R G B WH GR BL Grey Scale #13 C M Y K
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

AKADEMIA OBRONY NARODOWEJ

KANCELARIA TAJNA

AON 5733/2005

St. chor. szt. mgr Arkadiusz STRZELCZYK

ZBIÓR PRZEPISÓW NORMUJĄCYCH ZASADY OCHRONY INFORMACJI NIEJAWNYCH W RESORCIE OBRONY NARODOWEJ

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 58198
Akademii Obrony Narodowej

WARSZAWA 2005

Colour Chart #13
Blue Cyan Green Yellow Red Magenta White 3/Color Black
Inches Centimetres
DANES PICTA .COM

AKADEMIA OBRONY NARODOWEJ

KANCELARIA TAJNA

AON 5733/05

St. chor. szt. mgr Arkadiusz STRZELCZYK

ZBIÓR PRZEPISÓW NORMUJĄCYCH ZASADY OCHRONY INFORMACJI NIEJAWNYCH W RESORCIE OBRONY NARODOWEJ

Warszawa **2005**

SPIS TREŚCI

USTAWA z dnia 22 stycznia 1999 r.
o ochronie informacji niejawnych (Tekst ujednolicony po zmianie z 15 kwietnia 2005 r.) **s. 7-55**

ROZPORZĄDZENIE RADY MINISTRÓW z dnia 9 lutego 1999 r.
w sprawie wzorów: kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, odmowy wydania świadectwa bezpieczeństwa przemysłowego **s. 56-60**

ROZPORZĄDZENIE RADY MINISTRÓW z dnia 9 lutego 1999 r.
w sprawie organizacji kancelarii tajnych **s. 61-78**

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 lutego 1999 r.
w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych **s. 79-83**

ROZPORZĄDZENIE 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 **s. 84-95**

ROZPORZĄDZENIE MINISTRÓW SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1)] ORAZ OBRONY NARODOWEJ z dnia 27 listopada 2003 r.
w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach **s. 96-101**

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ
z dnia 13 września 2002 r. **w sprawie przechowywania i rejestrowania dokumentacji postępowań dyscyplinarnych oraz prowadzenia ewidencji ukarań żołnierzy** **s. 102-106**

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ
z dnia 6 lutego 2003 r. **w sprawie zasad organizacji obsługi bibliotecznej w jednostkach organizacyjnych Ministerstwa Obrony Narodowej oraz zasad współdziałania bibliotek publicznych wykonaniu tej obsługi** **s. 107-108**

ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ
z dnia 5 listopada 2004 r. **w sprawie trybu udzielania żołnierzom w czynnej służbie wojskowej zezwoleń na rozpowszechnianie rezultatów ich działalności naukowej literackiej, artystycznej lub publicystycznej, zawierających informacje niejawne** **s. 109-110**

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** **s. 111-118**

DECYZJA NR 31/MON MINISTRA OBRONY NARODOWEJ
z dnia 8 marca 2000 r. **w sprawie zasad opracowywania planów ochrony jednostek organizacyjnych resortu Obrony Narodowej** **s. 119-123**

DECYZJA Nr 100/MON MINISTRA OBRONY NARODOWEJ
z dnia 6 czerwca 2000 r. **w sprawie jednostki certyfikującej właściwej w Ministerstwie Obrony Narodowej do certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych** **s. 124**

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** **s. 125-134**

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** **s. 135-150**

DECYZJA Nr 16/MON MINISTRA OBRONY NARODOWEJ
z dnia 25 stycznia 2001 r. **w sprawie szkolenia w zakresie ochrony informacji niejawnych** **s. 151-154**

DECYZJA Nr 29/MON MINISTRA OBRONY NARODOWEJ
z dnia 22 lutego 2001 r. **w sprawie trybu certyfikacji 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** **s. 155-160**

DECYZJA NR 278/MON MINISTRA OBRONY NARODOWEJ
z dnia 15 października 2003 r. **w sprawie sprawdzenia prawidłowości oznaczenia klauzulami tajności dokumentów zawierających informacje niejawne stanowiące tajemnicę państwową, wytworzonych przed dniem 10 maja 1990r.** **s. 161-162**

DECYZJA NR 40/MON MINISTRA OBRONY NARODOWEJ
z dnia 9 lutego 2004 r. **w sprawie szczegółowych zasad i trybu przeprowadzania postępowań sprawdzających, wydawania certyfikatów bezpieczeństwa NATO i UE oraz ich dokumentowania** **s. 163-204**

ZARZĄDZENIE NR 49/MON MINISTRA OBRONY NARODOWEJ
z dnia 5 sierpnia 2002r. **w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych** **s. 205-254**

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** **s. 255-279**

USTAWA z dnia 6 czerwca 1997 r.
Kodeks karny. Rozdział XXXIII. Przestępstwa przeciwko ochronie informacji **s. 280-281**

Inne przepisy **s. 282-290**

Dz.U.1999.11.95
akty zmieniające:
Dz.U. 2000 nr 12 poz. 136 2000.02.23
Dz.U. 2000 nr 39 poz. 462 2001.01.31
Dz.U. 2001 nr 22 poz. 247 2001.04.08
Dz.U. 2001 nr 27 poz. 298 2001.03.30
Dz.U. 2001 nr 56 poz. 580 2001.07.01
Dz.U. 2001 nr 123 poz. 1353 2002.01.01
Dz.U. 2001 nr 154 poz. 1800 2002.01.01
Dz.U. 2002 nr 74 poz. 676 2002.06.29
Dz.U. 2002 nr 89 poz. 804 2002.07.01
Dz.U. 2002 nr 153 poz. 1271 2004.01.01
Dz.U. 2003 nr 17 poz. 155 2003.07.01
Dz.U. 2001 nr 110 poz. 1189 2003.01.01
Dz.U. 2004 nr 29 poz. 257
Dz.U. 2005 nr 85 poz. 727

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.)[2].

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 nie będąca 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 Wojskowe Służby Informacyjne,
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
Komitet Ochrony Informacji Niejawnych

(Art. 5-13) - skreślony

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 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 Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej niezbędnej pomocy służbom ochrony państwa przy wykonywaniu czynności w ramach prowadzonych postępowań sprawdzających.

Art. 15.
W stosunkach międzynarodowych szef Agencji Bezpieczeństwa Wewnętrznego i szef Wojskowych Służb Informacyjnych pełnią funkcję krajowych władz 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 nie kontrolowanych, 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 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 1995 r. nr 13, poz. 59, z 1996 r. nr 64, poz. 315 i nr 89, poz. 402, z 1997 r. nr 28, poz. 153, nr 79, poz. 484, nr 96, poz. 589, nr 121, poz. 770 i nr 133, poz. 883 oraz z 1998 r. nr 148, poz. 966, nr 155, poz. 1016 i nr 162, poz. 1116 i 1126), 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 Wojskowych Służb Informacyjnych.

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 zawarte 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, Wojskowych Służb Informacyjnych oraz byłego Urzędu Ochrony Państwa, 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 i 155 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 i 155 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) Wojskowe Służby Informacyjne - w przypadku ubiegania się osoby o zatrudnienie lub zlecenie prac związanych z obronnością państwa:

a) wobec żołnierzy pozostających w służbie czynnej 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, Wojskowe Służby Informacyjne 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, 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 nie dających 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) 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).
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 Wojskowych Służb Informacyjnych, 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 Wojskowych Służb Informacyjnych, 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 Wojskowych Służb Informacyjnych, 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. skreślony.

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 Naczelnego Sądu Administracyjnego [Od 1 stycznia 2004 r. wyrazy „Naczelnego Sądu Administracyjnego" zastępuje się wyrazami „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 Wojskowych Służb Informacyjnych.
2. Do postępowania odwoławczego przed szefem Agencji Bezpieczeństwa Wewnętrznego lub szefem Wojskowych Służb Informacyjnych 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 Wojskowych Służb Informacyjnych 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 oraz z 2004 r. Nr 162, poz. 1692).

Art. 48k.
1. Naczelny Sąd Administracyjny [Od 1 stycznia 2004 r. wyrazy „Naczelny Sąd Administracyjny" zastępuje się wyrazami „Sąd administracyjny"] rozpoznaje skargę na posiedzeniu niejawnym.

2. Przepisów art. 39, art. 47, art. 52 ust. 2 oraz art. 54 ust. 3 i 4 ustawy z 11 maja 1995 r. o Naczelnym Sądzie Administracyjnym (Dz. U. nr 74, poz. 368 i nr 104, poz. 515, z 1997 r. nr 75, poz. 471, nr 106, poz. 679, nr 114, poz. 739 i nr 144, poz. 971, z 1998 r. nr 162, poz. 1126, z 1999 r. nr 75, poz. 853 oraz z 2000 r. nr 2, poz. 5, nr 48, poz. 552, nr 60, poz. 704 i nr 91, poz. 1008) nie stosuje się.

[Od 1 stycznia 2004 r. ust. 2 otrzymuje brzmienie:

„2. Przepisów art. 55 § 2 i art. 106 § 2 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1270) 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 Naczelny Sąd Administracyjny [Od 1 stycznia 2004 r. wyrazy „Naczelny Sąd Administracyjny" zastępuje się wyrazami „sąd administracyjny"] niezwłocznie zwraca właściwej służbie ochrony państwa akta postępowania sprawdzającego.

Art. 48ł.
Do rewizji nadzwyczajnej [Od 1 stycznia 2004 r. wyrazy „rewizji nadzwyczajnej" zastępuje się wyrazami „skargi kasacyjnej"] stosuje się odpowiednio art. 48k ust. 1 i 3 oraz art. 48l ustawy.

Art. 48m.
1) służby ochrony państwa stosuje się do Policji, Żandarmerii Wojskowej, Straży Granicznej, Agencji Wywiadu lub Służby Więziennej,
2) Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Wojskowych Służb Informacyjnych stosuje się do Szefa Agencji Wywiadu, 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 nie posiadającej 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, spraw 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, 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 nie upoważnionym 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) Wojskowe Służby Informacyjne, 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 pkt 1 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 art. 71 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 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 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 przypisy 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 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 31 grudnia 1999 r.
4. Zezwolenia wydane na podstawie art. 16 ustawy, o której mowa w ust. 3, zachowują ważność nie dłużej niż do 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 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).

Art. 91.
[Stanowił, że ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia, a została ogłoszona w Dz. U. nr 11 z 8 lutego pod poz. 95].

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.

INSTRUKCJA

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)

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. 594, Nr 91, poz. 871, Nr 96, poz. 959, Nr 116, poz. 1205, Nr 146, poz. 1546 i Nr 273, poz. 2703.

Dz.U.99.18.157

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia 9 lutego 1999 r.

w sprawie wzorów: kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, odmowy wydania świadectwa bezpieczeństwa przemysłowego

(Dz. U. z dnia 5 marca 1999 r.)

Na podstawie art. 73 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) zarządza się, co następuje:

§ 1. Ustala się wzory:

1) kwestionariusza bezpieczeństwa przemysłowego, stanowiący załącznik nr 1 do rozporządzenia,

2) świadectwa bezpieczeństwa przemysłowego, stanowiący załącznik nr 2 do rozporządzenia,

3) odmowy wydania świadectwa bezpieczeństwa przemysłowego, stanowiący załącznik nr 3 do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem 11 marca 1999 r.

Załącznik nr 1

WZÓR

Po wypełnieniu „Poufne"
.....
(nazwa przedsiębiorcy, jednostki
naukowej lub badawczo-rozwojowej)

KWESTIONARIUSZ BEZPIECZEŃSTWA PRZEMYSŁOWEGO

1) Pełna nazwa przedsiębiorstwa, jednostki naukowej lub jednostki badawczo-rozwojowej (nr REGON).....
.....
.....

2) Pełny adres przedsiębiorstwa, jednostki naukowej lub jednostki badawczo-rozwojowej: miasto, ulica, nr domu, kod pocztowy, województwo, powiat, gmina, nr telefonu - faksu, nr poczty elektronicznej .....
.....
.....

3) Status prawny .....
.....

4) Dane o strukturze organizacyjnej .....
.....

5) Dane o strukturze kapitałowej .....
.....

6) Dane dotyczące władz lub organów zarządzających .....
.....
.....

7) Dane dotyczące systemu ochrony informacji niejawnych, w tym:
a) systemu ochrony osób .....
.....
b) systemu ochrony materiałów .....
c) systemu zabezpieczenia obiektów .....

8) Wykaz pracowników uprawnionych do dostępu do informacji niejawnych:
....
....
....
....

9) Wykaz pracowników, którzy powinni mieć dostęp do informacji niejawnych w związku z postępowaniem zmierzającym do zawarcia umowy lub jej wykonaniem:
....
....
....
....

10) Wykaz osób odpowiedzialnych za ochronę przekazanych jednostce organizacyjnej, wymienionej w pkt 1, informacji niejawnych:

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

11) Wszelkie zmiany dotyczące danych zawartych w kwestionariuszu przekazuje się w formie uzupełnienia do kwestionariusza.

....
(miejscowość i data)
(pieczęć imienna i
podpis kierownika
jednostki organizacyjnej)

UWAGA: W przypadku braku miejsca, informacje należy podać na dodatkowych arkuszach, wskazując punkty, których dotyczy uzupełnienie.

Załącznik nr 2

.....
(pieczęć nagłówkowa służby ochrony państwa z adresem i nr telefonu)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO Nr .....

Zaświadcza się, że dnia .....,

.....
(nazwa służby ochrony państwa)

wydała.....
(nazwa przedsiębiorstwa, jednostki naukowej, jednostki badawczo - rozwojowej, nr REGON)

mieszczącemu się w .....
(adres przedsiębiorstwa, jednostki naukowej, jednostki badawczo - rozwojowej)

na podstawie art. 69 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95)

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

stwierdzając, że jednostka ta posiada zdolność do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą ..... w zakresie

.....
(oznaczenie umowy)

przed nieuprawnionym ujawnianiem.

..... m.p. .....

(miejscowość i data)

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

Załącznik nr 3

.....

(pieczęć nagłówkowa służby ochrony państwa z adresem i nr telefonu)

ODMOWA WYDANIA

ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO Nr .....

Na podstawie art. 69/70* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95)

.....

(nazwa służby ochrony państwa)

ODMÓWIŁA WYDANIA ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO

.....

(nazwa przedsiębiorstwa, jednostki naukowej, jednostki badawczo - rozwojowej, nr REGON)

stwierdzając, że ww. jednostka organizacyjna nie posiada zdolności do zapewnienia ochrony informacji niejawnych oznaczonych klauzulą .....

w zakresie .....

(oznaczenie umowy)

.....

zapewnienia ochrony informacji niejawnych oznaczonych klauzulą .....

.....

(miejscowość i data)

m.p.

.....

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

* Niepotrzebne skreślić

Dz.U.99.18.156
Dz.U.03.17.156 - tekst ujednolicony

ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia 9 lutego 1999 r.

w sprawie organizacji kancelarii tajnych

(Dz. U. z dnia 5 marca 1999 r.)

Na podstawie art. 53 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) zarządza się, co następuje:

§ 1.
1. Rozporządzenie określa wymagania w zakresie:

1) organizacji kancelarii tajnych,
2) stosowania środków ochrony fizycznej,
3) trybu obiegu informacji niejawnych,
4) wzoru karty zapoznania się z dokumentem,

2. Wymagań w zakresie, o którym mowa w ust. 1 pkt 1-3 nie stosuje się w jednostkach organizacyjnych w art. 53 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.

