recertyfikacyjnego / kontroli okresowej*, zgłoszonego(ych)* do audytu certyfikacyjnego / recertyfikacyjnego * przez ..... pismem nr ..... z dnia ....., znajdującego(ych)* się w:

.....

(nazwa i adres instytucji, jednostki wojskowej)

Upoważnienie niniejsze ważne jest za okazaniem legitymacji służbowej.

Ważność upoważnienia upływa z dniem .....

(pieczęć urzędowa)

.....
(pieczęć imienna i podpis osoby wydającej upoważnienie)

Ważność upoważnienia przedłuża się do dnia .....

(pieczęć urzędowa)

.....
(pieczęć imienna i podpis osoby wydającej upoważnienie)

* - w oryginale wybrać odpowiednią formę

Załącznik nr 2

CERTYFIKAT BEZPIECZEŃSTWA
dla pomieszczenia / zespołu pomieszczeń *

.....

w .....
(nazwa jednostki wojskowej, jednostki, komórki organizacyjnej)

/ ..... /
(dokładny adres)

Zaświadcza się, że Stała Komisja do Certyfikacji i Kontroli, działając na podstawie pkt 2 decyzji nr ...../MON Ministra Obrony Narodowej z dnia ..... 2006 roku w sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach i komórkach organizacyjnych resortu obrony narodowej, w dniu ..... roku przeprowadziła audyt certyfikacyjny pomieszczenia / zespołu pomieszczeń *
.....

w .....

Komisja stwierdziła, że skontrolowane(y)* pomieszczenie / zespół pomieszczeń * jest zorganizowane(y)* w sposób zapewniający wymagany poziom bezpieczeństwa i ochrony informacji niejawnych, do klauzuli ..... włącznie.

W związku z powyższym potwierdzam, że wymienione(y)* pomieszczenie / zespół pomieszczeń *

zapewnia wymagany poziom bezpieczeństwa i ochrony informacji niejawnych, do klauzuli

..... włącznie.

Certyfikat ważny jest do: ..... roku.

SZEF
WOJSKOWYCH SŁUŻB INFORMACYJNCYH

m.p.

(podpis)

.....
(stopień, imię i nazwisko)

WARSZAWA, dnia .....

WSI/SKCiK – nr kolejny / typ pomieszczenia / rok kalendarzowy (nr egzemplarza)

* - w oryginale wybrać odpowiednią formę

WZÓR

ZARZĄDZENIE Nr 25/ MON

MINISTRA OBRONY NARODOWEJ

z dnia 17 listopada 2005 r.

w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych

Na podstawie art. 53 ust. 3 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
Postanowienia ogólne

§ 1.
Zarządzenie określa:

1) organizację i funkcjonowanie kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych, odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

2) stosowanie środków ochrony fizycznej;

3) organizację, funkcjonowanie i zabezpieczenie kancelarii tajnych na okrętach bojowych i pomocniczych jednostkach pływających Marynarki Wojennej;

4) zasady rejestrowania, kompletowania i niszczenia materiałów niejawnych;

5) organizację pracy kancelarii tajnych, ich ochronę oraz obieg dokumentów podczas ćwiczeń, wojny, a także w czasie realizacji zadań w misjach organizacji międzynarodowych;

6) wzory urządzeń ewidencyjnych.

§ 2.
Określenia użyte w zarządzeniu oznaczają:

1) ustawa - ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych;

2) jednostka organizacyjna – Ministerstwo Obrony Narodowej, jednostkę nie wchodzącą w skład Ministerstwa podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną;

3) komórka organizacyjna Ministerstwa Obrony Narodowej – Sekretariat Ministra, departament, generalny zarząd, samodzielny zarząd, biuro, samodzielne szefostwo;

4) kancelaria tajna - komórkę wchodzącą w skład pionu ochrony jednostki organizacyjnej, odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów niejawnych;

5) kancelaria tajna - zagraniczna - komórkę wchodzącą w skład pionu ochrony jednostki organizacyjnej, odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów niejawnych wymienianych z innymi państwami i organizacjami międzynarodowymi, na podstawie zawartych przez Rzeczpospolitą Polską umów międzynarodowych;

6) punkt obsługi dokumentów zagranicznych - wydzieloną część kancelarii tajnej odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów niejawnych wymienianych z innymi państwami i organizacjami międzynarodowymi na podstawie zawartych przez Rzeczpospolitą Polską umów międzynarodowych;

7) kancelaria ćwiczebna - komórkę tworzoną w jednostce organizacyjnej na czas ćwiczeń i treningów sztabowych, odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów niejawnych otrzymywanych, wytwarzanych i przetwarzanych w czasie ćwiczeń oraz treningów sztabowych;

8) kancelaria wojenna - komórkę tworzoną w jednostce organizacyjnej (komórce organizacyjnej Ministerstwa Obrony Narodowej), zgodnie z etatem na czas wojny, odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów bojowych zawierających informacje niejawne;

9) kierownik kancelarii - żołnierza zawodowego lub pracownika wojska, podległego pełnomocnikowi ochrony, kierującego pracą kancelarii tajnej lub tajnej - zagranicznej;

10) zastępca kierownika kancelarii – żołnierza zawodowego lub pracownika wojska zajmującego etatowe stanowisko zastępcy kierownika, podlegającego bezpośrednio kierownikowi kancelarii;

11) kancelista - żołnierza pełniącego zawodową służbę wojskową albo pracownika zatrudnionego w kancelarii tajnej lub tajnej - zagranicznej, podlegającego bezpośrednio kierownikowi kancelarii;

12) biblioteka tajna – komórkę wchodzącą w skład pionu ochrony jednostki organizacyjnej, odpowiedzialną za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie wydawnictw, czasopism, dokumentacji technicznej i materiałów filmowych, zawierających informacje niejawne stanowiące tajemnicę państwową lub służbową;

13) kierownik biblioteki – żołnierza zawodowego lub pracownika kierującego pracą biblioteki tajnej, podległego pełnomocnikowi ochrony;

14) bibliotekarz – żołnierza zawodowego lub pracownika pełniącego służbę wojskową albo zatrudnionego w bibliotece tajnej, podlegającego bezpośrednio kierownikowi biblioteki;

15) żołnierz - osobę pełniącą czynną służbę wojskową w jednostce organizacyjnej;

16) pracownik - osobę pozostającą w stosunku pracy z jednostką organizacyjną;

17) wykonawca - żołnierza lub pracownika zajmującego określone stanowisko służbowe, wykonującego zadania zgodnie z zakresem obowiązków, posiadającego stosowne poświadczenie bezpieczeństwa i przeszkolenie w zakresie ochrony informacji niejawnych;

18) wykonawca techniczny - wykonawcę odpowiedzialnego za utrwalanie informacji niejawnych w sposób określony w art. 2 pkt 5 ustawy;

19) urządzenie ewidencyjne - księgę, dziennik, wykaz, spis, rejestr lub kartotekę o ustalonych rubrykach, służącą do rejestrowania dokumentów zawierających informacje niejawne oraz umożliwiającą kontrolę ich stanu i obiegu;

20) dokumenty ćwiczebne - dokumenty zawierające informacje niejawne, otrzymane lub wytworzone w jednostce organizacyjnej podczas ćwiczeń i treningów sztabowych;

21) przesyłka - materiały w postaci odpowiednio zabezpieczonych, zaadresowanych i oznaczonych paczek lub listów;

22) akta - zbiór dokumentów ułożonych według rzeczowego wykazu akt, podszytych do teczek akt oznaczonych właściwą kategorią archiwalną i symbolem klasyfikacyjnym;

23) klasa systemów lub urządzeń alarmowych – kategorię jakości według Normy Obronnej NO-04-A004 Obiekty Wojskowe. Systemy Alarmowe. Wymagania dotyczące urządzeń;

24) pełnomocnik ochrony – pełnomocnika do spraw ochrony informacji niejawnych.

Rozdział 2

Organizacja i funkcjonowanie kancelarii tajnej oraz innej niż kancelaria tajna komórki organizacyjnej odpowiedzialnej za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych

§ 3.

1. Kancelarie tajne i tajne - zagraniczne, zwane dalej "kancelariami", tworzy się w jednostkach organizacyjnych, w których występują dokumenty zawierające informacje niejawne oznaczone klauzulą "Poufne" lub stanowiące tajemnicę państwową.

2. Kancelaria może przyjmować, rejestrować, przechowywać i wysyłać dokumenty niejawne oznaczone klauzulą „Zastrzeżone", na zasadach określonych w zatwierdzonych przez kierownika jednostki organizacyjnej szczegółowych wymaganiach w zakresie ochrony informacji niejawnych oznaczonych klauzulą „Zastrzeżone", o których mowa w art. 20 ust. 2 ustawy.

3. W szczególnie uzasadnionych przypadkach, za zgodą kierownika jednostki organizacyjnej i na określonych przez niego zasadach, kancelaria może przyjmować, rejestrować, przechowywać oraz wysyłać materiały jawne, pod warunkiem że będą one fizycznie oddzielone od materiałów niejawnych i rejestrowane w odrębnych urządzeniach ewidencyjnych.

4. W przypadkach uzasadnionych względami organizacyjnymi, w jednostce organizacyjnej można utworzyć więcej niż jedną kancelarię.

5. Kancelaria jednostki organizacyjnej może obsługiwać inne jednostki organizacyjne dyslokowane w tej samej strefie administracyjnej, nie mające w etacie kancelarii, pod warunkiem, iż dla każdej jednostki organizacyjnej będzie prowadzona odrębna ewidencja materiałów niejawnych, a dokumenty poszczególnych jednostek zostaną fizycznie od siebie oddzielone i będą kompletowane zgodnie z rzeczowymi wykazami akt obowiązującymi w tych jednostkach organizacyjnych.

6. W jednostkach organizacyjnych, w których występują wydawnictwa, czasopisma, dokumentacja techniczna lub materiały filmowe zawierające informacje niejawne oznaczone klauzulą „Poufne" lub wyższą, można utworzyć biblioteki tajne, zwane dalej „bibliotekami".

7. Dopuszcza się przyjmowanie, przechowywanie, ewidencjonowanie oraz wydawanie materiałów, o których mowa w ust. 6, przez kancelarię jednostki organizacyjnej, jeżeli warunki lokalowe kancelarii pozwalają na ich fizyczne oddzielenie od pozostałych przechowywanych w kancelarii dokumentów.

8. W jednostkach organizacyjnych, w których są przyjmowane, wytwarzane, przetwarzane, przechowywane lub przekazywane dokumenty planowania mobilizacyjnego, operacyjnego lub gotowości bojowej, wydziela się pomieszczenia przeznaczone do przechowywania, udostępniania i wytwarzania tych dokumentów, zwane dalej „kancelarią mobilizacyjną" oraz wyznacza rozkazem dziennym lub decyzją kierownika jednostki organizacyjnej osobę odpowiedzialną za ich

przyjmowanie, rejestrowanie, kompletowanie, przechowywanie oraz udostępnianie, zwaną dalej „kierownikiem kancelarii mobilizacyjnej".

9. Na stanowisko kierownika kancelarii, zastępcy kierownika kancelarii, kancelisty, kierownika biblioteki, bibliotekarza oraz kierownika kancelarii mobilizacyjnej wyznacza się żołnierza zawodowego lub pracownika , który posiada poświadczenie bezpieczeństwa odpowiednie dla klauzuli dokumentów niejawnych otrzymywanych, wytwarzanych, przetwarzanych, przekazywanych i przechowywanych w kancelarii, bibliotece lub kancelarii mobilizacyjnej, odbył szkolenie w zakresie ochrony informacji niejawnych, o którym mowa w art. 54 ust. 1 ustawy oraz szkolenie specjalistyczne, potwierdzone stosownymi zaświadczeniami.

§ 4.
1. Do obowiązków kierownika kancelarii, biblioteki oraz kancelarii mobilizacyjnej należy w szczególności:

1) przyjmowanie, rejestrowanie, przechowywanie oraz przekazywanie materiałów niejawnych otrzymywanych, wysyłanych oraz wytwarzanych na potrzeby wewnętrzne jednostki organizacyjnej, według zasad ustalonych w zarządzeniu;

2) prowadzenie wykazów osób upoważnionych do dostępu do informacji niejawnych, posiadających stosowne poświadczenia bezpieczeństwa;

3) udostępnianie i wydawanie materiałów niejawnych osobom, o których mowa w pkt 2;

4) rozliczanie wykonawców z powierzonych im dokumentów niejawnych.

2. Do obowiązków kierownika kancelarii należy ponadto:

1) prowadzenie ewidencji pieczęci urzędowych oraz służbowych posiadanych przez jednostkę organizacyjną lub obsługiwaną komórkę organizacyjną Ministerstwa Obrony Narodowej;

2) prowadzenie bieżącej kontroli sposobu wytwarzania dokumentów niejawnych przez wykonawców i wykonawców technicznych;

3) kompletowanie dokumentów oraz przygotowywanie akt do archiwizacji.

3. Kierownicy kancelarii tajnych - zagranicznych oraz kancelarii tajnych, w których zorganizowano punkty obsługi dokumentów zagranicznych, prowadzą na podstawie informacji otrzymywanych z Kancelarii Głównej Zagranicznej Ministerstwa Obrony Narodowej, wykaz kancelarii tajnych - zagranicznych i punktów obsługi dokumentów zagranicznych funkcjonujących w resorcie obrony narodowej.

4. Szczegółowe obowiązki kierownika kancelarii oraz kierownika biblioteki określa pełnomocnik ochrony, natomiast kierownika kancelarii mobilizacyjnej kierownik komórki odpowiedzialnej w jednostce organizacyjnej odpowiednio za problematykę planowania operacyjnego, mobilizacyjnego lub gotowości bojowej, w porozumieniu z pełnomocnikiem ochrony.

§ 5.
1. Przekazanie obowiązków na stanowisku kierownika kancelarii lub kierownika biblioteki następuje na podstawie protokołu zdawczo-odbiorczego, w obecności pełnomocnika ochrony, osoby zdającej oraz przyjmującej obowiązki.

2. Przekazanie obowiązków na stanowisku kierownika kancelarii mobilizacyjnej następuje na zasadach określonych w ust. 1, w obecności kierownika komórki, o której mowa w § 4 ust. 4.

3. W protokole, o którym mowa w ust. 1, wyszczególnia się:

1) nazwy i numery urządzeń ewidencyjnych, na podstawie których dokonano sprawdzenia stanu faktycznego dokumentów niejawnych pozostających na ewidencji kancelarii, biblioteki albo kancelarii mobilizacyjnej oraz pozycje zapisów w tych urządzeniach;

2) informacje dotyczące zgodności lub niezgodności stanu faktycznego dokumentów niejawnych ze stanem ewidencyjnym;

3) ewentualne uwagi osoby przyjmującej obowiązki dotyczące ujawnionych nieprawidłowości w zakresie ewidencjonowania i obiegu dokumentów.

4. Protokół zdawczo - odbiorczy podpisuje przekazujący oraz przyjmujący obowiązki, a zatwierdza osoba, o której mowa odpowiednio w ust. 1 albo w ust. 2. Jeden egzemplarz protokołu przechowuje się w kancelarii jednostki organizacyjnej, natomiast drugi przechowuje przełożony osoby zdającej obowiązki.

5. Dodatkowy egzemplarz protokołu może być wydany przekazującemu lub zdającemu obowiązki, na jego żądanie.

6. Na czas okresowej nieobecności, kierownika kancelarii lub biblioteki (urlop, choroba, wyjazd służbowy) zastępuje jego zastępca lub inna osoba pełniąca obowiązki służbowe w tej komórce, a w razie ich braku osoba posiadająca stosowne poświadczenie bezpieczeństwa oraz odbyte przeszkolenia, o których mowa w § 3 ust. 9, wyznaczona rozkazem dziennym lub decyzją kierownika jednostki organizacyjnej.

7. Kierownika kancelarii mobilizacyjnej zastępuje żołnierz zawodowy lub pracownik wojska wyznaczony rozkazem dziennym albo decyzją kierownika jednostki organizacyjnej, spełniający warunki określone w § 3 ust. 9.

8. Kierownik kancelarii przekazuje protokolarnie zastępującej go osobie, nie będącej zastępcą kierownika kancelarii lub kancelistą, wyłącznie urządzenia ewidencyjne i materiały niezbędne do prowadzenia bieżącej pracy kancelarii. Szafy z pozostałymi dokumentami niejawnymi zamyka i oznakowuje swoją pieczęcią numerową.

9. Obowiązki osób, o których mowa w ust. 1 i 2, jeżeli nie mogą one osobiście uczestniczyć w przekazywaniu obowiązków, przekazuje komisja powołana przez kierownika jednostki organizacyjnej. Do składu komisji przekazującej obowiązki na stanowisku kierownika kancelarii lub biblioteki wyznacza się pełnomocnika ochrony albo upoważnionego przez niego pracownika pionu ochrony; w pracach komisji przekazującej obowiązki na stanowisku kierownika kancelarii mobilizacyjnej uczestniczy kierownik komórki, o której mowa w § 4 ust. 4 lub upoważniona przez niego osoba.

10. Przewodniczący komisji, o której mowa w ust. 9, podpisuje protokół zdawczo-odbiorczy oraz oznakowuje swoją pieczęcią numerową sejfy, szafy i skrzynie z nie przekazanymi dokumentami niejawnymi.

Rozdział 3
Środki ochrony fizycznej

§ 6.
1. Kancelarie, biblioteki oraz kancelarie mobilizacyjne lokalizuje się w zespołach pomieszczeń lub pomieszczeniu spełniających następujące warunki bezpieczeństwa:

1) usytuowanych, z zastrzeżeniem ust. 2, w budynku o konstrukcji murowanej, betonowej lub innej o podobnych właściwościach (parametrach) konstrukcyjnych, z wejściem co najmniej ze strefy administracyjnej;

2) oddzielonych od innych pomieszczeń stałymi przegrodami budowlanymi o rozwiązaniach konstrukcyjno-materiałowych zapewniających bezpieczeństwo pożarowe i bezpieczeństwo konstrukcji, pozbawionymi zbędnych otworów, a w przypadku, gdy ściany zewnętrzne lub stropy stanowią granicę strefy bezpieczeństwa, powinny być wykonane z materiałów niepalnych i spełniać wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej klasy 15, o grubości 25 cm lub konstrukcji betonowej o grubości co najmniej 15 cm;

3) wyposażonych w drzwi wejściowe stalowe lub drewniane pełne o grubości co najmniej 4 cm, obustronnie obite blachą stalową o grubości co najmniej 2mm, blokowane na 4 krawędziach, zabezpieczone przed wyłamaniem 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 uniemożliwiający pozostawienie pomieszczenia otwartego;

4) z oknami zabezpieczonymi w sposób uniemożliwiający wgląd do pomieszczeń z zewnątrz z zainstalowaniem w otworach okiennych, z zastrzeżeniem pkt 5, kraty wykonanej w ramie z płaskownika stalowego o przekroju nie mniejszym niż 45x6 mm, z prętów stalowych o średnicy co najmniej 20 mm, usytuowanych pionowo w rozstawie nie większym niż 150 mm, wzmocnionej płaskownikami stalowymi o przekroju nie mniejszym niż 45x6 mm, usytuowanymi w poziomie, w odstępach nie większych niż 500 mm, z tym że jeżeli ze względów architektoniczno – budowlanych nie ma możliwości zainstalowania kraty, dopuszcza się zamontowanie okna antywłamaniowego, wyposażonego w szyby co najmniej klasy P-6, a rama i szyby powinny posiadać świadectwa kwalifikacyjne;

5) otwory okienne, których dolna krawędź znajduje się na wysokości powyżej 5 m od poziomu otaczającego terenu, lub górna krawędź więcej niż 3 m od poziomu dachu, wyposaża się w jedno z następujących zabezpieczeń:

a) siatkę stalową o grubości drutu nie mniejszej niż 2 mm, o oczkach nie większych niż 20x20 mm,
b) folię antywłamaniową,
c) szyby o podwyższonej odporności na stłuczenie;

6) otwory wentylacyjne i techniczne o powierzchni powyżej 500 cm^2 zabezpiecza się na poziomie stropów siatką stalową o średnicy oczka nie większej niż 10 mm albo systemem alarmowym.

2. Zabrania się lokalizowania kancelarii, bibliotek i kancelarii mobilizacyjnych na poddaszach.

3. Kancelarie, biblioteki i kancelarie mobilizacyjne powinny być, w miarę możliwości, rozmieszczone w zespołach pomieszczeń składających się co najmniej z trzech pomieszczeń z przeznaczeniem na:

1) pokój pracy dla personelu;
2) pomieszczenie magazynowe służące do przechowywania materiałów niejawnych;
3) pomieszczenie przeznaczone do zapoznawania się wykonawców z dokumentami niejawnymi (czytelnię) albo do pracy z dokumentami planowania mobilizacyjnego, operacyjnego lub gotowości bojowej.

4. Pomieszczenie magazynowe, o którym mowa w ust. 3 pkt 2 wyposaża się w drzwi stalowe lub drewniane, wykonane z litego drewna, o grubości co najmniej 2 cm, obustronnie obite blachą stalową o grubości co najmniej 1 mm, zabezpieczone przed wyłamaniem od strony zawiasów, wyposażone w zamek szyfrowy, o zmiennym nastawieniu, co najmniej trzyzapadkowy, o cichym przesuwie skali nastawień, skoku nastawień nie większym niż 1,5 podziałki, posiadający minimum 100 podziałek na pokrętle.

5. Część kancelarii, biblioteki lub kancelarii mobilizacyjnej przeznaczoną do przechowywania materiałów niejawnych oraz wykonywania pracy przez personel tych komórek organizacyjnych, odgradza się barierką albo ścianą działową z okienkiem od części przeznaczonej do wydawania i udostępniania dokumentów niejawnych lub pracy z dokumentami planowania mobilizacyjnego, operacyjnego lub gotowości bojowej.

6. W pomieszczeniach, o których mowa w ust. 1, instaluje się przeciwpożarowy system alarmowy, system sygnalizujący próby siłowego otwarcia drzwi wejściowych i okien, ruch w pomieszczeniach oraz próby napadu. Powinny być, w miarę możliwości instalowane telewizyjne systemy nadzoru do prowadzenia ciągłej obserwacji zewnętrznej drzwi wejściowych i okien w kancelariach mobilizacyjnych oraz kancelariach, w których są przechowywane materiały niejawne oznaczone klauzulą „Ściśle tajne".

7. Instalowane systemy powinny spełniać parametry określone w Normie Obronnej NO-04-A004 Obiekty Wojskowe. Systemy Alarmowe. oraz odpowiadać następującym klasom:

1) SA4 – w przypadku przechowywania dokumentów zawierających informacje niejawne oznaczone klauzulą „Ściśle tajne";

2) SA3 – w przypadku przechowywania dokumentów zawierających informacje niejawne oznaczone klauzulą „Tajne" i „Poufne".

8. Pomieszczenia kancelarii, bibliotek oraz kancelarii mobilizacyjnych zalicza się do strefy bezpieczeństwa klasy I.

9. Kancelarię oraz kancelarię mobilizacyjną wyposaża się w:

1) urządzenia do przechowywania dokumentów niejawnych:

a) szafy stalowe klasy C - do przechowywania dokumentów zawierających informacje niejawne stanowiące tajemnicę państwową, oznaczonych klauzulą „Ściśle tajne",
b) szafy stalowe klasy B - do przechowywania dokumentów zawierających informacje niejawne stanowiące tajemnicę państwową, oznaczonych klauzulą „Tajne" oraz informacje niejawne stanowiące tajemnicę służbową oznaczonych klauzulą „Poufne",
c) szafy stalowe klasy A - do przechowywania dokumentów zawierających informacje niejawne stanowiące tajemnicę służbową, oznaczonych klauzulą „Zastrzeżone";

2) regały lub meble przeznaczone do przechowywania teczek akt lub wydawnictw;

3) sprzęt kwaterunkowo – biurowy;

4) pojemniki lub worki służące do przechowywania dokumentów niejawnych przeznaczonych do zniszczenia oraz do ewakuacji materiałów;

5) urządzenia do niszczenia dokumentów na miał papierowy lub tnące na paski o maksymalnych wymiarach 1,5x25 mm.

10. Bibliotekę wyposaża się w sprzęt wyszczególniony w ust. 9 w pkt 2 – 4, a w przypadku przechowywania materiałów niejawnych oznaczonych klauzulą „Ściśle tajne" dodatkowo w szafę stalową klasy C.

11. Warunki techniczne, którym powinny odpowiadać szafy, o których mowa w ust. 9 pkt 1, określa załącznik nr 1 do zarządzenia.

12. Na drzwiach urządzeń, o których mowa w ust. 9 pkt 1, nakleja się kartę informacyjną, której wzór określa załącznik nr 2 do zarządzenia.

13. Kancelarie i biblioteki powinny być, w miarę możliwości, wyposażone w sprzęt informatyczny przystosowany do odczytu informacji niejawnych zapisanych na elektronicznych nośnikach informacji.

14. W szczególnie uzasadnionych przypadkach, uniemożliwiających spełnienie któregokolwiek warunków, o których mowa w ust. 1, zgody na zastosowanie alternatywnych środków bezpieczeństwa udziela szef właściwej służby ochrony państwa.

§ 7.
1. Kancelarie i kancelarie mobilizacyjne przechowują materiały zawierające informacje niejawne stanowiące tajemnicę państwową oraz służbową w urządzeniach do przechowywania dokumentów, o których mowa w § 6 ust. 9 pkt 1, odrębnych dla każdej klauzuli tajności, państwa i organizacji międzynarodowej, z zastrzeżeniem ust. 2 i 3.

2. Materiały, o których mowa w ust. 1, mogą być przechowywane w jednym urządzeniu do przechowywania dokumentów, pod warunkiem, że jego konstrukcja pozwala na ich fizyczne rozdzielenie i zamknięcie w odrębnych skrytkach.

3. Materiały o różnych klauzulach tajności, a także jawne mogą być przechowywane wspólnie, jeżeli wynika to z rzeczowego wykazu akt.

4. Wydawnictwa, czasopisma, dokumentacja techniczna, teczki akt oraz inne materiały o dużych rozmiarach zawierające informacje niejawne stanowiące tajemnicę państwową lub służbową, pozostające na ewidencji kancelarii lub biblioteki, przechowuje się, z zastrzeżeniem ust. 5 i 6, na regałach w pomieszczeniach magazynowych, o których mowa w § 6 ust. 3 pkt 2. Materiały o różnych klauzulach tajności powinny być od siebie fizycznie oddzielone.

5. Jeżeli kancelaria nie posiada pomieszczenia magazynowego, materiały, o których mowa w ust. 4, przechowuje w się pomieszczeniach pracy dla personelu w urządzeniach do przechowywania dokumentów, o których mowa w § 6 ust. 9 pkt 1 lub zamykanych i pieczętowanych meblach albo regałach.

6. Materiały niejawne, w pomieszczeniach służbowych nie spełniających standardów bezpieczeństwa, określonych w § 6 ust. 1, 6 i 7, a także materiały oznaczone klauzulą „Ściśle tajne" oraz dokumenty planowania mobilizacyjnego, operacyjnego i gotowości bojowej należy przechowywać wyłącznie w urządzeniach do przechowywania dokumentów niejawnych, o których mowa w § 6 ust. 9 pkt 1.

7. Zabrania się przechowywania materiałów zawierających informacje niejawne stanowiące tajemnicę państwową oraz służbową oznaczonych klauzulą „Poufne" w pomieszczeniach zlokalizowanych poza strefami bezpieczeństwa.

§ 8.
1. Sprzątanie pomieszczeń kancelarii, bibliotek oraz kancelarii mobilizacyjnych, może odbywać się wyłącznie w obecności ich etatowego personelu.

2. Na czas sprzątania, personel pomieszczeń, o których mowa w ust. 1, zabezpiecza dokumenty niejawne w sposób uniemożliwiający przypadkowe ujawnienie ich treści osobom nieupoważnionym.

§ 9.
Zabrania się wnoszenia do pomieszczeń, o których mowa w § 8 ust. 1, prywatnych i służbowych urządzeń służących do rejestracji obrazu, dźwięku, kopiowania oraz transmisji informacji.

§ 10.
1. Po zakończeniu pracy kierownicy kancelarii, bibliotek oraz kancelarii mobilizacyjnych lub wyznaczeni przez nich pracownicy, zamykają i plombują urządzenia do przechowywania dokumentów niejawnych oraz zabezpieczają pomieszczenia służbowe.

2. Zasady zdawania, przechowywania i wydawania kluczy użytku bieżącego do pomieszczeń służbowych i urządzeń, o których mowa w ust. 1, ustala kierownik jednostki organizacyjnej w planie ochrony.

3. Klucze zapasowe, kody dostępu oraz kody systemu alarmowego do pomieszczeń kancelarii i biblioteki, w tym pomieszczeń magazynowych, o których mowa w § 6 ust. 3 pkt 2, a także znajdujących się w tych pomieszczeniach urządzeń do przechowywania dokumentów, zapisane na formularzu, umieszczone w opieczętowanych i odpowiednio oznaczonych kopertach, przechowuje pełnomocnik ochrony lub wyznaczona przez niego osoba. Wzór formularza określa załącznik nr 3 do zarządzenia.

4. Klucze zapasowe, kody dostępu oraz kody systemu alarmowego do pomieszczeń kancelarii mobilizacyjnej i znajdujących się w niej urządzeń do przechowywania dokumentów przechowuje osoba wyznaczona rozkazem dziennym lub decyzją kierownika jednostki organizacyjnej, w sposób określony w ust. 3.

5. Formularze oraz koperty, o których mowa w ust. 3, oznacza się klauzulą tajności odpowiadającą klauzuli najwyżej sklasyfikowanej informacji, przechowywanej w kancelarii, bibliotece lub kancelarii mobilizacyjnej.

6. Zabrania się zapisywania przez użytkowników kodów dostępu oraz wynoszenia poza teren jednostki organizacyjnej kluczy, o których mowa w ust. 2.

7. Kody dostępu, o których mowa w ust. 3 i 4, zmienia się:

1) w urządzeniach i zamkach nowo instalowanych, a następnie w odstępach czasowych nie przekraczających 6 miesięcy;

2) po każdej naprawie lub konserwacji zamka;

3) po przekazaniu obowiązków przez osobę pełniącą służbę albo zatrudnioną w kancelarii, bibliotece i kancelarii mobilizacyjnej ;

4) w przypadku ujawnienia kodu osobie nieupoważnionej.

8. W razie utraty lub zagubienia kluczy, o których mowa w ust. 2 - 4, należy wymienić zamki.

Rozdział 4

Zasady organizacji, funkcjonowania i zabezpieczenia kancelarii tajnych na okrętach bojowych i pomocniczych jednostkach pływających Marynarki Wojennej

§ 11.

1. Kancelarię na okręcie bojowym i pomocniczej jednostce pływającej organizuje się w pomieszczeniach spełniających następujące warunki bezpieczeństwa:

1) zlokalizowanych pod pokładem głównym okrętu lub wyjątkowo w nadbudówce;

2) oddzielonych od innych pomieszczeń trwałymi ścianami (szotami) bez otworów konstrukcyjnych, z konstrukcją ścian (szotów) uniemożliwiającą przedostanie się do wewnątrz przy użyciu narzędzi ręcznych;

3) nie posiadających okien (iluminatorów), a gdy jest to niemożliwe, okna (iluminatory) powinny być nieotwieralne, wykonane ze szkła o zwiększonej odporności na włamanie (klasy od P5 do P8) i zabezpieczone w sposób uniemożliwiający wgląd z zewnątrz;

4) posiadających otwory wentylacyjne i inne otwory w ścianach (szotach), pokładach lub sufitach, jeżeli są większe niż 500 cm², zabezpieczone przed penetracją siatką stalową o średnicy oczka 10 mm albo systemem alarmowym;

5) wyposażonych w drzwi wejściowe (włazy) wykonane ze stali, zabezpieczone przed włamaniem od strony zawiasów i ryglowane na trzech pozostałych płaszczyznach, zamykane na zamki odpowiadające wymaganiom określonym w § 6 ust. 1 pkt 3.

2. Pomieszczenia kancelarii zalicza się do strefy bezpieczeństwa klasy I.

3. Pomieszczenia kancelarii powinny być chronione ogólnookrętową instalacją przeciwpożarową.

4. W kancelarii instaluje się systemy sygnalizujące próby siłowego otwarcia drzwi wejściowych (włazu), ruch w pomieszczeniach oraz system sygnalizacji napadu.

5. Instalowane systemy i urządzenia alarmowe powinny spełniać warunki, o których mowa w § 6 ust. 7.

6. Kancelarię wyposaża się w szafę stalową klasy C, wyposażoną w zamykane skrytki umożliwiające odrębne przechowywanie dokumentów o różnych klauzulach tajności oraz urządzenia, o których mowa w § 6 ust. 5 i ust. 9 pkt 5.

7. Podczas postoju w porcie, dokumenty niejawne przechowuje się w kancelarii okrętu.

8. Na okrętach, na których nie ma możliwości zorganizowania kancelarii, dokumenty niejawne przechowuje się w kabinie dowódcy okrętu, wyposażonej zgodnie z § 6 ust. 9 pkt 1.

9. Podczas pobytu okrętu na morzu, jeżeli jest to konieczne ze względu na wykonywane zadania, dowódca okrętu może zezwolić na przekazanie dokumentu niejawnego na główne stanowisko dowodzenia na zasadach określonych w § 19 ust. 10, z tym że dokument musi pozostawać pod stałą kontrolą służby wachtowej.

10. Fakt przekazania dokumentów niejawnych, o których mowa w ust. 9, podlega odnotowaniu w dzienniku zdarzeń.

Rozdział 5
Zasady rejestrowania, kompletowania i niszczenia materiałów niejawnych

§ 12.
Kancelaria przyjmuje, rejestruje, przechowuje, przekazuje i wysyła dokumenty zawierające informacje niejawne oraz prowadzi następujące urządzenia ewidencyjne:

1) „Rejestr teczek dokumentów niejawnych, dzienników i książek ewidencyjnych", zwany dalej „Rejestrem dokumentacji", którego wzór określa załącznik nr 4 do zarządzenia;

2) „Dziennik korespondencji", którego wzór określa załącznik nr 5 do zarządzenia;

3) „Książkę ewidencji wydawnictw, dokumentacji technicznej oraz materiałów filmowych", zwanej dalej „Książką ewidencji wydawnictw", której wzór określa załącznik nr 6 do zarządzenia, jeżeli w kancelarii są przechowywane i ewidencjonowane wydawnictwa, czasopisma, dokumentacja techniczna albo materiały filmowe;

4) „Książkę ewidencji pieczęci", której wzór określają odrębne przepisy;

5) „Wykaz osób upoważnionych do dostępu do informacji niejawnych", którego wzór określa załącznik nr 7 do zarządzenia;

6) „Kartotekę wydanych dokumentów", w skład której wchodzą:

a) „Rejestr wydanych dokumentów", zwany dalej „RWD", którego wzór określa załącznik nr 8 do zarządzenia,
b) „Skorowidz rejestru wydanych dokumentów", zwany dalej „Skorowidzem RWD", którego wzór określa załącznik nr 9 do zarządzenia;

7) „Wykaz przesyłek nadanych", którego wzór określają odrębne przepisy;

8) „Książkę doręczeń przesyłek miejscowych", zwaną dalej „Książką doręczeń", której wzór określa załącznik nr 10 do zarządzenia;

9) „Kartę zapoznania się z dokumentem oznaczonym klauzulą „ Ściśle tajne" / „Tajne", zwanej dalej „Kartą zapoznania się z dokumentem", której wzór określają odrębne przepisy;

10) „Metrykę elektronicznego nośnika informacji", której wzór określa załącznik nr 11 do zarządzenia;

§ 13.
1. Strony urządzeń ewidencyjnych w formie broszur numeruje się, w sposób określony w odrębnych przepisach, a na ostatniej stronie urządzenia zamieszcza się adnotację o sumarycznej ilości stron poświadczoną podpisem kierownika kancelarii i odciskiem pieczęci „Do pakietów" oraz wpisuje datę sporządzenia adnotacji, z zastrzeżeniem § 14 ust. 5.

2. W urządzeniach ewidencyjnych, o których mowa w ust. 1, z wyłączeniem urządzeń wskazanych w § 12 pkt 3 - 6, § 26 ust. 3 oraz w § 38 ust. 2 pkt 1, zaznacza się początek i koniec roku kalendarzowego, a po zakończeniu roku sporządza się adnotację informującą o pozycji zapisu, na której zakończono ewidencję, potwierdzoną podpisem kierownika kancelarii i pieczęcią „Do pakietów" oraz wpisuje datę sporządzenia adnotacji.

3. Zapisów w urządzeniach ewidencyjnych dokonuje się czarnym lub niebieskim tuszem albo atramentem.

4. Zmiany zapisów w urządzeniach ewidencyjnych nanosi się kolorem czerwonym poprzez skreślenie pierwotnego zapisu i umieszczenie obok nowego uwierzytelnionego czytelnym podpisem dokonującego zmiany w rubryce „Uwagi" urządzenia ewidencyjnego, odciskiem pieczęci „Do pakietów" oraz wpisaniem daty wprowadzenia zmiany. Zabrania się wycierania, zamazywania i zaklejania zapisów w urządzeniach ewidencyjnych.

5. Adnotacji o skróceniu albo przedłużeniu okresu ochrony dokumentu niejawnego, a także zmianie lub zniesieniu jego klauzuli tajności dokonuje się w rubryce „Uwagi" urządzenia ewidencyjnego i uwierzytelnia w sposób, określony w ust. 4.

§ 14.
1. „Rejestr dokumentacji" jest nadrzędnym urządzeniem ewidencyjnym w stosunku do innych urządzeń ewidencyjnych prowadzonych przez kancelarię.

2. W „Rejestrze dokumentacji" rejestruje się:

1) urządzenia ewidencyjne, o których mowa w § 12 pkt 2 – 4 oraz 6 lit. b;
2) teczki akt;
3) księgi rozkazów dziennych, meldunków, protokołów finansowych, materiałowych, uzbrojenia i sprzętu wojskowego, jeżeli zawierają informacje niejawne lub stanowią materiał archiwalny.

3. Każdy tom urządzenia ewidencyjnego, teczki akt lub księgi, o których mowa w ust. 2, rejestruje się pod odrębną pozycją.

4. „Rejestru dokumentacji" nie rejestruje się w żadnym urządzeniu ewidencyjnym.

5. „Rejestr dokumentacji" opatruje się adnotacją o ilości stron, poświadczoną podpisem pełnomocnika ochrony oraz pieczęcią urzędową jednostki organizacyjnej, w sposób określony w § 13 ust. 1.

6. Ewidencję dokumentów w „Rejestrze dokumentacji" prowadzi się w cyklu rocznym, rozpoczynając każdego roku kalendarzowego numerowanie od liczby „1".

7. W wykazie dokumentów na kolejny rok kalendarzowy nie umieszcza się dokumentów zaewidencjonowanych w latach poprzednich i nadal prowadzonych.

8. Numer ewidencyjny dokumentu zarejestrowanego w „Rejestrze dokumentacji" składa się ze skróconej nazwy rejestru, symbolu klauzuli tajności, pozycji zapisu w wykazie, o którym mowa w ust. 7, łamanej przez rok kalendarzowy, w którym dokument zarejestrowano (np. RTD Pf-7/2005).

§ 15.
1. W „Dzienniku korespondencji" rejestruje się dokumenty niejawne otrzymywane i wysyłane (wchodzące i wychodzące), dokumenty decyzyjne oraz materiały wytworzone na potrzeby wewnętrzne jednostki lub komórki organizacyjnej.

2. Dopuszcza się rejestrowanie w jednym „Dzienniku korespondencji" dokumentów otrzymywanych i wysyłanych.

3. W odrębnych „Dziennikach korespondencji" rejestruje się:

1) dokumenty decyzyjne wydawane przez kierownika jednostki organizacyjnej, których ewidencję prowadzi kancelaria, przy czym:

a) na poszczególne rodzaje dokumentów decyzyjnych (zarządzenia, decyzje, rozkazy) zakłada się odrębne dzienniki,
b) liczba porządkowa, pod którą wpisano dokument decyzyjny w dzienniku, poprzedzona symbolem klauzuli tajności, jest równocześnie jego numerem ewidencyjnym,
c) numerację dokumentów decyzyjnych rozpoczyna się w każdym roku kalendarzowym od liczby 1,
d) „Dziennik korespondencji" prowadzi się do całkowitego wykorzystania wszystkich kart;

2) dokumenty uzyskane od innych państw oraz organizacji międzynarodowych w ramach realizacji umów międzynarodowych.

4. Po wykorzystaniu wszystkich stron „Dziennika korespondencji", zakłada się następny tom i zachowuje ciągłość dotychczasowej numeracji.

5. Zarejestrowanie korespondencji otrzymanej polega na:

1) opatrzeniu pierwszej strony dokumentu pieczęcią wpływu oraz odciśnięciu pieczęci formularzowej na załącznikach, z zastrzeżeniem, iż pieczęci formularzowej nie używa się do załączników w formie dokumentów personalnych, dowodów materiałowo-finansowych, wydawnictw oraz dokumentów przesyłanych do akceptacji lub podpisu;

2) wpisaniu w kolejnej pozycji „Dziennika korespondencji":

a) numeru porządkowego, poprzedzonego właściwym symbolem klauzuli tajności, który jest jednocześnie numerem ewidencyjnym dokumentu,
b) danych ewidencyjnych dokumentu, nadanych przez nadawcę (numer wychodzący i data wysłania),
c) informacji o ilości stron dokumentu wraz z załącznikami,
d) informacji o ilości załączników i ich stron lub nazwy i liczby elektronicznych nośników informacji,

jeżeli załączniki stanowią elektroniczne nośniki informacji,
e) w rubryce „Uwagi", informacji o klauzuli tajności pisma przewodniego, jeżeli jest ona niższa niż klauzula najwyżej sklasyfikowanego załącznika;

3) wpisaniu na dokumencie, w odpowiednich polach odcisku pieczęci, daty zarejestrowania dokumentu, zgodnie z zapisem w „Dzienniku korespondencji" oraz danych wymienionych w pkt 2 lit. a i d.

6. Korespondencję opatrzoną adnotacją „Do rąk własnych" rejestruje się bez otwierania wewnętrznego opakowania przesyłki, poprzez:

1) wpisanie w odpowiednich rubrykach „Dziennika korespondencji" zapisów umieszczonych na opakowaniu wewnętrznym przesyłki oraz daty wpływu dokumentu;

2) zamieszczenie w rubryce „Uwagi" „Dziennika korespondencji" adnotacji „Do rąk własnych";

3) odciśnięcie na opakowaniu pieczęci wpływu i wpisaniu numeru ewidencyjnego według "Dziennika korespondencji" oraz daty wpływu przesyłki.

7. Jeżeli przesyłka opatrzona adnotacją „Do rąk własnych" zawiera kilka dokumentów, to każdy z nich rejestruje się pod odrębną pozycją „Dziennika korespondencji", a na opakowaniu wewnętrznym przesyłki umieszcza odciski pieczęci wpływu, w ilości odpowiadającej liczbie dokumentów, z wpisanymi numerami ewidencyjnymi poszczególnych materiałów.

8. Przesyłkę opatrzoną adnotacją „Do rąk własnych" przekazuje się bezpośrednio adresatowi, a w razie jego nieobecności osobie przez niego upoważnionej.

9. Przesyłkę, o której mowa w ust. 8, można zwrócić do kancelarii w stanie otwartym lub zamkniętym.

10. W przypadku, gdy przesyłka zostanie zwrócona do kancelarii w otwartym opakowaniu, podlega zarejestrowaniu na zasadach określonych w ust. 5, z tym, że zachowuje się numer ewidencyjny wpisany na opakowaniu i uzupełnia nie zapisane rubryki „Dziennika korespondencji".

11. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki opatrzonej adnotacją „Do rąk własnych" w kancelarii w stanie zamkniętym, kierownik kancelarii dokonuje czynności, o których mowa w ust. 10 przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten podlega odnotowaniu w rubryce „Uwagi" „Dziennika korespondencji".

12. Przy przyjmowaniu przesyłek do kancelarii:

1) sprawdza się:

a) prawidłowość adresu,
b) całość pieczęci i opakowania,
c) zgodność odcisków pieczęci z nazwą nadawcy,
d) zgodność numerów na opakowaniu przesyłki z numerami wyszczególnionymi w „Wykazie przesyłek wydanych", „Wykazie przesyłek nadanych" lub „Książce doręczeń";

2) w przypadku zauważenia nieprawidłowości lub podejrzeń co do zawartości przesyłki, kierownik kancelarii odmawia jej przyjęcia powiadamiając o tym pełnomocnika ochrony;

3) w przypadku stwierdzenia uszkodzenia odcisku pieczęci lub opakowania, kierownik kancelarii sporządza wraz z przewoźnikiem protokół uszkodzenia (jego wzór określają odrębne przepisy), którego jeden egzemplarz otrzymuje przewoźnik, drugi nadawca przesyłki, a trzeci pełnomocnik ochrony jednostki organizacyjnej będącej adresatem.

13. Po otwarciu przesyłki kancelaria sprawdza czy:

1) zawartość przesyłki odpowiada wyszczególnionym na kopercie wewnętrznej numerom ewidencyjnym;
2) liczba stron, załączników i stron załączników jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.

14. Stwierdzone nieprawidłowości dokumentuje się w protokole otwarcia przesyłki, którego jeden egzemplarz dołącza się do dokumentu, a drugi przesyła się do nadawcy. Fakt sporządzenia protokołu otwarcia przesyłki podlega odnotowaniu w rubryce „Uwagi" „Dziennika korespondencji".

15. Zarejestrowanie korespondencji wysyłanej odbywa się na zasadach, określonych w ust. 5, z tym, że zamiast pieczęci wpływu używa się pieczęci nagłówkowej, a w odpowiednich rubrykach „Dziennika korespondencji" wpisuje się nazwę adresata, ilość stron dokumentu wraz z załącznikami, ilość załączników oraz stron załączników pozostających w aktach lub nazwę i liczbę elektronicznych nośników informacji, jeżeli załączniki stanowią elektroniczne nośniki informacji, numer ewidencyjny według „Dziennika ewidencji wykonanych dokumentów" lub innego urządzenia ewidencyjnego oraz wykonawcę.

16. W rubryce „Uwagi" „Dziennika korespondencji" wpisuje się datę przekazania dokumentu, numer oraz pozycję zapisu w „Książce doręczeń" albo numer i pozycję zapisu w „Wykazie przesyłek nadanych", za którym dokument przekazano adresatowi lub przewoźnikowi.

17. Jeżeli w kancelarii nie pozostawia się żadnego egzemplarza wysyłanego dokumentu, w rubrykach „Dziennika korespondencji" przeznaczonych do zapisywania informacji o ilości stron dokumentu, ilości załączników oraz stron załączników – wpisuje się poziome kreski, natomiast w rubryce „Uwagi" zamieszcza adnotację o treści „tylko adresat".

18. Przed zarejestrowaniem w „Dzienniku korespondencji" dokumentu przekazanego do wysłania, kierownik kancelarii sprawdza się czy dokument:

1) został właściwie wykonany i oznaczony;

2) wytworzono w ilości egzemplarzy podanej w rozdzielniku;

3) zawiera dane określające faktyczną ilość stron, załączników i stron załączników przesyłanych do adresata oraz pozostawianych w aktach;

4) został podpisany przez osobę uprawnioną do podpisywania dokumentów.

19. W razie niespełnienia jednego z warunków, o których mowa w ust. 18, kierownik kancelarii zwraca dokument wykonawcy do poprawienia lub uzupełnienia.

20. Dokumenty niejawne sporządzone w jednostce organizacyjnej na potrzeby własne ewidencjonuje się w „Dzienniku korespondencji" jak korespondencję otrzymaną.

21. W przypadku odłączenia od pisma przewodniego jednego lub więcej załączników, w rubryce „Uwagi" „Dziennika korespondencji" zamieszcza się adnotację zawierającą jedną z następujących informacji:

1) nazwę urządzenia ewidencyjnego oraz numery pozycji, pod którymi zarejestrowano odłączone załączniki;

2) numer wychodzący według „Dziennika korespondencji", za którym załączniki odesłano do innej jednostki organizacyjnej lub komórki organizacyjnej Ministerstwa Obrony Narodowej;

3) numer i pozycję protokołu zniszczenia, albo adnotację o zniszczeniu potwierdzoną podpisami kierownika kancelarii (zastępcy kierownika lub kancelisty) i wykonawcy, w zależności od klauzuli tajności zniszczonego załącznika.

§ 16.
1. W „Książce ewidencji wydawnictw" rejestruje się dokumenty niejawne wytwarzane na potrzeby jednostki organizacyjnej lub otrzymane, które są:

1) wydawnictwami;

2) czasopismami wojskowymi;

3) materiałami szkoleniowymi i informacyjnymi;

4) dokumentacją techniczną;

5) gotowymi materiałami filmowymi.

2. Dokumenty, o których mowa w ust. 1 rejestruje się wpisując w „Książce ewidencji wydawnictw":

1) pod odrębną pozycją tytuł każdego z otrzymanych dokumentów, według kolejności ich wpływu;

2) ilość i numery egzemplarzy każdego tytułu dokumentu;

3) numer i datę faktury, asygnaty lub pisma przewodniego, za którymi dokumenty przysłano.

3. Liczba porządkowa pozycji, o której mowa w ust. 2 pkt 1, poprzedzona symbolem klauzuli tajności, jest numerem ewidencyjnym wszystkich egzemplarzy danego tytułu dokumentu.

4. Na okładce, stronie tytułowej każdego egzemplarza rejestrowanego dokumentu oraz nie zszytych z nim załącznikach odciska się pieczęć biblioteczną zawierającą nazwę kancelarii lub pieczęć „Do pakietów" oraz wpisuje numer ewidencyjny, o którym mowa w ust. 3.

5. Asygnaty, faktury i pisma przewodnie, za którymi przesłano dokumenty, wskazane w ust. 1, opatruje się numerem, pod którym zarejestrowano w „Książce ewidencji wydawnictw" pierwszy wymieniony w nich materiał.

6. Dokumentację techniczną oraz gotowe materiały filmowe, o których mowa w ust. 1 pkt 4 i 5, ewidencjonuje się w oddzielnych „Książkach ewidencji wydawnictw". W razie otrzymywania niewielu tytułów w ciągu roku kalendarzowego, ewidencję tych materiałów można prowadzić łącznie z wydawnictwami i czasopismami wojskowymi.

7. Negatywy filmów oraz pozytywy zawierające informacje niejawne ewidencjonuje się oddzielnie; w razie dodatkowego wytwarzania pozytywów, rejestruje się je pod odrębną pozycją.

§ 17.
1. Kancelaria prowadzi ewidencję pieczęci urzędowych, służbowych, kamieni, godeł i znaków do plombowania oraz pakietów z pieczęciami na czas wojny posiadanych przez jednostkę organizacyjną lub komórkę organizacyjną Ministerstwa Obrony Narodowej.

2. Wzory pieczęci stosowanych w kancelarii określa załącznik nr 12 do zarządzenia.

3. Pieczęcie, o których mowa w ust. 1, ewidencjonuje się w „Książce ewidencji pieczęci".

4. „Książkę ewidencji pieczęci" prowadzi się do wykorzystania jej wszystkich kart.

5. Kancelaria prowadzi i uaktualnia na bieżąco wykaz osób upoważnionych przez kierownika jednostki organizacyjnej lub komórki organizacyjnej Ministerstwa Obrony Narodowej do posługiwania się pieczęciami urzędowymi i służbowymi.

§ 18.
1. W „Wykazie osób upoważnionych do dostępu do informacji niejawnych" wpisuje się imiona i nazwiska wykonawców upoważnionych do dostępu do informacji niejawnych, zakres i okres ważności posiadanych przez te osoby poświadczeń lub certyfikatów bezpieczeństwa.

2. „Wykaz osób upoważnionych do dostępu do informacji niejawnych" wykonuje się w układzie alfabetycznym lub z uwzględnieniem struktury organizacyjnej jednostki organizacyjnej.

3. „Wykaz osób upoważnionych do dostępu do informacji niejawnych" rejestruje się w „RWD" kierownika kancelarii.

§ 19.
1. W „RWD" rejestruje się:

1) dokumenty służące do utrwalania informacji niejawnych:

a) zeszyty pracy, notatniki, mapy, arkusze papieru przeznaczone do wykonywania dokumentów, brudnopisów lub odręcznego wykonywania czystopisów, druki meldunków i sprawozdań, bloki szyfrogramów i telegramów,
b) kalki i taśmy maszynowe, taśmy karbonizowane (jednorazowego użytku),
c) elektroniczne nośniki informacji;

2) urządzenia ewidencyjne wymienione w § 12 pkt 5, 8 i 10, § 24 ust. 1 oraz § 38 ust. 2 pkt 2;

3) załączniki odłączone od pism przewodnich, nie podlegające ewidencji w innych urządzeniach.

2. „RWD" służy ponadto do dokumentowania faktu pobrania i zwrotu wydawanych przez kancelarię wykonawcom:

1) dokumentów niejawnych zarejestrowanych w innych urządzeniach ewidencyjnych, jeżeli:

a) rubryka urządzenia ewidencyjnego, przeznaczona do pokwitowania dokumentu, została całkowicie wykorzystana,
b) rodzaj dokumentu albo dekretacja sporządzona na nim wskazują, że będzie on udostępniany większej liczbie osób;

2) wydawnictw, dokumentacji technicznej, materiałów filmowych, map, teczek akt i innych dokumentów zarejestrowanych w urządzeniach ewidencyjnych, które nie mają rubryk przeznaczonych do kwitowania pobieranych i zwracanych dokumentów.

3. „RWD" rejestruje się w „Skorowidzu RWD":

1) imiennie dla wykonawców;
2) w kolejności zgodnej ze strukturą organizacyjną jednostki organizacyjnej;
3) według numerów ewidencyjnych lub sygnatur, jeżeli są prowadzone dla poszczególnych dokumentów albo wydawnictw.

4. Numerem ewidencyjnym karty „RWD" jest numer porządkowy, pod którym została ona zarejestrowana w „Skorowidzu RWD".

5. Numer ewidencyjny dokumentu zarejestrowanego w „RWD" składa się z nazwy urządzenia, numeru karty, o którym mowa w ust. 4, łamanego przez liczbę porządkową pozycji, pod którą wpisano do karty dokument, poprzedzoną symbolem klauzuli tajności (np. RWD 10/Pf-8).

6. W przypadkach, określonych w ust. 2, zapisy rozpoczyna się od wpisania w kolumnie 2 „RWD" numeru ewidencyjnego dokumentu lub sygnatury wydawnictwa, bez wpisywania w kolumnie 1 numeru porządkowego.

7. Na grzbietach oraz kartach bloków telegramów, brudnopisów i innych materiałów zbroszurowanych zarejestrowanych w „RWD", przeznaczonych do wyrywania stron, wpisuje się numer ewidencyjny, o którym mowa w ust. 5, łamany przez numer karty (np. RWD 10/Pf-8/1, 2, 3...). Fakt wydarcia karty kierownik kancelarii potwierdza na grzbiecie dokumentu podpisem oraz odciskiem pieczęci „Do pakietów".

8. Dokumenty zarejestrowane w „RWD", po zwróceniu ich do kancelarii, podlegają zniszczeniu lub przerejestrowaniu do „RWD" innego wykonawcy albo innego urządzenia ewidencyjnego.

9. W przypadku przerejestrowania materiału niejawnego do „RWD" innego wykonawcy lub zaewidencjonowania w innym urządzeniu ewidencyjnym, w dotychczasowej ewidencji dokonuje się adnotacji o przerejestrowaniu dokumentu z wyszczególnieniem nowego numeru ewidencyjnego.

10. „RWD" przeznaczone do rejestrowania dokumentacji służby dyżurnej zakłada się w dwóch egzemplarzach, z których jeden przechowuje się w kancelarii, a drugi stanowiący podstawę do przekazywania przez służbę materiałów niejawnych - w pomieszczeniu tej służby.

11. Po wykorzystaniu wszystkich pozycji w „RWD", dołącza się nową kartę zachowując poprzednio nadany numer i ciągłość numeracji.

§ 20.
1. Do „Wykazu przesyłek nadanych" wpisuje się przesyłki pocztowe przekazywane przewoźnikowi lub adresatowi, jeżeli są dostarczane bezpośrednio przez przedstawiciela nadawcy albo adresata.

2. „Wykazów przesyłek nadanych" nie ewidencjonuje się w żadnym urządzeniu ewidencyjnym. Wykazom nadaje się kolejne numery, zaczynając numerowanie w każdym roku kalendarzowym od cyfry „1".

3. Przewoźnik potwierdza przyjęcie przesyłek do przekazania na dwóch egzemplarzach wykazu, o którym mowa w ust. 1, zapisem liczbowym i słownym o ilości przyjętych przesyłek oraz uwierzytelnia podpisem i odciskiem pieczęci „Do pakietów", przy czym jeden egzemplarz wykazu pozostaje w kancelarii nadawcy, a drugi jest przeznaczony dla przewoźnika.

4. W przypadku przekazywania informacji niejawnych stanowiących tajemnicę państwową, dodatkowy trzeci egzemplarz „Wykazu przesyłek nadanych", przesyła się wraz z przesyłką adresatowi, który potwierdza na nim odbiór przesyłki i odsyła do nadawcy.

5. W przypadku przekazania przez kancelarię materiałów niejawnych bezpośrednio upoważnionemu przedstawicielowi adresata, potwierdza on odbiór przesyłki podpisem i odciskiem pieczęci „Do pakietów" na drugim egzemplarzu „Wykazu przesyłek nadanych", przeznaczonym dla kancelarii nadawcy.

6. Jeżeli przesyłki są doręczane adresatowi przez upoważnionego przedstawiciela nadawcy, kierownik kancelarii sporządza „Wykaz przesyłek nadanych" w trzech egzemplarzach, z których:

1) pierwszy, po pokwitowaniu przyjęcia przesyłki przez kierownika kancelarii adresata, osoba doręczająca zwraca do kancelarii nadawcy;

2) drugi, osoba doręczająca przekazuje wraz z przesyłką kierownikowi kancelarii adresata;

3) trzeci, zawierający pokwitowanie odbioru przesyłki przez osobę doręczającą, przechowuje się w kancelarii nadawcy i niszczy bezpośrednio po otrzymaniu egzemplarza, o którym mowa w pkt 1.

7. Kierownik kancelarii potwierdza przyjęcie przesyłek od przewoźnika na dwóch egzemplarzach „Wykazu przesyłek wydanych", przy czym jeden egzemplarz wykazu pozostaje u przewoźnika, a drugi jest przeznaczony dla kancelarii.