§ 2.
1. Kierownik jednostki organizacyjnej, w której występują dokumenty zawierające informacje niejawne oznaczone klauzulami „ściśle tajne", „tajne" lub „poufne", jest obowiązany do utworzenia kancelarii tajnej, zwanej dalej „kancelarią".

2. Kancelarią kieruje kierownik kancelarii, wyznaczany przez kierownika jednostki organizacyjnej na wniosek pełnomocnika do spraw ochrony informacji niejawnych, zwanego dalej „pełnomocnikiem ochrony".

3. W uzasadnionych przypadkach w jednostce organizacyjnej można utworzyć oddziały kancelarii; kierownik kancelarii jest obowiązany do koordynowania prac tych oddziałów.

4. Wyznaczony do prowadzenia oddziału kancelarii pracownik pionu ochrony wykonuje obowiązki kierownika kancelarii.

§ 3.
Do obowiązków kierownika kancelarii należy w szczególności:

1) bezpośredni nadzór nad obiegiem dokumentów niejawnych w jednostce organizacyjnej,

2) udostępnianie lub wydawanie dokumentów, o których mowa w § 2 ust. 1, osobom posiadającym stosowne poświadczenie bezpieczeństwa,

3) egzekwowanie zwrotu dokumentów zawierających informacje niejawne,

4) kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii tajnej oraz jednostce organizacyjnej,

5) wykonywanie poleceń pełnomocnika ochrony,

6) prowadzenie bieżącej kontroli postępowania z dokumentami zawierającymi informacje niejawne, które zostały udostępnione pracownikom.

§ 4.
1. W przypadku zmiany na stanowisku kierownika kancelarii sporządza się, w dwóch egzemplarzach, protokół zdawczo-odbiorczy w obecności pełnomocnika ochrony, kierownika zdającego obowiązki oraz osoby przejmującej obowiązki kierownika. Protokół przechowywany jest w kancelarii, drugi egzemplarz zaś - u pełnomocnika ochrony.

2. W przypadku czasowej nieobecności kierownika kancelarii jego obowiązki przejmuje upoważniony pracownik kancelarii, a w razie braku stałego pracownika w kancelarii, kancelarię przejmuje protokolarnie, posiadający stosowne poświadczenie bezpieczeństwa, inny pracownik wyznaczony przez pełnomocnika ochrony.

3. W przypadku likwidacji kancelarii ust. 1 stosuje się odpowiednio.

§ 5.
1. Kancelaria powinna być zlokalizowana w strefie bezpieczeństwa na piętrze, z wyłączeniem poddaszy.

2. Kancelaria powinna być oddzielona od innych pomieszczeń trwałymi, niepalnymi, o dużej wytrzymałości ścianami i stropami.

3. Drzwi kancelarii powinny być metalowe lub obite blachą stalową o grubości 2 mm, z zabezpieczeniem antywłamaniowym, oraz wyposażone w dwa zamki o skomplikowanym mechanizmie.

4. Okna kancelarii powinny być zabezpieczone stalowymi kratami oraz przed obserwacją kancelarii z zewnątrz.

5. Wyposażenie kancelarii powinny stanowić szafy pancerne z zamkami o skomplikowanym mechanizmie.

6. W kancelarii można zainstalować system nadzoru wizyjnego wyłącznie w celu kontroli dostępu do pomieszczeń.

7. W kancelarii można wydzielić pomieszczenie, w którym osoby posiadające poświadczenie bezpieczeństwa mogą zapoznawać się z dokumentami na miejscu.

§ 6.
1. Zabrania się przechowywania w kancelarii dokumentów nie zawierających informacji niejawnych, chyba że wchodzą one w skład zbioru dokumentów.

2. Dokumenty zawierające informacje niejawne oznaczone klauzulą „ściśle tajne", „tajne" i „poufne" muszą być przechowywane oddzielnie w odrębnych szafach pancernych bądź ich częściach, jeżeli pozwalają one na osobne zamknięcie dokumentów.

3. Dokumenty oznaczone klauzulą „zastrzeżone" mogą być przechowywane poza kancelarią, w innych pomieszczeniach jednostki organizacyjnej, jeżeli będą umieszczane w meblach biurowych zamykanych na klucz.

4. Kierownik jednostki organizacyjnej może wyrazić zgodę na przechowywanie dokumentów zawierających informacje niejawne poza kancelarią, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do ich klauzul tajności, na czas niezbędny do realizacji zadań związanych z dostępem do tych informacji.

5. Przedmioty lub urządzenia o dużych wymiarach, stanowiące bądź zawierające informacje tajne, przechowuje się w oddzielnych pomieszczeniach spełniających wymogi kancelarii.

§ 7.
1. Po zakończeniu pracy kierownik kancelarii jest obowiązany sprawdzić prawidłowość zamknięcia szaf pancernych, a następnie zamyka i plombuje pomieszczenia kancelarii.

2. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do kancelarii oraz szaf pancernych określa plan ochrony.

3. Zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych, określa także plan ochrony.

4. Wszelkie nieprawidłowości związane z naruszeniem zasad, o których mowa w ust. 1-3, należy niezwłocznie zgłaszać pełnomocnikowi ochrony.

§ 8.
Kancelaria przyjmuje, rejestruje, przechowuje, przekazuje i wysyła dokumenty zawierające informacje niejawne, oznaczone klauzulami „ściśle tajne", „tajne" i „poufne", oraz prowadzi rejestry dokumentów:

1) dziennik korespondencji dokumentów oznaczonych klauzulą „ściśle tajne", którego wzór określa załącznik nr 1 do rozporządzenia,

2) dziennik korespondencji dokumentów oznaczonych klauzulą „tajne", którego wzór określa załącznik nr 2 do rozporządzenia,

3) dziennik korespondencji dokumentów oznaczonych klauzulą „poufne", którego wzór określa załącznik nr 3 do rozporządzenia,

4) karty zapoznania się z dokumentami oznaczonymi klauzulami „ściśle tajne i tajne", których wzór określa załącznik nr 4 do rozporządzenia,

5) książkę doręczeń przesyłek miejscowych, której wzór określa załącznik nr 5 do rozporządzenia,

6) dziennik ewidencji wykonanych dokumentów oznaczonych klauzulą „ściśle tajne", „tajne" i „poufne", którego wzór określa załącznik nr 6 do rozporządzenia,

7) wykaz przesyłek nadanych, którego wzór określa załącznik nr 7 do rozporządzenia,

8) rejestr teczek dokumentów niejawnych, dzienników i książek ewidencyjnych, którego wzór określa załącznik nr 8 do rozporządzenia.

§ 9.
1. Przesyłki lub dokumenty zawierające informacje niejawne stanowiące tajemnicę państwową przyjmuje się za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.

2. Przy przyjmowaniu przesyłki sprawdza się:

1) prawidłowość adresu,
2) całość pieczęci i opakowania,
3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
4) zgodność numerów na przesyłce z numerami w wykazie przesyłek nadanych lub w książce doręczeń.

3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania pracownik kancelarii kwitujący odbiór przesyłki sporządza wraz z doręczającym protokół uszkodzenia, przekazując go nadawcy, kierownikowi jednostki organizacyjnej i przewoźnikowi - jeżeli pośredniczył w obiegu przesyłek.

4. Po otwarciu przesyłki:

1) sprawdza się, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,
2) ustala się, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych pismach.

5. Kierownik kancelarii w razie stwierdzenia nieprawidłowości, o których mowa w ust. 3 i 4, odmawia jej przyjęcia.

§ 10.
1. Kierownik kancelarii lub uprawniony pracownik rejestruje przyjęte dokumenty:

1) oznaczone klauzulą „ściśle tajne" - w dzienniku korespondencji dokumentów oznaczonych klauzulą „ściśle tajne";
2) oznaczone klauzulą „tajne" - w dzienniku korespondencji dokumentów oznaczonych klauzulą „tajne";
3) oznaczone klauzulą „poufne" - w dzienniku korespondencji dokumentów oznaczonych klauzulą „poufne".

2. Dla każdego dokumentu zawierającego informacje niejawne oznaczone klauzulami „ściśle tajne" i „tajne", z chwilą zarejestrowania w odpowiednim dzienniku korespondencji, zakłada się kartę zapoznania się z dokumentem, którą dołącza się do dokumentu.

3. Kierownik kancelarii lub osoba upoważniona przekazuje dokumenty oznaczone klauzulą „poufne" właściwemu pracownikowi, za pokwitowaniem w dzienniku korespondencji.

4. Dokumenty oznaczone klauzulą „ściśle tajne" i „tajne" kierownik kancelarii udostępnia upoważnionym pracownikom jednostki organizacyjnej, czyniąc odpowiednią adnotację w dzienniku korespondencji.

5. Dokumenty oznaczone klauzulą „ściśle tajne" lub „tajne", które są niezbędne do wykorzystania w celach określonych w art. 49 ustawy o ochronie informacji niejawnych, mogą być wydane poza kancelarię osobie spoza jednostki organizacyjnej posiadającej odpowiednie poświadczenie bezpieczeństwa. Dokument wydaje kierownik kancelarii na podstawie pisemnej zgody kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej za pokwitowaniem w dzienniku korespondencji oraz ze stosowną adnotacją w karcie zapoznania się z dokumentem.

§ 11.
1. Kancelaria nie otwiera przesyłek oznaczonych „do rąk własnych", wpisując do dziennika korespondencji z opakowania nadawcę, numer i datę wpływu pisma; w rubryce „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 w dzienniku korespondencji. Przesyłkę przekazuje się bezpośrednio adresatowi, a w razie jego nieobecności, osobie przez niego upoważnionej do odbioru - za pokwitowaniem w dzienniku korespondencji.

3. Zatrzymanie przez kierownika jednostki organizacyjnej dokumentu, adresowanego „do rąk własnych", odnotowuje się w dzienniku korespondencji w rubryce „Uwagi".

4. Przesyłki oznaczone „do rąk własnych", po wykorzystaniu, zwraca się do kancelarii w stanie otwartym bądź zamkniętym.

§ 12.
Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu tych przesyłek w książce doręczeń przesyłek miejscowych odnotowuje się godzinę doręczenia.

§ 13.
1. Każdą otrzymaną i wysyłaną przesyłkę wpisuje się do kolejnej pozycji właściwego dziennika korespondencji.

2. Zapisów w dziennikach korespondencji dokonuje się atramentem lub tuszem, a zmiany zapisów w tych dziennikach - kolorem czerwonym, z datą i czytelnym podpisem dokonującego zmiany.

3. Zabrania się wycierania i zamazywania zapisów w dziennikach korespondencji.

§ 14.
Dokumenty ostatecznie załatwionej sprawy, z wyjątkiem oznaczonych klauzulą „zastrzeżone", wszywa się do teczki, zgodnie z rzeczowym podziałem akt, i całość kwalifikuje według dokumentu o najwyższej klauzuli tajności.

§ 15.
Do obiegu dokumentów oznaczonych klauzulą „zastrzeżone" stosuje się przepisy właściwych instrukcji kancelaryjnych.

§ 16.
1. Akta spraw zakończonych przechowuje się w kancelarii tajnej przez okres dwóch lat. Po upływie tego okresu akta przekazuje się do archiwum zakładowego lub składnicy akt, jeżeli jednostka organizacyjna takim dysponuje.

2. Zasady brakowania i archiwizowania dokumentów regulują odrębne przepisy.

§ 17.
Rozporządzenie wchodzi w życie z dniem 11 marca 1999 r.

ZAŁĄCZNIK Nr 1

DZIENNIK KORESPONDENCJI DOKUMENTÓW OZNACZONYCH KLAUZULĄ „ŚCIŚLE TAJNE"

Strona lewa

Wpływ sprawy								
Numer kolejny sprawy	Data wpływu dokumentu	Nazwa instytucji nadawcy dokumentu	Numer i data dokumentu otrzymanego	Jakiej sprawy dokument dotyczy	Ilość stron dokumentu	Ilość załączników i ilość arkuszy załączników	Komu przekazano dokument (nazwisko i imię)	Podpis i data pobierają dokum.
1	2	3	4	5	6	7	8	9

Strona prawa

	Załatwienie sprawy				
Korespondencja uzupełniająca (numer, data, nadawca dodatkowego dokumentu)	Data i potwierdzenie wysłania dokumentu	Adresat	Liczba stron dokumentu	Ilość załączników i ilość arkuszy załączników	Uwagi
10	11	12	13	14	15

ZAŁĄCZNIK Nr 2

DZIENNIK KORESPONDENCJI DOKUMENTÓW OZNACZONYCH KLAUZULĄ „TAJNE”

Strona lewa

Wpływ dokumentu						Przekazanie dokumentu		
Numer kolejny sprawy	Data wpływu dokumentu	Nazwa instytucji nadawcy dokumentu	Numer i data dokumentu otrzymanego	Jakiej sprawy dokument dotyczy	Ilość stron dokumentu	Ilość załączników i ilość arkuszy załączników	Komu przekazano dokument (nazwisko i imię)	Podpis i data pobierającego dokument
1	2	3	4	5	6	7	8	9

Strona prawa

	Sposób załatwienia					
Informacje uzupełniające	Data i potwierdzenie zwrotu dokumentu	Data wysłania dokumentu	Adresat	Liczba stron dokumentu	Ilość załączników i ilość arkuszy załączników	Uwagi
10	11	12	13	14	15	16

ZAŁĄCZNIK Nr 3

DZIENNIK KORESPONDENCJI DOKUMENTÓW OZNACZONYCH KLAUZULĄ „POUFNE"

Strona lewa

Wpływ dokumentu							Przekazanie dokumentu	
Numer kolejny sprawy	Data wpływu dokum.	Nazwa instytucji nadawcy dokumentu	Numer i data dokumentu otrzymanego	Jakiej sprawy dokument dotyczy	Ilość stron dokumentu	Ilość załączników ilość ark. załączników	Komu przekazano dokument (nazwisko i imię)	Podpis i data pobierającego dokument
1	2	3	4	5	6	7	8	9

Strona prawa

	Sposób załatwienia					
Informacje uzupełniające	Data i potwierdzenie zwrotu dokumentu	Data wysłania dokumentu	Adresat	Liczba stron dokumentu	Ilość załączników i ilość arkuszy załączników	Uwagi
10	11	12	13	14	15	16

ZAŁĄCZNIK Nr 4

KARTA ZAPOZNANIA SIĘ Z DOKUMENTEM OZNACZONYM KLAUZULĄ „ŚCIŚLE TAJNE”*) „TAJNE” *) nr .....

	Udostępnienie dokumentu					Zwrot dokumentu			
Lp.	Numer i nazwa dokumentu	Klauzula	Imię Nazwisko	Data	Podpis	Imię Nazwisko	Data	Podpis	Uwagi
1	2	3	4	5	6	7	8	9	10

*) Niepotrzebne skreślić.