8. Kierownik kancelarii wpisuje w rubryce „Uwagi" wykazu, o którym mowa w ust. 7, numery ewidencyjne pod jakimi poszczególne przesyłki zostały zarejestrowane w „Dzienniku korespondencji".

9. Kancelaria przechowuje wykazy, o których mowa w ust. 1 i 7, w specjalnie przeznaczonych do tego celu segregatorach.

10. Szczegółowe zasady stosowania „Wykazu przesyłek nadanych" oraz „Wykazu przesyłek wydanych" określają odrębne przepisy.

§ 21.
1. W „Książce doręczeń" rejestruje się fakt doręczenia dokumentów do kancelarii adresata, stacjonującego w tym samym kompleksie, bezpośrednio przez personel kancelarii nadawcy.

2. Kierownik kancelarii adresata potwierdza odbiór materiałów niejawnych podpisem w odpowiedniej rubryce „Książki doręczeń", uwierzytelnionym odciskiem pieczęci „Do pakietów".

3. „Książkę doręczeń" wykorzystuje się do czasu zapisania w niej wszystkich pozycji.

4. „Książkę doręczeń" ewidencjonuje się w „RWD" kierownika kancelarii.

§ 22.
1. „Kartę zapoznania się z dokumentem" zakłada się i dołącza do każdego dokumentu niejawnego zawierającego informację stanowiącą tajemnicę państwową, z chwilą jego zarejestrowania w „Dzienniku korespondencji" lub innym urządzeniu ewidencyjnym.

2. W „Karcie zapoznania się z dokumentem" dokumentuje się każdorazowe udostępnienie wykonawcom dokumentów, o których mowa w ust. 1.

3. Fakt zapoznania się z dokumentem niejawnym wchodzącym w skład zbioru dokumentów, rejestruje się w „Karcie zapoznania się z dokumentem" wystawionej dla całego zbioru.

4. Przepis ust. 3 stosuje się odpowiednio do teczek akt.

5. „Kart zapoznania się z dokumentem" nie zakłada się dla urządzeń ewidencyjnych, notatników oraz brudnopisów dokumentów, o których mowa w ust. 1.

6. „Kartę zapoznania się z dokumentem" przesyła się lub archiwizuje wraz z dokumentem, którego dotyczy albo z protokołem jego zniszczenia.

§ 23.
1. W „Metryce elektronicznego nośnika informacji", zwanej dalej „metryką", rejestruje się dane dotyczące informacji niejawnych zapisanych na nośniku.

2. Metrykę zakłada kancelaria, która zarejestrowała nośnik wykonawcy.

3. Metryki nie zakłada się dla nośników przeznaczonych do użytku bieżącego wykonawców.

4. Przed zwróceniem nośnika do kancelarii wykonawca uzupełnia w metryce zapisy dotyczące ilości zapisanych na nośniku folderów i plików oraz ilości zajętego miejsca.

5. Metrykę przekazuje się lub przesyła wraz z nośnikiem, którego dotyczy.

§ 24.
1. Wykonawcy techniczni, oficerowie bezpieczeństwa obszaru terminala systemu PL_NS NOAN oraz osoby wyznaczone przez kierownika jednostki organizacyjnej albo komórki organizacyjnej Ministerstwa Obrony Narodowej wytwarzającej dokumenty niejawne prowadzą „Dziennik ewidencji wykonanych dokumentów", którego wzór zawiera załącznik nr 13.

2. „Dziennik ewidencji wykonanych dokumentów" służy do rejestrowania dokumentów zawierających informacje niejawne, wytworzonych w poszczególnych komórkach organizacyjnych jednostki organizacyjnej, w szczególności techniką maszynopisania, komputerową, kreślenia, powielania lub naświetlania.

3. Dla każdej techniki wytwarzania dokumentów prowadzi się odrębny "Dziennik ewidencji wykonanych dokumentów".

4. „Dziennik ewidencji wykonanych dokumentów" rejestruje się w „RWD" osób, o których mowa w ust. 1.

5. Dokumenty zawierające informacje niejawne stanowiące tajemnicę państwową lub służbową oznaczoną klauzulą „Poufne", przeznaczone dla adresatów zagranicznych oraz dokumenty wytworzone w systemie PL_NS NOAN rejestruje się w „Dziennikach ewidencji wykonanych dokumentów", ujętych w ewidencji kancelarii tajnej – zagranicznej lub punktu obsługi dokumentów zagranicznych.

6. Zarejestrowanie dokumentu w „Dzienniku ewidencji wykonanych dokumentów" polega na wpisaniu pod kolejną pozycją dziennika nazwy dokumentu, nazwiska wykonawcy i wykonawcy technicznego, ilości egzemplarzy oraz ilości stron, przy czym liczba porządkowa pozycji, poprzedzona numerem ewidencyjnym dziennika i symbolem klauzuli tajności, łamana przez dwie ostatnie cyfry roku kalendarzowego, w którym wytworzono dokument jest jego numerem ewidencyjnym (np. DEWD 17/Z-6/Z-25/05.

7. Dodatkowo wytworzony dokument zawierający informacje niejawne, w szczególności odpis, kopię lub reprodukcję rejestruje się każdorazowo pod odrębną pozycją „Dziennika ewidencji wykonanych dokumentów". Wykonanie kopii, odpisu lub reprodukcji wymaga pisemnej zgody kierownika jednostki organizacyjnej (komórki organizacyjnej Ministerstwa Obrony Narodowej) dysponującej dokumentem lub upoważnionej przez niego osoby, zamieszczonej na tym dokumencie.

8. „Dziennik ewidencji wykonanych dokumentów" prowadzi się do całkowitego wykorzystania jego kart, rozpoczynając każdego roku kalendarzowego numerowanie od cyfry „1".

9. Kierownik kancelarii co najmniej raz w miesiącu rozlicza „Dziennik ewidencji wykonanych dokumentów" poprzez wpisanie w odpowiedniej rubryce tego dziennika numerów pod jakimi wytworzone dokumenty zarejestrowano w urządzeniach ewidencyjnych kancelarii.

§ 25.
1. Biblioteka przyjmuje, rejestruje, przechowuje, udostępnia i przekazuje wydawnictwa, czasopisma wojskowe, dokumentację techniczną, a także gotowe materiały filmowe zawierające informacje niejawne oraz prowadzi następujące urządzenia ewidencyjne:

1) „Książkę ewidencji wydawnictw";

2) „Wykaz osób upoważnionych do dostępu do informacji niejawnych";

3) „Kartotekę", z zastrzeżeniem ust. 2, w skład której wchodzą:

a) „Skorowidz kart czytelnika", zwany dalej „Skorowidzem", którego wzór określa załącznik nr 14 do zarządzenia,
b) „Karta czytelnika", której wzór określa załącznik nr 15 do zarządzenia,
c) „Karta wydawnictwa", której wzór określa załącznik nr 16 do zarządzenia;

4) „Kartę zapoznania się z dokumentem".

2. Urządzeń ewidencyjnych, o których mowa w ust. 1 pkt 3 nie prowadzą biblioteki wyposażone w systemy informatycznej obsługi biblioteki.

3. Urządzenia ewidencyjne wyszczególnione ust. 1 pkt 1 oraz pkt 3 lit. a, rejestruje kancelaria jednostki organizacyjnej w „Rejestrze dokumentacji", natomiast urządzenie wymienione w pkt 2 ewidencjonuje się w „RWD" kierownika biblioteki .

4. „Kartę czytelnika" rejestruje się w „Skorowidzu" zgodnie z układem alfabetycznym.

5. Numerem ewidencyjnym karty czytelnika jest numer porządkowy, pod którym karta została zaewidencjonowana w „Skorowidzu".

6. „Karta czytelnika" służy do dokumentowania faktu pobrania i zwrotu wydawanych przez bibliotekę wykonawcom materiałów niejawnych, o których mowa w ust. 1.

7. W „Karcie wydawnictwa" dokumentuje się obieg materiałów niejawnych wydawanych przez bibliotekę. Karta pozwala na ustalenie ilości i numerów egzemplarzy wydawnictw pozostających w bibliotece oraz wypożyczonych, a także nazwisk osób, które je pobrały.

8. W bibliotekach, o których mowa w ust. 2, obieg materiałów niejawnych dokumentuje system informatycznej obsługi biblioteki. System ten powinien zapewniać możliwość przeglądania kont czytelników oraz kartotek egzemplarzy, uwzględniających historię wypożyczeń. Operacje pobrania i zwrotu materiałów niejawnych dokumentuje się w postaci wydruków pokwitowań (rewersów).

9. Pokwitowania (rewersy), o których mowa w ust. 8, powinny zawierać:

1) nazwę operacji (wypożyczenie lub zwrot);

2) datę przeprowadzenia operacji;

3) numer biblioteczny, numer egzemplarza oraz nazwę lub tytuł materiału niejawnego;

4) nazwisko i imię osoby, która materiał pobrała lub zdała;

5) miejsce na podpis wykonawcy lub pracownika biblioteki.

10. Do urządzeń ewidencyjnych, o których mowa w ust 1 pkt 1, 2 i 4 przepisy § 13 ust 3 i 4 oraz § 16, 18 i 22 stosuje się odpowiednio.

§ 26.
1. Kancelaria mobilizacyjna przyjmuje, rejestruje, przechowuje i udostępnia dokumenty planowania mobilizacyjnego, operacyjnego lub gotowości bojowej oraz prowadzi następujące urządzenia ewidencyjne:

1) „Dziennik korespondencji";

2) „Wykaz osób upoważnionych do dostępu do informacji niejawnych";

3) „Kartę zapoznania się z dokumentem";

4) „Dziennik ewidencji wykonanych dokumentów".

2. Urządzenie ewidencyjne wymienione w ust. 1 pkt 1 rejestruje się w „Rejestrze dokumentacji" kancelarii jednostki organizacyjnej, natomiast urządzenia wymienione w pkt 2 i 4 ewidencjonuje się w „RWD" kierownika kancelarii mobilizacyjnej.

3. „Dziennik korespondencji" przeznaczony do rejestrowania dokumentów planowania mobilizacyjnego, operacyjnego i gotowości bojowej prowadzi się zachowując ciągłość zapisów przez okres obowiązywania planu mobilizacyjnego.

4. Jeżeli dokumenty, o których mowa w ust. 3, zostały wykonane w ilości większej niż jeden egzemplarz, to każdy z tych egzemplarzy, a także załączniki do nich rejestruje się pod odrębną pozycją dziennika.

5. Dokumenty planowania mobilizacyjnego, operacyjnego i gotowości bojowej przekazuje się poza jednostkę organizacyjną wyłącznie za pośrednictwem kancelarii.

6. Do urządzeń ewidencyjnych, o których mowa w ust. 1 przepisy § 13 ust. 3 i 4 oraz §15, 18, 22 i 24 stosuje się odpowiednio.

§ 27.

1. Kancelaria oraz biblioteka przekazują materiały zawierające informacje niejawne oznaczone klauzulą „Poufne" lub stanowiące tajemnicę państwową wyłącznie wykonawcom posiadającym stosowne poświadczenia bezpieczeństwa albo pisemną zgodę osoby wymienionej w art. 49 ustawy, których pomieszczenia są zlokalizowane w strefie bezpieczeństwa i wyposażone w urządzenia do przechowywania dokumentów, o których mowa w § 6 ust. 9 pkt 1, za pokwitowaniem w „Dzienniku korespondencji" lub innym urządzeniu ewidencyjnym, z zastrzeżeniem ust. 3.

2. Kierownik kancelarii udostępnia lub przekazuje materiały niejawne osobom, o których mowa w ust. 1 na podstawie zamieszczonej na materiale dekretacji kierownika jednostki organizacyjnej albo osoby upoważnionej przez kierownika jednostki organizacyjnej do dekretowania dokumentów.

3. Urządzenia do przechowywania dokumentów, o których mowa w § 6 ust. 9 pkt 1, mogą być wykorzystywane wyłącznie przez jednego wykonawcę, chyba że konstrukcja urządzenia pozwala na fizyczne oddzielenie posiadanych przez wykonawców dokumentów i zamknięcie ich w odrębnych skrytkach.

4. Za zgodą kierownika jednostki organizacyjnej, zezwala się na przekazanie materiałów niejawnych oznaczonych klauzulą „Poufne" lub „Tajne" wykonawcom nie posiadającym urządzeń, o których mowa w § 6 ust.9 pkt 1, jeżeli spełniają oni pozostałe warunki określone w ust. 1.

5. Wykonawca, któremu udostępniono materiały niejawne na zasadach określonych w ust. 4, ma obowiązek zachowania środków bezpieczeństwa uniemożliwiających dostęp do tych materiałów przez osoby nieuprawnione oraz zwrócić je do kancelarii lub biblioteki przed zakończeniem dnia pracy.

6. Wykonawcom, których pomieszczenia służbowe znajdują się w strefie administracyjnej, materiały niejawne oznaczone klauzulą „Poufne" oraz stanowiące tajemnicę państwową udostępnia się w pomieszczeniu lub części kancelarii albo biblioteki przeznaczonym do zapoznawania się z materiałami niejawnymi, o którym mowa w § 6 ust. 3 pkt 3.

7. Dokumenty planowania mobilizacyjnego, operacyjnego i gotowości bojowej udostępnia się wyłącznie w pomieszczeniu kancelarii mobilizacyjnej, o którym mowa w § 6 ust. 3 pkt 3.

8. Wykonawcy przechowujący materiały niejawne w pomieszczeniach służbowych, udający się na urlopy, szkolenia oraz w podróże służbowe mają obowiązek zdania ich do kancelarii lub przekazania osobie zastępującej, jeżeli czas nieobecności
osoby w jednostce organizacyjnej wyniesie więcej niż dwa tygodnie.

9. Przesyłki opatrzone adnotacją „Pilne" kancelaria przekazuje adresatom bezzwłocznie wpisując w rubryce „Uwagi" urządzenia ewidencyjnego datę oraz godzinę doręczenia.

10. Udostępnianie wykonawcom materiałów niejawnych oznaczonych klauzulą „Zastrzeżone" odbywa się na zasadach określonych przez kierownika jednostki organizacyjnej.

11. Przekazane przez kancelarię lub bibliotekę materiały niejawne wykonawca ewidencjonuje w prowadzonym przez siebie „Dzienniku wykonawcy", którego wzór zawiera załącznik nr 17 do zarządzenia.

12. Przekazywanie dokumentów niejawnych poza jednostkę organizacyjną odbywa się wyłącznie przez kancelarię i za zgodą kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej.

13. Zezwala się na czasowe przekazywanie dokumentów niejawnych, zawierających informacje stanowiące tajemnicę służbową, pomiędzy wykonawcami z tej samej jednostki organizacyjnej, za pokwitowaniem w „Dzienniku wykonawcy", o którym mowa w ust. 11.

§ 28
1. Dokumenty ostatecznie załatwionych spraw, zawierające informacje niejawne, otrzymane i wytworzone w jednostce organizacyjnej podlegają:

1) skompletowaniu w teczki akt, jeżeli stanowią materiały archiwalne lub posiadają wartość praktyczną dla jednostki organizacyjnej, w sposób określony w zarządzeniu Nr 3/MON Ministra Obrony Narodowej z dnia 2 lutego 2005 r. w sprawie zasad i trybu postępowania z materiałami archiwalnymi i inną dokumentacją w resorcie obrony narodowej (Dz. Urz. MON Nr 2, poz. 4);

2) zwrotowi do nadawcy, jeżeli określił on taki sposób postępowania z przesłanymi materiałami;

3) bieżącemu niszczeniu.

2. Dokumenty oraz zbiory dokumentów dotyczące spraw ostatecznie załatwionych, przechowuje się w kancelarii przez okres nie dłuższy niż 5 lat, a po upływie tego czasu przekazuje się do archiwum zakładowego lub składnicy akt.

3. W jednostkach organizacyjnych nie posiadających archiwum zakładowego lub składnicy akt, materiały, o których mowa w ust. 2, przechowuje się w kancelarii tajnej lub innym pomieszczeniu zapewniającym ich ochronę odpowiednio do przyznanej klauzuli tajności, przez okres oznaczony w rzeczowym wykazie akt.

§ 29.
1. Dokumenty niejawne nie będące materiałami archiwalnymi i nie posiadające wartości praktycznej dla jednostki organizacyjnej, które nie zostały wszyte do teczek akt, nieaktualne wydawnictwa, dokumentacja techniczna, czasopisma wojskowe oraz elektroniczne nośniki informacji podlegają niszczeniu.

2. Dokumenty, o których mowa w ust. 1, zakwalifikowane do zniszczenia, niszczą odpowiednio:

1) co najmniej trzyosobowa komisja, powoływana okresowo przez kierownika jednostki organizacyjnej lub komisja dokonująca kontroli rocznej stanu ochrony informacji niejawnych;

2) wykonawca i odpowiednio kierownik kancelarii, zastępca kierownika kancelarii lub kancelista;

3) wykonawca i wykonawca techniczny.

3. Komisyjnemu niszczeniu podlegają:

1) dokumenty zawierające informacje niejawne stanowiące tajemnicę państwową;

2) wydawnictwa, czasopisma wojskowe, dokumentacja techniczna oraz materiały filmowe zawierające informacje niejawne stanowiące tajemnicę państwową lub służbową;

3) dokumenty planowania mobilizacyjnego i gotowości bojowej zawierające informacje stanowiące tajemnicę państwową lub służbową.

4. Niszczenie dokumentów zawierających informacje niejawne stanowiące tajemnicę służbową, nie wymienionych w ust. 3, odbywa się w obecności osób, o których mowa w ust.2 pkt 2 lub 3, a fakt zniszczenia dokumentuje się w rubryce „Uwagi" urządzenia ewidencyjnego adnotacją o treści: „Zniszczono dnia..", potwierdzoną wpisaniem daty i czytelnymi podpisami osób niszczących dokumenty.

5. Komisyjne zniszczenie dokumentów dokumentuje się w protokole zniszczenia, którego wzór określa załącznik nr 18 do zarządzenia.

6. Protokół zniszczenia stanowi dla kierownika kancelarii, biblioteki lub kierownika kancelarii mobilizacyjnej podstawę do zdjęcia z ewidencji wyszczególnionych w nim dokumentów, poprzez naniesienie w rubryce „Uwagi" odpowiedniego urządzenia ewidencyjnego adnotacji o treści: „protokół zniszczenia nr wch. ... z dnia.., poz. nr .." oraz uwierzytelnienie wpisu wpisaniem daty, podpisem i odciskiem pieczęci „Do pakietów".

§ 30.
Dokument uważa się za ostatecznie zniszczony, jeżeli został pocięty na paski o wymiarach maksymalnych 1,5x25 mm, zmielony na miał papierowy, spalony w piecu albo rozpuszczony w kadziach z ługiem w zakładach papierniczych pod nadzorem osób, o których mowa w § 29 ust. 2.

§ 31.
Sposoby i procedury niszczenia elektronicznych nośników informacji oraz informacji utrwalonych na tych nośnikach określają odrębne przepisy.

§ 32.
1. Jeżeli w jednostce organizacyjnej, z przyczyn technicznych, ostateczne zniszczenie materiałów niejawnych, o których mowa w § 29 ust. 3 i 4, jest niemożliwe, niszczy się je wstępnie przez kilkakrotne przedarcie, przy czym wstępnego zniszczenia dokonuje odpowiednio kierownik kancelarii, biblioteki lub kierownik kancelarii mobilizacyjnej, pod nadzorem członków komisji albo wykonawcy.

2. Wstępnie zniszczone dokumenty, do chwili ich przewiezienia do wytypowanej jednostki organizacyjnej lub wyspecjalizowanego zakładu, w celu ostatecznego zniszczenia, przechowuje się w workach lub pojemnikach odpowiednio w : kancelarii, bibliotece, kancelarii mobilizacyjnej albo innym pomieszczeniu jednostki organizacyjnej zabezpieczonym jak kancelaria. Worki i pojemniki, w których przechowywane są materiały niejawne, o których mowa w § 29 ust. 3, podlegają oplombowaniu przez przewodniczącego komisji.

3. Osoby, o których mowa w ust. 1, nadzorujące niszczenie dokumentów niejawnych, zapewniają zachowanie warunków uniemożliwiających wgląd do nich osobom nieupoważnionym.

4. Zabrania się wywożenia częściowo zniszczonych dokumentów niejawnych oraz kopert i innych opakowań, w których otrzymano dokumenty niejawne, na wysypiska śmieci.

§ 33.
1. W razie likwidacji (rozformowania) jednostki organizacyjnej przeprowadza się postępowanie likwidacyjne dokumentów niejawnych poprzez:

1) wyznaczenie komisji, w celu sprawdzenia stanu faktycznego dokumentów niejawnych użytku bieżącego, teczek akt, wydawnictw oraz pieczęci i stempli posiadanych przez jednostkę organizacyjną;

2) przekazanie materiałów archiwalnych i pozostałych dokumentów niejawnych w trybie określonym w zarządzeniu, o którym mowa w § 28 ust. 1 pkt 1;

3) zwrot wydawnictw wojskowych, wojskowych map topograficznych oraz pieczęci i stempli do jednostki organizacyjnej, z której zostały przysłane.

2. Kierownik kancelarii likwidowanej jednostki organizacyjnej może być przeniesiony na inne stanowisko służbowe z chwilą całkowitego rozliczenia i przekazania dokumentów niejawnych pozostających na ewidencji jednostki organizacyjnej.

Rozdział 6
Organizacja pracy kancelarii tajnych, ich ochrona oraz obieg dokumentów podczas ćwiczeń, wojny, a także w czasie realizacji zadań w misjach organizacji międzynarodowych

§ 34.
1. Środki ochrony fizycznej, określone w rozdziale 3, stosuje się również w czasie ćwiczeń oraz podczas realizacji zadań w misjach międzynarodowych, o ile przepisy niniejszego rozdziału nie stanowią inaczej.

2. Kancelaria prowadzi, zgodnie z decyzją kierownika jednostki organizacyjnej, i na bieżąco uaktualnia, wykaz dokumentów zawierających informacje niejawne, przeznaczonych do zabrania w razie ogłoszenia alarmu bojowego, przy czym wykaz ten powinien zawierać wyłącznie dokumenty niezbędne do prowadzenia działań bojowych lub do przeprowadzenia ćwiczenia.

§ 35.
Kierownik jednostki organizacyjnej zapewnia niezbędne siły i środki do przewozu wyposażenia kancelarii i jej dokumentacji podczas ćwiczeń lub w warunkach bojowych.

§ 36.
1. W jednostce organizacyjnej na czas ćwiczeń organizuje się kancelarię ćwiczebną.

2. Kierownik jednostki organizacyjnej określa w rozkazie dziennym rejon rozmieszczenia kancelarii ćwiczebnej oraz wyznacza:

1) kierownika kancelarii ćwiczebnej, spośród personelu kancelarii;

2) kancelistów.

3. Liczba kancelistów w kancelarii ćwiczebnej powinna zapewnić ciągłość pracy kancelarii.

4. Na kancelistę można wyznaczyć żołnierza rezerwy, który spełnia warunki określone w § 3 ust. 9.

§ 37.
1. Kancelarię ćwiczebną organizuje się:

1) na bazie etatowej kancelarii - jeżeli ćwiczenia odbywają się w rejonie stałego zakwaterowania jednostki organizacyjnej;

2) w oddzielnych samochodach, budowlach, schronach lub kontenerach, rozmieszczonych w rejonie stanowiska dowodzenia, jak najbliżej „Centrum Dowodzenia" - jeżeli ćwiczenia odbywają się w warunkach polowych, przy czym:

a) obszar wokół kancelarii powinien być ogrodzony i posiadać nie więcej niż jedno strzeżone wejście,
b) w kancelarii przez cały czas powinien przebywać personel,
c) materiały niejawne powinny być przechowywane w szafach lub skrzyniach metalowych,
d) kancelaria powinna mieć zapewnioną całodobową ochronę na czas ćwiczeń.

2. Zasady rozmieszczania i zabezpieczenia kancelarii, o których mowa w ust. 1, stosuje się odpowiednio dla kancelarii wojennych.

§ 38.
1. Kancelaria ćwiczebna rejestruje dokumenty niejawne na zasadach określonych w rozdziale 5 w specjalnie założonych na czas ćwiczeń oddzielnych urządzeniach ewidencyjnych wymienionych w § 12 pkt 2, 5 – 10 oraz § 24 ust.1, z tym, że na dokumentach ćwiczebnych przed klauzulą tajności umieszcza się kryptonim ćwiczenia lub jeżeli ćwiczenie takiego kryptonimu nie posiada, wyraz „ĆWICZEBNE".

2. Urządzania ewidencyjne kancelarii ćwiczebnej rejestruje się odpowiednio:

1) „Dziennik korespondencji" – w „Rejestrze dokumentacji" etatowej kancelarii jednostki organizacyjnej;

2) „Skorowidz rejestrów", „Dziennik ewidencji wykonanych dokumentów" oraz „Książkę doręczeń" – w oddzielnym „RWD" kancelarii etatowej, stanowiącym rejestr urządzeń ewidencyjnych kancelarii ćwiczebnej.

3. Urządzenia, o których mowa w ust. 2:

1) wykorzystuje się w kolejnych ćwiczeniach, aż do całkowitego zapisania wszystkich stron;

2) wypełnia się zapisami ewidencyjnymi od nowa dla każdego ćwiczenia, rozpoczynając zapis od cyfry „1', po wpisaniu kryptonimu lub nazwy ćwiczenia.

§ 39.
Po zakończeniu ćwiczeń kierownik kancelarii ćwiczebnej:

1) przed opuszczeniem rejonu ćwiczenia sprawdza zgodność stanu faktycznego dokumentów i materiałów niejawnych ze stanem ewidencyjnym wykazanym w urządzeniach ewidencyjnych kancelarii ćwiczebnej oraz składa meldunek kierownikowi ćwiczenia o rezultacie czynności sprawdzających;

2) po powrocie do rejonu stałego zakwaterowania jednostki organizacyjnej, nie później jednak niż w ciągu miesiąca od dnia zakończenia ćwiczenia:

a) wszywa do odrębnych teczek akt, zgodnie z rzeczowym wykazem akt, dokumenty otrzymane i wytworzone w czasie ćwiczeń, stanowiące wartość archiwalną lub szkoleniową,
b) wydziela, w porozumieniu z kierownikami komórek organizacyjnych, dokumenty przeznaczone do

zniszczenia, nie przedstawiające wartości archiwalnej ani szkoleniowej,
c) dokonuje adnotacji w urządzeniach ewidencyjnych kancelarii ćwiczebnej o wszyciu dokumentów do teczek akt lub ich zniszczeniu,

d) rozlicza się z dokumentów, urządzeń ewidencyjnych oraz pieczęci zabranych na ćwiczenia.

§ 40.
1. Przygotowanie kancelarii do działania na czas wojny podejmuje kierownik kancelarii zgodnie z decyzją kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej, a w szczególności:

1) w okresie pokoju:

a) kompletuje w skrzyniach metalowych dokumentację, urządzenia ewidencyjne, materiały pomocnicze, przewidziane do zabrania przez kancelarię po ogłoszeniu wyższych stanów gotowości bojowej,
b) aktualizuje zapisy ewidencyjne dotyczące dokumentacji, o której mowa w lit. a, w zakresie zmian w tej dokumentacji, wprowadzonych przez kierowników właściwych komórek pozostających w strukturach jednostek organizacyjnych,
c) prowadzi ewidencję materiałów zawierających informacje niejawne, wypożyczonych z kancelarii, a ujętych w wykazie, o którym mowa w § 34 ust. 2,
d) określa zadania realizowane przez personel kancelarii po ogłoszeniu wyższych stanów gotowości bojowej oraz podczas działania kancelarii w warunkach bojowych;

2) w czasie osiągania wyższych stanów gotowości bojowej:

a) zapewnia sprawne załadowanie na przydzielone środki transportu skrzyń z materiałami, o których mowa w pkt 1 lit. a, oraz sprzętu umożliwiającego natychmiastowe rozwinięcie i funkcjonowanie kancelarii wojennej,
b) zamyka i opieczętowuje urządzenia do przechowywania dokumentów, o których mowa w § 6 ust. 9 pkt 1 i pomieszczenia kancelarii, przekazuje służbie dyżurnej klucze oraz wykaz zabieranych dokumentów niejawnych i urządzeń ewidencyjnych,
c) zapewnia rozwinięcie oraz przygotowanie kancelarii wojennej do pracy w wyznaczonym rejonie.

2. Przepisu ust. 1 pkt 2 lit. a i b nie stosuje się, jeżeli jednostka organizacyjna nie opuszcza miejsca stałego zakwaterowania.

3. Liczbę kancelarii wojennych oraz ich wewnętrzną strukturę określają etaty czasu „W" poszczególnych jednostek organizacyjnych.

4. Kancelarię jednostki organizacyjnej biorącej udział w misji organizacji międzynarodowej organizuje się na zasadach obowiązujących dla kancelarii wojennej.

§ 41.
1. Kancelaria wojenna jednostki organizacyjnej rejestruje dokumenty zawierające informacje niejawne na zasadach określonych w rozdziale 5, w urządzeniach ewidencyjnych wymienionych w § 12 pkt 1, 2 i 4 – 10 oraz § 24 ust. 1.

2. Kancelaria wojenna oprócz urządzeń ewidencyjnych, o których mowa w ust. 1, może prowadzić inne urządzenia określone:

1) w przepisach obowiązujących na czas wojny;

2) przez kierownika jednostki organizacyjnej;

3) przez dowódcę międzynarodowych sił biorących udział w misji organizacji międzynarodowej.