ZAŁĄCZNIK Nr 5

KSIĄŻKA DORĘCZEŃ PRZESYŁEK MIEJSCOWYCH

Data	Odbiorca i jego adres	Znak pisma (rodzaj przesyłki)	Potwierdzenie odbioru (data, pieczęć i podpis)

ZAŁĄCZNIK Nr 6

DZIENNIK EWIDENCJI WYKONANYCH DOKUMENTÓW OZNACZONYCH KLAUZULĄ „ŚCIŚLE TAJNE", „TAJNE" I „POUFNE" (techniką maszynopisania, kopiowania, powielania, fotografowania itp.)

strona lewa

	Pokwitowanie dokumentu oddanego do wykonania				
Lp.	Data oddania brudnopisu do przepisania - dokumentu do reprodukcji	Adresat bądź nazwa dokumentu	Nazwisko pracownika lub nazwa komórki organizacyjnej oddającej dokument do reprodukcji	Nr dokumentu z dziennika korespondencji, klauzula tajności i liczba stron	Nazwisko wykonującego dokument
1	2	3	4	5	6

strona prawa

Liczba wykonanych		Pokwitowanie odbioru wykonanego dokumentu			Adnotacje		Uwagi
egzemplarzy	arkuszy	imię i nazwisko	data	podpis	o wysłaniu (Nr wychodzący)	o zniszczeniu	
7	8	9	10	11	12	13	14

ZAŁĄCZNIK Nr 7

...., dnia ..... r.
(pieczęć nagłówkowa
jednostki organizacyjnej)

WYKAZ PRZESYŁEK NADANYCH

przekazanych przez .....
(nazwa i adres wysyłającego)

do wysłania .....
(nazwa przewoźnika lub nazwisko doręczyciela)

Lp.	Numer przesyłki	Rodzaj przesyłki	Do kogo adresowany	Uwagi
1	2	3	4	5

.....
(podpis sporządzającego wykaz) Ogółem przesyłek .....

.....
(podpis doręczającego)

.....
(podpis przyjmującego)

.....
(data i godzina) Słownie:.....

m.p.
(pieczęć przewoźnika)

ZAŁĄCZNIK Nr 8

REJESTR TECZEK DOKUMENTÓW NIEJAWNYCH, DZIENNIKÓW I KSIĄŻEK EWIDENCYJNYCH

Lp.	Nazwa teczki, dziennika, książki itp.	Klauzula tajności	Data rozpoczęcia	Data zakończenia	Liczba arkuszy (pozycji)	Uwagi
1	2	3	4	5	6	7

Dz.U.99.18.162

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia 25 lutego 1999 r.

w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych

(Dz. U. z dnia 5 marca 1999 r.)

Na podstawie art. 60 ust. 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) zarządza się, co następuje:

§ 1.
Rozporządzenie określa podstawowe wymagania bezpieczeństwa systemów i sieci teleinformatycznych, zwanego dalej „bezpieczeństwem teleinformatycznym", w zakresie ochrony fizycznej, elektromagnetycznej i kryptograficznej oraz bezpieczeństwa transmisji, w sieciach lub systemach teleinformatycznych służących do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, a także wytyczne do opracowania szczególnych wymagań bezpieczeństwa tych systemów i sieci.

§ 2.
1. Ilekroć w rozporządzeniu jest mowa o:

1) ustawie - należy przez to rozumieć ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95),
2) przetwarzaniu informacji niejawnych - należy przez to rozumieć wytwarzanie, przetwarzanie, przechowywanie lub przekazywanie informacji niejawnych,
3) uwierzytelnieniu - należy przez to rozumieć usługę (funkcję) kryptograficzną pozwalającą sprawdzić i potwierdzić autentyczność wymienianych informacji lub podmiotów uczestniczących w wymianie,
4) algorytmach kryptograficznych - należy przez to rozumieć metodę działania, przekształcającą dane w celu ukrycia lub ujawnienia ich zawartości informacyjnej,
5) kluczach kryptograficznych - należy przez to rozumieć ciąg symboli, od którego w sposób istotny zależy wynik działania algorytmu kryptograficznego.

2. Bezpieczeństwo teleinformatyczne zapewnia się przez:

1) ochronę fizyczną,
2) ochronę elektromagnetyczną,
3) ochronę kryptograficzną,
4) bezpieczeństwo transmisji,
5) kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej.

§ 3.
Kierownik jednostki organizacyjnej jest obowiązany zapewnić bezpieczeństwo teleinformatyczne przed przystąpieniem do przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.

§ 4.
Służby ochrony państwa mogą dopuścić do stosowania w systemie lub sieci teleinformatycznej, bez konieczności przeprowadzania badań, urządzenie, które spełnia wymagania bezpieczeństwa określone w rozporządzeniu, jeżeli otrzymało certyfikat właściwej krajowej władzy bezpieczeństwa w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego.

§ 5.
Ochronę fizyczną systemu lub sieci teleinformatycznej zapewnia się przez:

1) umieszczenie urządzeń systemu lub sieci teleinformatycznej w strefach bezpieczeństwa w zależności od:

a) klauzuli tajności informacji niejawnych,
b) ilości informacji niejawnych,
c) zagrożeń w zakresie ujawnienia, utraty, modyfikacji przez osobę nieuprawnioną,

2) instalację środków zabezpieczających pomieszczenia, w których znajdują się urządzenia systemu lub sieci teleinformatycznej, w szczególności przed:

a) nieuprawnionym dostępem,
b) podglądem,
c) podsłuchem.

§ 6.
Przetwarzanie informacji niejawnych, stanowiących tajemnicę państwową lub stanowiących tajemnicę służbową, oznaczonych klauzulą „poufne", w urządzeniach systemu lub sieci teleinformatycznych odbywa się w strefach bezpieczeństwa.

§ 7.
Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się przez umieszczenie urządzeń, połączeń i linii w strefach bezpieczeństwa gwarantujących spełnienie wymogów zabezpieczenia elektromagnetycznego lub zastosowanie urządzeń, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie i filtrowanie zewnętrznych linii zasilających i sygnałowych.

§ 8.
1. Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków zabezpieczających informacje niejawne stanowiące tajemnicę państwową przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych informacji lub uwierzytelnienie podmiotów, lub uwierzytelnienie informacji.

2. Ochronę kryptograficzną systemu lub sieci teleinformatycznej stosuje się przy przekazywaniu w formie elektronicznej informacji, o których mowa w ust. 1, poza strefy bezpieczeństwa.

§ 9.
1. Przemieszczanie urządzeń teleinformatycznych, w których pamięci są informacje niejawne stanowiące tajemnicę państwową lub służbową oznaczone klauzulą „poufne", poza strefy bezpieczeństwa wymaga stosowania kryptograficznych metod i środków ochrony tych informacji lub innych środków ochrony, gwarantujących ich zabezpieczenie przed nieuprawnionym ujawnieniem.

2. Przepis ust. 1 stosuje się do elektronicznych nośników danych zawierających informacje niejawne, stanowiące tajemnicę państwową lub służbową oznaczone klauzulą „poufne", przemieszczanych poza strefy bezpieczeństwa.

§ 10.
1. Do kryptograficznej ochrony informacji niejawnych stanowiących tajemnicę państwową stosuje się, odpowiednie dla klauzuli „tajne" i „ściśle tajne", algorytmy kryptograficzne oraz środki gwarantujące ochronę tych algorytmów, kluczy kryptograficznych oraz innych istotnych parametrów zabezpieczenia, a w szczególności haseł dostępu.

2. Właściwymi do potwierdzenia przydatności algorytmów i środków, o których mowa w ust. 1, w celu ochrony informacji niejawnych o określonej klauzuli tajności, są służby ochrony państwa.

§ 11.
1. Podłączenie urządzenia systemu lub sieci teleinformatycznej, w którym są przetwarzane informacje niejawne stanowiące tajemnicę państwową, do powszechnie dostępnego urządzenia systemu lub sieci jest dopuszczalne pod warunkiem zastosowania metod i środków, o których mowa w § 8.

2. Podłączenie urządzenia systemu lub sieci teleinformatycznej, w którym są przetwarzane informacje niejawne stanowiące tajemnicę służbową, do powszechnie dostępnego urządzenia systemu lub sieci jest dopuszczalne pod warunkiem zastosowania właściwych mechanizmów kontroli dostępu, o których mowa w § 12 ust. 2.

§ 12.
1. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej:

1) kierownik jednostki organizacyjnej określa warunki i sposób przydzielania uprawnień ich użytkownikom,
2) administrator systemów i sieci teleinformatycznych określa warunki oraz sposób przydzielania tym użytkownikom kont i haseł, a także zapewnia właściwe wykorzystanie mechanizmów, o których mowa w ust. 2.

2. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych przetwarzanych w tych systemach lub sieciach.

§ 13.
System lub sieć teleinformatyczna, w której są przetwarzane informacje niejawne stanowiące tajemnicę państwową, projektuje się, organizuje i eksploatuje w sposób uniemożliwiający niekontrolowany dostęp jednej osoby do wszystkich zasobów systemu lub sieci, a w szczególności do danych, oprogramowania i urządzeń.

§ 14.
1. Szczególne wymagania bezpieczeństwa opracowuje się, po dokonaniu analizy przewidywanych zagrożeń, indywidualnie dla każdego systemu lub sieci teleinformatycznej, w której mają być przetwarzane informacje niejawne, z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej.

2. Szczególne wymagania bezpieczeństwa formułuje się na etapie projektowania nowego systemu lub sieci teleinformatycznej, a następnie uzupełnia i rozwija wraz z wdrażaniem, eksploatacją i modernizacją tego systemu lub sieci.

§ 15.
Szczególne wymagania bezpieczeństwa systemu lub sieci teleinformatycznych powinny określać wielkość i lokalizację stref bezpieczeństwa oraz środki ich ochrony odpowiednie dla danej jednostki organizacyjnej.

§ 16.
Przy opracowaniu szczególnych wymagań bezpieczeństwa należy uwzględnić:

1) charakterystykę systemu lub sieci teleinformatycznej,
2) dane o budowie systemu lub sieci teleinformatycznej,
3) określenie środków ochrony zapewniających bezpieczeństwo informacji niejawnych, przetwarzanych w systemie lub sieci teleinformatycznej, przed możliwością narażenia ich bezpieczeństwa, a w szczególności nieuprawnionym ujawnieniem,
4) zadania administratora systemu lub sieci teleinformatycznej i pracownika pionu, o których mowa w art. 63 ust. 1 ustawy.

§ 17.
Charakterystyka systemu lub sieci teleinformatycznej powinna określać:

1) klauzulę tajności informacji niejawnych, które będą przetwarzane w systemie lub sieci teleinformatycznej,
2) kategorie uprawnień użytkowników systemu lub sieci teleinformatycznej w zakresie dostępu do przetwarzanych w nich informacji niejawnych, w zależności od klauzuli tajności tych informacji.

§ 18.
Dane o budowie systemu lub sieci teleinformatycznej zawierają informacje dotyczące tego systemu lub sieci w zakresie:

1) lokalizacji,
2) typu wykorzystywanych w nich urządzeń oraz oprogramowania,
3) sposobu realizowania połączeń wewnętrznych oraz zewnętrznych,
4) konfiguracji sprzętowej,
5) środowiska eksploatacji.

§ 19.

Środki ochrony, o których mowa w § 16 pkt 3, powinny uwzględniać wskazanie osób odpowiedzialnych za bezpieczeństwo systemu lub sieci teleinformatycznej oraz określać procedury bezpieczeństwa związane z jego eksploatacją i kontrolą, a także wskazywać szczegółowe wymagania w zakresie szkoleń dla administratorów, pracowników pionu i wszystkich użytkowników systemu lub sieci.

§ 20.

Rozporządzenie wchodzi w życie z dniem 11 marca 1999 r.

Dz.U.99.18.168
Dz.U.05.39.375

ROZPORZĄDZENIE

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. z dnia 5 marca 1999 r.)

Na podstawie art. 53 ust. 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) zarządza się, co następuje:

§ 1.
Rozporządzenie określa sposób przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem przez podmioty wykonujące czynności lub świadczące usługi w tym zakresie, zwane dalej „przewoźnikami".

§ 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 (Dz. U. Nr 11, poz. 95), 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 Spraw Wewnętrznych i Administracji, 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, które uzyskały koncesję na prowadzenie usług pocztowych,
5) przedsiębiorców, którzy uzyskali koncesję na prowadzenie działalności 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 listów 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 listy za pośrednictwem przewoźników, powinny być opakowane w dwie nieprzezroczyste i mocne koperty, przy czym na kopertach muszą być umieszczone:

1) 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 korespondencyjnym.

2) 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 muszą mieć odciśniętą pieczęć „do pakietów" i zabezpieczone przezroczystą taśmą samoprzylepną, przy czym na kopercie zewnętrznej, zamiast taśmy samoprzylepnej, może być stosowana pieczęć z laku.

3. Materiały zawierające informacje niejawne stanowiące tajemnicę służbową, nadawane w postaci listów, przekazuje się jako listy polecone lub wartościowe, w dwóch nieprzezroczystych mocnych kopertach, które oznacza się tak jak w ust. 1.

4. Materiały zawierające informacje niejawne stanowiące tajemnicę państwową, nadawane w postaci paczek przewożonych przez przewoźników, muszą być opakowane w dwie nieprzeźroczyste 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 wartościowe w dwóch nieprzeźroczystych warstwach mocnego papieru, przy czym na opakowaniu zewnętrznym nie umieszcza się klauzuli tajności.

6. Do oznaczania materiałów, o których mowa w ust. 3 i 5, stosuje się odpowiednio ust. 1, z tym że sposób adresowania określają odrębne przepisy.

§ 6.
1. Przesyłki przyjmowane przez przewoźników, o których mowa w § 2 ust. 2 pkt 1-3, w zasadzie nie powinny przekraczać następujących wymiarów i masy:

1) listy - 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, sporządzanych przez nadawcę.

2. Wykaz przesyłek nadanych sporządzany jest w dwóch egzemplarzach, po jednym egzemplarzu dla przewoźnika i nadawcy przesyłki.

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 nie odpowiadającej wymaganiom określonym w § 6 ust. 1 lub może odmówić przyjęcia przesyłki nie odpowiadającej wymaganiom określonym w § 5.

5. W przypadku odmowy przyjęcia przesyłki, o której mowa w ust. 4, przewoźnik wykreśla ją z wykazu przesyłek nadanych, potwierdzając to podpisem osoby odmawiającej przyjęcia przesyłki i odciskiem pieczęci przewoźnika na obu egzemplarzach wykazu.

6. W przypadku przekazania materiałów bez pośrednictwa przewoźników, o których mowa w § 2 ust. 2, adresat przesyłki potwierdza pisemnie nadawcy ich odbiór.

7. Wzór wykazu przesyłek nadanych stanowi załącznik nr 1 do rozporządzenia.

§ 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 przedziału 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),
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 1 i 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 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 Rzeczypospolitej Polskiej, a w przypadku, o którym mowa w ust. 2, także na terenie kraju wówczas, gdy przesyłki przekazywane są bezpośrednio od nadawcy do odbiorcy na terenie tej samej miejscowości przy spełnieniu następujących warunków:

1) 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,
2) przewożone materiały są zabezpieczone przed zniszczeniem oraz dostępem osób nieuprawnionych.

4. Konwojentów wyposaża się w dokumenty niezbędne do wykonania zadania:

1) instrukcję postępowania z ochranianymi i przewożonymi przesyłkami,
2) środki łączności umożliwiające kontakt z konwojem podczas całej podróży.

§ 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.
Trasę przewozu przesyłki zawierającej informacje niejawne stanowiące tajemnicę państwową lub służbową, oznaczonej klauzulą „poufne", przewoźnik, o którym mowa w § 2 ust. 2 pkt 4 i 5, uzgadnia z nadawcą, jej dostarczenie zaś powinno odbyć się bez zbędnej zwłoki.