3. Kierownik kancelarii wojennej wykonuje czynności zapewniające:

1) pełną ewidencję stanu dokumentów i innych materiałów wytworzonych, otrzymanych, przekazanych i utraconych przez jednostkę organizacyjną oraz ich obiegu;

2) odtworzenie stanu faktycznego dokumentów znajdujących się w jednostce organizacyjnej.

§ 42.
1. Kancelaria wojenna przesyła wojskowe przesyłki pocztowe za pośrednictwem poczty polowej.

2. Kancelaria jednostki organizacyjnej biorąca udział w misji organizacji międzynarodowej przesyła wojskowe przesyłki pocztowe:

1) do kraju – za pośrednictwem właściwej komórki organizacyjnej Ministerstwa Spraw Zagranicznych lub kurierów;

2) pomiędzy jednostkami międzynarodowymi - za pośrednictwem poczty zorganizowanej przez dowódcę sił międzynarodowych biorących udział w misji.

§ 43.
1. Akta wytworzone i zdobyte w czasie działań bojowych kompletuje się na zasadach określonych w przepisach, o których mowa w § 28 ust. 1 pkt 1.

2. Kierownik kancelarii wojennej niszczy wyłącznie brudnopisy dokumentów, z zastrzeżeniem ust. 3.

3. W razie groźby opanowania kancelarii wojennej przez nieprzyjaciela kierownik kancelarii, na rozkaz kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej, niszczy za pomocą środków szybko niszczących dokumenty niejawne, przy czym w pierwszej kolejności należy niszczyć dokumenty planowania operacyjnego, dowodzenia, materiały kryptograficzne oraz inne materiały zawierające informacje niejawne oznaczone klauzulą „Ściśle tajne".

4. W sytuacjach zagrożenia, gdy kontakt z osobami, o których mowa w ust. 3, jest niemożliwy, decyzję o zniszczeniu dokumentów podejmuje kierownik kancelarii.

Rozdział 7
Postanowienia końcowe

§ 44.
1. Pomieszczenia kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych podlegają certyfikacji na zasadach określonych w odrębnych przepisach.

2. Pomieszczenia kancelarii, bibliotek i kancelarii mobilizacyjnych należy dostosować do wymogów określonych w zarządzeniu, w terminie 3 lat od dnia jego wejścia w życie.

3. Do czasu wyposażenia jednostek organizacyjnych w urządzenia do przechowywania dokumentów spełniających wymagania techniczne, o których mowa w § 6 ust. 9 pkt 1, dopuszcza się przechowywanie dokumentów zawierających informacje niejawne stanowiące tajemnicę służbową w sejfach i szafach stalowych starego typu, nie dłużej jednak niż do dnia 31 grudnia 2008 r.

§ 45.
Traci moc zarządzenie Nr 49/ MON Ministra Obrony Narodowej z dnia 7 sierpnia 2002 r. w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 15, poz. 149 z późn. zm.).

§ 46.
Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

ZAŁĄCZNIKI

Załącznik nr 1 - klasyfikacja i wymagania techniczne urządzeń do przechowywania dokumentów niejawnych

Załącznik nr 1

KLASYFIKACJA I WYMAGANIA TECHNICZNE URZĄDZEŃ DO PRZECHOWYWANIA DOKUMENTÓW NIEJAWNYCH

I. SZAFA STALOWA KLASY C.

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne powinny być wykonane ze stali konstrukcyjnej wyższej jakości, o grubości minimum 5 mm, a w przypadku konstrukcji wielopłaszczowej, grubość płaszcza zewnętrznego winna wynosić minimum 3 mm. Połączenia korpusu szafy powinny zapewnić dostateczną sztywność.
2. Konstrukcja i kształt szafy powinny zapewniać wygodne i bezpieczne przechowywanie dokumentów. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy powinny być jednoskrzydłowe, osadzone na wewnętrznych zawiasach lub umieszczonych na zewnątrz sworzniach zalutowanych mosiądzem lub zaspawanych, blokowane na czterech krawędziach. Stosowanie szaf z drzwiami dwuskrzydłowymi wymaga uzgodnienia z Wojskowymi Służbami Informacyjnymi.
4. Konstrukcja szafy powinna uniemożliwiać zamknięcie drzwi bez wcześniejszej pełnej blokady na wszystkich krawędziach. Szczelina pomiędzy drzwiami a korpusem nie powinna być większa niż 2 mm.
5. Mechanizm dźwigniowy rygli w drzwiach powinien być zabezpieczony przed nieuprawnionym uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglujący, w tym:
   1) zamek mechaniczny kluczowy wielozastawkowy z możliwością wyjęcia klucza tylko w pozycji zamkniętej, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem;
   2) zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skoku nastawień nie większym niż jedna działka i posiadający minimum 100 podziałek na pokrętle (minimum 1000000 kombinacji). Czas otwarcia zamka przez osobę nieuprawnioną drogą wybierania kolejnych kombinacji powinien wynosić nie mniej niż 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem radiologicznym (promieniowanie co najmniej 10 curie, Co-60 z odległości 760 mm). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy do ustawiania szyfru. W przypadku przechowywania narodowych materiałów niejawnych, dopuszcza się również stosowanie elektronicznego zamka szyfrowego, pod warunkiem spełnienia przez niego takich samych wymagań odporności na włamanie co zamek mechaniczny szyfrowy.

6. Szafa powinna być wyposażona w zabezpieczenie mechaniczne, blokujące rygiel w stanie zamkniętym przy próbie włamania z zewnątrz przez uderzenie w rygiel z przodu.
7. Drzwi i korpus powinny być wyposażone w nieusuwalne kołki z otworami do przewlekania sznurka oraz miseczkę do odciskania pieczęci numerowej lub inne urządzenie umożliwiające stwierdzenie próby nieuprawnionego otwarcia, w szczególności jednorazowe plomby plastikowe, liczniki otwarcia drzwi, sygnalizatory elektroniczne.
8. Podstawa szafy powinna posiadać te same rozmiary co wierzch. W podstawie powinien znajdować się zaślepiony otwór umożliwiający zakotwiczenie jej do podłoża. Konstrukcja dna szafy powinna wytrzymać siły minimum 50 kN.
9. Zespoły i części przeznaczone do montażu powinny odpowiadać swoim rysunkom wykonawczym i warunkom technicznym podanym na tych rysunkach.
10. Podstawowa przestrzeń magazynowa szafy powinna pomieścić w szufladach lub regałach dokumenty o rozmiarach A3 lub A4.
11. Dokumentacja techniczna szafy przeznaczona dla nabywcy powinna zawierać:
    1) rysunki złożeniowe części ruchomych i elementów montażowych wraz z rysunkami mechanizmu blokującego;
    2) rysunki przekrojów pionowych i poziomych, zwymiarowane, z podanymi tolerancjami wykonawczymi;
    3) ilość, układ i cechy zamków, mechanizmu ryglowego oraz urządzeń ryglowania awaryjnego, układ, miejsce, typ rygli drzwiowych, ich wymiary (rzut i przekroje) oraz napęd;
    4) szczegóły przymocowania i montażu lub zamocowania wszystkich elementów mających znaczenie dla fizycznego bezpieczeństwa, w szczególności konstrukcję i położenie złącz oraz połączeń;
    5) oznakowanie, rozmieszczenie i wymiary wszystkich otworów przechodzących przez materiały zabezpieczające z uwzględnieniem obszarów szczególnie chronionych;
    6) określenie charakteru i położenia wszelkich przewodów lub urządzeń w ramach systemów wykrywania penetracji, potrzebnych w celu zamontowania w szczególności elektromechanicznych urządzeń zabezpieczających, urządzeń alarmowych, o ile takie występują w wyrobie;
    7) listę wszystkich zamków, które mogą być użyte zamiennie, z podaniem producenta i numeru modelu;
    8) inne cechy charakteryzujące szafę.
12. Szafa powinna posiadać certyfikat wydany przez jednostkę certyfikującą, potwierdzający zgodność wyrobu z wymaganiami klasy C.
13. Szafa powinna posiadać tabliczkę, wydaną przez jednostkę certyfikującą, zamontowaną na wewnętrznej górnej stronie drzwi, zawierającą następujące dane:
    1) nazwę wyrobu;

2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
3) numer fabryczny;
4) rok produkcji;
5) klasę wyrobu;
6) numer certyfikatu;
7) masę.

II. SZAFA STALOWA KLASY B

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne powinny być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 3 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
2. Konstrukcja i kształt szafy powinny zapewniać wygodne i bezpieczne przechowywanie dokumentów. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy powinny być jednoskrzydłowe lub dwuskrzydłowe wyposażone w mechanizm dźwigniowy, blokujący je co najmniej na trzech krawędziach.
4. Konstrukcja powinna uniemożliwiać zamknięcie drzwi na zamki bez wcześniejszej blokady na wszystkich krawędziach szafy. Szczelina pomiędzy drzwiami a korpusem nie powinna być większa niż 2 mm.
5. Mechanizm dźwigniowy rygli w drzwiach powinien być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglujący, w tym:
   1) zamek mechaniczny kluczowy wielozastawkowy z możliwością wyjęcia klucza tylko w pozycji zamkniętej, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem;
   2) zamek mechaniczny szyfrowy o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skali nastawień nie większej niż półtorej działki i posiadający minimum 100 podziałek na pokrętle (minimum 1000000 kombinacji). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Z szafą powinny być dostarczone dwa komplety kluczy do zmiany kodu. W przypadku przechowywania narodowych materiałów niejawnych, dopuszcza się również stosowanie elektronicznego zamka szyfrowego, pod warunkiem spełnienia przez niego takich samych wymagań odporności na włamanie co zamek mechaniczny szyfrowy.
6. Drzwi i korpus powinny być wyposażone w nieusuwalne kołki z otworami do przewlekania sznurka oraz miseczkę do odciskania pieczęci numerowej lub inne urządzenie umożliwiające

stwierdzenie próby nieuprawnionego otwarcia, w szczególności jednorazowe plomby plastikowe, liczniki otwarcia drzwi, sygnalizatory elektroniczne.

7. Podstawa szafy powinna posiadać te same rozmiary co wierzch. W podstawie powinien znajdować się zaślepiony otwór umożliwiający zakotwiczenie jej do podłoża. Konstrukcja dna szafy powinna wytrzymać siły minimum 50 kN.
8. Zespoły i części przeznaczone do montażu powinny odpowiadać swoim rysunkom wykonawczym i warunkom technicznym podanym na tych rysunkach.
9. Podstawowa przestrzeń magazynowa szafy powinna pomieścić w szufladach lub regałach dokumenty o rozmiarach A3 lub A4.
10. Dokumentacja techniczna szafy przeznaczona dla nabywcy powinna zawierać:
    1) rysunki złożeniowe części ruchomych i elementów montażowych wraz z rysunkami mechanizmu blokującego;
    2) rysunki przekrojów pionowych i poziomych, zwymiarowane, z podanymi tolerancjami wykonawczymi;
    3) ilość, układ i cechy zamków, mechanizmu ryglowego oraz urządzeń ryglowania awaryjnego, układ, miejsce, typ rygli drzwiowych, ich wymiary (rzut i przekroje) oraz napęd;
    4) szczegóły przymocowania i montażu lub zamocowania wszystkich elementów mających znaczenie dla fizycznego bezpieczeństwa, w szczególności konstrukcję i położenie złącz i połączeń;
    5) oznakowanie, rozmieszczenie i wymiary wszystkich otworów przechodzących przez materiały zabezpieczające z uwzględnieniem obszarów szczególnie chronionych;
    6) określenie charakteru i położenia wszelkich przewodów lub urządzeń w ramach systemów wykrywania penetracji, potrzebnych w celu zamontowania w szczególności elektromechanicznych urządzeń zabezpieczających, urządzeń alarmowych, o ile takie występują w wyrobie;
    7) listę wszystkich zamków, które mogą być użyte zamiennie, z podaniem producenta i numeru modelu;
    8) inne cechy charakteryzujące szafę.
11. Szafa powinna posiadać certyfikat wydany przez jednostkę certyfikującą, potwierdzający zgodność wyrobu z wymaganiami klasy B.
12. Szafa powinna posiadać tabliczkę zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:
    1) nazwę wyrobu;
    2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
    3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu;
    4) masę.

SZAFA STALOWA KLASY A

1. Szafa powinna być wyposażona w zamek mechaniczny kluczowy wielozastawkowy.
2. Konstrukcja zamka powinna umożliwiać wyjęcie klucza tylko w pozycji zamkniętej.
3. Szafa może być jedno lub dwudrzwiowa.
4. Drzwi powinny być wyposażone w nieusuwalne kołki z otworami do przewlekania sznurka i nieusuwalną miseczkę do odciskania pieczęci numerowej.

STRZEŻ TAJEMNICY PAŃSTWOWEJ I SŁUŻBOWEJ

SZAFA nr fabryczny .....

Odpowiedzialny: ..... nr pieczęci .....
..... nr pieczęci .....
..... nr pieczęci .....

PRZED OPUSZCZENIEM MIEJSCA PRACY SPRAWDŹ ZABEZPIECZENIE POWIERZONYCH CI DOKUMENTÓW

KLAUZULA TAJNOŚCI

Egz. nr .....

KOD DO SEJFU NR .....

ADRES : .....

.....

PRAWO POBRANIA POSIADAJĄ:

1. .....
(stopień, imię i nazwisko)

2. .....
(stopień, imię i nazwisko)

3. .....
(stopień, imię i nazwisko)

(miejsce zagięcia kartki)

KOMBINACJA ZAMKA SZYFROWEGO

FORMULARZ TEN POWINIEN BYĆ ZAGIĘTY W POŁOWIE I ODPOWIEDNIO ZAMKNIĘTY W NIEPRZEŹROCZYSTEJ KOPERCIE

INSTYTUCJA:	**ODDZIAŁ:**	**WYDZIAŁ:**
NR POJEMNIKA/SEJFU:	**NR POMIESZCZENIA:**	**DATA OSTATNIEJ ZMIANY KOMBINACJI:**

KOMBINACJA*/**

1. **OBRÓT W LEWO** ..... **RAZY DO NUMERU** .....
2. **OBRÓT W PRAWO** ..... **RAZY DO NUMERU** .....
3. **OBRÓT W LEWO** ..... **RAZY DO NUMERU** .....
4. **OBRÓT W PRAWO** ..... **RAZY DO NUMERU** .....
5. **OBRÓT W LEWO** ..... **RAZY DO NUMERU** .....

* JEŚLI KOMBINACJA ZACZYNA SIĘ PRZEKRĘCANIEM POKRĘTŁA ZAMKA SZYFROWEGO W LEWO, ZACZYNAMY OPIS OD POZYCJI 1

JEŚLI KOMBINACJA ZACZYNA SIĘ PRZEKRĘCANIEM POKRĘTŁA ZAMKA SZYFROWEGO W PRAWO,

ZACZYNAMY OPIS OD POZYCJI *2*.

** WYPEŁNIAĆ MIĘKKIM OŁÓWKIEM

(miejsce zagięcia kartki)



Załącznik nr 4

REJESTR TECZEK DOKUMENTÓW NIEJAWNYCH, DZIENNIKÓW I KSIĄŻEK EWIDENCYJNYCH

Strona lewa

Lp.	Nazwa teczki, dokumentu, książki itp.	Klauzula tajności	Data rozpoczęcia
1	2	3	4

Strona prawa

Data zakończenia	Liczba stron	Adnotacje o przekazaniu do archiwum lub zniszczeniu	Uwagi
5	6	7	8

Załącznik nr 5

DZIENNIK KORESPONDENCJI

Strona lewa

Numer kolejny zapisu	Numer i data dokumentu otrzymanego	Nazwa instytucji nadawcy (przy odbiorze), adresat (przy wysyłce)	Jakiej sprawy dotyczy	Liczba		
				Stron dokumentu wraz z załącznikami	Załączników	Stron załączników
1	2	3	4	5	6	7

Numer według dziennika ewidencji wykonanych dokumentów	Kto (wydział, stanowisko) wykonał dokument, komu przekazani lub numer RWD	Pokwitowanie i data		Symbol (numer) akt, w których jest dokument przechowywany lub jego kopia	Uwagi
		Wykonawcy pobierającego dokument do załatwienia	Pracownika kancelarii potwierdzającego zwrot dokumentu		
8	9	10	11	12	13

Załącznik nr 6

KSIĄŻKA EWIDENCJI WYDAWNICTW, DOKUMENTACJI

Strona lewa

....

Nr porządkowy Nazwa dokumentu

Lp.	O t r z y m a n o				
	Nr i data faktury (pisma)	S k ą d	Liczba egz.	Nr Nr egz.	Liczba załączników i ich stron

....

Nr porządkowy **Nazwa dokumentu**

Lp.	O t r z y m a n o				
	Nr i data faktury (pisma)	S k ą d	Liczba egz.	Nr Nr egz.	Liczba załączników i ich stron

Strona prawa

..... Sygnatura ..... Rok wydania ..... Klauzula tajności

Wysłano				Pozostało		Nr Nr teczki i stron podszytych faktur (pism)	Adnotacje o wysłaniu lub zniszczeniu dokumentu	Uwagi
Nr i data faktury (pisma)	Dokąd	Liczba egz.	Nr Nr egz.	Liczba egz.	Nr Nr egz.			

..... Sygnatura ..... Rok wydania ..... Klauzula tajności

Wysłano				Pozostało		Nr Nr teczki i stron podszytych faktur (pism)	Adnotacje o wysłaniu lub zniszczeniu dokumentu	Uwagi
Nr i data faktury (pisma)	Dokąd	Liczba egz.	Nr Nr egz.	Liczba egz.	Nr Nr egz.			

Załącznik nr 7

WYKAZ

osób .....

(nazwa jednostki organizacyjnej)

upoważnionych do dostępu do informacji niejawnych

Lp.	Stopień wojskowy	Imię i nazwisko	Nazwa komórki organizacyjnej	Zakres i numer poświadczenia bezpieczeństwa	Termin ważności poświadczenia bezpieczeństwa do klauzuli			Uwagi
					Ściśle tajne	Tajne	Poufne/ Zastrzeżone	
1	2	3	4	5	6	7	8	9

Załącznik nr 8

REJESTR WYDANYCH DOKUMENTÓW Nr .....

.....	.....	.....
stopień wojskowy	**imię i nazwisko lub nazwa dokumentu**	**nazwa jednostki lub komórki organizacyjnej**

M. p.

Lp.	Nr ewidencyjny dokumentu	Nazwa dokumentu lub stopień wojskowy i nazwisko wykonawcy	Ilość stron lub nr egz.	Data i pokwitowanie wykonawcy	Data i pokwitowanie kancelarii	Adnotacja o zniszczeniu lub przerejestrowaniu
1	2	3	4	5	6	7

Załącznik nr 9

SKOROWIDZ RWD

Strona lewa

Lp.	Stopień wojskowy	Imię i nazwisko lub nazwa komórki organizacyjnej	Data założenia

Strona prawa

Data zakończenia	Adnotacje o zniszczeniu	Uwagi

Załącznik nr 10

KSIĄŻKA DORĘCZEŃ

Lp.	Data przyjęcia przesyłki (dzień, miesiąc, godzina)	Numer ewidencyjny dokumentu	Adresat	Potwierdzenie odbioru dokumentu	
				Stopień wojskowy, imię i nazwisko	Pieczęć data i podpis
1	2	3	4	5	6

Załącznik nr 11

METRYKA ELEKTRONICZNEGO NOŚNIKA INFORMACJI

.....

(rodzaj i nr ewidencyjny nośnika)

Do pakietów ...

Lp.	Nazwa dokumentu lub krótki opis zawartości nośnika	Ilość folderów/ilość plików	Zajętość nośnika w j.m.	Stopień wojskowy, imię i nazwisko osoby utrwalającej informacje	Data i podpis	Adnotacja o zniszczeniu nośnika lub usunięciu pliku /folderu
1	2	3	4	5	6	7

WZORY PIECZĘCI DO OZNAKOWYWANIA:

1) dokumentów wymienianych w ramach realizacji porozumień międzynarodowych:

L. p.	Wzór pieczęci	Opis pieczęci	Uwagi
1	2	3	4
1	MINISTERSTWO OBRONY NARODOWEJ *..... MINISTRY OF NATIONAL DEFENCE **..... File No ..... Warsaw-POLAND	Pieczęć nagłówkowa prostokątna o długości 54 mm i szerokości 33 mm, wypukła do tuszu	* Nazwa instytucji (jednostki) w języku polskim, ** Nazwa instytucji (jednostki) w języku angielskim
2	MINISTERSTWO OBRONY NARODOWEJ *..... MINISTRY OF NATIONAL DEFENCE **..... File No ..... Received on ..... Enclosure ..... Sheets	Pieczęć wpływu pism - prostokątna o długości 54 mm i szerokości 27 mm., wypukła do tuszu.	*Nazwa instytucji (jednostki) w języku polskim. ** Nazwa instytucji (jednostki) w języku angielskim.
3	M N ANGIELSKA NAZWA INSTYTUCJI POLSKA NAZWA INSTYTUCJI	Pieczęć do pakietów o średnicy 30 mm wypukła do tuszu oraz wklęsła do laku z napisami na otoku "✱MON✱i nazwa instytucji w języku polskim" oraz "✱MOND✱i nazwa instytucji w języku angielskim"	
4	MINISTERSTWO OBRONY NARODOWEJ *..... MINISTRY OF NATIONAL DEFENCE **.....	Pieczęć firmująca prostokątna o długości 54 mm i szerokości 20 mm, wypukła do tuszu.	* Nazwa instytucji (jednostki) w języku polskim, ** Nazwa instytucji (jednostki) w języku angielskim
5	DOKUMENTY PODLEGAJĄ CODZIENNEMU ZWROTOWI DO KANCELARII *	Pieczęć informacyjna wypukła do tuszu o długości 75 mm i szerokości 24 mm.	* Skrót nazwy instytucji (jednostki)
6	RESTRICTED ZASTRZEŻONE	Pieczęć informacyjna wypukła do tuszu o długości 42 mm i szerokości 12 mm.	

1	2	3	4
7	**UNCLASSIFIED** **Jawne**	**Pieczęć informacyjna wypukła do tuszu o długości 40 mm i szerokości 12 mm.**	
8	**CONFIDENTIAL** **Poufne**	**Pieczęć informacyjna wypukła do tuszu o długości 52 mm i szerokości 12 mm.**	
9	**SECRET** **Tajne**	**Pieczęć informacyjna wypukła do tuszu o długości 33 mm i szerokości 12 mm.**	
10	**TOP SECRET** **ściśle tajne**	**Pieczęć informacyjna wypukła do tuszu o długości 53 mm i szerokości 12 mm.**	
11	**TO BE DELIVERED PERSONALLY** **do rąk własnych**	**Pieczęć informacyjna wypukła do tuszu o długości 53 mm i szerokości 12 mm.**	
12	**URGENT** **Pilne**	**Pieczęć informacyjna wypukła do tuszu o długości 35 mm i szerokości 12 mm.**	
13	**REGISTERED LETTER** **Polecony**	**Pieczęć informacyjna wypukła do tuszu o długości 37 mm i szerokości 12 mm.**	
14	**N A T O**	**Pieczęć informacyjna prostokątna wypukła do tuszu o długości 44 mm i szerokości 15 mm.**	
15	**U Z E**	**Pieczęć informacyjna prostokątna wypukła do tuszu o długości 30 mm i szerokości 15 mm.**	
16	Enclosure No ..... to..... of ..... Załącznik Nr ..... do pisma Nr	**Pieczęć formularzowa wypukła do tuszu o długości 54 mm i szerokości 22 mm.**	
17	Disposed on ..... 1. ..... 2. ..... Signatures Zniszczono dn. ..... 1. ..... 2. ..... podpisy	**Pieczęć formularzowa wypukła do tuszu o długości 54 mm i szerokości 28 mm.**	

dokumentów krajowych:

1	2	3	4
.	.*..... **Nr .....** ..... (data) .... (miejsce postoju instytucji, j.w.)	**Pieczęć nagłówkowa prostokątna o długości 54 mm i szerokości 33 mm, wypukła do tuszu**	***Nazwa instytucji (jednostki) lub numer - dwie pieczęcie jeżeli jednostka posiada pełną nazwę i numer jednostki.**
2.	*..... **Nr .....** **Wpłynęło .....** **Zał. ..... Ark. .....**	**Pieczęć wpływu pism - prostokątna o długości 54 mm i szerokości 27 mm., wypukła do tuszu.**	
3.	JEDNOSTKA WOJSKOWA 2183 *Do pakietów*	**Pieczęć do pakietów o średnicy 30 mm wypukla do tuszu oraz wklęsła do laku z nazwą lub nr instytucji (jednostki) na otoku - dwie pieczęcie jeżeli jednostka posiada pełną nazwę i numer jednostki.**	
4.	*..... ..... (miejsce postoju)	**Pieczęć nagłówkowa prostokątna o długości 54 mm i szerokości 33 mm, wypukła do tuszu**	***Nazwa instytucji (jednostki) lub nr -dwie piecz. jeżeli jednostka posiada pełną nazwę i numer jed.**
5.	**ZASTRZEŻONE**	**Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości**	
6.	**P O U F N E**	**Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości**	
7.	**T A J N E**	**Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości**	
8.	**ŚCIŚLE TAJNE**	**Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości**	

1	2	3	4
9.	**PILNE**	**Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości**	
10.	**BARDZO PILNE**	**Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości**	
11.	**Do rąk własnych**	**Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości**	
12.	Zniszczono dn. ..... 1. ..... 2. ..... podpisy	**Pieczęć formularzowa wypukła do tuszu o długości 54 mm i szerokości 15 mm**	
13.	**P O U F N E** **RWD Nr .....**	**Pieczęć formularzowa wypukła do tuszu o długości 28 mm i szerokości 26 mm.**	
14.	**T A J N E** **RWD Nr .....**	**Pieczęć formularzowa wypukła do tuszu o długości 28 mm i szerokości 26 mm.**	
15.	**ŚCIŚLE TAJNE** **RWD Nr .....**	**Pieczęć formularzowa wypukła do tuszu o długości 60 mm i szerokości 26 mm.**	
16.	**Niniejszy (a) ..... zawiera .....** **(.....) kart (stron) po-numerowanych, przesznurowanych i opieczęto- wanych.** **Dn. „....." 200... r.** **.....** **(kierownik kancelarii)**	**Pieczęć formularzowa wypukła do tuszu o długości 70 mm i szerokości 26 mm.**	
17.	**Zał. Nr....** **Stron .....** **Wchodz.** **Do pisma Nr ....z dn.....** **Wychodz.**	**Pieczęć formularzowa wypukła do tuszu o długości 62 mm i szerokości 20 mm.**	

DZIENNIK EWIDENCJI WYKONANYCH DOKUMENTÓW
(techniką maszynopisania, powielania, kreślenia itp.)

Strona lewa

Lp.	Data oddania brudnopisu do przepisania lub dokumentu do powielenia	Adres albo nazwa dokumentu	Nazwisko osoby sporządzającej dokument	Nr brudnopisu i numery stron (nr dokumentu i liczba stron)	Nazwisko osoby wykonującej dokument
1	2	3	4	5	6

Strona prawa

Liczba wykonanych		Pokwitowanie odbioru			Adnotacje		Uwagi
egzemplarzy	**stron**	**Imię i nazwisko**	**Data**	**Podpis**	**o wysłaniu**	**o zniszczeniu**	
7	8	9	10	11	12	13	14

SKOROWIDZ KART CZYTELNIKA

Strona lewa

Lp.	Stopień wojskowy	Imię i nazwisko	Data założenia

Strona prawa

Data zakończenia	Adnotacje o zniszczeniu	Uwagi

Załącznik nr 15

KARTA CZYTELNIKA Nr.....

Nazwisko.....

Imię.....

Komórka organizacyjna.....

tel. sł.....

Numer biblioteczny	Numer egzemplarza	TYTUŁ	Wypożyczenie		Zwrot	
			Data	Podpis czytelnika	Data	Podpis pracownika biblioteki
1	2	3	4	5	6	7

Załącznik nr 16

Karta wydawnictwa Nr .....

Autor / sygnatura.....

Tytuł.....

Rok wydania.....

Ilość egzemplarzy..... Nr egz. .....

Ilość stron pojedynczego egz. .....

Stopień, nazwisko i imię	**Nr karty czytelnika**	**Nr egz.**	**Data pobrania**	**Data zwrotu**	**Uwagi**
1	2	3	4	5	6

Załącznik nr 17

DZIENNIK WYKONAWCY

Strona lewa

Lp.	Numery dokumentów			Ilość stron dokumentu	Skąd wpłynął lub dokąd wysłano dokument	Czego dokument dotyczy lub jego nazwa
	Wchodzący	Wychodzący	Według dziennika. ewidencji wykonanych dokumentów			
1	2	3	4	5	6	7

Strona prawa

Komu przekazano dokument		Nr teczki w której znajduje się pismo	Uwagi
Stopień wojskowy, imię i nazwisko	Data i podpis		
8	9	10	11

Załącznik nr 18

ZEZWALAM
na zniszczenie dokumentów
wyszczególnionych w protokóle

.....
(stanowisko, stopień wojskowy, imię, nazwisko)

PROTOKÓŁ ZNISZCZENIA DOKUMENTÓW

Zgodnie z rozkazem dziennym (decyzją) nr.....z dnia .....

komisja w składzie: - przewodniczący .....
(stopień wojskowy, imię i nazwisko)

- członkowie: .....
(stopień wojskowy, imię i nazwisko)

.....
(stopień wojskowy, imię i nazwisko)
zakwalifikowała niżej wymienione dokumenty do zniszczenia:

Lp.	Nazwa dokumentu, teczki przedmiotowej i jej numer	Numer ewidencyjny	Nr wg dziennika ewid. wydr. dokumentów	Ilość egz.	Nr egz.	Ilość Stron Inna jednostka miary	Uwagi
1	2	3	4	5	6	7	8

Dokumenty wymienione pod pozycją ..... zostały zniszczone
1)wstępnie w dniu.....przez przedarcie. Pojemnik ze zniszczonymi wstępnie materiałami opieczętowano pieczęcią numerową nr.....

Imiona, nazwiska oraz podpisy:
- osoby, która wstępnie zniszczyła dokumenty,
- osób nadzorujących wstępne zniszczenie;

2)ostatecznie w dniu..... przez.....
(określenie sposobu zniszczenia materiału)

Imiona, nazwiska oraz podpisy:
Przewodniczący: .....
Członkowie: .....
.....

ZARZĄDZENIE 3/MON MINISTRA OBRONY NARODOWEJ

z dnia 2 lutego 2005 r.

w sprawie zasad i trybu postępowania z materiałami archiwalnymi i inną dokumentacją w resorcie Obrony Narodowej

Rozdział 1

Postanowienia ogólne

§ 1.

1. Zarządzenie określa:

   1) zasady klasyfikowania i kwalifikowania dokumentacji ze względu na okresy jej przechowywania;

   2) zasady i tryb przekazywania materiałów archiwalnych do archiwów;

   3) zasady i tryb brakowania dokumentacji niearchiwalnej.

2. Szczegółowe zasady i tryb postępowania z materiałami archiwalnymi i inną dokumentacją Służby Kontrwywiadu Wojskowego regulują odrębne przepisy

§ 2.

Określenia użyte w zarządzeniu oznaczają:

1) ustawa - ustawę z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2002r. Nr 171, póz. 1396 i Nr 241, póz. 2074, z 2003r. Nr 137, póz. 1302 oraz z 2004r. Nr 173, póz. 1808 i Nr 202, poz.2065);

2) minister - Ministra Obrony Narodowej, jako organ administracji rządowej;

3) ministerstwo - Ministerstwo Obrony Narodowej, jako urząd administracji rządowej obsługujący ministra;

4) resort obrony narodowej - dział administracji rządowej kierowany przez ministra, w skład którego wchodzą: minister jako kierownik resortu, ministerstwo jako urząd, jednostki organizacyjne podległe lub nadzorowane przez ministra oraz Siły Zbrojne Rzeczypospolitej Polskiej;

5) komórka organizacyjna - Sekretariat Ministra, departament, generalny zarząd, samodzielny zarząd, biuro;

6) jednostka organizacyjna - jednostkę nie wchodzącą w skład ministerstwa, podległą ministrowi lub przez niego nadzorowaną, w tym przedstawicielstwo, kontyngent, misję wojskową działającą poza granicami kraju i przedsiębiorstwo państwowe, dla którego jest on organem założycielskim;

7) archiwum - państwowe archiwum wyodrębnione jednostek organizacyjnych podległych lub nadzorowanych przez ministra, jako jednostka organizacyjna powołana do gromadzenia, ewidencji, przechowywania, opracowania, zabezpieczenia i udostępniania materiałów archiwalnych oraz prowadzenia działalności informacyjnej, a także sprawowania nadzoru w komórkach organizacyjnych i jednostkach organizacyjnych w zakresie kształtowania zasobu archiwalnego oraz postępowania z materiałami archiwalnymi i dokumentacją niearchiwalną;

8) zasób archiwalny- materiały archiwalne powstałe i powstające w toku działalności komórek organizacyjnych i jednostek organizacyjnych oraz do nich napływające, stanowiące wyodrębnioną część państwowego zasobu archiwalnego;

9) gromadzenie zasobu archiwalnego - uzupełnianie zasobu archiwalnego poprzez kolejne dopływy materiałów archiwalnych do archiwów;

10) brakowanie-wydzielanie dokumentacji innej (niearchiwalnej) do niszczenia, po upływie okresu jej przechowywania;

11) kategorie archiwalne - grupy dokumentacji wyróżnione w zależności od posiadanej wartości historycznej lub praktycznej, oznaczone symbolami literowymi: A, B, BE, Bc;

12) zespół archiwalny- organicznie powiązane ze sobą zaarchiwalizowane materiały archiwalne wytworzone i zgromadzone w wyniku działalności komórki (jednostki) organizacyjnej;

13) twórca zespołu archiwalnego - komórkę organizacyjna lub jednostkę organizacyjna;

14) materiały archiwalne - wszelkiego rodzaju akta i dokumenty, korespondencję, dokumentację finansową, techniczną i statystyczną, mapy i plany, fotografie, filmy i mikrofilmy, nagrania dźwiękowe i wideofonowe oraz inną dokumentację, bez względu na sposób jej wytwarzania, mającą znaczenie jako źródło informacji, o wartości historycznej, o działalności resortu obrony narodowej oraz o jego stosunkach z innymi armiami i organizacjami międzynarodowymi - powstałe w przeszłości i powstające współcześnie, które ze względu na swoją wartość historyczną kwalifikują się do wieczystego przechowywania w archiwum;

15) kwalifikacja archiwalna - zaliczanie dokumentacji przez twórcę zespołu archiwalnego do odpowiednich kategorii archiwalnych;

16) klasyfikacja archiwalna - system podziału i układu dokumentów według grup rzeczowych ustalony przez twórcę zespołu w wykazie akt;

17) *rzeczowy wykaz akt* - wykaz haseł wyróżniający klasyfikację dokumentacji archiwalnej i niearchiwalnej sporządzony przez komórkę organizacyjną lub jednostkę organizacyjną;

18) archiwizacja - ogół czynności związanych z klasyfikowaniem, kwalifikowaniem, kompletowaniem i przekazywaniem do archiwów materiałów archiwalnych oraz ich ewidencjonowaniem i przechowywaniem w tych archiwach;

19) sygnatura archiwalna - znak rozpoznawczy nadany jednostce archiwalnej lub niearchiwalnej, określający jej miejsce w obrębie zespołu i umożliwiający jej zidentyfikowanie;

20) szef archiwum - dyrektora, kierownika archiwum.

§3.

1. Dokumentacja powstająca w komórkach organizacyjnych i jednostkach organizacyjnych oraz do nich napływająca jest przechowywana przez te komórki organizacyjne i jednostki organizacyjne przez okres ustalony w zarządzeniu.

2. Po upływie okresu, o którym mowa w ust. 1:

1) dokumentacja stanowiąca materiał archiwalny jest przekazywana do właściwego archiwum, na zasadach i w trybie określonym w rozdziale 3;

2) dokumentacja inna niż wymieniona w pkt 1 podlega ekspertyzie i brakowaniu w komórkach organizacyjnych i jednostkach organizacyjnych, na zasadach i w trybie określonym w rozdziale 4.

§ 4.

Materiał archiwalny, o którym mowa w § 3 ust. 2 pkt 1, stanowi zasób archiwalny.

Rozdział 2

Klasyfikowanie i kwalifikowanie dokumentacji

§ 5.

Dokumentacja może być zakwalifikowana do kategorii „A" lub „B".

§ 6.

1. Do kategorii „A" kwalifikuje się materiały archiwalne.

2. Do kategorii „B" kwalifikuje się inną dokumentację, zwaną dalej „dokumentacją niearchiwalną".

3. Dokumentację niearchiwalną, ze względu na okresy przechowywania, oznacza się:

   1) symbolem „B" z dodaniem cyfry arabskiej określającej liczbę lat przechowywania podlegającą, po upływie okresu przechowywania, ekspertyzie kwalifikacji i brakowaniu;

   2) symbolem „BE" z dodaniem cyfry arabskiej określającej liczbę lat przechowywania podlegającą, po upływie okresu przechowywania, ponownej kwalifikacji po przeprowadzeniu obowiązkowej ekspertyzy archiwalnej;

   3) symbolem „Bc" oznacza się dokumentację mającą wyłącznie przydatność praktyczną podlegającą ekspertyzie kwalifikacji i brakowaniu po ustaniu jej przydatności dla komórki organizacyjnej lub jednostki organizacyjnej.

§ 7.

1. Materiały archiwalne przechowuje się wieczyście.

2. Okresy przechowywania dokumentacji niearchiwalnej określane cyframi arabskimi liczy się w pełnych latach kalendarzowych, poczynając od dnia 1 stycznia roku następnego po roku, w którym została zamknięta teczka aktowa odpowiedniej kategorii poprzez jej ponumerowanie i przesznurowanie oraz opisanie pierwszej strony okładki teczki aktowej.

§ 8.

Klasyfikacja archiwalna dokumentacji polega na:

1) dokonaniu jej podziału na kategorie „A" lub „B";

2) oznaczeniu materiałów archiwalnych kategorii „A" symbolem „A";

3) oznaczeniu dokumentacji niearchiwalnej kategorii „B" symbolami, o których mowa w § 6 ust. 3;

4) oznaczeniu materiałów archiwalnych i dokumentacji niearchiwalnej symbolami klasyfikacyjnymi według jednolitego rzeczowego wykazu akt, zwanego dalej „wykazem akt", stanowiącym załącznik Nr 1 do zarządzenia.

§ 9.

1. Kwalifikacji i klasyfikacji dokumentacji, według zasad określonych w § 5 - 8, dokonuje się, począwszy od pierwszego dokumentu, który został wytworzony lub wpłynął w danej sprawie.

2. W szczególnie uzasadnionych przypadkach kwalifikacji i klasyfikacji dokumentacji można dokonać po zakończeniu sprawy.

3. Kierownicy komórek organizacyjnych i jednostek organizacyjnych:

   1) odpowiadają za prawidłową kwalifikację i klasyfikację dokumentacji powstającej w komórkach lub jednostkach organizacyjnych oraz do nich nadsyłanej;

   2) opracowują i zatwierdzają rzeczowy wykaz akt komórki lub jednostki organizacyjnej w uzgodnieniu z szefem właściwego archiwum;

4. Podstawę do opracowania rzeczowego wykazu akt, o którym mowa w ust. 3 pkt 2 oraz jego układ i formę, stanowią dokumenty organizacyjno-etatowe i zakresy działania komórki lub jednostki organizacyjnej oraz ustalenia zawarte w załączniku Nr 1 do zarządzenia.

§10.

1.Wcelu zbadania i oceny wartości historycznej oraz praktycznej wytworzonej dokumentacji niearchiwalnej, w tym właściwe jej zaliczenie do kategorii „B", przeprowadza się ekspertyzę archiwalną lub ekspertyzę kwalifikacji.

2. Prowadzi się ekspertyzy:

   1) archiwalną w odniesieniu do dokumentacji niearchiwalnej kategorii „B" oznaczonej symbolem „BE" z odpowiednią cyfrą arabską;

   2) kwalifikacji w odniesieniu do dokumentacji niearchiwalnej kategorii „B" oznaczonej symbolem „B" z odpowiednią cyfrą arabską lub „Bc", według zasad i w trybie określonym w rozdziale 4.

3. Do przeprowadzenia ekspertyzy archiwalnej kierownik komórki organizacyjnej lub jednostki organizacyjnej powołuje komisję składającą się z co najmniej trzech przedstawicieli komórki lub jednostki organizacyjnej, dla której ekspertyza ma być przeprowadzona, przy współudziale przedstawiciela właściwego archiwum.

4. Po przeprowadzeniu ekspertyzy archiwalnej dokumentacji niearchiwalnej kategorii „B" oznaczonej symbolem „BE" z odpowiednią cyfrą arabską komisja może zaproponować:

   1) wydłużenie okresu przechowywania dokumentacji niearchiwalnej kategorii „B" oznaczając symbolem „B" z dodaniem cyfry arabskiej określającej liczbę lat dalszego przechowywania;

   2) zmianę kwalifikacji dokumentacji niearchiwalnej kategorii „B" na kategorię „A";

   3) brakowanie i zniszczenie.

5. Komisja, po wykonaniu czynności, o których mowa w ust. 1 i 4, sporządza w dwóch egzemplarzach:

   1) protokół oceny dokumentacji niearchiwalnej, według wzoru stanowiącego załącznik Nr 2 do zarządzenia;

   2) spis akt przekazanych do archiwum lub wydzielonych do zniszczenia, według wzoru stanowiącego załącznik Nr 3 do zarządzenia;

6. Protokół i spis, o których mowa w ust. 5 podlegają odpowiednio zatwierdzeniu lub wyrażeniu zgody przez kierownika komórki organizacyjnej lub jednostki organizacyjnej.

7. Po zatwierdzeniu lub wyrażeniu zgody jeden egzemplarz protokołu i spisu pozostaje w komórce organizacyjnej lub jednostce organizacyjnej, drugi egzemplarz jest przekazywany do właściwego archiwum.

8. W sprawach, o których mowa w ust. 4, decyzję podejmuje szef właściwego archiwum, która jest wiążąca dla kierownika komórki organizacyjnej lub jednostki organizacyjnej.

Rozdział 3

Przekazywanie materiałów archiwalnych do archiwów

§ 11.

1. Komórki organizacyjne i jednostki organizacyjne przekazują materiały archiwalne do właściwego archiwum nie później niż po upływie 15 lat od ich wytworzenia.

2. Termin określony w ust. 1 nie dotyczy:

1) materiałów archiwalnych, których okres przechowywania określony jest odrębnymi przepisami;

2) materiałów archiwalnych gromadzonych i przechowywanych w jednostkach organizacyjnych, o których mowa w § 3 ust. 1 pkt 2 i ust. 2 zarządzenia Ministra Obrony Narodowej w sprawie organizacji archiwów wyodrębnionych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej oraz zakresu ich działania.

§ 12.

1. W razie ustania działalności (likwidacja, rozformowanie) komórki organizacyjnej lub jednostki organizacyjnej dokumenty przekazuje się:

1) materiały archiwalne-właściwemu archiwum;

2) materiały archiwalne niezbędne do dalszej działalności, dla których nie upłynął 15-letni okres od ich wytworzenia - komórce organizacyjnej lub jednostce organizacyjnej przejmującej zadania i funkcje komórki organizacyjnej lub jednostki organizacyjnej, której działalność ustała;

3) dokumentację niearchiwalną - komórce organizacyjnej lub jednostce organizacyjnej przejmującej zadania i funkcje komórki organizacyjnej lub jednostki organizacyjnej, której działalność ustała.

2. W razie braku następcy prawnego, materiały archiwalne i dokumentację niearchiwalną wytworzoną i zgromadzoną przez komórkę organizacyjną lub jednostkę organizacyjną, o której mowa w ust. 1, jeżeli okres przechowywania nie upłynął, przekazuje się właściwej rzeczowo komórce organizacyjnej lub jednostce organizacyjnej, wskazanej w dokumencie decyzyjnym dotyczącym likwidacji lub rozformowania danej komórki organizacyjnej lub jednostki organizacyjnej.

§ 13.

1. Kierownik komórki organizacyjnej lub jednostki organizacyjnej powiadamia, o zamiarze przekazania materiałów archiwalnych, szefa właściwego archiwum, przedstawiając dwa egzemplarze spisu akt, sporządzonego według wzoru określonego w załączniku Nr 3 do zarządzenia.

2. Szef archiwum, o którym mowa w ust. 1:

1) sprawdza, pod względem formalnym, sposób opracowania nadesłanych spisów akt;

2) odsyła jeden egzemplarz akceptowanego spisu akt określając na tym dokumencie termin przekazania materiałów archiwalnych do archiwum;

3) odsyła spisy akt do ponownego sporządzenia, w przypadku stwierdzenia w nich braków formalnych.

3. W przypadku zaistnienia sytuacji, o której mowa w ust. 2 pkt 3, przepisy ust. 1 stosuje się odpowiednio.

§ 14.

1. Przekazanie i przyjęcie materiałów archiwalnych następuje na podstawie akceptowanych spisów akt.

2. Przyjęcie materiałów archiwalnych przez archiwum polega na:

1) sprawdzeniu, pod względem formalnym, stanu przygotowania przekazywanych materiałów archiwalnych;

2) przyjęciu ilościowym materiałów archiwalnych, na podstawie spisów akt.

3. Archiwum odmawia przyjęcia materiałów archiwalnych w przypadku nie spełnienia przez nie wymogów, określonych w zarządzeniu.

4. Odmowa, o której mowa w ust. 3, wymaga pisemnego uzasadnienia.

5. Koszty związane z przygotowaniem i konserwacją materiałów archiwalnych oraz ich przekazaniem do archiwum ponosi komórka organizacyjna lub jednostka organizacyjna przekazująca te materiały.

§ 15.

1. Postępowanie w komórce organizacyjnej lub jednostce organizacyjnej z materiałami archiwalnymi i dokumentacją niearchiwalną polega na:

1) podziale rzeczowym akt;

2) prawidłowym ułożeniu dokumentacji wewnątrz teczek akt, ich opisaniu i nadaniu właściwego układu;

3) sporządzeniu ewidencji i technicznym zabezpieczeniu.

2. Podział rzeczowy akt polega na założeniu (wydzieleniu) odpowiednich teczek akt, oddzielnie dla kategorii „A" i „B", a w niej na każdy symbol literowy wraz z określoną cyfrą arabską, w ilości wynikającej z rzeczowego wykazu akt komórki organizacyjnej lub jednostki organizacyjnej.

3. Materiały archiwalne i dokumentacja niearchiwalną powinny być układane w odpowiednich teczkach akt, o których mowa w ust. 2, w kolejności załatwionych spraw, natomiast w ramach sprawy - chronologicznie poczynając od pierwszego pisma wszczynającego sprawę.

4. Opisanie wierzchniej strony okładki każdej teczki akt następuje według wzoru, stanowiącego załącznik Nr 4 do zarządzenia.

5. Nadanie dokumentom, o których mowa w ust. 1, właściwego układu polega na ułożeniu teczek akt, zgodnie ze strukturą organizacyjną komórki organizacyjnej lub jednostki organizacyjnej obowiązującą w czasie, w którym dokumenty te powstały w ramach poszczególnych komórek wewnętrznych lub organizacyjnych, według kolejności symboli klasyfikacyjnych rzeczowego wykazu akt komórki organizacyjnej lub jednostki organizacyjnej.

6. Sporządzenie ewidencji materiałów archiwalnych polega na umieszczeniu ich w:

1) spisie akt, o którym mowa w § 13 ust. 1, wypełnionym pismem maszynowym lub techniką elektroniczną, w kolejności zgodnej z nadanym układem;

2) karcie inwentarzowej, sporządzonej według wzoru, określonego w załączniku Nr 5 do zarządzenia;

3) karcie personalnej, sporządzonej według wzoru, określonego w załączniku Nr 6 do zarządzenia.

7. W przypadku sporządzenia spisu akt techniką elektroniczną, jego zapis przekazuje się właściwemu archiwum w postaci wydruku i na nośniku elektronicznym, w formacie określonym przez szefa archiwum.

§ 16.

1. Spis akt sporządza się w dwóch egzemplarzach, z których jeden przeznaczony jest dla archiwum, drugi dla komórki organizacyjnej lub jednostki organizacyjnej przekazującej materiały archiwalne.

2. Karty, o których mowa w § 15 ust. 6 pkt 2 i 3 sporządza się w jednym egzemplarzu, odpowiednio dla każdej teczki aktowej.

3. W przypadku konieczności sporządzenia dodatkowej ewidencji, w szczególności w formie inwentarza lub skorowidza, wykonanej techniką elektroniczną, szef archiwum określa sposób jej wykonania.
4. Do spisu akt materiałów archiwalnych przeznaczonych do przekazania do archiwum należy dołączyć informację zawierającą podstawowe dane dotyczące zmian organizacyjnych, jakie nastąpiły w czasie, z którego pochodzą przekazywane materiały archiwalne.
5. W przypadku przekazywania materiałów archiwalnych komórki organizacyjnej lub jednostki organizacyjnej, której działalność ustała, do spisu akt należy dołączyć:
   1) podstawowe dane dotyczące organizacji i zakresu działania komórki organizacyjnej lub jednostki organizacyjnej w ujęciu chronologicznym;
   2) spis materiałów archiwalnych i dokumentacji niearchiwalnej, przekazanych komórce organizacyjnej lub jednostce organizacyjnej, przejmującej zadania i funkcje komórki organizacyjnej lub jednostki organizacyjnej, której działalność ustała albo komórce organizacyjnej lub jednostce organizacyjnej, o której mowa w § 12 ust. 2.

§ 17.

Przekazywane materiały archiwalne, w zależności od ich formy zewnętrznej należy :

1) przesznurować w teczkach akt po usunięciu spinaczy i innych elementów metalowych;
2) umieścić w odpowiednich opakowaniach, wykonanych z materiałów chroniących przed uszkodzeniem mechanicznym, elektromagnetycznym, chemicznym lub biologicznym;
3) zapakować w pudła lub paczki w postaci ustalonej z szefem właściwego archiwum, w zależności od rodzaju materiałów archiwalnych, zaopatrzone w etykiety z nazwą komórki organizacyjnej lub jednostki organizacyjnej wraz z sygnaturami teczek lub innych materiałów archiwalnych.

§ 18.

Materiały archiwalne stanowiące dokumentację techniczną, statystyczną, geologiczną, kartograficzną i geodezyjną, fonograficzną i fotograficzną oraz utrwaloną na innych nośnikach, należy uporządkować i przygotować do przekazania w sposób uzgodniony z szefem właściwego archiwum.

Rozdział 4

Brakowanie dokumentacji niearchiwalnej

§ 19.

1. Dokumentacja niearchiwalna, z wyłączeniem dokumentacji kategorii „B" oznaczonej symbolem „BE", podlega brakowaniu w komórkach organizacyjnych i jednostkach organizacyjnych, po upływie okresu jej przechowywania, określonego w rzeczowym wykazie akt komórki organizacyjnej lub jednostki organizacyjnej.
2. Brakowaniu nie podlega dokumentacja niearchiwalna niezbędna do prac bieżących w komórce organizacyjnej lub jednostce organizacyjnej, zwłaszcza konieczna do zachowania dla celów kontrolnych i dowodowych, w sprawach mających być przedmiotem postępowania sądowego lub dyscyplinarnego.

§ 20.

1. Brakowania dokonuje się *przez:*
   1) przeprowadzenie ekspertyzy kwalifikacji dokumentacji niearchiwalnej;

2) sporządzenie spisu akt, według wzoru określonego w załączniku Nr 3 do zarządzenia, dokumentacji niearchiwalnej przeznaczonej do zniszczenia i protokołu oceny tej dokumentacji, oddzielnie dla:

a) oznaczonej symbolem „B" z dodaniem cyfry arabskiej,

b) oznaczonej symbolem „Bc".

2. Protokół, o którym mowa w ust. 1 pkt 2, sporządza się według wzoru, stanowiącego załącznik Nr 7 do zarządzenia.

3. Brakowanie dokumentacji niearchiwalnej dokonuje się po dniu 1 stycznia roku następnego po roku, w którym wygasa okres jej przechowywania.

4. Brakowania dokumentacji niearchiwalnej kategorii „B" oznaczonej symbolem „Bc" można dokonać bezpośrednio po utracie przez tę dokumentację przydatności praktycznej dla komórki organizacyjnej lub jednostki organizacyjnej.

§ 21.

1 Czynności brakowania dokumentacji niearchiwalnej dokonuje komisja wewnętrzna powołana przez kierownika komórki organizacyjnej lub jednostki organizacyjnej.

2. Przepisy § 10 ust. 6 - 8 stosuje się odpowiednio.

§ 22.

Informacje o wybrakowaniu dokumentacji niearchiwalnej zamieszcza się w:

1) spisie akt, o którym mowa w § 20 ust. 1 pkt 2;

2) rejestrze spisów akt, sporządzonym według wzoru, stanowiącego załącznik Nr 8 do zarządzenia.

§ 23.

1. Zezwolenie na zniszczenie dokumentacji niearchiwalnej, zwane dalej „zezwoleniem", wydaje szef właściwego archiwum.

2. Podstawę do wydania zezwolenia stanowi zatwierdzony spis akt i protokół, o których mowa w § 10 ust. 5 oraz § 20 ust. 1 pkt 2.

3. Zezwolenie sporządza się według wzoru stanowiącego załącznik Nr 9 do zarządzenia, w dwóch egzemplarzach, z których jeden pozostaje w archiwum, drugi jest przeznaczony dla komórki organizacyjnej lub jednostki organizacyjnej brakującej dokumentację niearchiwalna.

§ 24.

1. Bezpośredni nadzór nad fizycznym niszczeniem wybrakowanej dokumentacji niearchiwalnej sprawuje komisja wyznaczona przez kierownika komórki organizacyjnej lub jednostki organizacyjnej, która dokonała jej wybrakowania.

2. Fizyczne zniszczenie wybrakowanej dokumentacji powinno nastąpić w sposób uniemożliwiający odtworzenie jej treści.

3. Komórka organizacyjna lub jednostka organizacyjna powiadamia na piśmie właściwe archiwum o zniszczeniu wybrakowanej dokumentacji niearchiwalnej, w terminie do 14 dni od daty jej zniszczenia.

Rozdział 5

Przepisy końcowe

§ 25.

Traci moc zarządzenie Szefa Sztabu Generalnego WP Nr 56/Sztab z dnia 13.10.1988 r. oraz „Instrukcja o zasadach archiwalizacji dokumentacji wojskowej" - sygn. Szt. Gen. 1344/88.

§ 26.

Zarządzenie wchodzi w życie po upływie **14** dni od dnia ogłoszenia.