§ 14.
1. W czasie przewożenia przesyłki niedopuszczalne jest pozostawienie jej bez nadzoru konwojentów, a w szczególności oddawanie do publicznie 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 ochrony nadawcy lub adresata przesyłki.

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

1) materiały powinny być przewożone przez nadawców lub odbiorców pod ochroną co najmniej dwóch uzbrojonych w broń palną konwojentów, według instrukcji kierownika kancelarii tajnej nadawcy lub upoważnionego przez niego pracownika,
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) przewożone materiały należy zabezpieczyć przed zniszczeniem oraz dostępem osób nieuprawnionych.

2. Odstępstwo od warunku posiadania broni palnej, o którym mowa w ust. 1 pkt 1, jest możliwe wówczas, gdy przesyłki przekazywane są bezpośrednio od nadawcy do odbiorcy na terenie tej samej miejscowości.

§ 16.
1. W przypadku uszkodzenia opakowania 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, o którym mowa w ust. 1, stanowi załącznik nr 2 do rozporządzenia.

§ 17.
1. Przewoźnik wydaje przesyłki upoważnionemu przedstawicielowi adresata na podstawie wykazu przesyłek wydanych, sporządzonego przez przewoźnika.

2. Wzór wykazu, o którym mowa w ust. 1, stanowi załącznik nr 3 do rozporządzenia.

3. Upoważniony przedstawiciel adresata, przed odebraniem przesyłki, obowiązany jest przedstawić upoważnienie.

4. Wzór upoważnienia, o którym mowa w ust. 3, stanowi załącznik nr 4 do rozporządzenia.

§ 18.
Przesyłkę nie odebraną w terminie trzech dni od daty zawiadomienia adresata o jej nadejściu odsyła się do nadawcy, jeżeli odrębne przepisy nie określają innego terminu.

§ 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 niezwłocznie - 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 5 i 6.

3. Organizację i zasady ochrony materiałów, o których mowa w ust. 1, określają odrębne przepisy.

§ 21.
1. W przypadku gdy zachodzi konieczność pilnego wywozu za granicę materiałów przez przedstawiciela naczelnego lub centralnego organu państwowego, 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) posiada stosowne poświadczenie 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) będzie miała zapewniony środek łączności umożliwiający szybki kontakt z jednostką delegującą,
5) będzie miała zapewnione za granicą miejsce zamieszkania uniemożliwiające lub utrudniające dostęp osób nieuprawnionych lub 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, jest obowiązany powiadomić o potrzebie wywozu materiałów właściwą służbę ochrony państwa. W przypadku konieczności zdeponowania materiałów, o której mowa w ust. 5, informuje Ministerstwo Spraw Zagranicznych lub właściwe polskie przedstawicielstwo dyplomatyczne.

3. Osoba wywożąca za granicę materiały musi być wyposażona w instrukcję określającą zasady postępowania z tymi materiałami, wydaną przez kierownika jednostki organizacyjnej.

4. Uchylony.

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.

6. W przypadku wywożenia za granicę materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone" przepisów ust. 2, 3 i 5 nie stosuje się.

§ 22.
Rozporządzenie wchodzi w życie z dniem 11 marca 1999 r.

ZAŁĄCZNIK Nr 1

.....
(pieczęć nagłówkowa
jednostki nadającej)

....., dnia ....-....-.... r.
(miejscowość)

WYKAZ Nr .....
PRZESYŁEK NADANYCH

przez .....
(nazwa jednostki organizacyjnej)
..... w .....
(nazwa przewoźnika)

Lp.	Nazwa nadawcy i nr pakowania	Rodzaj przesyłki	Adresat	Uwagi
1	2	3	4	5

Ogółem przesyłek ....
(liczbowo) (podpis sporządzającego
wykaz)
....
(słownie) (podpis przyjmującego przesyłki)
.....
(data przyjęcia)
.....
(pieczęć do pokwitowań przewoźnika)

Pouczenie: Wykaz wypełnić maszynowo lub odręcznie w sposób czytelny. W kolumnie 3 wpisać literę symbolizującą rodzaj przesyłki: L - dla listu, P - dla paczki, I - inne.

ZAŁĄCZNIK Nr 2

.....
(pieczęć nagłówkowa
przewoźnika)
Egz. nr .....

....., dnia ...-...-.....r.
(miejscowość)

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 3

.....
(pieczęć nagłówkowa
placówki przewoźnika)

....., dnia ...-...-.....r.
(miejscowość)

WYKAZ Nr ...
PRZESYŁEK WYDANYCH

.....
(nazwa jednostki organizacyjnej odbierającej przesyłki)

.....
(nazwa przewoźnika)

Lp.	Numer pakowania	Rodzaj przesyłki	Nadawca	Uwagi
1	2	3	4	5

Ogółem przesyłek ....
(liczbowo) (podpis sporządzającego
wykaz)

....
(słownie) (podpis wydającego przesyłki)

.....
(podpis przyjmującego przesyłki)

.....
(data przyjęcia)

.....
(pieczęć do pokwitowań adresata)

Pouczenie: Wykaz wypełnić maszynowo lub odręcznie w sposób czytelny. W kolumnie 3 wpisać literę symbolizującą rodzaj przesyłki: L - dla listu, P - dla paczki, I - inne.

Załącznik nr 4

	.....
	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:

m.p.	m.p.	m.p.	m.p.
20..... r.	20..... r.	20..... r.	20..... r.

Dz.U.03.211.2071

ROZPORZĄDZENIE
MINISTRÓW SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1)]
ORAZ OBRONY NARODOWEJ

z dnia 27 listopada 2003 r.

w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach

(Dz. U. z dnia 12 grudnia 2003 r.)

Na podstawie art. 23 ust. 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.2) zarządza się, co następuje:

§ 1.
1. Rozporządzenie określa sposób oznaczania materiałów, w tym klauzulami tajności, oraz sposób umieszczania klauzul na materiałach będących w posiadaniu jednostek organizacyjnych, określonych w art. 1 ust. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, zwanej dalej „ustawą".

2. Przez oznaczenie materiałów klauzulami tajności należy rozumieć umieszczenie tych klauzul na materiałach.

§ 2.
1. Nadaną klauzulę tajności nanosi się w sposób wyraźny, w pełnym brzmieniu.

2. Zmiany nadanej klauzuli lub jej zniesienia dokonuje się przez jej skreślenie i wpisanie obok niej nowej klauzuli z podaniem daty, imienia i nazwiska oraz podpisem dokonującego zmiany lub zniesienia, uwierzytelnionym pieczęcią do tuszu z napisem „Do pakietów". Zmianę klauzuli lub jej zniesienie bez wpisania daty, imienia i nazwiska oraz podpisu dokonującego zmiany lub zniesienia, uwierzytelnionego pieczęcią, uważa się za niedokonane. Skreślenia oraz pozostałych wpisów dokonuje się kolorem czerwonym. Wycieranie, wywabianie lub zamazywanie klauzuli, która podlega zmianie lub zniesieniu, i dokonanych zmian jest niedozwolone.

3. Zmianę lub zniesienie klauzuli dokumentu lub przedmiotu należy odnotować w odpowiednich dziennikach ewidencyjnych lub rejestrach materiałów niejawnych, z podaniem podstawy zmiany lub zniesienia klauzuli.

4. Zmiany lub zniesienia klauzuli tajności dokumentu lub przedmiotu, w sposób określony w ust. 2 i 3, dokonują:

1) kierownik kancelarii tajnej lub pracownik kancelarii - w odniesieniu do dokumentów przechowywanych w kancelarii tajnej,

2) kierownik archiwum - w odniesieniu do dokumentów przechowywanych w archiwum - na pisemne polecenie osoby, o której mowa w art. 21 ust. 1 lub art. 25 ust. 5 ustawy, oraz po upływie okresów ochrony, o których mowa w art. 25 ust. 1, 3 i 4.

§ 3.
Materiałom w postaci dokumentów zawierających informacje niejawne nadaje się odpowiednią klauzulę tajności oraz oznacza się w następujący sposób:

1) na pierwszej stronie dokumentu umieszcza się:

a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej,

b) w prawym górnym rogu, od góry w kolejności pionowej:
- nazwę miejscowości i datę sporządzenia dokumentu,
- klauzulę tajności,
- numer egzemplarza dokumentu, a w przypadku, gdy dokument sporządzono w jednym egzemplarzu, napis: „Egzemplarz pojedynczy",

c) w lewym dolnym rogu numer, pod jakim dokument został zarejestrowany w dzienniku ewidencji wykonanych dokumentów,

d) w prawym dolnym rogu klauzulę tajności oraz numer strony łamany przez liczbę stron całego dokumentu,

e) w przypadku pism korespondencyjnych dodatkowo:
- w lewym górnym rogu pod nazwą jednostki lub komórki organizacyjnej sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej oraz numer, pod którym dokument został zarejestrowany w odpowiednim dzienniku, łamany przez dwie ostatnie cyfry roku, w którym pismo zostało sporządzone, poprzedzony cyframi: „00" - w przypadku dokumentu oznaczonego klauzulą „ściśle tajne", cyfrą „0" - w przypadku dokumentu oznaczonego klauzulą „tajne", literami „Pf" - w przypadku dokumentu oznaczonego klauzulą „poufne", literą „Z" - w przypadku dokumentu oznaczonego klauzulą „zastrzeżone", oddzielonymi od numeru rejestracyjnego myślnikiem, a także w zależności od potrzeb - inne oznaczenia ułatwiające ustalenie miejsca sporządzenia dokumentu w jednostce lub komórce organizacyjnej nadawcy lub też przynależność dokumentu do określonej sprawy,
- w prawym górnym rogu od góry 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 dokumentu umieszcza się:

a) w prawym górnym rogu w kolejności pionowej:
- klauzulę tajności,
- numer egzemplarza dokumentu, a w przypadku sporządzenia dokumentu w jednym egzemplarzu napis: „Egzemplarz pojedynczy",

b) w lewym dolnym rogu numer, pod jakim dokument został zarejestrowany w dzienniku ewidencji wykonanych dokumentów, łamany przez dwie ostatnie cyfry roku, w którym dokument został wykonany, poprzedzony cyframi lub literami oznaczającymi klauzulę tajności, o których mowa w pkt 1 lit. e tiret pierwsze, oddzielonymi od tego numeru myślnikiem,

c) w prawym dolnym rogu klauzulę tajności, numer strony łamany przez liczbę stron całego dokumentu;

3) na ostatniej stronie dokumentu umieszcza się:

a) w prawym górnym rogu w kolejności pionowej:
- klauzulę tajności,
- numer egzemplarza dokumentu, a w przypadku sporządzenia dokumentu w jednym egzemplarzu napis: „Egzemplarz pojedynczy",

b) z lewej strony pod treścią:
- liczbę załączników, jeżeli są dołączone do dokumentu,
- klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiednim dzienniku,
- liczbę stron lub kart 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 do osoby podpisującej dokument,

c) z prawej strony pod treścią dokumentu i adnotacją o załącznikach w kolejności pionowej: stanowisko oraz imię i nazwisko osoby podpisującej dokument,

d) w lewym dolnym rogu w kolejności pionowej:
- liczbę wykonanych egzemplarzy,
- adresatów poszczególnych egzemplarzy dokumentu lub adnotację: „Adresaci według rozdzielnika",
- nazwisko osoby, która sporządziła dokument, oraz nazwisko osoby, która wykonała dokument,
- numer, pod jakim dokument został zewidencjonowany w dzienniku ewidencji wykonanych dokumentów,

e) w prawym dolnym rogu klauzulę tajności oraz numer strony łamany przez liczbę stron całego dokumentu;

4) w trwale oprawionych książkach, dziennikach korespondencyjnych, broszurach, reprodukcjach oraz innych zbiorach dokumentów klauzule tajności umieszcza się:

a) po prawej stronie na górze i dole zewnętrznych ścianek okładki oraz na stronie tytułowej, jeżeli dokument ją posiada,

b) po prawej stronie na górze i na dole pozostałych stron, w przypadku dokumentów drukowanych jednostronnie,

c) po prawej stronie na górze i na dole przy zewnętrznym marginesie na stronach nieparzystych oraz po lewej stronie na górze i na dole przy zewnętrznym marginesie na stronach parzystych, w przypadku dokumentów drukowanych dwustronnie;

5) pod numerem egzemplarza, o którym mowa w pkt 1 lit. b tiret trzecie, można zamieścić dyspozycję dla adresata o treści:

a) „udzielanie informacji zawartej w dokumencie bez zgody kierownika jednostki (komórki) organizacyjnej jest zakazane",

b) „wykonanie kopii bez zgody kierownika jednostki (komórki) organizacyjnej jest zakazane",

c) „wykonanie odpisu bez zgody kierownika jednostki (komórki) organizacyjnej jest zakazane",

d) „wykonanie kopii stron od ..... do ..... oraz od ..... do ..... bez zgody kierownika jednostki (komórki) organizacyjnej jest zakazane",

e) „wykonanie odpisu od ..... do ..... oraz od ..... do ..... bez zgody kierownika jednostki (komórki) organizacyjnej jest zakazane",

f) „wykonanie wypisu (wyciągu) od ..... do ..... oraz od ..... do ..... bez zgody kierownika jednostki (komórki) organizacyjnej jest zakazane";

6) w uzasadnionych przypadkach na dokumentach zawierających informacje niejawne pod numerem egzemplarza, o którym mowa w pkt 1 lit. b tiret trzecie, można zamieszczać dyspozycję dla adresata o treści: „do zapoznania w trybie obiegowym" lub zapis o treści „dokument podlega ochronie do .....", jeżeli dokument podlega krótszemu okresowi ochrony, niż przewiduje ustawa.

§ 4.
Na materiałach w postaci wykresów, map, rysunków i innych dokumentów graficznych klauzulę tajności umieszcza się pod legendą, blokiem tytułowym lub skalą oraz na stronach zewnętrznych w miejscach widocznych po złożeniu. Na materiałach tych umieszcza się w zależności od klauzuli tajności oznaczenia:

1) sygnaturę literowo-cyfrową, poprzedzoną cyframi lub literami oznaczającymi klauzulę tajności, o których mowa w § 3 pkt 1 lit. e tiret pierwsze, a w przypadku załączników - sygnaturę literowo-cyfrową materiału macierzystego;

2) numer egzemplarza materiału, a w przypadku załączników - numer kolejny załącznika;

3) adresatów poszczególnych egzemplarzy materiału, a w przypadku załączników - łączną ilość egzemplarzy załączników.

§ 5.
1. Na dokumentach stanowiących załączniki, na pierwszej stronie w ich górnej prawej części, umieszcza się dodatkowo napis: „Załącznik nr ..... do pisma nr ..... z dnia .....".

2. Jeżeli przy piśmie przewodnim lub dokumencie 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 lub dokumencie można zamieścić, w sposób określony w § 3 pkt 5, dyspozycję wskazującą klauzulę tajności tego dokumentu po trwałym odłączeniu od niego załączników;
3) umieszczony na dokumencie numer według dziennika ewidencji wykonanych dokumentów

poprzedza się cyframi lub literami odpowiadającymi klauzuli tajności wskazanej w dyspozycji, o której mowa w pkt 2.

3. Na piśmie przewodnim, o którym mowa w ust. 2, jeżeli jego treść jest jawna, nie umieszcza się numeru według dziennika ewidencji wykonanych dokumentów, a przy jego ewidencjonowaniu, w rubryce „uwagi" dziennika korespondencji, należy wpisać adnotację: „pismo przewodnie jawne".