Minister Obrony Narodowej:

J. Szmajdziński

Symbole klasyfikacyjne		Hasła klasyfikacyjne	Kategorie dokumentacji		Uwagi
			własnej	otrzymanej	
1		2	3	4	5
1		Dokumentacja normatywno-organizacyjna			
	1	Projekty ustaw, rozporządzeń i uchwal dotyczące obronności kraju i Sił Zbrojnych.	A	Bc	
	2	Prognozy, koncepcje, projekty rozwoju Sił Zbrojnych, komórki lub jedn. org., służby.	A	Bc	
	3	Rozkazy, zarządzenia, wytyczne i inne dokumenty wyższych przełożonych, stanowiące podstawę prawną organizacji i zakresu działania własnej jednostki.	A	Bc	
	4	Rozkazy, zarządzenia i inne dokumenty organizacji i zakresu działania jednostek podległych.	A	Bc	
	5	Rozkazy, zarządzenia, wytyczne, instrukcje, regulaminy oraz inne dokumenty organizacyjno-merytoryczne.	A	Bc	
	6	Opinie własnych aktów normatywnych.	B10	-	
	7	Opinie zewnętrznych aktów normatywnych.	Bc	Bc	
	8	Wykładnie aktów prawnych.	A	Bc	
	9	Etaty jednostek.	A	Bc	
	10	Etaty ćwiczebne.	Bc	Bc	
	11	Zakresy działania (statuty).	A	Bc	
	12	Regulaminy pracy jednostki.	A	Bc	
	13	Schematy strukturalno-organizacyjne.	A	Bc	
	14	Ewidencja (dyslokacja) jednostek podległych.	A	Bc	
	15	Pisma okólne, biuletyny informacyjne i inne materiały powtarzalne, otrzymane z instytucji nadrzędnych lub jednostek podległych do wiadomości i służbowego wykorzystania.		Bc	

1		2	3	4	5
2		Dokumentacja operacyjna			
	1.	Dane o teatrach działań wojennych i kierunkach operacyjnych.	A	Bc	
	2.	Dane o armiach obcych.	A	Bc	
	3.	Materiały operacyjne dotyczące przygotowania teatru działań wojennych.	A	Bc	
	4.	Dane całościowe perspektywicznego rozwoju rodzajów wojsk i służb.	A	Bc	
	5.	Analizy i oceny sytuacji wojskowo-politycznej.	A	Bc	
	6.	Plany osiągania wyższych stanów gotowości bojowej jednostki.	Bc	Bc	
	7.	Plany rozmieszczenia i wyposażenia stałych obiektów wojskowych.	A	Bc	
	8.	Zasady maskowania wojsk.	A	Bc	
	9.	Dokumentacja służby operacyjnej i wewnętrznej jednostki.	BE5	Bc	
	10.	Zasady organizacji i prowadzenia działań bojowych.	A	Bc	
	11.	Dokumentacja współdziałania Sił Zbrojnych RP z siłami zbrojnymi innych państw.	A	Bc	
	12.	Dokumentacja współdziałania Sił Zbrojnych RP z NATO.	A	Bc	
	13.	Dokumentacja współdziałania Sił Zbrojnych RP z siłami zbrojnymi innych państw w ramach misji pokojowych, stabilizacyjnych i obserwacyjnych.	A	Bc	
3		Dokumentacja mobilizacyjna			
	1.	Rozkazy, zarządzenia, wytyczne, instrukcje dotyczące planowania i organizacji mobilizacji.	A	Bc	
	2.	Normatywy określające zadania mobilizacyjne komórki lub jednostki organizacyjnej.	A	Bc	
	3.	Plany mobilizacyjne jednostki z okresu poprzedzającego stan zagrożenia lub wojny.	A	Bc	
	4.	Plany mobilizacyjne jednostki czasu pokojowego.	Bc	Bc	
	5.	Dokumentacja roku obliczeniowego.	Bc	Bc	
4		Dokumentacja szkoleniowa			
	1.	Zasady planowania, organizacji i metodyki szkolenia.	A	Bc	
	2.	Normatywy określające zasady planowania, organizacji i metodyki szkolenia, otrzymane do służbowego wykorzystania: konspekty zajęć teoretycznych i praktycznych.	Bc	Bc	
	3.	Programy oraz plany szkolenia ogólnowojskowego i specjalistycznego, wieloletnie i roczne.	A	Bc	
	4.	Programy rozwoju szkolnictwa wojskowego.	A	Bc	
	5.	Plany i sprawozdania rozwoju bazy szkoleniowej, wieloletnie i roczne.	A	Bc	
	6.	Ewidencja ośrodków szkoleniowych.	A	Bc	
	7.	Plany i sprawozdania ze szkolenia poza wojskiem, wieloletnie i roczne.	A	Bc	
	8.	Analizy i oceny stanu wyszkolenia (całościowe) protokoły egzaminacyjne, świadectwa nauki.	A	Bc	

1		2	3	4	5
	9.	Sprawozdania, meldunki z realizacji szkolenia z jednostek podległych.	B10	Bc	
	10.	Podstawowa ewidencja szkolonych.	B50	-	
	11.	Dokumentacja ćwiczeń kompleksowych.	BE20	Bc	
	12.	Prace dyplomowe.	BE50	Bc	
	13.	Dokumentacja z ćwiczeń doskonalących.	Bc	Bc	
5		Dokumentacja planistyczno-sprawozdawcza			
	1.	Przepisy dotyczące organizacji oraz metodyki planowania i sprawozdawczości.	A	Bc	
	2.	Plany i sprawozdania wieloletnie oraz zmiany ustaleń planowych (wersje ostateczne).	A	Bc	
	3.	Projekty wstępne oraz opracowania robocze planów i sprawozdań.	Bc	Bc	
	4.	Plany i sprawozdania roczne jednostkowe jednostek zbiorcze.	A	Bc	
	5.	Plany i sprawozdania z jednostek podległych.	Bc	-	
	6.	Plany, sprawozdania z komórek i jednostek organizacyjnych, niewykorzystane w planach i sprawozdaniach całościowych.	A	Bc	
	7.	Materiały planistyczno-sprawozdawcze z komórek i jednostek organizacyjnych niewykorzystane w planach i sprawozdaniach całościowych.	Bc	Bc	
	8.	Plany i sprawozdania półroczne, kwartalne problemowych miesięczne.	Bc	Bc	
6		Dokumentacja statystyczna			
	1.	Zbiorcze opracowania zagadnień problemowych.	A	Bc	
	2.	Materiały źródłowe do opracowań statystycznych.	Bc	Bc	
	3.	Analizy i oceny statystyczne problemowe i kompleksowe.	A	Bc	
	4.	Analizy i oceny wycinkowe niewykorzystane w opracowaniach całościowych.	Bc	Bc	
7		Dokumentacja inspekcyjno-kontrolna			
	1.	Przepisy określające zasady prowadzenia inspekcji i kontroli.	A	Bc	
	2.	Protokoły oraz zarządzenia pokontrolne doraźnych kontroli kompleksowych i problemowych.	A	Bc	
	3.	Protokoły z kontroli doraźnych i wycinkowych.	BE10	Bc	
	4.	Protokoły oraz zarządzenia pokontrolne z kontroli kompleksowych i problemowych jednostek podległych.	A	Bc	
	5.	Meldunki z realizacji zaleceń pokontrolnych	A	Bc	
	6.	Harmonogramy z realizacji zaleceń pokontrolnych.	Bc	Bc	
	7.	Protokoły z kontroli gospodarki materiałowo-finansowej jednostki.	BE20	Bc	
	8.	Protokoły z kontroli wewnętrznych jednostki.	B10	Bc	

1		2	3	4	5
8		Dokumentacja działalności kadrowej			
	1.	Rozkazy, zarządzenia, wytyczne i inne dokumenty normujące służbę lub pracę w wojsku.	A	Bc	
	2.	Rozkazy personalne.	A	Bc	
	3.	Wyciągi z rozkazów personalnych.	Bc	Bc	
	4.	Zbiorcze zestawienia żołnierzy i pracowników wojska.	A	Bc	
	5.	Ewidencja żołnierzy i pracowników jednostki.	B50	-	
	6.	Zestawienia i analizy stanu osobowego z jednostek podległych.	Bc	Bc	
	7.	Analizy i oceny kadrowe.	A	Bc	
	8.	Skorowidze osobowe żołnierzy i pracowników wojska.	B 50	Bc	
	9.	Wykazy imienne żołnierzy i pracowników wojska.	Bc	Bc	
	10.	Protokoły przyjęcia - przekazania obowiązków kierownika komórki lub jednostki organizacyjnej.	A	Bc	
	11.	Protokoły przyjęcia - przekazania obowiązków osób funkcyjnych z komórek lub jednostek organizacyjnych.	B-10	Bc	
	12.	Teczki akt personalnych oficerów od stopnia pułkownika wzwyż.	A	-	
	13.	Teczki akt personalnych pozostałych żołnierzy zawodowych.	BE50	-	
	14.	Teczki akt personalnych pracowników wojska.	BE50	-	
	15.	Zbiorcze analizy i oceny próśb, skarg i wniosków.	A	Bc	
	16.	Ewidencja próśb skarg i wniosków.	B-10	-	
	17.	Prośby, skargi i wnioski.	Bc	Bc	
9.		Dokumentacja morale i dyscypliny wojskowej			
	1.	Meldunki i informacje o nastrojach	A	Bc	
	2.	Oceny i analizy morale żołnierzy	A	Bc	
	3.	Sprawozdania i oceny dyscypliny wojskowej	A	Bc	
	4.	Dokumentacja postępowań dyscyplinarnych wobec żołnierzy zasadniczej służby wojskowej, absolwentów szkoły wyższej odbywających przeszkolenie wojskowe lub żołnierzy rezerwy odbywających ćwiczenia wojskowe	B5		
	5.	Dokumentacja postępowań dyscyplinarnych wobec innych żołnierzy niż wymienieni w pkt 4	B 10	-	
	6.	Rejestr postępowań dyscyplinarnych	BE 15	-	
	7.	Rejestr wypadków, przestępstw i wykroczeń	A	-	
	8.	Meldunki o wypadkach i naruszeniach dyscypliny	BE 15	Bc	
	9.	Ewidencja meldunków o wypadkach i naruszeniach dyscypliny	B 15	-	
	10.	Meldunki o żołnierzach podejrzanych o popełnienie przestępstwa	B 15	Bc	
	11.	Ewidencja meldunków o żołnierzach podejrzanych o popełnienie przestępstwa	BE 15	-	
10		Dokumentacja katastrof i wypadków			
	1.	Dokumentacja katastrof, wypadków lotniczych i morskich oraz opisy i analiza przyczyn ich powstawania	A	Bc	
	2.	Meldunki o wypadkach drogowych i kolejowych	BE 15	Bc	
	3.	Meldunki o wypadkach związanych z dyslokacją i obsługą sprzętu wojskowego	BE 15	Bc	
	4.	Meldunki o wypadkach związanych z nieostrożnym obchodzeniem się z bronią	BE 15	Bc	

1		2	3	4	5
11		Dokumentacja działalności naukowo-badawczej			
	1.	Przepisy normujące działalność naukowo-badawczą.	A	Bc	
	2.	Programy prac naukowo-badawczych, wieloletnie i	A	Bc	
	3.	Opracowania końcowe prac naukowo-badawczych.	A	Bc	
	4.	Materiały pomocnicze wykorzystane w opracowaniach syntetycznych.	Bc	Bc	
	5.	Opracowania etapowe prac naukowo-badawczych, które nie znalazły odzwierciedlenia w opracowaniach końcowych.	A	Bc	
	6.	Opracowania naukowo-badawcze wykonane na zlecenie własnej komórki lub jednostki organizacyjnej.	A	Bc	
	7.	Opracowania naukowo-badawcze otrzymane do wiadomości i służbowego wykorzystania.	Bc	Bc	
	8.	Protokoły rad naukowych i komisji metodycznych.	A	Bc	
	9.	Ewidencja prac naukowo-badawczych.	A	-	
	10.	Dokumentacja obsługi działalności naukowo-badawczej i wydawniczej.	B-10	Bc	
	11.	Plany wydawnicze, wieloletnie i roczne.	A	Bc	
12		Dokumentacja wynalazczości i nowatorstwa			
	1.	Przepisy dotyczące wynalazczości i nowatorstwa.	A	Bc	
	2.	Sprawozdania, analizy i oceny wynalazczości i nowatorstwa.	A	Bc	
	3.	Protokoły komisji wynalazczości i nowatorstwa.	B10	Bc	
	4.	Ewidencja wniosków wynalazczych i nowatorskich -wdrożonych.	A	~	
13		Dokumentacja finansowa			
	1.	Przepisy ekonomiczno-finansowe.	A	Bc	
	2.	Zasady wynagradzania i premiowania żołnierzy zawodowych i pracowników wojska.	A	Bc	
	3.	Preliminarze, sprawozdania , analizy finansowe, wieloletnie i roczne instytucji centralnych, okręgów wojskowych, rodzajów sił zbrojnych.	A	Bc	
	4.	Preliminarze i sprawozdania finansowe oddziału gospodarczego.	B15	Bc	
	5.	Korespondencja uzgodnieniowa dotycząca należności i zadłużeń oddziału gospodarczego.	Bc	Bc	
	6.	Protokoły kontroli finansowej oddziału gospodarczego.	BE20	Bc	
	7.	Listy plac.	B50	-	
	8.	Karty zbiorcze płac.	B50	-	
	9.	Materiały źródłowe do obliczenia wysokości wynagrodzenia, premii i	Bc	Bc	
	10.	Listy zaopatrzenia finansowego żołnierzy zasadniczej służby wojskowej.	B50	Bc	
	11.	Ewidencja obrotu gotówkowego oddziału gospodarczego.	B10	-	
	12.	Dowody księgowania.	B3	Bc	
14		Dokumentacja gospodarki sprzętowo - materiałowej			
	1.	Przepisy normujące gospodarkę sprzętem i materiałami w wojsku.	A	Bc	
	2.	Tabele należności sprzętu i materiałów.	A	Bc	
	3.	Protokoły zdawczo-odbiorcze sprzętu i materiałów.	B10	Bc	
	4.	Asygnaty przychodowo-rozchodowe.	Bc	Bc	

1		2	3	4	5
	5.	Ewidencja sprzętu i materiałów oddziału gospodarczego.	B10	-	
	6.	Ewidencja sprzętu i materiałów pododdziału.	Bc	-	
	7.	Kartoteki magazynowe.	Bc	-	
	8.	Protokoły (spisy) inwentaryzacji sprzętu i materiałów.	B10	Bc	
	9.	Protokoły zużycia, brakowania sprzętu i materiałów.	B10	Bc	
	10.	Ewidencja oraz materiały wyjaśniające straty i szkody w mieniu wojskowym.	B10	Bc	
15		Dokumentacja inwestycyjna i eksploatacyjna			
	1.	Normatywy dotyczące projektowania, wykonawstwa i eksploatacji obiektów	A	Bc	
	2.	Zbiorcze zestawienia, analizy i oceny wykorzystania obiektów koszarowych i zasobów	A	Bc	
	3.	Dokumentacja eksploatacji nieruchomości wojskowych.	BE10	Bc	
	4.	Dokumentacja prawna i techniczno-eksploatacyjna obiektów zabytkowych oraz budowli o szczególnych rozwiązaniach konstrukcyjnych i walorach	A	Bc	
	5.	Dokumentacja wykonawcza, harmonogramy robót.	Bc	Bc	
	6.	Organizacja i programowanie prac projektowych.	A	Bc	
	7.	Protokoły zaawansowania prac projektowych.	Bc	Bc	
	8.	Ewidencja inwestycji.	A	-	
16		Dokumentacja współpracy krajowej i zagranicznej			
	1.	Ogólne zasady współpracy.	A	Bc	
	2.	Programy z pobytów delegacji i sprawozdania z przebiegu rozmów.	A	Bc	
	3.	Umowy i porozumienia dwustronne i wielostronne.	A	Bc	
	4.	Sprawozdania z realizacji umów.	A	Bc	
	5.	Dokumentacja obsługi delegacji zagranicznych.	B10	Bc	
	6.	Dokumentacja obsługi delegacji krajowych.	Bc	Bc	
17		Dokumentacja ochrony informacji niejawnych			
	1.	Rozkazy, zarządzenia i wytyczne w sprawie ochrony informacji niejawnych.	A	Bc	
	2.	Instrukcje kancelaryjne i archiwalne.	A	Bc	
	3.	Rzeczowe wykazy akt.	A	Bc	
	4.	Akta postępowań sprawdzających.	B10	-	
	5.	Trwale urządzenia ewidencyjne.	B10	-	
	6.	Pomocnicze urządzenia ewidencyjne.	Bc	-	
	7.	Protokoły kontroli stanu ochrony informacji niejawnych.	B10	Bc	
	8.	Oceny stanu ochrony informacji niejawnych.	B5	Bc	
	9.	Plany ochrony.	Bc	Bc	
	10.	Wykaz stanowisk i prac zleconych, z którymi wiąże się dostęp do informacji niejawnych oraz osób dopuszczonych do pracy lub służby na stanowiskach.	B10	Bc	
	11.	Protokoły z ocen dokumentacji niearchiwalnej.	B15	Bc	
	12.	Spisy akt przekazanych do archiwum, wydzielonych do zniszczenia.	B15	Bc	
	13.	Zezwolenia na zniszczenie dokumentacji niearchiwalnej.	B15	Bc	

1		2	3	4	5
18	Dokumentacja archiwów wojskowych				
	1.	Rozkazy, zarządzenia i wytyczne dotyczące organizacji i działalności archiwów wojskowych.	A	Bc	
	2.	Rejestry spisów akt.	A	-	
	3.	Spisy akt przekazanych do archiwum, wydzielonych do zniszczenia.	A	-	
	4.	Inwentarze archiwalne.	A	-	
	5.	Korespondencja w sprawach poświadczeń.	BE10	-	
	6.	Ewidencja akt udostępnionych.	Bc	-	
	7.	Korespondencja w sprawach selekcji, ekspertyz i niszczenia akt.	B10	-	

Załącznik Nr 2 do zarządzenia Nr 3/MON Ministra Obrony Narodowej
z dnia 2 lutego 2005 r. (póz. 4)

ZATWIERDZAM

Miejscowość, data.....

(kierownik komórki lub jedn. org.)

Protokół oceny dokumentacji niearchiwalnej

Komisja w składzie: (stopnie wojskowe, imiona, nazwiska i stanowiska służbowe członków komisji)

.....

.....

.....

.....

.....

dokonała ekspertyzy kwalifikacji dokumentacji niearchiwalnej kategorii „B", oznaczonej symbolem „B"/"Bc" * i stwierdza, że dokumentacja niearchiwalna wyszczególniona w załączonym spisie akt podlega zniszczeniu w skutek upłynięcia okresu jej przechowywania i utraty przydatności praktycznej.

Zał.:

Przewodniczący komisji : .....

Członkowie komisji: .....

.....

.....

(podpisy)

* - niepotrzebne skreślić

Załącznik Nr 3 do zarządzenia Nr 3/MON Ministra Obrony Narodowej
z dnia 2 lutego 2005 r. (póz. 4)

Miejscowość, data

(pieczęć nagłówkowa komórki lub jedn. org.)

Spis akt nr ...../..... *

(nazwa komórki lub jednostki organizacyjnej)

przekazanych do archiwum / wydzielonych do zniszczenia* *

Lp.	Nr teczki (dokumentu)	Tytuł teczki (dokumentu)	Kategoria archiwalna	Data		Ilość stron	Sygnatura archiwum wojskowego *	Uwagi
				RozpocZęto	Zakończono			
1	2	3	4	5	6	7	8	9

Razem pozycji..... (słownie)

Zgadzam się na przekazanie/zniszczenie** .....

akt wymienionych w spisie .....

.....
(podpis kierownika komórki lub jedn. org.)

.....
(podpisy: przyjmującego i zdającego
albo przewodniczącego komisji kwalifikacyjnej)

* - nadaje archiwum
** - niepotrzebne skreślić

Załącznik Nr 4 do zarządzenia Nr 3/MON Ministra Obrony Narodowej z dnia 2 lutego 2005 r. (póz. 4)

WZÓR

.....
(mowa komórki lub jednostki organizacyjnej)

.....
(nr wg RTD)

Teczka akt nr .....

.....
(symbol klasyfikacyjny i tytuł)

.....

(informacje o rodzaju dokumentacji zawartej w teczce)

KATEGORIA .....

Rozpoczęto dnia: .....

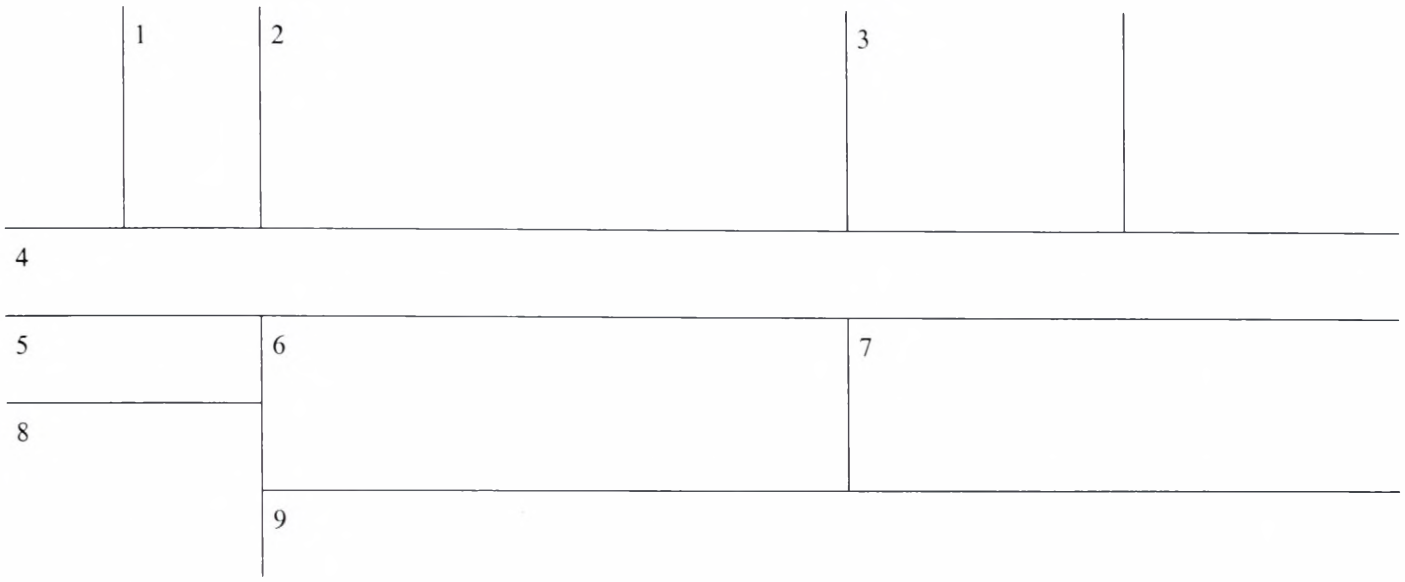
Zakończono dnia: .....

Ilość stron: .....

Załącznik Nr 5 do zarządzenia Nr 3/MON Ministra Obrony Narodowej
z dnia 2 lutego 2005 r. (póz. 4)

WZÓR

Karta inwentarzowa



Opis karty inwentarzowej:

1 - skrót nazwy archiwum

2 - nazwa zespołu (nazwa twórcy zespołu akt)

3 - sygnatura archiwalna

4 - tytuł jednostki odzwierciedlający jej zawartość

5 - daty skrajne opisywanej jednostki archiwalnej

6 - opis zewnętrzny (techniczny) jednostki archiwalnej m.in. ilość stron

7 - sygnatury dawne kancelaryjne i archiwalne w kolejności ich stosowania

8 - dodatkowe informacje istotne dla opisu jednostki archiwalnej

9 - uwagi (w tym słowa kluczowe i hasła służące do sporządzania innych pomocy archiwalnych)

Załącznik Nr 6 do zarządzenia Nr 3/MON Ministra Obrony Narodowej
z dnia 2 lutego 2005 r. (póz. 4)

WZÓR

Karta personalna

Stopień wojskowy .....

Nazwisko i imiona .....

.....

imię ojca .....

rok urodzenia .....

Nr teczki akt ..... **Sygn. archiwum** ..... *

Uwagi:

* - nadaje archiwum

Załącznik Nr 7 do zarządzenia Nr 3/MON Ministra Obrony Narodowej
z dnia 2 lutego 2005 r. (póz. 4)

ZATWIERDZAM

Miejscowość, data.....

(kierownik komórki lub jedn. org.)

Protokół oceny dokumentacji niearchiwalnej

Komisja w składzie: (stopnie wojskowe, imiona, nazwiska i stanowiska służbowe członków komisji)

.....

.....

.....

.....

.....

dokonała ekspertyzy kwalifikacji dokumentacji niearchiwalnej kategorii „B", oznaczonej symbolem „B"/"Bc" * i stwierdza, że dokumentacja niearchiwalna wyszczególniona w załączonym spisie akt podlega zniszczeniu w skutek upłynięcia okresu jej przechowywania i utraty przydatności praktycznej.

Zał.:

Przewodniczący komisji : .....

Członkowie komisji: .....

.....

.....

(podpisy)

- - niepotrzebne skreślić

Załącznik Nr 8 do zarządzenia Nr 3/MON Ministra Obrony Narodowej
z dnia 2 lutego 2005 r. (póz.

(nazwa komórki lub jednostki organizacyjnej)

REJESTR SPISÓW AKT

Rozpoczęto dnia: .....
Zakończono dnia: .....

stron: ...../ .....
(słownie)

Lp.	Data spisu akt	Nazwa komórki lub jednostki organizacyjnej.	Rok powstania akt	Ilość teczek		Rozliczenie z akt			Rozmieszczenie akt			Uwagi
				Wg spisu akt	przyjętych	zniszczono	przekazano	pozostało	sala	szafa	pion	
1	2	3	4	5	6	7	8	9	10	11	12	13

Załącznik Nr 9 do zarządzenia Nr 3/MON Ministra Obrony Narodowej
z dnia 2 lutego 2005 r. (póz. 4

WZÓR

Wzór pierwszej i drugiej strony zezwolenia na zniszczenie

..... Miejscowość, data .....
nazwa archiwum wojskowego

ZEZWOLENIE

Wyrażam zgodę/nie wyrażam zgody* na zniszczenie dokumentacji niearchiwalnej wyszczególnionej w spisie akt nr ..... / .....oprócz poz. .....

.....

.....

.....

.....

.....
(szef, kierownik archiwum wojskowego)

m. p.

* - niepotrzebne skreślić

Stwierdza się, że dokumentacja niearchiwalna wymieniona w spisie akt nr ..... / ..... została w naszej obecności zniszczona przez .....
(sposób zniszczenia)

w dniu ..... w .....
(nazwa instytucji niszczącej)

Przewodniczący: .....

Członkowie: .....

.....

DECYZJA Nr 390/MON

MINISTRA OBRONY NARODOWEJ

z dnia 28 września 2006 r.

w sprawie ograniczeń w używaniu urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w komórkach i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426) ustala się, co następuje:

1. Użyte w decyzji określenia oznaczają:

1) strefa administracyjna — strefę, o której mowa w art. 57 pkt 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 oraz z 2006 r. Nr 104, poz. 708 i 711 i Nr 149, poz. 1078), zwanej dalej „ustawą";

2) specjalna strefa bezpieczeństwa — strefę, o której mowa w art. 58 ust. 1 ustawy;

3) strefa bezpieczeństwa klasy I — strefę, o której mowa w § 9 ust. 4 pkt 1 rozporządzenia 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 (Dz. U. Nr 215, poz. 1821), zwanego dalej „rozporządzeniem";

4) strefa bezpieczeństwa klasy II — strefę, o której mowa w § 9 ust. 4 pkt 2 rozporządzenia.

2. W komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych zabrania się wnoszenia służbowych i prywatnych urządzeń służących do rejestracji obrazu lub dźwięku, kopiowania lub transmisji informacji, w tym dyktafonów, telefonów komórkowych i telefonów bezprzewodowych, z wyjątkiem urządzeń będących na wyposażeniu pomieszczeń służbowych, do:

1) stref bezpieczeństwa klasy I;

2) specjalnych stref bezpieczeństwa;

3) sal konferencyjnych, sal odpraw, pomieszczeń użytkowanych przez osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej przez ich sekretariaty oraz kierowników (dyrektorów, szefów, komendantów, prezesów, dowódców) jednostek lub komórek organizacyjnych — podczas prowadzenia w nich odpraw, narad i spotkań służbowych, których przedmiotem są informacje niejawne.

3. Zezwala się na korzystanie — za zgodą — ze służbowych telefonów komórkowych w strefach bezpieczeństwa klasy II, przy czym:

1) zgodę wydają kierownicy (dyrektorzy, szefowie, komendanci, prezesi, dowódcy) jednostek lub komórek organizacyjnych, o których mowa w pkt 2, zwani dalej „kierownikami jednostek (komórek) organizacyjnych" i zamieszczają ją w rozkazie dziennym (decyzji) prowadzonym na szczeblu jednostki (komórki) organizacyjnej;

2) zgoda obejmuje strefy bezpieczeństwa klasy II we wszystkich komórkach organizacyjnych Ministerstwa Obrony Narodowej oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

3) zgoda powinna zawierać: dane osoby której przydziela się telefon (stopień wojskowy, imię i nazwisko), rodzaj (typ) aparatu (nazwę firmy) i jego numer fabryczny oraz nazwę operatora sieci telefonicznej i numer telefonu;

4) zabrania się dokonywać jakichkolwiek zmian w konfiguracji przydzielonego telefonu;

5) użytkownik telefonu powinien posiadać przy sobie wyciąg z rozkazu (decyzji) zawierający zgodę, o której mowa w ppkt 1.

4. W przypadkach szczególnych, uzasadnionych ważnymi względami losowymi lub charakterem realizowanych zadań służbowych, na pisemny wniosek zainteresowanej osoby, kierownik jednostki (komórki) organizacyjnej może zezwolić tej osobie na posługiwanie się telefonem prywatnym w strefach bezpieczeństwa klasy II macierzystej jednostki (komórki) organizacyjnej, w ściśle określonym (niezbędnym) czasie.

5. Zgodę na jednorazowe (okresowe) wniesienie i korzystanie na terenie stref bezpieczeństwa klasy II danej jednostki (komórki) organizacyjnej z innych niż wymienione w pkt 3 urządzeń służbowych służących do rejestracji obrazu lub dźwięku, kopiowania lub transmisji informacji, niezbędnych do realizacji zadań, wydają w postaci pisemnego zezwolenia kierownicy jednostek (komórek) organizacyjnych.

6. W przypadkach organizowania w pomieszczeniach położonych w strefach bezpieczeństwa klasy II konferencji prasowych, spotkań i innych tego rodzaju przedsięwzięć z udziałem przedstawicieli mediów, za zgodą organizatorów dopuszcza się wnoszenie przez nich urządzeń, o których mowa w pkt 2, stanowiących ich narzędzia pracy i korzystanie z nich, pod warunkiem zapewnienia stałego nadzoru i przebywania tych osób w ściśle określonych miejscach (rejonie).

7. Osoby przybyłe do jednostki lub komórki organizacyjnej (goście, interesanci) oddają do depozytu urządzenia służące do rejestracji obrazu lub dźwięku, kopiowania lub transmisji informacji, na które nie mają pozwolenia na ich użytkowanie w strefach bezpieczeństwa klasy II. Informacja o obowiązku zdeponowania tego rodzaju urządzeń powinna być umieszczona w widocznym miejscu.

8. Kierownicy jednostek organizacyjnych oraz Dyrektor Generalny Ministerstwa Obrony Narodowej w odniesieniu do komórek organizacyjnych Ministerstwa, spowodują:
1) zorganizowanie w strefach administracyjnych, zgodnie z wytycznymi opracowanymi przez podległych im pełnomocników do spraw ochrony informacji niejawnych, punktów depozytowych (szafki depozytowe, itp.) dla służbowych i prywatnych urządzeń służących do rejestracji obrazu lub dźwięku, kopiowania lub transmisji informacji, w tym telefonów komórkowych — dla osób, o których mowa w pkt 7, w ramach posiadanych przez siebie środków finansowych;
2) sukcesywne wyposażanie obiektów, w miarę przydzielanych na ten cel środków finansowych, w urządzenia (bramki) do wykrywania m.in. telefonów komórkowych oraz sal konferencyjnych (odpraw) w urządzenia do zakłócania pracy telefonów komórkowych;
3) oznakowanie stref bezpieczeństwa.

9. Decyzja wchodzi w życie z dniem 1 stycznia 2007 r.

DECYZJA Nr 488/MON

MINISTRA OBRONY NARODOWEJ

z dnia 30 listopada 2006 r.

w sprawie wprowadzenia do użytku w resorcie obrony narodowej „Tymczasowej instrukcji organizacji obiegu informacji niejawnych o klauzuli zastrzeżone w resortowej sieci teleinformatycznej MIL-WAN"

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w związku z art. 20 pkt 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 oraz z 2006 r. Nr 104, poz. 708 i 711 i Nr 149, poz. 1078) ustala się, co następuje:

1. Wprowadza się do użytku w resorcie obrony narodowej „Tymczasową instrukcję organizacji obiegu informacji niejawnych o klauzuli zastrzeżone w resortowej sieci teleinformatycznej MIL-WAN", stanowiącą załącznik do decyzji.

2. Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

---

* Po upływie 6 miesięcy od wejścia instrukcji w życie zainteresowane instytucje dokonają oceny jej funkcjonowania.

TYMCZASOWA INSTRUKCJA ORGANIZACJI OBIEGU INFORMACJI NIEJAWNYCH O KLAUZULI ZASTRZEŻONE W RESORTOWEJ SIECI TELEINFORMATYCZNEJ MIL-WAN*)

Postanowienia ogólne

1. Resortowa sieć teleinformatyczna MIL-WAN jest przeznaczona do wymiany (transmisji) informacji do klauzuli „Zastrzeżone" włącznie pomiędzy jednostkami i komórkami organizacyjnymi resortu obrony narodowej. Postanowienia instrukcji normują wytwarzanie, przekazywanie, odbieranie oraz ewidencjonowanie informacji (dokumentów) jawnych oraz o klauzuli „Zastrzeżone".

2. Określenia użyte w instrukcji oznaczają:

1) nośnik elektroniczny — materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej;

2) dokument (informacja) roboczy — informacja pozostająca w fazie opracowywania, dotycząca roboczych wersji (projektów) dokumentów, nie posiadająca podpisu osoby uprawnionej lub upoważnionej do jej akceptacji;

3) dokument (informacja) finalny — dokument autoryzowany (podpisany lub zatwierdzony) przez osobę uprawnioną lub upoważnioną do wykonywania tej czynności — pozostający w aktach;

4) informacja systemowa — informacja zabezpieczająca realizację czynności organizacyjno-technologicznych oraz kontrolnych w sieci teleinformatycznej, mająca bezpośredni wpływ na jej prawidłowe funkcjonowanie oraz bezpieczeństwo przetwarzanych w sieci informacji;

5) autoryzacja dokumentu — podpisanie lub zatwierdzenie dokumentu przez uprawnioną lub upoważnioną osobę;

6) kancelaria — komórka lub wyznaczona osoba funkcyjna odpowiedzialna za przyjmowanie, rejestrowanie, przechowywanie, obieg i udostępnianie dokumentów o klauzuli „Zastrzeżone" w jednostce lub komórce organizacyjnej;

7) kancelaria elektroniczna — zestaw komputerowy podłączony do sieci MIL-WAN i posiadający adres elektroniczny w tej sieci, obsługiwany przez operatora poczty uprawnionego do przekazywania i odbierania wersji elektronicznych informacji finalnych do innych adresatów w sieci oraz umożliwiający przechowywanie, drukowanie lub kopiowanie informacji niejawnych wysyłanych i odbieranych za jej pośrednictwem. Każdej kancelarii elektronicznej przyporządkowany jest unikalny adres na serwerze MSExchange (np: kancelaria.elektroniczna.XXXXX@umon.wp.pl, gdzie XXXXX — oznacza nazwę komórki organizacyjnej w Urzędzie Ministra Obrony Narodowej obsługiwanej przez tę kancelarię elektroniczną; kancelaria.elektroniczna.XXXXX@dmw.wp.pl — oznacza nazwę komórki w Dowództwie Marynarki Wojennej obsługiwanej przez tę kancelarię elektroniczną). Umieszczenie adresu kancelarii elektronicznej w książce adresowej poczty elektronicznej oznacza jej gotowość do pracy;

8) operator poczty — pracownik z kancelarii lub inna osoba (osoby) uprawniona decyzją/rozkazem kierownika jednostki (komórki) organizacyjnej do odbierania i wysyłania elektronicznych wersji dokumentów finalnych poprzez kancelarię elektroniczną;

9) DEWD — Dziennik Ewidencji Wykonanych Dokumentów;

10) RWD — Rejestr Wydanych Dokumentów.

Zasady wykorzystania sieci MIL-WAN do wymiany informacji niejawnych o klauzuli „ZASTRZEŻONE"

3. W każdej jednostce (komórce) organizacyjnej wykorzystującej sieć MIL-WAN do przekazywania i odbierania informacji niejawnych o klauzuli „ZASTRZEŻONE" należy:

1) zapewnić, aby zestaw komputerowy przeznaczony do pełnienia funkcji kancelarii elektronicznej był włączony w godzinach służbowych i sukcesywnie sprawdzany na obecność przychodzącej poczty; wskazane jest, aby zestaw znajdował się w pomieszczeniu kancelarii obsługującej daną jednostkę/komórkę organizacyjną;

2) wyznaczyć — w miarę możliwości — przynajmniej jeden zestaw komputerowy do pełnienia roli zapasowej kancelarii elektronicznej; elektroniczny adres kancelarii (zasadniczej i zapasowej) ustalany jest przez administratora sieci MIL-WAN w porozumieniu z pełnomocnikiem do spraw ochrony informacji niejawnych jednostki organizacyjnej.

4. Elektroniczna wersja informacji finalnej przesyłana pocztą elektroniczną jest traktowana jako dokument podpisany lub zatwierdzony (autoryzowany) przez uprawnioną lub upoważnioną osobę.

5. Pisma korespondencyjne (przewodnie), przeznaczone do przesyłania przez sieć MIL-WAN, wykonawca sporządza w ustalonym przez organizatora sieci — co do wersji pakiecie biurowym — lub programie pocztowym i oznacza jako wykonane w egzemplarzu pojedynczym.

6. Załączniki dołączane do pisma przewodniego sporządza się w formacie uzgodnionym z adresatem, umożliwiającym ich odtworzenie lub dalsze przetwarzanie.

7. Wszystkie dokumenty przeznaczone do przesyłania siecią MIL-WAN (pisma przewodnie i edytowalne załączniki) oznacza się zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 205, poz. 1696).

8. Informacje niejawne (dokumenty) finalne przesyła się tylko przez operatora poczty i tylko do adresatów ujętych w rozdzielnikach (zamieszczanych w pismach lub przy dużej ilości adresatów sporządzanych na oddzielnym dokumencie).

9. Zezwala się na przesyłanie niejawnych informacji roboczych pomiędzy użytkownikami sieci MIL-WAN bez pisma przewodniego.

10. Wszystkie wydrukowane informacje niejawne są ewidencjonowane przez osobę wykonującą te czynności w DEWD przeznaczonym do ewidencji dokumentów wytworzonych w kancelarii elektronicznej lub w którym są ewidencjonowane dokumenty wytwarzane na stacji roboczej użytkownika sporządzającego dokument.

11. Wykorzystanie sieci MIL-WAN do zdalnego użytkowania systemów teleinformatycznych lub przesyłania informacji niejawnych pomiędzy systemami teleinformatycznymi różnych szczebli kierowania (dowodzenia) może być realizowane po dokonaniu uzgodnień organizatorów tych systemów z administratorem sieci MIL-WAN; uzgodnienia te powinny być zawarte w dokumentacji eksploatacyjnej tych systemów oraz ich szczególnych wymaganiach bezpieczeństwa (SWB) i procedurach bezpiecznej eksploatacji (PBE).

12. Dopuszcza się stosowanie w sieci MIL-WAN jawnych nośników elektronicznych oznaczonych napisem „JAWNE", ale wyłącznie do przetwarzania, przechowywania lub przekazywania informacji jawnych.

13. Używanie nie zarejestrowanych lub nie oznaczonych nośników informacji jest dozwolone tylko w przypadku, gdy zawierają one licencjonowane lub dopuszczone pisemnym rozkazem, decyzją itp. oprogramowanie lub dane niezbędne do jego użytkowania. Przed włożeniem do stacji roboczej nośniki te muszą mieć włączoną blokadę zapisu (posiadać właściwość) uniemożliwiającą zapisywanie na nich informacji.

14. Ewidencjonowanie oraz postępowanie z nośnikami elektronicznymi uzależnia się od rodzaju zapisywanych na nich informacji:

1) informacje robocze zapisuje się na dysku twardym komputera przeznaczonego do pełnienia funkcji kancelarii elektronicznej lub stacji roboczej użytkownika, albo na nośnikach będących w bieżącym użytkowaniu wykonawców;

2) elektroniczne wersje informacji finalnych przeznaczone do archiwizacji zapisuje się na dysku twardym komputera przeznaczonego do pełnienia funkcji kancelarii elektronicznej i sukcesywnie, zgodnie z instrukcją „Zasady zakładania kont poczty elektronicznej w systemie teleinformatycznym MIL-WAN" wydaną przez Szefa Generalnego Zarządu Dowodzenia i Łączności, zapisuje się na zarejestrowanych, odpowiednio oznaczonych zewnętrznych nośnikach elektronicznych. Informacje przeznaczone do archiwizacji nie mogą być modyfikowane, zmieniane ani kasowane, nie można zmieniać przeznaczenia nośnika i używać do zapisywania innych informacji — nie przeznaczonych do archiwizacji. Nośnikowi zewnętrznemu zakłada się i prowadzi „Metrykę elektronicznego nośnika informacji", na zasadach określonych w § 24 pkt 3 zarządzenia Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 21, poz. 203).

Wytwarzanie, ewidencjonowanie, wysyłanie i odbieranie autoryzowanych dokumentów (informacji) niejawnych:

15. Wytwarzanie, ewidencjonowanie i wysyłanie dokumentów:

1) wykonawca opracowuje treść merytoryczną dokumentu, oznaczając go jako „Egz. pojedynczy", wpisuje do dokumentu numer ewidencyjny zgodnie z DEWD, w którym zarejestrował wytworzony dokument oraz nanosi pozostałe, wymagane oznaczenia, wpisuje adresatów pisma albo w przypadku wielu adresatów opracowuje oddzielny rozdzielnik i drukuje dokument wraz z rozdzielnikiem;

2) po wydrukowaniu, uzupełnia ewidencję w DEWD i przedstawia dokument do autoryzacji (podpisania lub zatwierdzenia);

3) po uzyskaniu autoryzacji, przekazuje dokument do kancelarii celem zarejestrowania w „Dzienniku Korespondencji";

4) uzupełnia wersję elektroniczną dokumentu o datę podpisania, numer kancelaryjny i datę zarejestrowania pisma w „Dzienniku korespondencji" oraz wpisuje znak „(—)" przed nazwiskiem osoby podpisującej; wzory oznaczenia przez wykonawcę dokumentów (informacji) przygotowanych do przesłania w formie elektronicznej określają załączniki Nr 1a i Nr 3a;

5) nadaje dokumentowi status „tylko do odczytu" i przekazuje go operatorowi poczty wraz z podpisanym dokumentem tradycyjnym (finalnym), wpisując uprzednio na nim symbol klasyfikacyjny teczki, w której ma on być, zgodnie z rzeczowym wykazem akt, przechowywany w aktach;

6) operator poczty kopiuje dane z nośnika elektronicznego (jeżeli dokument do wysłania znajdował się na nośniku zewnętrznym) na dysk twardy i zwraca nośnik wykonawcy;

7) przesyła dokument, za pomocą sieci MIL-WAN, do kancelarii elektronicznej adresata (kancelarii elektronicznych adresatów umieszczonych w rozdzielniku);

8) po potwierdzeniu przez serwer pocztowy dostarczenia przesyłki, operator poczty u dołu na ostatniej stronie pisma finalnego wpisuje: „przesłano w formie elektronicznej", datę, godzinę, imię i nazwisko oraz składa podpis, a następnie przekazuje pismo do kancelarii, wraz z załączonym potwierdzeniem (potwierdzeniami w przypadku dwóch lub więcej adresatów) serwera o dostarczeniu przesyłki do adresata, wzory oznaczenia dokumentów finalnych u nadawcy określają załączniki Nr 1 i Nr 3;

9) operator poczty, w przypadku braku możliwości przesłania wersji elektronicznej dokumentu do adresata za pomocą sieci MIL-WAN, powiadamia o tym wykonawcę dokumentu celem podjęcia przedsięwzięć zapewniających jego przesłanie do adresata;

10) kancelaria umieszcza wydrukowany (podpisany lub zatwierdzony) dokument wraz z załączonym potwierdzeniem (potwierdzeniami) serwera o dostarczeniu przesyłki w teczce, zgodnie z adnotacją wykonawcy dokumentu.

16. Odbieranie i ewidencjonowanie dokumentów (informacji):

1) operator poczty jest zobowiązany do systematycznego sprawdzania skrzynki odbiorczej w kancelarii elektronicznej;

2) po otrzymaniu przesyłki ustala plik, znajdujący się w skrzynce odbiorczej, zawierający pismo korespondencyjne (przewodnie), wyświetla je na monitorze i po stwierdzeniu, że dokument przesłano do właściwego adresata drukuje go na zestawie komputerowym kancelarii elektronicznej;

3) niejawne pismo korespondencyjne (przewodnie) ewidencjonuje w DEWD i wpisuje numer pozycji z DEWD na pierwszej stronie pisma;

4) z pismami przewodnimi zawierającymi informacje jawne postępuje według zasad określonych przez kierownika jednostki (komórki) organizacyjnej;

5) drukuje lub kopiuje na nośniki elektroniczne albo dysk twardy zestawu komputerowego kancelarii elektronicznej załączniki do pisma oraz ewidencjonuje w DEWD wydrukowane niejawne załączniki;

6) wpisuje na pierwszej stronie każdego wydrukowanego (niejawnego) załącznika Nr z DEWD;

7) dokonuje wpisu w „Metryce elektronicznego nośnika informacji" o skopiowanych informacjach na nośnik elektroniczny — jeżeli jest ona dla tego nośnika prowadzona;

8) wpisuje na ostatniej stronie pisma przewodniego informacje o wydrukowanych lub skopiowanych załącznikach, według wzoru określonego w załączniku Nr 4;

9) wpisuje datę i godzinę odbioru przesyłki na piśmie korespondencyjnym (przewodnim i załącznikach) oraz składa pod nimi podpis; wzory oznaczenia odebranych u adresata i wydrukowanych informacji określają załączniki Nr 2 i Nr 4;

10) przekazuje pismo korespondencyjne (przewodnie oraz wydrukowane lub skopiowane na nośniki elektroniczne załączniki) do kancelarii;

11) kancelaria ewidencjonuje pismo w „Dzienniku korespondencji", wpisując dodatkowo:

a) w kolumnie dziewiątej — „otrzymano z MIL-WAN"

b) w kolumnie trzynastej — Nr RWD zewnętrznego nośnika elektronicznego, na który skopiowano załączniki — jeżeli czynność taka była wykonywana;

12) operator odbieranej poczty w przypadku stwierdzenia przesłania dokumentu na błędny adres:

a) przesyła do operatora poczty wysyłającego informację o błędnie wysłanym dokumencie, podając jego dane ewidencyjne (Nr wychodzący i datę podpisania),

b) wymazuje (kasuje) błędnie przesłane informacje z pamięci zestawu komputerowego kancelarii elektronicznej lub skopiowane na zewnętrzne nośniki elektroniczne (jeżeli informacje na te nośniki zostały skopiowane),

c) niszczy wydrukowane dokumenty przesłane na błędny adres; fakt zniszczenia dokumentów niejawnych odnotowuje, w tym DEWD, w którym zostały one zaewidencjonowane, za podpisem dwóch osób zgodnie z § 29 pkt 2, 3, 4 zarządzenia Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r.

Załączniki

Załącznik Nr 1

Wzór pisma finalnego (u nadawcy)

Nazwa jednostki (instytucji)

Sygnatura komórki/jednostki organizacyjnej

Nr rejestracyjny/rok
data rejestracji

.....
(nazwa miejscowości, data)
ZASTRZEŻONE
Egz. pojedynczy

Adresaci wg rozdzielnika

Dot: ćwiczenia „Odra 2006".

Treść pisma

WZÓR

DYREKTOR

.....
płk Jan MAŁECKI

Przesłano w formie elektronicznej
data, godzina, imię, nazwisko podpis operatora poczty

Wykonano w 1 egz. – a/a
Sporządził i wykonał: ppłk Klasa
Adresaci wersji elektronicznej (35 kB):
Dowódca JW 3456
Dowódca JW 5678
Dowódca JW 6745

RWD 12/Z-16/Z-32/06

Załącznik Nr 1a

Wzór elektronicznej wersji pisma przygotowanej do przesłania u nadawcy

Nazwa jednostki (instytucji)

Sygnatura komórki/jednostki organizacyjnej

Nr rejestracyjny/rok data rejestracji

.....
(nazwa miejscowości, data)

ZASTRZEŻONE

Egz. pojedynczy

Adresaci wg rozdzielnika

Dot: ćwiczenia „Odra 2006".

Treść pisma

WZÓR

DYREKTOR

(-) płk Jan MAŁECKI

Wykonano w 1 egz. – a/a
Sporządził i wykonał: ppłk Klasa
Adresaci wersji elektronicznej (35 kB):
Dowódca JW 3456
Dowódca JW 5678
Dowódca JW 6745

RWD 12/Z-16/Z-32/06

ZASTRZEŻONE Str. 1/1

Załącznik Nr 2

Wzór pisma wydrukowanego i zaewidencjonowanego u adresata w *„Dzienniku Korespondencji"*

Nazwa jednostki (instytucji)

Sygnatura komórki/jednostki organizacyjnej

Nr rejestracyjny/rok data rejestracji

Nr rejestracyjny data rejestracji

.....
(nazwa miejscowości, data)

ZASTRZEŻONE

Egz. pojedynczy

Adresaci wg rozdzielnika

Dot: ćwiczenia „Odra 2006".

Treść pisma

WZÓR

Pismo – wydrukowano i zaewidencjonowano w DEWD Nr RWD ..... – na 1 str.

DYREKTOR

(-) płk Jan MAŁECKI

Wykonano w 1 egz. – a/a
Sporządził i wykonał: ppłk Klasa
Adresaci wersji elektronicznej (35 kB):
Dowódca JW 3456
Dowódca JW 5678
Dowódca JW 6745

Odebrał:
data, godzina, imię, nazwisko, podpis operatora poczty

RWD 12/Z-16/Z-32/06

ZASTRZEŻONE Str. 1/1

Załącznik Nr 3

Wzór pisma finalnego (u nadawcy)

Nazwa jednostki (instytucji)

Sygnatura komórki/jednostki organizacyjnej

Nr rejestracyjny/rok data rejestracji

.....
(nazwa miejscowości, data)

ZASTRZEŻONE

Egz. pojedynczy

„jawne po odłączeniu załączników"

Adresat

Dot.: planu modernizacji obiektów kompleksu Nr 4.

Treść pisma

W załączeniu przesyłam do służbowego wykorzystania dokumentację dotyczącą planu modernizacji obiektów Kompleksu Nr 4 w postaci następujących plików:

- Plan modernizacji kompleksu Nr 4.doc (wyk. Word 97),
- Szkic kompleksu Nr 4.cdr (wyk. CorelDRAW 9),
- Rzuty pionowe bloków Nr 1, 2, 3.cdr (wyk. CorelDRAW 9),
- Zestawienie kosztów.xls (wyk. Excel 97).

Załączniki:

- Zał. Nr 1 — Zastrzeżone — Nr RWD 28/Z-5/Z-1/06 – Plan modernizacji kompleksu Nr 4 na 34 str. – do akt, wersja elektroniczna — Plan modernizacji kompleksu Nr 4.doc /389kB/ — tylko adresat,
- Zał. Nr 2 — Zastrzeżone — Nr RWD 28/Z-5/Z2/06 — Szkic kompleksu Nr 4 — do akt, — wersja elektroniczna — Szkic kompleksu Nr 4.cdr (232kB) — tylko adresat,
- Zał. Nr 3 — Zastrzeżone — Nr RWD 28/Z-5/Z-3/06 — Rzuty pionowe bloków — do akt, — wersja elektroniczna — Rzuty pionowe bloków.cdr (432kB) — tylko adresat.
- Zał. Nr 4 — Jawne — Zestawienie kosztów na 11 str. — do akt, — wersja elektroniczna — Zestawienie kosztów.xls — (456kB) — tylko adresat.

DYREKTOR

.....
płk Stefan ŻAK

Wykonano w 1 egz. - a/a
Wersja elektroniczna — 30 kB — adresat
Sporządził i wykonał: mjr Kłos

Przesłano w formie elektronicznej
data, godzina, imię, nazwisko, podpis
operatora poczty

ZASTRZEŻONE Str. 1/1

Załącznik Nr 3a

Wzór elektronicznej wersji pisma przygotowanego do przesłania u nadawcy

Nazwa jednostki (instytucji)

Sygnatura komórki/jednostki organizacyjnej

Nr rejestracyjny/rok data rejestracji

.....
(nazwa miejscowości, data)

ZASTRZEŻONE

Egz. pojedynczy

„jawne po odłączeniu załączników"

Adresat

Dot.: planu modernizacji obiektów kompleksu Nr 4.

Treść pisma

W załączeniu przesyłam do służbowego wykorzystania dokumentację dotyczącą planu modernizacji obiektów Kompleksu Nr 4 w postaci następujących plików:

- Plan modernizacji kompleksu Nr 4.doc (wyk. Word 97),
- Szkic kompleksu Nr 4.cdr (wyk. CorelDRAW 9),
- Rzuty pionowe bloków Nr 1, 2, 3.cdr (wyk. CorelDRAW 9),
- Zestawienie kosztów.xls (wyk. Excel 97).

Załączniki:

- Zał. Nr 1 — Zastrzeżone — Nr RWD 28/Z-5/Z-1/06 –Plan modernizacji kompleksu Nr 4 na 34 str. – do akt, wersja elektroniczna — Plan modernizacji kompleksu Nr 4.doc /389kB/ — tylko adresat,
- Zał. Nr 2 — Zastrzeżone — Nr RWD 28/Z-5/Z-2/06 — Szkic kompleksu Nr 4 — do akt, — wersja elektroniczna — Szkic kompleksu Nr 4.cdr (232kB) — tylko adresat,
- Zał. Nr 3 — Zastrzeżone — Nr RWD 28/Z-5/Z-3/06 — Rzuty pionowe bloków — do akt, — wersja elektroniczna — Rzuty pionowe bloków.cdr (432kB) — tylko adresat.
- Zał. Nr 4 — Jawne — Zestawienie kosztów na 11 str. — do akt, — wersja elektroniczna — Zestawienie kosztów.xls — (456kB) — tylko adresat.

DYREKTOR

(-) płk Stefan ŻAK

Wykonano w 1 egz. - a/a
Wersja elektroniczna — 30 kB — adresat
Sporządził i wykonał: mjr Kłos

ZASTRZEŻONE Str. 1/1

Załącznik Nr 4

Wzór pisma wydrukowanego i zaewidencjonowanego u adresata w *„Dzienniku Korespondencji"*

Nazwa jednostki (instytucji)

.....
(nazwa miejscowości, data)

ZASTRZEŻONE
Egz. pojedynczy

„jawne po odłączeniu załączników"

Sygnatura komórki/jednostki organizacyjnej	Nr rejestracyjny/rok data rejestracji	Nr rejestracyjny data rejestracji

Adresat

Dot.: planu modernizacji obiektów kompleksu Nr 4.

W załączeniu przesyłam do służbowego wykorzystania dokumentację dotyczącą planu modernizacji obiektów Kompleksu Nr 4 w postaci następujących plików:

- Plan modernizacji kompleksu Nr 4.doc (wyk. Word 97),
- Szkic kompleksu Nr 4.cdr (wyk. CorelDRAW 9),
- Rzuty pionowe bloków Nr 1, 2, 3.cdr (wyk. CorelDRAW 9),
- Zestawienie kosztów.xls (wyk. Excel 97).

Załączniki:

- Zał. Nr 1 – Zastrzeżone – Nr RWD 28/Z-5/Z-1/06 – Plan modernizacji kompleksu Nr 4 na 34 str. – do akt, wersja elektroniczna – Plan modernizacji kompleksu Nr 4.doc /389kB/ – tylko adresat,
- Zał. Nr 2 – Zastrzeżone – Nr RWD 28/Z-5/Z-2/06 – Szkic kompleksu Nr 4 – do akt, – wersja elektroniczna – Szkic kompleksu Nr 4.cdr (232kB) – tylko adresat,
- Zał. Nr 3 – Zastrzeżone – Nr RWD 28/Z-5/Z-3/06 – Rzuty pionowe bloków – do akt, – wersja elektroniczna – Rzuty pionowe bloków.cdr (432kB) – tylko adresat.
- Zał. Nr 4 – Jawne – Zestawienie kosztów na 11 str. – do akt, – wersja elektroniczna – Zestawienie kosztów.xls – (456kB) – tylko adresat.

DYREKTOR

(-) płk Stefan ŻAK

Wykonano w 1 egz. - a/a
Wersja elektroniczna – 30 kB – adresat
Sporządził i wykonał: mjr Kłos

Odebrał:
data, godzina, imię, nazwisko,
podpis operatora poczty

Zał. Nr 1 – wydrukowano i zaewidencjonowano w DEWD Nr RWD 13/Z-45/Z-20/06 – na 34 str.
Zał. Nr 2 i zał. Nr 3 skopiowano na CD-R Nr RWD 23/Z-14/06
Zał. Nr 4 – wydrukowano – na 11 str.

ZASTRZEŻONE Str. 1/1

WYTYCZNE
MINISTRA OBRONY NARODOWEJ

z dnia 23 stycznia 2007 r.

w sprawie ochrony informacji niejawnych oraz obiektów wojskowych w jednostkach organizacyjnych podporządkowanych Ministrowi Obrony Narodowej lub przez niego nadzorowanych w 2007 r.

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426), w celu zwiększenia skuteczności ochrony informacji niejawnych oraz obiektów wojskowych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, polecam:

1. W zakresie postępowań sprawdzających i szkolenia:

1) do końca marca wdrożyć w podległych jednostkach organizacyjnych znowelizowane decyzje Ministra Obrony Narodowej regulujące funkcjonowanie resortowego systemu ochrony informacji niejawnych;

2) kierować sukcesywnie na szkolenia uzupełniające, prowadzone przez Służbę Kontrwywiadu Wojskowego, pełnomocników ochrony jednostek organizacyjnych, którzy ukończyli szkolenie specjalistyczne przed 2002 rokiem;

3) przeszkolić do końca roku kierowników i pracowników bibliotek tajnych oraz kancelarii prowadzących ewidencję i przechowujących materiały planowania operacyjnego, planowania mobilizacyjnego i gotowości bojowej, którzy nie posiadają zaświadczenia o ukończeniu szkolenia specjalistycznego, o którym mowa w § 3 ust. 9 zarządzenia Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 21, poz. 203);

4) zorganizować szkolenie uzupełniające dla kierowników i pracowników kancelarii tajnych, którzy ukończyli szkolenie specjalistyczne przed dniem wejścia w życie ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm.);

5) organizować szkolenia uzupełniające, połączone z rozliczeniem z realizacji zadań merytorycznych, dla pełnomocników ochrony z podległych jednostek organizacyjnych;

6) każde ćwiczenie i trening sztabowy poprzedzać wydaniem przez pełnomocnika ochrony jednostki organizacyjnej wytycznych w sprawie ochrony informacji niejawnych podczas ćwiczenia oraz przeszkoleniem osób uczestniczących w ćwiczeniu w zakresie ochrony informacji niejawnych;

7) informować pełnomocnika ochrony bezpośrednio nadrzędnej jednostki organizacyjnej o organizowanych przez siebie szkoleniach specjalistycznych i uzupełniających dla pracowników pionów ochrony; angażować przedstawicieli Służby Kontrwywiadu Wojskowego, Departamentu Ochrony Informacji Niejawnych oraz pionów ochrony bezpośrednio nadrzędnych jednostek organizacyjnych do prowadzenia zajęć szkoleniowych;

8) kierować osoby wyznaczane na stanowiska pełnomocników ochrony od szczebla dywizji wzwyż, przed objęciem obowiązków służbowych, na krótkotrwałe praktyki w pionach ochrony bezpośrednio nadrzędnych jednostek organizacyjnych;

9) uzupełniać na bieżąco oraz systematycznie analizować wykazy stanowisk i prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych oraz osób dopuszczonych do pracy lub służby na tych stanowiskach pod kątem aktualności tych wykazów, a także rozliczać z materiałów niejawnych oraz wstrzymywać dostęp do informacji niejawnych osobom, których poświadczenia bezpieczeństwa tracą ważność;

10) wnioski o wszczęcie kolejnych postępowań sprawdzających wobec osób zatrudnionych na stanowiskach, z którymi może się łączyć dostęp do informacji niejawnych, składać co najmniej 6 miesięcy przed upływem terminów ważności posiadanych przez te osoby poświadczeń bezpieczeństwa;

11) stosownie do zaleceń pokontrolnych Biura Bezpieczeństwa NATO, wystąpić do Służby Kontrwywiadu Wojskowego o wydanie certyfikatów bezpieczeństwa NATO osobom zatrudnionym na stanowiskach, z którymi może się łączyć dostęp do informacji niejawnych NATO oznaczonych klauzulą „Poufne" lub wyższą.