§ 6.
Na materiałach zawierających informacje niejawne w formie mikrofilmów, negatywów, fotografii, nośników do zapisów informacji w postaci cyfrowej i taśm magnetycznych, a także na odbitkach, kliszach, matrycach i dyskach optycznych, w sprzęcie elektronicznym z wbudowaną pamięcią lub na innych nośnikach danych elektronicznych klauzulę tajności umieszcza się w sposób widoczny na obudowie lub opakowaniu, nanosząc jednocześnie oznaczenia zgodnie z § 3 pkt 1 lit. a i lit. e tiret pierwsze.

§ 7.
Zapis na taśmach magnetycznych lub filmowych zawierających informacje niejawne rozpoczyna się i kończy informacją o klauzuli tajności.

§ 8.
1. Na materiałach w postaci przedmiotów zawierających informacje niejawne stanowiące tajemnicę państwową lub służbową albo przedmiotach stanowiących tajemnicę, niewymienionych w rozporządzeniu, klauzulę tajności nanosi się w widocznym miejscu przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub podobnych oznaczeń, nanosząc na nie oznaczenia zgodnie z § 3 pkt 1 lit. A i lit. e tiret pierwsze.

2. Obudowy lub opakowania, w których znajdują się materiały zawierające informacje niejawne, oznacza się taką klauzulą, jaką posiada materiał o najwyższym stopniu tajności.

§ 9.
1. Na kopiach, odpisach, wypisach, wyciągach lub tłumaczeniach dokumentu zawierającego informacje niejawne umieszcza się numer, pod którym zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów.

2. Na kopii, odpisie, wypisie, wyciągu lub tłumaczeniu:

1) umieszcza się w prawym górnym rogu na wszystkich stronach napis: „Kopia", „Odpis", „Wypis", „Wyciąg" lub „Tłumaczenie z języka - ..... (nazwa języka) ..... - (imię i nazwisko tłumacza)" oraz dodatkowo na pierwszej stronie numer egzemplarza wykonanej kopii, odpisu, wypisu, wyciągu lub tłumaczenia;

2) pod podpisem osoby, o której mowa w § 3 pkt 3 lit. c, umieszcza się 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.

3. Zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza podpisem kierownik jednostki lub komórki organizacyjnej albo osoba upoważniona, a tłumaczenia - osoba dokonująca tłumaczenia.

4. Fakt sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia odnotowuje się na dokumencie, z którego sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie, poprzez 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) pozycji dziennika ewidencji wykonanych dokumentów, pod którą zarejestrowano kopię, odpis, wypis, wyciąg lub tłumaczenie.

5. Odcisk pieczęci lub informację, o której mowa w ust. 4, zamieszcza się na dokumencie przed sporządzeniem jego kopii, odpisu, wypisu, wyciągu lub tłumaczenia.

§ 10.
Traci moc rozporządzenie Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach (Dz. U. Nr 18, poz. 167 oraz z 2001 r. Nr 121, poz. 1305).

§ 11.
Rozporządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

---

1) Minister Spraw Wewnętrznych i Administracji kieruje działem administracji rządowej - sprawy wewnętrzne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 14 marca 2002 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. Nr 35, poz. 325 i Nr 58, poz. 533).
2) 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 oraz z 2003 r. Nr 17, poz. 155.

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 2002r. 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 1do rozporządzenia Ministra Obrony Narodowej
z dnia 13 września 2002 r. (poz. 1294)

WZÓR

Lewa strona

REJESTR POSTĘPOWAŃ DYSCYPLINARNYCH

Pozycja rejestru	Data zarejestro-wania	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

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 6 lutego 2003 r.

w sprawie zasad organizacji obsługi bibliotecznej w jednostkach organizacyjnych Ministerstwa Obrony Narodowej oraz zasad współdziałania bibliotek publicznych wykonaniu tej obsługi

(Dz. U. z dnia 28 lutego 2003 r.)

Na podstawie art. 26 ust. 2 ustawy z dnia 27 czerwca 1997 r. o bibliotekach (Dz.U. Nr 85, poz. 539, z 1998 r. Nr 106, 668, z 2001 r. Nr 129, poz. 1440 oraz z 2002 r. Nr 113, poz. 984) zarządza się, co następuje:

§ 1.1. Biblioteki wojskowe organizowane i prowadzone w jednostkach organizacyjnych Ministerstwa Obrony Narodowej, zwane dalej „bibliotekami", stanowią resortową sieć biblioteczną.
2. Podmiotami organizującymi biblioteki, o których mowa w ust. 1, są: dowódcy, szefowie, komendanci, dyrektorzy komórek organizacyjnych i jednostek organizacyjnych Ministerstwa Obrony Narodowej, zwani dalej „organizatorami".

§ 2. Organizator zapewnia bibliotekom warunki działalności, odpowiadające ich zadaniom, a w szczególności:
1) warunki lokalowe, poprzez:
a) usytuowanie biblioteki w punkcie dostępnym dla ogółu użytkowników,
b) wydzielenie pomieszczeń na czytelnię i magazyn biblioteczny,
c) wyodrębnienie, w miarę możliwości, dodatkowych pomieszczeń dla bibliotekarza do prac administracyjnych, przygotowania materiałów bibliotecznych;
2) środki finansowe na wyposażenie i prowadzenie działalności bibliotecznej, a w szczególności na:
a) zakup materiałów bibliotecznych,
b) doskonalenie zawodowe pracowników związanych z działalnością biblioteczną.

§ 3. Biblioteki zapewniają obsługę biblioteczną żołnierzom, pracownikom wojska oraz ich rodzinom, a także w miarę możliwości udostępniają swoje zbiory innym podmiotom.

§ 4.1. Do podstawowych zadań biblioteki należy:
1) gromadzenie, opracowanie, przechowywanie, udostępnianie i ochrona materiałów bibliotecznych;
2) obsługa użytkowników i prowadzenie działalności informacyjnej w oparciu o zbiory własne i inne źródła.
2. Do zadań biblioteki może ponadto należeć: prowadzenie działalności bibliograficznej, dokumentacyjnej, wydawniczej, edukacyjnej, popularyzatorskiej i instrukcyjno-metodycznej.

§ 5. Gromadzenie, przechowywanie, ewidencjonowanie i udostępnianie przez biblioteki gromadzonych materiałów o charakterze ściśle tajnym, tajnym, poufnym lub zastrzeżonym nie może naruszać obowiązujących przepisów o ochronie informacji niejawnych.

§ 6.1. Biblioteki, na wniosek organizatora, mogą być włączone w skład ogólnokrajowej sieci bibliotecznej.
2. Biblioteki mogą zawierać, za zgodą organizatora, porozumienia o współpracy z innymi bibliotekami i instytucjami w sprawie wspólnego prowadzenia obsługi bibliotecznej, w szczególności w zakresie:

1) udostępniania i wymiany informacji oraz materiałów bibliotecznych;
2) organizacji imprez związanych z upowszechnianiem czytelnictwa oraz promocją literatury;
3) doskonalenia zawodowego, organizacji szkoleń, praktyk bibliotecznych, udzielania porad i pomocy instrukcyjno-metodycznej.

2. Porozumienie, o którym mowa w ust.2, może dotyczyć również łączenia zbiorów bibliotecznych bibliotek wojskowych oraz zbiorów bibliotek wojskowych ze zbiorami innych bibliotek.

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

Minister Obrony Narodowej: *J. Szmajdziński*

Dz.U.2004.246.2470

ROZPORZĄDZENIE
MINISTRA OBRONY NARODOWEJ

z dnia 5 listopada 2004 r.

w sprawie trybu udzielania żołnierzom w czynnej służbie wojskowej zezwoleń na rozpowszechnianie rezultatów ich działalności naukowej, literackiej, artystycznej lub publicystycznej, zawierających informacje niejawne

(Dz. U. z dnia 18 listopada 2004 r.)

Na podstawie art. 64 ust. 4 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2004 r. Nr 241, poz. 2416) zarządza się, co następuje:

§ 1.
Minister Obrony Narodowej wydaje zezwolenie na rozpowszechnianie rezultatów działalności naukowej, literackiej, artystycznej lub publicystycznej żołnierza, zawierających informacje niejawne, na pisemny wniosek, zwany dalej „wnioskiem", tego żołnierza, redaktora naczelnego, wydawcy, przedsiębiorcy albo dowódcy jednostki wojskowej, zwanych dalej „wnioskodawcami".

§ 2.
1. Wnioskodawca składa wniosek do Ministra Obrony Narodowej za pośrednictwem pełnomocnika Ministra Obrony Narodowej do spraw ochrony informacji niejawnych.
2. Wniosek zawiera:

1) imię i nazwisko lub nazwę wnioskodawcy;
2) nazwę jednostki lub komórki organizacyjnej, w której żołnierz pełni czynną służbę wojskową;
3) przedmiot działalności naukowej, literackiej, artystycznej lub publicystycznej żołnierza, ze wskazaniem elementów zawierających informacje niejawne;
4) sposób i warunki rozpowszechniania działalności, o której mowa w pkt 3.

§ 3.
1. Pełnomocnik Ministra Obrony Narodowej do spraw ochrony informacji niejawnych może żądać od wnioskodawcy uzupełnienia wniosku, w szczególności przez przedstawienie całości lub części rezultatów działalności naukowej, literackiej, artystycznej lub publicystycznej żołnierza, zawierających informacje niejawne.
2. Pełnomocnik Ministra Obrony Narodowej do spraw ochrony informacji niejawnych przekazuje Ministrowi Obrony Narodowej wniosek wraz ze swoją opinią w terminie 30 dni od dnia złożenia wniosku.

§ 4.

1. Minister Obrony Narodowej wydaje decyzję w sprawie zezwolenia lub odmowy zezwolenia na rozpowszechnianie rezultatów działalności naukowej, literackiej, artystycznej lub publicystycznej żołnierza w terminie nie dłuższym niż 90 dni od dnia złożenia wniosku.

2. Decyzję, o której mowa w ust. 1, przekazuje się wnioskodawcy oraz pełnomocnikowi Ministra Obrony Narodowej do spraw ochrony informacji niejawnych. Jeżeli wniosek złożył redaktor naczelny, wydawca, przedsiębiorca albo dowódca jednostki wojskowej, decyzję przekazuje się także zainteresowanemu żołnierzowi.

§ 5.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.1)

---

1) Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Obrony Narodowej z dnia 1 lipca 1992 r. w sprawie trybu uzyskiwania przez żołnierzy zezwolenia na rozpowszechnianie rezultatów swojej działalności naukowej, literackiej, artystycznej lub publicystycznej, zawierających wiadomości stanowiące tajemnicę państwową lub służbową (Dz. U. Nr 58, poz. 287), które traci moc z dniem wejścia w życie niniejszego rozporządzenia, na podstawie art. 17 ustawy z dnia 29 października 2003 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz o zmianie niektórych innych ustaw (Dz. U. Nr 210, poz. 2036 oraz z 2004 r. Nr 116, poz. 1203).

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

Na podstawie § 2 pkt 6 i 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) oraz w związku z art. 18 ust. 2 i art. 63 ust. 1 pkt 1) ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95), w celu realizacji zamierzeń związanych z powołaniem pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzeniem i sprawnym działaniem pionów ochrony w jednostkach organizacyjnych resortu Obrony Narodowej ustala się, co następuje:

§ 1

1) W Ministerstwie Obrony Narodowej tworzy się stanowisko pełnomocnika do spraw ochrony informacji niejawnych oraz podległy mu pion ochrony - Biuro Ochrony Informacji Niejawnych;

2) W dowództwach rodzajów sił zbrojnych, okręgów wojskowych, korpusów, dywizji i brygad oraz w akademiach wojskowych, wyższych szkołach oficerskich, bazach materiałowo - technicznych, centrach szkolenia, a także w samodzielnych pułkach - równorzędnych, tworzy się stanowiska pełnomocników do spraw ochrony informacji niejawnych tych dowództw i jednostek oraz podległe im piony ochrony, zgodnie z ideową strukturą organizacyjną określoną w załącznikach nr 2-5;

3) W pozostałych jednostkach organizacyjnych nie wymienionych w ppkt 1 i 2, określonych w Statucie Ministerstwa Obrony Narodowej stanowiącym załącznik do rozporządzenia Rady Ministrów z dnia 16 lutego 1999 r. w sprawie nadania Statutu Ministerstwu Obrony Narodowej (Dz. U. Nr 29, poz. 267) tworzy się stanowiska pełnomocników do spraw ochrony informacji niejawnych tych jednostek oraz podległe im piony ochrony o strukturach organizacyjnych określonych przez kierowników tych jednostek, stosownie do potrzeb.

§ 2

1) Stanowisko pełnomocnika ochrony jest stanowiskiem etatowym. Pełnomocnik ochrony podlega bezpośrednio kierownikowi jednostki organizacyjnej (dowódcy, szefowi, dyrektorowi jednostki lub instytucji wojskowej);

2) W jednostce organizacyjnej, poniżej szczebla samodzielnego pułku (równorzędnego) dopuszcza się połączenie tego stanowiska z innym stanowiskiem, już istniejącym w etacie tej jednostki;

3) Zmian w etatach związanych z utworzeniem stanowisk, o którym mowa w ppkt 1 i 2 dokonuje Generalny Zarząd Planowania Strategicznego na wniosek kierowników jednostek organizacyjnych, wymienionych w pkt 1 ppkt 1-3.

§ 3
1) Pełnomocnikiem ochrony nie może być kierownik kancelarii tajnej i osoba będąca jej pracownikiem;

2) Pełnomocnika ochrony, w okresie jego nieobecności, może zastępować osoba spełniająca warunki, określone w art. 18 ust. 5 ustawy z dni 22 stycznia 1999 r. 0 ochronie informacji niejawnych.

§ 4 (zmieniony DECYZJĄ NR 80/MON z dnia 10.05.2001r.)
1) Administratora systemu lub sieci teleinformatycznej, w której są przetwarzane informacje niejawne w ramach danej jednostki organizacyjnej (jednostki wojskowej), wyznacza jej kierownik (dowódca).

2) Administratora systemu lub sieci teleinformatycznej, w której są przetwarzane informacje niejawne, obejmujących swoim zasięgiem jedną komórkę organizacyjną Ministerstwa Obrony Narodowej, wyznacza dyrektor (szef) tej komórki, a administratora systemu lub sieci teleinformatycznej, w której są przetwarzane informacje niejawne, obejmujących swoim zasięgiem co najmniej dwie komórki organizacyjne Ministerstwa Obrony Narodowej, wyznacza Dyrektor Generalny Ministerstwa Obrony Narodowej, na wspólny wniosek dyrektorów (szefów) tych komórek.

3) Administratora systemu lub sieci teleinformatycznej, w której są przetwarzane informacje niejawne, obejmujących swoim zasięgiem jednostki organizacyjne podległe dowódcom rodzajów sił zbrojnych, wyznaczają dowódcy rodzajów sił zbrojnych.

4) Administratora systemu lub sieci teleinformatycznej, w której są przetwarzane informacje niejawne, wykraczających swoim zasięgiem poza Ministerstwo Obrony Narodowej lub rodzaj sił zbrojnych, wyznacza Minister Obrony Narodowej na wniosek Szefa Sztabu Generalnego WP.

5) O wyznaczeniu administratora systemu lub sieci teleinformatycznej, w której są przetwarzane informacje niejawne, informuje się właściwego pełnomocnika ochrony.