2. W zakresie bezpieczeństwa teleinformatycznego:

1) poprzez systematyczny nadzór służbowy wyeliminować przypadki przetwarzania informacji niejawnych, zwłaszcza podczas ćwiczeń poza miejscem stałej dyslokacji, w systemach i sieciach teleinformatycznych nie posiadających akredytacji bezpieczeństwa teleinformatycznego;

2) prowadzić ewidencję systemów i sieci teleinformatycznych funkcjonujących w podległych jednostkach organizacyjnych, w tym sprzętu w wykonaniu specjalnym, a także nadzorować gospodarkę materiałową tym sprzętem;

3) na podstawie prowadzonej ewidencji przygotowywać dla kierowników jednostek organizacyjnych, w nakazanych przepisami terminach, wnioski do Szefa Służby Kontrwywiadu Wojskowego o przeprowadzenie audytów recertyfikacyjnych pomieszczeń wydzielonych, w których są przetwarzane informacje niejawne, a także badań kontrolnych elektromagnetycznej emisji ujawniającej zestawów komputerowych klasy „Tempest", Bezpiecznych Stanowisk Komputerowych i kabin ekranujących;

4) systematycznie prowadzić w jednostce organizacyjnej bieżącą kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych z ich Szczególnymi Wymaganiami Bezpieczeństwa oraz sposobu przestrzegania przez użytkowników zasad zawartych w Procedurach Bezpiecznej Eksploatacji;

5) w ramach szkolenia uzupełniającego systematycznie szkolić użytkowników systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane lub przesyłane informacje niejawne, a także co najmniej raz w roku organizować szkolenie uzupełniające dla administratorów systemów i sieci teleinformatycznych z podległych jednostek organizacyjnych;

6) nadzorować deklasyfikację, wycofywanie oraz niszczenie elektronicznych nośników cyfrowych, na których zapisano informacje niejawne;

7) stosować, we wszystkich systemach i sieciach teleinformatycznych, w których są przetwarzane, wytwarzane, przechowywane i przesyłane informacje niejawne, oprogramowanie antywirusowe i na bieżąco je aktualizować;

8) wdrożyć w podległych jednostkach organizacyjnych przepisy decyzji Nr 488/MON Ministra Obrony Narodowej z dnia 30 listopada 2006 r. w sprawie wprowadzenia do użytku w resorcie obrony

narodowej „Tymczasowej instrukcji organizacji obiegu informacji niejawnych o klauzuli „Zastrzeżone" w resortowej sieci teleinformatycznej MIL-WAN".

3. W zakresie nadzoru nad ochroną informacji niejawnych:

1) w terminie do 15 października poinformować pełnomocnika ochrony bezpośrednio nadrzędnej jednostki organizacyjnej o planowanych przez siebie do realizacji na rok następny kontrolach problemowych;

2) informować pełnomocnika bezpośrednio nadrzędnej jednostki organizacyjnej o stwierdzanych w czasie kontroli faktach utraty dokumentów niejawnych oraz naruszeniach przepisów o ochronie informacji niejawnych;

3) podczas kontroli problemowych, prowadzonych w podległych jednostkach organizacyjnych, wyrywkowo sprawdzać stan faktyczny dokumentów niejawnych pobranych przez wykonawców, zwłaszcza materiałów zawierających informacje stanowiące tajemnicę państwową;

4) w czasie kontroli rocznej za rok 2007 dokonać przeglądu wytworzonych w jednostce organizacyjnej dokumentów zawierających informacje stanowiące tajemnicę służbową, którym upływa okres ochrony pod kątem jego ewentualnego przedłużenia;

5) nadzorować przebieg kontroli rocznej i półrocznej stanu ochrony informacji niejawnych w jednostce organizacyjnej;

6) w protokołach, meldunkach i notatkach z kontroli każdorazowo formułować konkretne wnioski oraz skierowane do określonych osób terminowe zadania (zalecenia) zawierające sposób usunięcia stwierdzonych nieprawidłowości;

7) wyniki działalności kontrolnej wykorzystywać szeroko w działalności profilaktycznej i szkoleniowej oraz do wypracowywania procedur zmierzających do usprawnienia systemu ochrony informacji niejawnych w jednostce organizacyjnej;

8) w ocenach stanu ochrony informacji niejawnych za 2006 r. sformułować dla komórek wewnętrznych jednostki organizacyjnej oraz osób funkcyjnych zadania zmierzające do wyeliminowania występujących w jednostce nieprawidłowości oraz udoskonalenia obowiązującego systemu ochrony informacji niejawnych.

4. W zakresie bezpieczeństwa przemysłowego:

1) uczestniczyć każdorazowo przy zawieraniu przez jednostkę organizacyjną umów dotyczących zlecenia przedsiębiorcy, jednostce naukowej lub badawczo-rozwojowej zadań związanych z dostępem do informacji niejawnych; określać w instrukcjach bezpieczeństwa przemysłowego szczegółowy sposób ochrony przez przedsiębiorcę przekazywanych informacji, w tym także ochrony materiałów wytworzonych przez niego w trakcie realizacji umowy oraz skutki jakie poniesie przedsiębiorca w przypadku niezapewnienia bezpieczeństwa przekazywanym mu informacjom;

2) materiały niejawne przekazywać przedsiębiorcom z chwilą ustalenia, że posiadają oni zdolność do zapewnienia bezpieczeństwa informacjom niejawnym, które zostaną im udostępnione w ramach realizacji umowy. Należy kontrolować okresowo, w czasie obowiązywania umowy, sposób ochrony przekazywanych dokumentów niejawnych.

5. W zakresie funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych:

1) zaplanować środki finansowe na wykonanie zabezpieczeń oraz wyposażenie pomieszczeń kancelarii, bibliotek i kancelarii mobilizacyjnych tak, aby do końca 2008 roku osiągnąć standardy wynikające z przepisów zarządzenia Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych;

2) rozważyć możliwość zorganizowania kancelarii tajnej wraz z punktem obsługi dokumentów zagranicznych, na bazie istniejącej kancelarii zagranicznej, w jednostkach organizacyjnych, w których kancelarie tajne nie spełniają wymaganych standardów w zakresie zabezpieczenia fizycznego i elektronicznego;

3) materiały niejawne innych jednostek organizacyjnych obsługiwanych przez kancelarię tajną jednostki organizacyjnej, jeżeli nie są one dyslokowane w tej samej strefie administracyjnej, udostępniać wyłącznie w pomieszczeniach kancelarii tajnej;

4) przekazać do właściwego archiwum lub odpowiednio wybrakować materiały archiwalne i niearchiwalne, które są nieprzydatne dla prowadzenia praktycznej działalności przez jednostkę organizacyjną.

6. W zakresie ochrony obiektów jednostek organizacyjnych resortu:

1) wdrożyć w podległych jednostkach organizacyjnych rozporządzenie Ministra Obrony Narodowej w sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, a także przejąć zadania związane z ochroną obiektów wojskowych jednostek organizacyjnych;

2) nadzorować na bieżąco realizację planów ochrony obiektów wojskowych oraz aktualizować je stosownie do pojawiających się zagrożeń i potrzeb;

3) realizować proces budowy, rozbudowy oraz modernizacji systemów ochrony technicznej obiektów wojskowych uwzględniając obowiązujące parametry funkcjonalne i wymagania taktyczno-użytkowe dla systemów i urządzeń alarmowych, a także wymogi w zakresie dokumentacji projektowo-kosztorysowej i procedury przetargowe;

4) dążyć do zwiększenia udziału wart cywilnych oraz specjalistycznych uzbrojonych formacji ochronnych przedsiębiorców w ochronie fizycznej obiektów jednostek organizacyjnych;

5) organizować, co najmniej raz w roku, szkolenia instruktażowo-metodyczne z ochrony obiektów, podczas których prezentować przykładowe działanie sił ochronnych, a także wykorzystanie systemów i urządzeń alarmowych oraz systemów kontroli dostępu. Do prowadzenia zajęć angażować przedstawicieli Służby Kontrwywiadu Wojskowego, Departamentu Ochrony Informacji Niejawnych oraz pionów ochrony bezpośrednio nadrzędnych jednostek organizacyjnych;

6) raz na kwartał organizować dla całego stanu osobowego szkolenia instruktażowo-metodyczne z pozorowanym naruszeniem systemu ochrony w celu doskonalenia procedur postępowania sił ochronnych i stanów osobowych w zakresie przeciwdziałania zagrożeniom ze strony zorganizowanych grup przestępczych i terrorystycznych;

7) sporządzić, zgodnie z wzorcem określonym przez Departament Ochrony Informacji Niejawnych, oraz przesłać do 30 maja bieżącego roku do szczebla bezpośrednio nadrzędnego sprawozdanie z ochrony obiektów jednostki organizacyjnej za rok 2006, a także zestawienie zbiorcze do weryfikacji

wartości pieniężnych norm rzeczowych na eksploatację systemów i urządzeń alarmowych oraz zestawienie ilościowo-jakościowe specjalistycznego sprzętu ochrony obiektów;

8) systematycznie nadzorować i kontrolować stan ochrony obiektów wojskowych w podległych jednostkach organizacyjnych; wyniki kontroli wykorzystywać do podnoszenia skuteczności funkcjonujących systemów ochrony.

7. Wytyczne podlegają ogłoszeniu w Dzienniku Urzędowym Ministra Obrony Narodowej.

MINISTERSTWO OBRONY NARODOWEJ

Dz.U.00.64.740

U M O W A

między Stronami Traktatu Północnoatlantyckiego o ochronie informacji,

sporządzona w Brukseli dnia 6 marca 1997 r.

(Dz. U. z dnia 7 sierpnia 2000 r.)

Dz.U.03.141.1368

ROZPORZĄDZENIE
MINISTRA OBRONY 1)

z dnia 18 lipca 2003 r.

w sprawie terenów zamkniętych niezbędnych dla obronności państwa

(Dz. U. z dnia 3 sierpnia 2003 r.)

Dz.U.01.157.1853

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 14 grudnia 2001 r.

w sprawie wzoru upoważnienia do udostępnienia żołnierzom Żandarmerii Wojskowej danych osobowych, uzyskanych przez uprawnione organy, służby i instytucje państwowe w wyniku wykonywania czynności operacyjno-rozpoznawczych lub prowadzenia kontroli operacyjnej.

Dz.U.99.60.647
Dz.U.02.176.1446
Dz.U.06.19.148

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 19 czerwca 1999 r.

w sprawie ochrony przez specjalistyczne uzbrojone formacje ochronne terenów komórek i jednostek organizacyjnych resortu obrony narodowej.

(Dz. U. z dnia 12 lipca 1999 r.)
tekst ujednolicony

Dz.U.99.58.619
Dz.U.06.19.147

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 2 czerwca 1999 r.

w sprawie wewnętrznych służb ochrony działających na terenach komórek i jednostek organizacyjnych resortu obrony narodowej.

(Dz. U. z dnia 26 czerwca 1999 r.)

DECYZJA Nr 326/MON
MINISTRA OBRONY NARODOWEJ

z dnia 25 października 2004 r.

w sprawie udzielania w resorcie obrony narodowej zamówień objętych tajemnicą państwową oraz jeżeli wymaga tego istotny interes bezpieczeństwa państwa

INSTRUKCJA O ZASADACH PRACY BIUROWEJ W RESORCIE OBRONY NARODOWEJ (Sygn. Szt. Gen. 1537/2002 Dz.U.01.123.1353

Dz.U.04.171.1800

USTAWA

z dnia 24 sierpnia 2001 r.

o Żandarmerii Wojskowej i wojskowych organach porządkowych

(Dz. U. z dnia 25 października 2001 r.)

Dz.U.01.157.1855

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 14 grudnia 2001 r.

w sprawie szczegółowych czynności wojskowych organów porządkowych wchodzących w skład służby wewnętrznej jednostki wojskowej.

(Dz. U. z dnia 31 grudnia 2001 r.)

Dz.U.01.157.1854

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 14 grudnia 2001 r.

w sprawie szczegółowych czynności wojskowych organów porządkowych wchodzących w skład służby garnizonowej.

(Dz. U. z dnia 31 grudnia 2001 r.)

W ZAKRESIE TELEINFORMATYKI

1. BTPO-701A
2. DBBT-301B
3. DBBT-801A
4. DBBT-802A

Dz.U.01.157.1838

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 18 grudnia 2001 r.

w sprawie użycia środków przymusu bezpośredniego oraz broni palnej przez żołnierzy wojskowych organów porządkowych.

(Dz. U. z dnia 31 grudnia 2001 r.)

Dz.U.01.157.1837
Dz.U.04.247.2476

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 18 grudnia 2001 r.

w sprawie warunków i sposobów użycia środków przymusu bezpośredniego przez żołnierzy Żandarmerii Wojskowej.

(Dz. U. z dnia 31 grudnia 2001 r.)

Dz.U.01.157.1836

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia 18 grudnia 2001 r.

w sprawie warunków i sposobu postępowania przy użyciu broni palnej przez żołnierzy Żandarmerii Wojskowej.

(Dz. U. z dnia 31 grudnia 2001 r.)

DECYZJA NR 208/MON
MINISTRA OBRONY NARODOWEJ

z dnia 8 listopada 2000 r.

w sprawie wprowadzenia do użytku w resorcie Obrony Narodowej „Regulaminu oddziałów wart cywilnych".

Dz.U.03.179.1750

U S T A W A

z dnia 11 września 2003 r.

o służbie wojskowej żołnierzy zawodowych

Dz.U.04.52.520

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 18 marca 2004 r.

w sprawie wyjazdów za granicę żołnierzy zawodowych w celach niezwiązanych ze służbą wojskową

(Dz. U. z dnia 31 marca 2004 r.)

Dz.U.03.135.1271

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 17 lipca 2003 r.

w sprawie postępowania w razie wnoszenia napojów alkoholowych na teren obiektów wojskowych oraz wysokości opłaty za przechowywanie napojów alkoholowych w depozycie

DECYZJA Nr 90/MON
MINISTRA OBRONY NARODOWEJ

z dnia 23 marca 2006 r.

w sprawie oświadczeń o stanie majątkowym żołnierzy zawodowych

DECYZJA Nr 78/MON
MINISTRA OBRONY NARODOWEJ

z dnia 3 marca 2006 r.

w sprawie wprowadzenia dokumentów normalizacyjnych dotyczących obronności i bezpieczeństwa państwa

INNE

Dz.U.06.97.673

USTAWA

z dnia 14 lipca 1983 r.

o narodowym zasobie archiwalnym i archiwach

(tekst jednolity)

Dz.U.97.88.553

USTAWA

z dnia 6 czerwca 1997 r.

Kodeks karny

(Dz. U. z dnia 2 sierpnia 1997 r.)

Rozdział XXXIII

Przestępstwa przeciwko ochronie informacji

Dz.U.02.74.676
Dz.U.04.171.1800

USTAWA

z dnia 24 maja 2002r.

o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu

(Dz. U. z dnia 14 czerwca 2002r.)

Dz.U.02.156.1301
Dz.U.04.107.1135

USTAWA

z dnia 29 sierpnia 2002 r.

o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej

(Dz. U. z dnia 25 września 2002 r.)

Dz.U.02.113.985

USTAWA

z dnia 21 czerwca 2002 r.

o stanie wyjątkowym

(Dz. U. z dnia 20 lipca 2002 r.)

Dz.U.2005.219.1847

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 25 października 2005 r.

w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych, podporządkowanych Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw zagranicznych, ministrowi właściwemu do spraw finansów publicznych, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Kancelarii Sejmu, Szefowi Kancelarii Senatu i Szefowi Kancelarii Prezydenta

Dz.U.05.171.1430

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia 25 sierpnia 2005 r.

w sprawie szczegółowego trybu przygotowania i prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych

(Dz. U. z dnia 8 września 2005 r.)

Dz.U.05.174.1447

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia 29 sierpnia 2005 r.

w sprawie wysokości i trybu pobierania, przez służbę ochrony państwa, opłat za przeprowadzenie postępowania bezpieczeństwa przemysłowego, sprawdzeń oraz postępowań sprawdzających

(Dz. U. z dnia 9 września 2005 r.)

Dz.U.2003.198.1930
Dz.U.2004.273.2714
Dz.U.2006.165.1178

ROZPORZĄDZENIE
MINISTRA SPRAWIEDLIWOŚCI

z dnia 7 listopada 2003 r.

w sprawie udzielania informacji o osobach oraz o podmiotach zbiorowych na podstawie danych zgromadzonych w Krajowym Rejestrze Karnym

Dz.U.03.198.1929

ROZPORZĄDZENIE
MINISTRA SPRAWIEDLIWOŚCI

z dnia 7 listopada 2003 r.

w sprawie gromadzenia danych osobowych i danych o podmiotach zbiorowych w Krajowym Rejestrze Karnym oraz usuwania tych danych z Rejestru

(Dz. U. z dnia 21 listopada 2003 r.)

Dz.U.2003.98.901

ROZPORZĄDZENIE
MINISTRA KULTURY [1)]

z dnia 12 maja 2003 r.

w sprawie warunków przechowywania dokumentacji osobowej i płacowej pracodawców

Dz.U.03.70.643

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia 3 kwietnia 2003r.

w sprawie zakresu, warunków i trybu przekazywania Agencji Bezpieczeństwa Wewnętrznego informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez organy, służby i instytucje państwowe

Dz.U.2002.167.1375

ROZPORZĄDZENIE
MINISTRA KULTURY

z dnia 16 września 2002 r.

w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych

Dz.U.2001.13.116

ROZPORZĄDZENIE
MINISTRA KULTURY I DZIEDZICTWA NARODOWEGO

z dnia 13 grudnia 2000 r.

w sprawie określenia szczególnych wypadków i trybu wcześniejszego udostępniania materiałów archiwalnych

Dz.U.99.18.159

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia 25 lutego 1999 r.

w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów, służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających.

(Dz. U. z dnia 5 marca 1999 r.)

OCHRONA I OBRONA

Dz.U.05.145.1221

USTAWA

z dnia 22 sierpnia 1997 r.

o ochronie osób i mienia

Dz.U.05.151.1269

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI [1)]

z dnia 21 lipca 2005 r.

w sprawie stażu adaptacyjnego i testu umiejętności w toku postępowania w sprawie uznania nabytych w niektórych państwach kwalifikacji do wykonywania zawodu pracownika ochrony

(Dz. U. z dnia 10 sierpnia 2005 r.)

Dz.U.04.219.2219

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 21 września 2004 r.

w sprawie organów właściwych do stosowania w czasie stanu wojennego ograniczeń wolności i praw człowieka i obywatela wobec osób, których działalność zagraża bezpieczeństwu lub obronności państwa, oraz trybu postępowania w tych sprawach

(Dz. U. z dnia 8 października 2004 r.)

Dz.U.04.219.2218

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 21 września 2004 r.

w sprawie gotowości obronnej państwa

(Dz. U. z dnia 8 października 2004 r.)

Dz.U.02.194.1632

ROZPORZĄDZENIE
MINISTRA GOSPODARKI

z dnia 8 listopada 2002 r.

w sprawie w sprawie wymagań, jakim powinien odpowiadać plan postępowania na wypadek zagrożenia życia lub zdrowia ludzkiego, mienia oraz środowiska naturalnego.

(Dz. U. z dnia 23 listopada 2002 r.)

Dz.U.99.30.299

ROZPORZĄDZENIE
MINISTRA ZDROWIA I OPIEKI SPOŁECZNEJ

z dnia 23 marca 1999 r.

w sprawie badań lekarskich i psychologicznych osób ubiegających się o wydanie licencji oraz posiadających licencję pracownika ochrony fizycznej

(Dz. U. z dnia 12 kwietnia 1999 r.)

Dz.U.98.161.1108

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 18 grudnia 1998 r.

w sprawie określenia szczegółowych zasad współpracy specjalistycznych uzbrojonych formacji ochronnych z Policją, jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi (miejskimi)

(Dz. U. z dnia 29 grudnia 1998 r.)

Dz.U.98.144.933

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 18 listopada 1998 r.

w sprawie szczegółowego trybu działań pracowników ochrony, podejmowanych wobec osób znajdujących się w granicach chronionych obiektów i obszarów.

(Dz. U. z dnia 27 listopada 1998 r.)

Dz.U.98.129.858
Dz.U.00.17.221

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 14 października 1998 r.

w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne

(Dz. U. z dnia 23 października 1998 r.)

Dz.U.98.120.780

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 9 września 1998 r.

w sprawie określenia rodzajów obiektów, w których mogą być stosowane paralizatory elektryczne

(Dz. U. z dnia 16 września 1998 r.)

Dz.U.98.89.563

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 30 czerwca 1998 r.

w sprawie szczegółowych warunków i sposobów użycia przez pracowników ochrony środków przymusu bezpośredniego.

(Dz. U. z dnia 15 lipca 1998 r.)

Dz.U.98.86.543

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 30 czerwca 1998 r.

w sprawie szczegółowych warunków i sposobu postępowania pracowników ochrony przy użyciu broni palnej.

(Dz. U. z dnia 10 lipca 1998 r.)

Dz.U.1983.25.105

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH

z dnia 11 maja 1983 r.

w sprawie zasad i trybu postępowania w razie wnoszenia napojów alkoholowych na tereny objęte zakazem ich wnoszenia

Dz.U.1998.89.563

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 30 czerwca 1998 r.

w sprawie szczegółowych warunków i sposobów użycia przez pracowników ochrony środków przymusu bezpośredniego

Dz.U.1998.86.543

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 30 czerwca 1998 r.

w sprawie szczegółowych warunków i sposobu postępowania pracowników ochrony przy użyciu broni palnej

Dz.U.05.135.1132

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 19 lipca 2005 r.

w sprawie szczegółowych warunków i sposobu postępowania przy użyciu broni palnej przez policjantów oraz zasad użycia broni palnej przez oddziały i pododdziały zwarte Policji

(Dz. U. z dnia 22 lipca 2005 r.)

Dz.U.90.70.410
Dz.U.96.10.58
Dz.U.00.16.206
Dz.U.02.196.1657
Dz.U.03.175.1694
Dz.U.05.135.1133

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 17 września 1990 r.

w sprawie określenia przypadków oraz warunków i sposobów użycia przez policjantów środków przymusu bezpośredniego

(Dz. U. z dnia 12 października 1990 r.)

Dz.U.04.187.1943

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1)]

z dnia 12 sierpnia 2004 r.

w sprawie zakresu i sposobu współpracy Policji ze strażami gminnymi (miejskimi) oraz zakresu sprawowania przez Komendanta Głównego Policji nadzoru nad działalnością straży

(Dz. U. z dnia 27 sierpnia 2004 r.)

Dz.U.2006.177.1310

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia 27 września 2006 r.

w sprawie zakresu, warunków i trybu przekazywania Centralnemu Biuru Antykorupcyjnemu informacji przez organy, służby i instytucje państwowe

Dz.U.06.142.1018

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 4 sierpnia 2006 r.

w sprawie udzielania funkcjonariuszom Centralnego Biura Antykorupcyjnego niezbędnej pomocy przez instytucje państwowe, organy administracji rządowej i samorządu terytorialnego, przedsiębiorców, jednostki organizacyjne, organizacje społeczne oraz obywateli

DZ.U.2003.108.1023
DZ.U.2003.204.1987

ROZPORZĄDZENIE
MINISTRA SPRAWIEDLIWOŚCI

z dnia 18 czerwca 2003 r.

w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania tajemnicy państwowej, służbowej albo związanej z wykonywaniem zawodu lub funkcji

U S T A W A

z dnia 29 sierpnia 1997 r.

o ochronie danych osobowych

(Dz.U.2002.101.926 - tekst jednolity)

Dz.U.2005.32.284

ROZPORZĄDZENIE
MINISTRA KULTURY[1)]

z dnia 15 lutego 2005 r.

w sprawie warunków przechowywania dokumentacji osobowej i płacowej pracodawców

Dz.U.04.100.1025

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 29 kwietnia 2004 r.

w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych

Dz.U.04.100.1024

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 29 kwietnia 2004 r.

w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Dz.U.04.94.923

ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 22 kwietnia 2004 r.

w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych

KONWENCJA Nr 108
RADY EUROPY

sporządzona w Strasburgu dnia 28 stycznia 1981 r.

o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych

(Dz. U. z dnia 14 stycznia 2003 r.)

POLSKIE NORMY DLA SYSTEMÓW ALARMOWYCH

Systemy alarmowe

1. PN-E-08390-1: 1996
Systemy alarmowe – Terminologia. (w j. polskim), będzie wycofana

2. PN-93/E-08390/14: 1993
Systemy alarmowe – Wymagania ogólne – Zasady stosowania. (w j. polskim) (w części dotyczącej Systemów Sygnalizacji Włamania norma koliduje z przyjętą notą uznaniową normą „PN-EN 50131-1: 2002 Systemy alarmowe – Systemy sygnalizacji włamania – Część 1: Wymagania ogólne.", jej wycofanie uzależnione jest między innymi od ustanowienia normy PN-EN 50131-1: 2002 w j. polskim)

3. PN-EN 50130-4: 2002
Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów alarmowych, pożarowych, włamaniowych i osobistych. (w j. polskim)

4. PN-EN 50130-5: 2002
Systemy alarmowe – Część 5: Próby środowiskowe. (w j. polskim)

Systemy sygnalizacji włamania

1. PN-93/E-08390/22:1993
Systemy alarmowe - Włamaniowe systemy alarmowe - Ogólne wymagania i badania czujek.

2. PN-93/E-08390/23:1993
Systemy alarmowe - Włamaniowe systemy alarmowe - Wymagania i badania aktywnych czujek podczerwieni.

3. PN-93/E-08390/24:1993
Systemy alarmowe - Włamaniowe systemy alarmowe - Wymagania i badania ultradźwiękowych czujek Dopplera.

4. PN-93/E-08390/25:1993
Systemy alarmowe - Włamaniowe systemy alarmowe - Wymagania i badania mikrofalowych czujek Dopplera.

5. PN-93/E-08390/26:1993
Systemy alarmowe - Włamaniowe systemy alarmowe - Wymagania i badania pasywnych czujek podczerwieni.

6. PN-IEC 839-2-7:1996
Systemy alarmowe - Włamaniowe systemy alarmowe - Wymagania i badania pasywnych czujek stłuczenia szyby.

7. PN-E-08390-3:1998
Systemy alarmowe - Włamaniowe systemy alarmowe - Wymagania i badania central. (będzie wycofana)

8. PN-E-08390-5:2000
Systemy alarmowe - Włamaniowe systemy alarmowe - Wymagania i badania sygnalizatorów.

9. PN-EN 50131-6:2000
Systemy alarmowe - Systemy sygnalizacji włamania -Część 6: Zasilacze. 10. PN-EN 50131-1:2002 (U) Systemy alarmowe - Systemy sygnalizacji włamania - Część 1: Wymagania ogólne.

11. PN-EN 50131-5-3:2005 (U)
Systemy alarmowe - Systemy sygnalizacji włamania - Część 5-3: Wymagania dotyczące urządzeń stosowanych do połączeń wewnętrznych wykorzystujących techniki radiowe.

Systemy dozorowe CCTV stosowane w zabezpieczeniach

1. PN-EN 50132-2-1:2002 (U)
Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 2-1: Kamery telewizji czarno-białej.

2. PN-EN 50132-4-1:2002 (U)
Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 4-1: Monitory czarno-białe.

3. PN-EN 50132-5:2002 (U)
Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 5: Teletransmisja.

4. PN-EN 50132-7:2002 (U)
Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 7: Wytyczne stosowania.

Systemy kontroli dostępu stosowane w zabezpieczeniach

1. PN-EN 50133-1: 2000
Systemy alarmowe - Systemy kontroli dostępu -Część 1: Wymagania systemowe.

2. PN-EN 50133-2-1: 2002 (U)
Systemy alarmowe - Systemy kontroli dostępu -Część 2-1: Wymagania dla podzespołów.

3. PN-EN 50133-7: 2002 (U)
Systemy alarmowe - Systemy kontroli dostępu -Część 7: Wytyczne stosowania.

Systemy alarmowe osobiste

1. PN-EN 50134-1:2003 (U)
Systemy alarmowe - Systemy alarmowe osobiste -Część 1: Wymagania systemowe.

2. PN-EN 50134-2:2002 (U)
Systemy alarmowe - Systemy alarmowe osobiste -Część 2: Urządzenia wyzwalające.

3. PN-EN 50134-3:2002 (U)
Systemy alarmowe - Systemy alarmowe osobiste -Część 3: Jednostka lokalna i sterownik.

4. PN-EN 50134-5:2005 (U)
Systemy alarmowe - Systemy alarmowe osobiste -Część 5: Połączenia wewnętrzne i komunikacyjne.

5. PN-EN 50134-7:2001
Systemy alarmowe - Systemy alarmowe osobiste -Część 7: Wytyczne stosowania.

Urządzenia i systemy transmisji alarmu

1. PN-EN 50136-1 -1:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 1-1: Wymagania ogólne dla systemów transmisji alarmu.

2. PN-EN 50136-1-2:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 1-2: Wymagania dla systemów wykorzystujących specjalizowane tory transmisji.

3. PN-EN 50136-1-3:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 1-3: Wymagania dla systemów łączności cyfrowej wykorzystującej telefoniczną publiczną sieć komutowaną.

4. PN-EN 50136-1-4:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 1-4: Wymagania dla systemów łączności akustycznej wykorzystującej telefoniczną publiczną sieć komutowaną.

5. PN-EN 50136-2-1:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 2-1: Wymagania ogólne dla urządzeń transmisji alarmu.

6. PN-EN 50136-2-2:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 2-2: Wymagania dla urządzeń stosowanych w systemach wykorzystujących specjalizowane tory transmisji.

7. PN-EN 50136-2-3:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 2-3: Wymagania dla urządzeń stosowanych w systemach łączności cyfrowej wykorzystującej telefoniczną publiczną sieć komutowaną.

8. PN-EN 50136-2-4:2002 (U)
Systemy alarmowe - Urządzenia i systemy transmisji alarmu - Część 2-4: Wymagania dla urządzeń stosowanych w systemach łączności akustycznej wykorzystującej telefoniczną publiczną sieć komutowaną.