6) Administratorem systemu lub sieci teleinformatycznej nie może być pracownik pionu ochrony, z zastrzeżeniem pkt 7.

7) Przepis pkt 6 nie dotyczy Biura Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej.

§ 5
1) Dyrektor Generalny Ministerstwa Obrony Narodowej, w terminie 30 dni od wejścia w życie niniejszej decyzji, w porozumieniu z osobami zajmującymi kierownicze stanowiska w Ministerstwie opracuje:

a) projekt etatu Biura Ochrony Informacji Niejawnych oraz wskaże w etatach komórek organizacyjnych MON źródła pozyskania stanowisk etatowych, niezbędnych do utworzenia tego biura,

b) projekty: rozporządzenia Rady Ministrów zmieniającego rozporządzenie z dnia 16 lutego 1999 r. w sprawie nadania Statutu Ministerstwu Obrony Narodowej (Dz. U. Nr 29, poz. 267), decyzji Ministra Obrony Narodowej zmieniającej decyzję Nr 183/MON z dnia 20 listopada 1996 r. w sprawie bezpośredniej podległości jednostek organizacyjnych podporządkowanych Ministrowi Obrony Narodowej oraz przez niego nadzorowanych, a także przedsiębiorstw państwowych drą których jest on organem założycielskim (Dz. Rozk. MON z 1996 r. poz. 267 z późn. zm.);

2) Dowódcy rodzajów sił zbrojnych oraz kierownicy jednostek organizacyjnych, o których mowa w pkt 1 ppkt 3, w terminie 30 dni od dnia wejścia w życie niniejszej decyzji, przedstawią projekty etatów pionów ochrony w podległych jednostkach organizacyjnych w ramach przyznanych im całościowych limitów;

3) Szef Sztabu Generalnego WP, w terminie 60 dni od dnia złożenia projektów etatów, przygotuje i wyda dokumenty organizacyjno - etatowe umożliwiające realizację zadań, o których mowa w pkt 1.

§ 6
Właściwi dysponenci środków budżetowych, wyszczególnieni w decyzji Nr 250/MON Ministra Obrony Narodowej z dnia 23 grudnia 1999 r. w sprawie planowania i wykonywania budżetu resortu Obrony Narodowej (Dz. Rozk. MON poz. 125), zapewnią środki finansowe na realizację przedsięwzięć określonych niniejszą decyzją, w ramach budżetu będącego w ich dyspozycji.

§ 7
Osoby zajmujące kierownicze stanowiska w ministerstwie, kierownicy (dowódcy, szefowie, dyrektorzy, komendanci) jednostek organizacyjnych resortu Obrony Narodowej, w zakresie swojej właściwości, spowodują dokonanie odpowiednich zmian w dokumentach kompetencyjnych (odpowiednio w szczegółowych zakresach działania i zakresach działania) w trybie określonym w decyzji Nr PF 4/MON Ministra Obrony Narodowej z dnia 1 wrzenia 1998 r. w sprawie funkcjonowania systemu kompetencyjnego w resorcie Obrony Narodowej (niepubl.).

§ 8
Dowódca Garnizonu Warszawa w porozumieniu z Dyrektorem Biura Ochrony Informacji Niejawnych zapewni niezbędne siły i środki do ochrony fizycznej i technicznego zabezpieczenia komórek organizacyjnych Ministerstwa Obrony Narodowej, w ramach budżetu będącego w dyspozycji Dyrektora Departamentu Administracyjno - Koordynacyjnego.

§ 9
Szef Wojskowych Służb Informacyjnych określi szczegółowy zakres i tryb szkolenia pełnomocników ochrony oraz wzór umowy, o której mowa w art. 54 ust. 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych a w porozumieniu z Dyrektorem Departamentu Budżetowego określi zasady i tryb pokrywania kosztów tego szkolenia.

§ 10
Decyzja wchodzi w życie po upływie 7 dni od dnia podpisania.

Minister Obrony Narodowej: /-/ Janusz ONYSZKIEWICZ

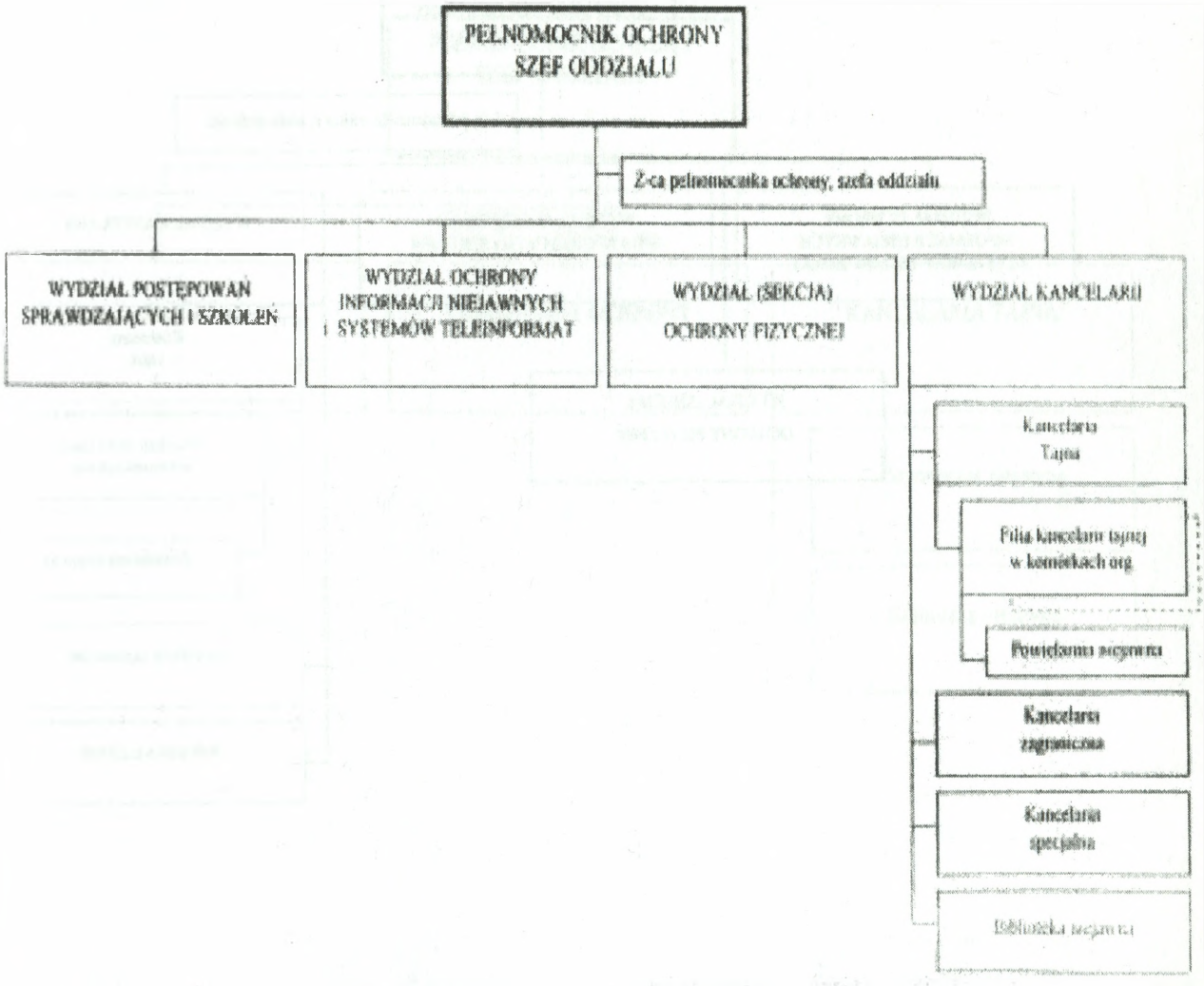
ZAŁĄCZNIKI DO DECYZJI:

Załącznik nr 1 - skreślony DECYZJĄ NR 333/MON z dnia 9 grudnia 2003r. zmieniającą decyzję w sprawie powołania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu Obrony Narodowej

Załącznik Nr 3

SCHEMAT IDEOWY STRUKTURY ORGANIZACYJNEJ ODDZIAŁU OCHRONY INFORMACJI NIEJAWNYCH

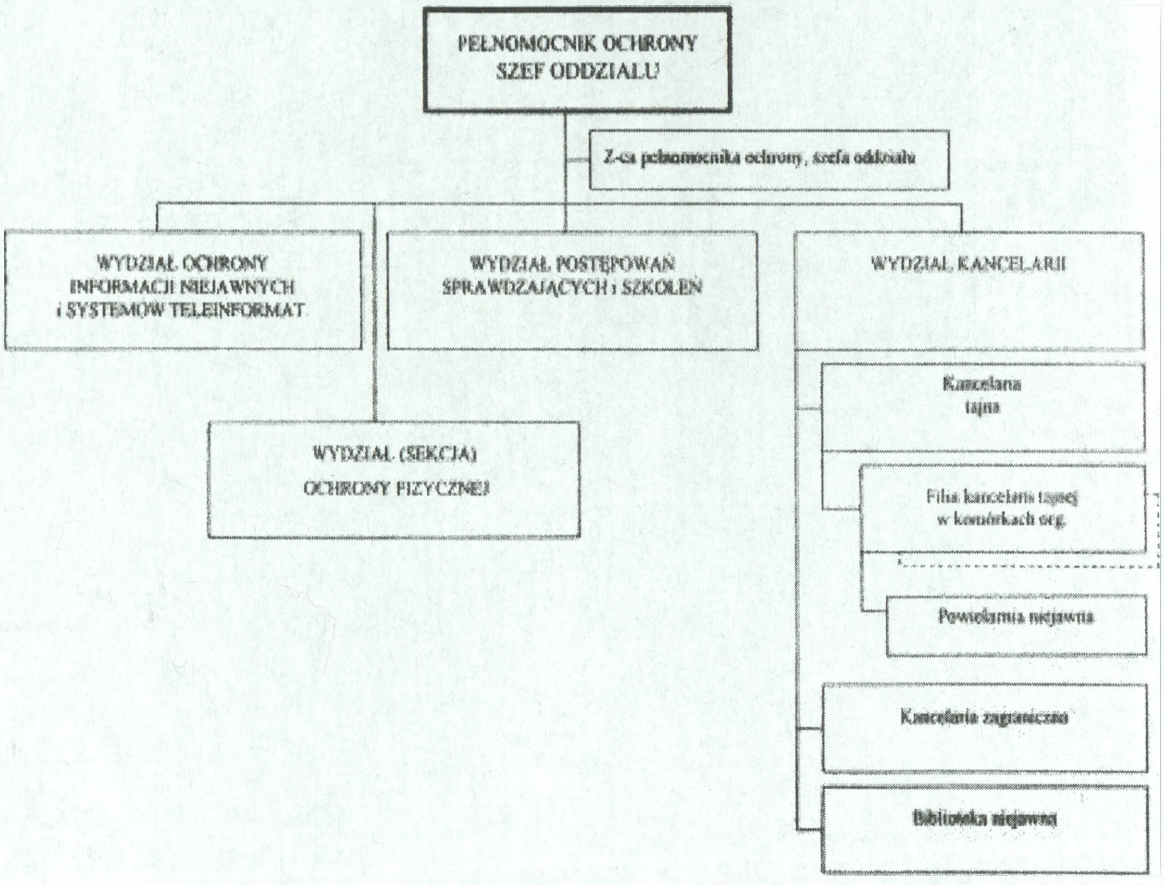
(w Dowództwie RSZ)



Załącznik Nr 3

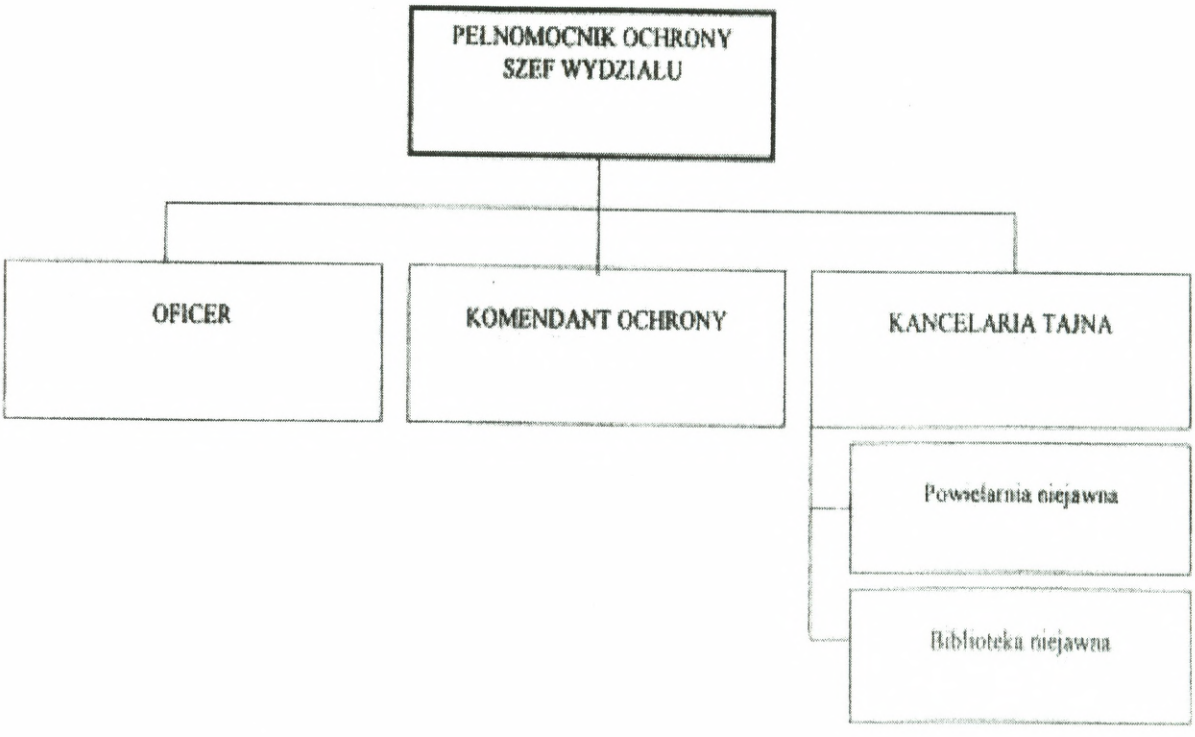
SCHEMAT IDEOWY STRUKTURY ORGANIZACYJNEJ ODDZIAŁU OCHRONY INFORMACJI NIEJAWNYCH

(w Dowództwie OW i Korpusie)



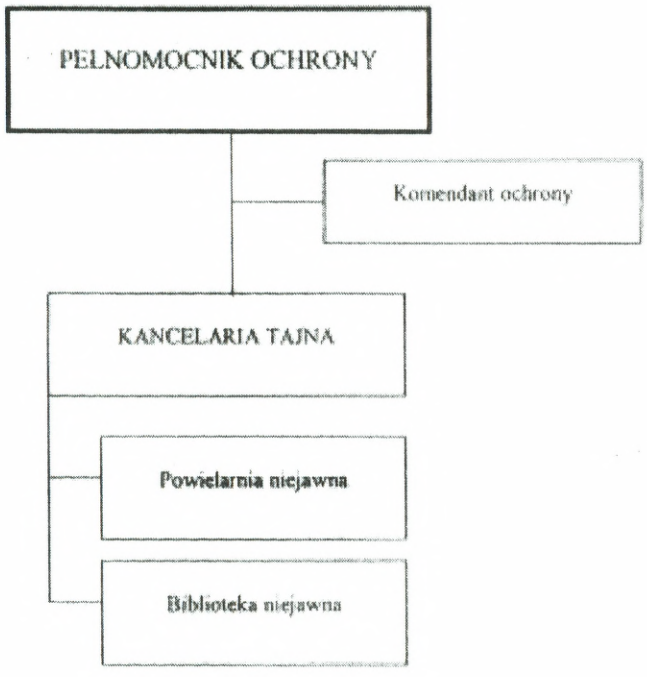
Załącznik Nr 4

SCHEMAT IDEOWY STRUKTURY ORGANIZACYJNEJ
WYDZIAŁU OCHRONY INFORMACJI NIEJAWNYCH NA SZCZEBLU DYWIZJI (równorzędnych)



Załącznik Nr 5

SCHEMAT IDEOWY STRUKTURY ORGANIZACYJNEJ
PIONU OCHRONY INFORMACJI NIEJAWNYCH NA SZCZEBLU BRYGADY, SAMODZIELNY PUŁK
(równorzędnych)



DECYZJA NR 31/MON

MINISTRA OBRONY NARODOWEJ

z dnia 8 marca 2000 r.

w sprawie zasad opracowywania planów ochrony jednostek organizacyjnych resortu Obrony Narodowej

Na podstawie § 2 pkt 6 i 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) oraz w związku z art. 18 ust. 4 pkt 6 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) ustalam:

§ 1
Plan ochrony jednostki organizacyjnej resortu Obrony Narodowej, zwany dalej planem ochrony, opracowuje pełnomocnik ochrony jednostki organizacyjnej resortu Obrony Narodowej, a zatwierdza jej dowódca (szef, dyrektor, kierownik).

§ 2
Pełnomocnik ochrony nadzoruje realizację planu ochrony oraz na bieżąco go aktualizuje, stosownie do pojawiających się zagrożeń.

§ 3
1. Plan ochrony składa się z dwóch części: graficznej i opisowej.

2. W części graficznej przedstawia się rozmieszczenie:

1) budynków mieszkalnych, magazynów, garaży i innych urządzeń rozmieszczonych w ochranianym obiekcie. Wszystkie budynki przedstawia się w formie rzutu płaskiego z góry i opisuje się je, np.: magazyn uzbrojenia, magazyn MPS, bomboskład, schronohangary, itd.;
2) technicznych środków wspomagających ochronę obiektów tj.: ogrodzeń, bram, furtek, wież wartowniczych, oświetlenia zewnętrznego, umocnień inżynieryjnych, stanowisk ogniowych, urządzeń alarmowych, kamer telewizyjnych oraz środków łączności wykorzystywanych przez służby ochronne;
3) posterunków wartowniczych (ochronnych), patroli i tras ich patrolowania oraz rejonów posterunków ochranianych przez psy wartownicze (obronne);
4) służb dyżurnych realizujących zadania ochronne;
5) stref bezpieczeństwa oraz rejonów szczególnej ochrony.

Ponadto w formie tabelarycznej przedstawia się podział sił i środków wydzielanych do ochrony danej komórki (jednostki) organizacyjnej lub obiektu wojskowego.

3. W części opisowej zawiera się:

1) analizę bezpieczeństwa i zagrożeń danej komórki (jednostki) organizacyjnej uwzględniającą ocenę:

a) zagrożeń zewnętrznych takich jak: wywiadowcze, terrorystyczne, dywersyjne i sabotażowe oraz kryminalne - uzyskanych od właściwych jednostek WSI, ŻW 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 ta problematyką;

2) ocenę aktualnego stanu ochrony komórki (jednostki) organizacyjnej;

3) skład służb dyżurnych oraz zasady organizacji i wykonywania przez nie ochrony tęrenów, obiektów i mienia wojskowego;

4) skład sił ochronnych (wart, patroli interwencyjnych, pododdziału alarmowego, specjalistycznych uzbrojonych formacji ochronnych itp.) oraz zasady organizacji i wykonywania przez nie ochrony terenów, obiektów i mienia wojskowego;

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

6) sposób zabezpieczenia broni i amunicji sił ochronnych;

7) dane dotyczące rodzaju zabezpieczeń technicznych wykorzystywanych w ochronie terenów, obiektów, mienia wojskowego oraz materiałów niejawnych;

8) określenie stref administracyjnych i bezpieczeństwa w komórce (jednostce) organizacyjnej i poszczególnych jej obiektach oraz sposobu ich ochrony;

9) organizację systemu kontroli dostępu (przepustkowego) do obiektów i do poszczególnych stref oraz sposób przechowywania i zabezpieczenia kluczy do wydzielonych pomieszczeń i obiektów podlegających szczególnej ochronie (magazyny broni, kasy itp.);

10) organizację systemu ochrony w godzinach służbowych, po ich zakończeniu oraz w dniach wolnych od zajęć służbowych;

11) sposób postępowania służb dyżurnych i sił ochronnych w sytuacjach kryzysowych (otrzymanie informacji o podłożeniu ładunku wybuchowego, napadzie, naruszeniu systemu ochrony, penetracji obiektu, itp.);

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

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

14) organizację współdziałania z wojskowymi i cywilnymi służbami mogą tymi udzielić wsparcia pyry ewakuacji personelu oraz pomocy medycznej;

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

§ 4
Część graficzną planu ochrony wykonuje się znakami umownymi stanowiącymi załącznik do decyzji.

§ 5
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 danej jednostki organizacyjnej resortu Obrony Narodowej lub obiektów wchodzących w jej skład.

§ 6
Plan ochrony obejmujący wszystkie ochraniane obiekty danej jednostki organizacyjnej resortu Obrony Narodowej przechowuje się w pomieszczeniu oficera dyżurnego jednostki.

§ 7
W wartowniach przechowuje się wyciągi z planów ochrony obiektów (rejonów), które ochraniane są przez daną wartę (służbę ochronną).

§ 8
Plan ochrony jest dokumentem niejawnym. Odpowiednią klauzulę tajności nadaje się stosownie do charakteru i przeznaczenia jednostki oraz realizowanych zadań ochronnych. Plan ochrony może być udostępniony, w niezbędnym zakresie, wyłącznie służbom dyżurnym (ochronnym) i osobom realizującym zadania przewidziane dla nich w tym planie.

§ 9
Decyzja wchodzi w życie po upływie trzech miesięcy od dnia podpisania.

Minister Obrony Narodowej: /-/ Janusz ONYSZKIEWICZ

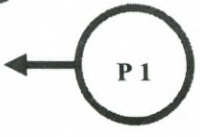
Załącznik do Decyzji
Ministra Obrony Narodowej Nr 31/MON
z dnia 8 marca 2000r.

ZESTAWIENIE PODSTAWOWYCH ZNAKÓW UMOWNYCH STOSOWANYCH W PLANACH OCHRONY

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

- rejon posterunku stałego trzyzmiennego - **nr 1**

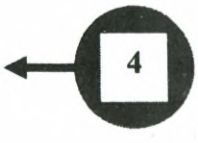
- rejon posterunku stałego dwuzmiennego - **nr 2**



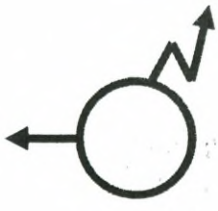
- posterunek ruchomy lub patrol **nr 1** (**P** – pieszy, **S** – na samochodzie, **M** – na motocyklu lub motorowerze, **R** – na rowerze)

- patrol z psem wartowniczym (obronnym)

- rejon posterunku psa wartowniczego (obronnego)



- posterunek ruchomy lub patrol (**nr 4**) wystawiany doraźnie oraz podczas osiągania WSGB



- posterunek ruchomy (patrol) z radiotelefonem lub z radiostacją

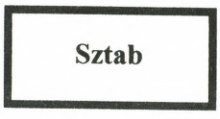
- ogrodzenie

- brama

- furtka

- wieża wartownicza

- punkt oświetlenia zewnętrznego



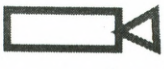
- chroniony budynek

- urządzenie alarmowe stosowane w ochronie zewnętrznej obiektu (budynku)

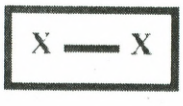
- urządzenie alarmowe stosowane w ochronie wewnętrznej obiektu (budynku)

- aparat telefoniczny lub miejsce do podłączenia urządzenia rozmównicznego

- radiotelefon bazowy dowódcy warty

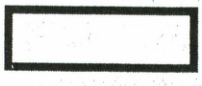


- kamera telewizyjna



- zapory inżynieryjne (kozły)

- stanowisko ogniowe



- **I** strefa bezpieczeństwa

- **II** strefa bezpieczeństwa

DECYZJA Nr 100/MON

MINISTRA OBRONY NARODOWEJ

z dnia 6 czerwca 2000 r.

w sprawie jednostki certyfikującej właściwej w Ministerstwie Obrony Narodowej do certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych

Na podstawie § 3 ust. 2 rozporządzenia Rady Ministrów z dnia 21 czerwca 1994 r. w sprawie zakresu i trybu stosowania przepisów ustawy o badaniach i certyfikacji do wyrobów produkowanych w kraju i importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa, a także właściwości organów w tych sprawach (Dz. U. Nr 80, poz. 370 i z 1998 r. Nr 53, poz. 330) oraz wynikających z ustawy o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95) potrzeb, zarządza się, co następuje:

§ 1

1. Jednostką certyfikującą właściwą w Ministerstwie Obrony Narodowej do prowadzenia certyfikacji wyrobów produkowanych w kraju i importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa jest - utworzona w tym celu, na podstawie odrębnych przepisów - Jednostka Certyfikująca Wyroby działająca w Wojskowych Służbach Informacyjnych.

2. Badania wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, będą wykonywane w akredytowanych laboratoriach badawczych.

3. Organizację wewnętrzną, i zakres zadań Jednostki Certyfikującej Wyroby określi Szef Wojskowych Służb Informacyjnych.

4. Szef Wojskowych Służb Informacyjnych spowoduje spełnienie wymagań akredytacyjnych Polskiego Centrum Badań i Certyfikacji dotyczących zasad działania podległej jednostki certyfikującej.

§ 2

Decyzja wchodzi w życie z dniem podpisania.

Minister Obrony Narodowej: /-/ Janusz ONYSZKIEWICZ

W porozumieniu:

Dyrektor Polskiego Centrum Badań i Certyfikacji:

/-/ mgr inż. Wojciech HENRYKOWSKI

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

W celu poddania szczególnej ochronie systemów i sieci teleinformatycznych, służących do wytwarzania, przechowywania, przetwarzania i przesyłania informacji niejawnych stanowiących tajemnicę państwową, przed ich nieuprawnionym ujawnieniem, 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
1. Ilekroć w decyzji jest mowa o:

1) jednostce organizacyjnej, należy przez to rozumieć Ministerstwo Obrony Narodowej lub jednostkę organizacyjną podporządkowaną Ministrowi Obrony Narodowej oraz przez niego nadzorowaną, a także przedsiębiorstwo państwowe, dla którego jest on organem założycielskim;
2) komórce organizacyjnej, należy przez to rozumieć komórkę organizacyjną Ministerstwa Obrony Narodowej;
3) kierowniku jednostki lub komórki organizacyjnej, należy przez to rozumieć dowódcę, dyrektora, szefa, komendanta jednostki lub komórki organizacyjnej.

2. Zadania w zakresie ochrony systemów i sieci teleinformatycznych realizują:

1) kierownik komórki lub jednostki organizacyjnej;
2) pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony";
3) administrator systemu lub sieci teleinformatycznej w rozumieniu art. 63, ust. 1 pkt 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95), zwanej dalej „ustawą";
4) organy bezpieczeństwa teleinformacyjnego:

a) Biuro Bezpieczeństwa Teleinformacyjnego,
b) Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki,
c) organy bezpieczeństwa systemów łączności i informatyki danego szczebla organizacyjnego;

5) Wojskowe Służby Informacyjne.

§ 2
1. Kierownik komórki organizacyjnej odpowiada za eksploatację i bezpieczeństwo systemów i lokalnych (wewnętrznych) sieci teleinformatycznych oraz terminali sieci rozległych, funkcjonujących w komórce organizacyjnej oraz ochronę informacji niejawnych wytwarzanych, przetwarzanych, przechowywanych i przesyłanych w tych systemach lub sieciach, a w szczególności za:

1) opracowanie i przekazanie do Wojskowych Służb Informacyjnych szczególnych wymagań bezpieczeństwa systemów autonomicznych i lokalnych sieci teleinformatycznych funkcjonujących w ramach komórki organizacyjnej;
2) wystąpienie z wnioskiem o wyznaczenie administratorów systemów i sieci teleinformatycznych na zasadach określonych w pkt 4 decyzji Nr 30/MON Ministra Obrony Narodowej z dnia 8 marca 2000 roku w sprawie powołania pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz utworzenia pionów ochrony w jednostkach organizacyjnych resortu Obrony Narodowej.

2. Kierownik jednostki organizacyjnej odpowiada za eksploatację i bezpieczeństwo systemów lub sieci teleinformatycznych funkcjonujących w jednostce organizacyjnej oraz ochronę informacji niejawnych wytwarzanych, przetwarzanych, przechowywanych i przesyłanych w tych systemach lub sieciach, a w szczególności za:

1) opracowanie i przekazanie do Wojskowych Służb Informacyjnych, szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej;
2) wyznaczenie osób funkcyjnych zgodnie z art. 63 ustawy.

3. Do Wojskowych Służb Informacyjnych przekazuje szczególne wymagania bezpieczeństwa systemów lub sieci teleinformatycznych, obejmujących swoim zasięgiem:

1) komórkę organizacyjną - jej kierownik, po uzyskaniu opinii Wojskowego Biura Bezpieczeństwa Łączności i Informatyki;
2) jednostkę organizacyjną - jej kierownik, po uzyskaniu opinii Wojskowego Biura Bezpieczeństwa Łączności i Informatyki, z zastrzeżeniem pkt 3, 4 i 6;
3) jednostkę organizacyjną podległą dowódcy rodzaju Sił Zbrojnych - jej kierownik, po uzyskaniu opinii organu bezpieczeństwa systemów łączności i informatyki właściwego dowództwa rodzaju Sił Zbrojnych;
4) rodzaj Sił Zbrojnych lub dowództwo rodzaju Sił Zbrojnych - dowódca rodzaju Sił Zbrojnych, po uzyskaniu opinii Wojskiego Biura Bezpieczeństwa Łączności i Informatyki;
5) resort Obrony Narodowej lub wykraczających poza niego - kierownik jednostki lub komórki organizacyjnej wdrażającej ten system lub sieć, po uzyskaniu opinii Wojskowego Biura Bezpieczeństwa Łączności i Informatyki;
6) jednostkę organizacyjną podległą Dowódcy Garnizonu Warszawa lub Dowództwo Garnizonu Warszawa - właściwy dowódca, stosując odpowiednio tryb postępowania określony w pkt 3 lub 4.

§ 3
1. Pełnomocnik ochrony odpowiada za ochronę systemów i sieci teleinformatycznych (systemów autonomicznych, sieci lokalnych (wewnętrznych) i terminali sieci rozległych, funkcjonujących w jednostce organizacyjnej) z zastrzeżeniem organizacyjnych, technicznych i programowych aspektów ochrony kryptograficznej, wymienionych w § 5, a w szczególności odpowiada za:

1) zapewnienie przestrzegania zasad ochrony informacji niejawnych przetwarzanych, przechowywanych i przesyłanych w systemie lub sieci teleinformatycznej, w tym właściwego obiegu dokumentów (wchodzących, wychodzących i nośników informacji);
2) zapewnienie bezpieczeństwa fizycznego obszaru, w którym usytuowany jest system, sieć lub terminal sieci rozległej;
3) zapewnienie dostępu do systemu wyłącznie osobom posiadającym odpowiednie poświadczenia bezpieczeństwa;

4) kontrolę znajomości procedur bezpieczeństwa przez wszystkich użytkowników systemu lub sieci teleinformatycznej;
5) organizację szkolenia użytkowników w zakresie ochrony informacji niejawnych przetwarzanych, przechowywanych i przesyłanych w funkcjonującym w jednostce organizacyjnej systemie lub sieci teleinformatycznej;
6) nadzór nad konfiguracją systemu, sieci lub terminali, przemieszczaniem sprzętu (terminali końcowych i urządzeń peryferyjnych) oraz nad prowadzeniem jego ewidencji.

2. Pełnomocnik ochrony uczestniczy w opracowywaniu:

1) programów organizacyjno - użytkowych, projektów technicznych przewidywanych do budowy systemów i sieci teleinformatycznych;
2) szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej.

3. Pełnomocnik ochrony, w przypadku stwierdzenia naruszeń bezpieczeństwa lub rozbieżności pomiędzy stanem faktycznym a zasadami ochrony systemu lub sieci teleinformatycznej, zawartymi w szczególnych wymaganiach bezpieczeństwa, będących poza sferą jego odpowiedzialności, informuje właściwy organ bezpieczeństwa systemów łączności i informatyki oraz Wojskowe Służby Informacyjne.

§ 4
Administrator systemu lub sieci teleinformatycznej odpowiada za:

1) codzienną obsługę techniczną systemu lub terminala;
2) sprawdzenie poprawności działania systemu;
3) opracowywanie projektów szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej oraz propozycji ich uaktualnienia;
4) wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemu lub sieci teleinformatycznej;
5) wdrażanie procedur ochrony antywirusowej;
6) opracowanie planów awaryjnych i planu napraw systemu lub sieci teleinformatycznej;
7) informowanie pełnomocnika ochrony oraz właściwego organu bezpieczeństwa systemów łączności i informatyki o stwierdzonych naruszeniach bezpieczeństwa systemu, sieci teleinformatycznej oraz wykrytych wirusach;
8) proponowanie zmian mających na celu poprawę bezpieczeństwa systemu lub sieci teleinformatycznej.

§ 5

1. Organy wymienione w § 1 ust. 2 pkt 4 odpowiadają za kryptograficzną ochronę informacji przetwarzanych, przechowywanych i przesyłanych w systemach i sieciach teleinformatycznych, w tym systemach dowodzenia przeznaczonych dla wąskiego grona osób funkcyjnych (łączności specjalnej, kodowej i utajnionej) oraz sprawowanie nadzoru nad eksploatacją technicznych i programowych środków ochrony tych systemów.

2. Biuro Bezpieczeństwa Teleinformacyjnego, podporządkowane szefowi Wojskowych Służb Informacyjnych, odpowiada za:

1) opracowywanie projektów dokumentów dotyczących ogólnych zasad bezpieczeństwa teleinformatycznego dla urządzeń, systemów i sieci teleinformatycznych;

2) dokonywanie corocznej i doraźnych ocen stanu bezpieczeństwa systemów i sieci teleinformatycznych;
3) badania i ocenę urządzeń i narzędzi kryptograficznych oraz mechanizmów zabezpieczeń tych urządzeń oraz systemów i sieci łączności specjalnej, kodowej i utajnionej w ramach procesu certyfikacyjnego;
4) opiniowanie i przedstawianie do zatwierdzenia szefom właściwych komórek Wojskowych Służb Informacyjnych szczególnych wymagań bezpieczeństwa systemów lub sieci teleinformatycznych;
5) dokonywanie sprawdzenia zgodności stanu faktycznego ze szczególnymi wymaganiami bezpieczeństwa systemów i sieci teleinformatycznych przy współudziale przedstawicieli organów bezpieczeństwa systemów łączności i informatyki danego szczebla organizacyjnego;
6) prowadzenie kontroli z zakresu bezpieczeństwa teleinformacyjnego;
7) generację i dystrybucję dokumentów kluczowych oraz haseł dostępu;
8) odbiór, zarządzanie i dystrybucję urządzeń kryptograficznych, publikacji kryptograficznych i dokumentów kluczowych uzyskiwanych w ramach wymiany międzynarodowej;
9) szkolenie z zakresu ochrony informacji niejawnych osób dokonujących odbioru technicznego urządzeń kryptograficznych, zakończone wydaniem zaświadczenia 0 odbyciu przeszkolenia z zakresu ochrony informacji niejawnych w przedmiocie odbioru technicznego urządzeń kryptograficznych określa załącznik nr 1 do decyzji;
10) opiniowanie programów szkolenia dotyczących problematyki bezpieczeństwa teleinformacyjnego w tym eksploatacji urządzeń i systemów ochrony kryptograficznej;
11) współpracę z Biurem Bezpieczeństwa Łączności i Informatyki Urzędu Ochrony Państwa.

3. Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki odpowiada za:

1) koordynację działalności organów bezpieczeństwa systemów łączności i informatyki rodzajów Sił Zbrojnych i Dowództwa Garnizonu Warszawa;
2) planowanie, organizowanie, prognozowanie rozwoju, eksploatację i nadzór nad funkcjonowaniem systemów łączności specjalnej, kodowej i utajnionej oraz ochrony kryptograficznej systemów i sieci teleinformatycznych na potrzeby resortu Obrony Narodowej, misji pokojowych, ćwiczeń oraz Wojennego Systemu Dowodzenia;
3) wprowadzenie, rozdział, ewidencję, wycofywanie oraz nadzór nad niszczeniem technicznych i programowych środków ochrony informacji (w tym nośników i dokumentacji);
4) zarządzanie bezpieczeństwem i wykorzystaniem oraz dystrybucję dokumentów szyfrowych, kodowych i kluczowych, a także ich ewidencję;
5) prowadzenie kontroli podległych organów bezpieczeństwa systemów łączności i informatyki w zakresie organizacji, funkcjonowania i eksploatacji systemów ochrony kryptograficznej, łączności szyfrowej, kodowej i utajnionej oraz zgodności stanu faktycznego ze szczególnymi wymaganiami bezpieczeństwa systemów i sieci teleinformatycznych;
6) planowanie i organizowanie szkoleń kadry łączności specjalnej i utajnionej oraz personelu kancelarii środków i materiałów kryptograficznych;
7) opracowanie wytycznych i instrukcji w zakresie organizacji, funkcjonowania i eksploatacji funkcjonujących oraz planowanych do uruchomienia systemów i sieci teleinformatycznych;
8) wydawanie i prowadzenie ewidencji pozwoleń na eksploatację sprzętu łączności specjalnej i utajnionej; wzór pozwolenia na eksploatację sprzętu łączności specjalnej i utajnionej określa załącznik nr 2 do decyzji;
9) opiniowanie szczególnych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, o których mowa w § 2 ust. 3 pkt 1, 2 i 4-6;

10) opracowanie szczególnych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, o których mowa w pkt 2;
11) udział w prowadzonych przez Biuro Bezpieczeństwa Teleinformacyjnego sprawdzeniach zgodności stanu faktycznego ze szczególnymi wymaganiami bezpieczeństwa systemów i sieci teleinformatycznych;
12) przedstawianie Wojskowym Służbom Informacyjnym dokumentów wymienionych w pkt 9, celem ich zatwierdzenia i uzyskania certyfikatu na system lub sieć teleinformatyczną.

4. Organy bezpieczeństwa systemów łączności i informatyki danego szczebla organizacyjnego odpowiadają za realizację zadań wymienionych w ust. 3 pkt 1-7 i 10-12, stosownie do zakresu kompetencji na swoim szczeblu organizacyjnym oraz opiniowanie szczególnych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, o których mowa w § 2 ust. 3 pkt 3.

5. Organy wymienione w § 1 ust. 2 pkt 4 współpracują z pełnomocnikiem ochrony w celu zapewnienia kompleksowej ochrony informacji niejawnych przetwarzanych, przechowywanych i przesyłanych w systemach i sieciach teleinformatycznych danej jednostki lub komórki organizacyjnej oraz udzielają merytorycznej pomocy w zakresie opracowywania szczególnych wymagań bezpieczeństwa oraz innych dokumentów dotyczących problematyki ochrony informacji niejawnych w systemach i sieciach teleinformatycznych. Współpraca rozpoczyna się na etapie projektowania i trwa do czasu wycofania z eksploatacji systemu lub sieci teleinformatycznej.

§ 6
Wojskowe Służby Informacyjne są właściwe do:

1) określania ogólnych zasad bezpieczeństwa teleinformatycznego dla systemów i sieci teleinformatycznych w formie dyrektyw, wytycznych i instrukcji wydanych przez szefa Wojskowych Służb Informacyjnych;
2) potwierdzania przydatności algorytmów kryptograficznych i środków gwarantujących ochronę tych algorytmów, kluczy kryptograficznych oraz innych istotnych parametrów zabezpieczenia, w szczególności haseł dostępu;
3) wnoszenia uwag do szczególnych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych, w których są przetwarzane, przechowywane i przesyłane informacje niejawne stanowiące tajemnicę służbową;
4) zatwierdzania szczególnych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych, w których są przetwarzane, przechowywane i przesyłane informacje niejawne stanowiące tajemnicę państwową;
5) wydawania certyfikatów dla systemów i sieci teleinformatycznych;
6) planowania, organizacji i prowadzenia specjalistycznych szkoleń administratorów systemów i sieci teleinformatycznych odpowiedzialnych za bieżącą kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa, zakończonych wydaniem zaświadczenia o odbyciu przeszkolenia; wzór zaświadczenia o odbyciu przeszkolenia z zakresu obowiązków administratora systemu lub sieci teleinformatycznej określa załącznik nr 3 do decyzji;
7) planowania, organizacji i prowadzenia specjalistycznych szkoleń pracowników pionu ochrony odpowiedzialnych za kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa, zakończonych wydaniem zaświadczenia o odbyciu przeszkolenia; wzór zaświadczenia o odbyciu przeszkolenia z zakresu obowiązków pracownika pionu ochrony; określa załącznik nr 4 do decyzji;

8) kontroli ochrony systemów i sieci teleinformatycznych oraz przestrzegania przepisów wydanych w tym zakresie.

§ 7
Zasady opracowywania szczególnych wymagań bezpieczeństwa systemów lub sieci teleinformatycznych, przetwarzających, przechowujących i przesyłających informacje niejawne reguluje zarządzenie Szefa Sztabu Generalnego WP z dnia 26 stycznia 2000 roku w sprawie opracowywania szczególnych wymagań bezpieczeństwa.

§ 8
Decyzja wchodzi w życie po upływie 7 dni od dnia podpisania.

Minister Obrony Narodowej: /-/ Bronisław KOMOROWSKI

ZAŁĄCZNIKI DO DECYZJI:

Załącznik nr 1

.....
(pieczęć nagłówkowa
z adresem i nr telefonu)

ZAŚWIADCZENIE
o odbyciu przeszkolenia z zakresu ochrony informacji niejawnych w przedmiocie odbioru technicznego urządzeń kryptograficznych
Nr .....

WZÓR

Stwierdza się, że Pan(i):

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

odbył(a) przeszkolenie z zakresu ochrony informacji niejawnych dla osób dokonujących odbioru technicznego urządzeń kryptograficznych typu .....
.....
.....

przeprowadzone przez Wojskowe Służby Informacyjne.

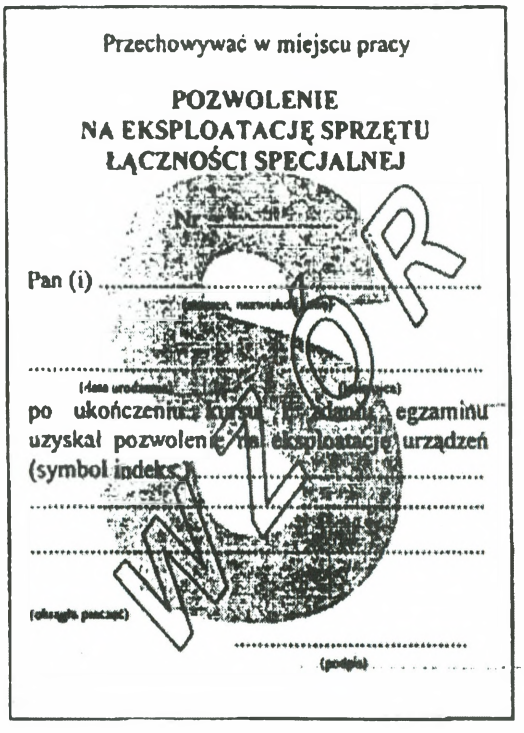
.....
(miejscowość i data)

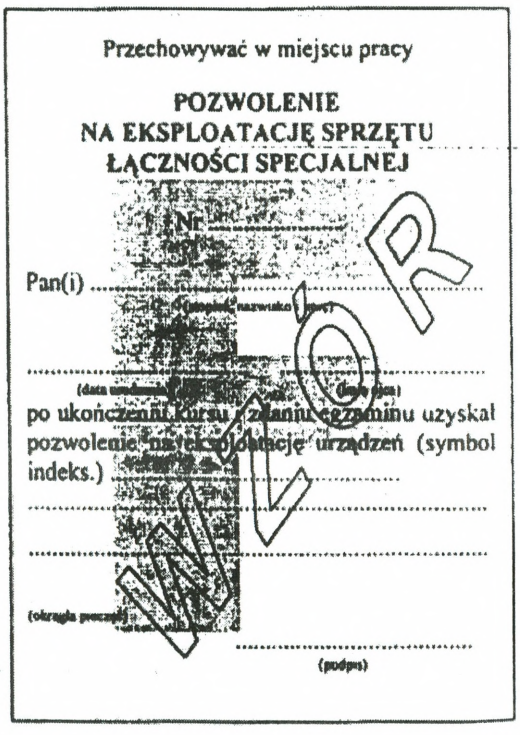
m. p.

.....
(pieczęć imienna i podpis
upoważnionego przedstawiciela WSI)

Załącznik nr

Wzory pozwoleń na eksploatację urządzeń łączności specjalnej i utajnionej.





Uwaga. Duże litery S, F, U, R – koloru żółtego

Załącznik nr 3

.....
(pieczęć nagłówkowa
z adresem i nr telefonu)

ZAŚWIADCZENIE
o odbyciu przeszkolenia z zakresu obowiązków administratora systemu lub sieci teleinformatycznej
Nr .....

WZÓR

Stwierdza się, że Pan(i):

- imię i nazwisko: .....
- data urodzenia: .....
- Nr 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. Nr 11, poz. 95) przeprowadzone przez Wojskowe Służby Informacyjne.

Nazwa systemu (sieci) teleinformatycznej .....
.....
.....

.....
(miejscowość i data)

m. p.

.....
(pieczęć imienna i podpis
upoważnionego przedstawiciela WSI)

Załącznik nr

.....
(pieczęć nagłówkowa
z adresem i nr telefonu)

ZAŚWIADCZENIE
o odbyciu przeszkolenia z zakresu obowiązków pracownika pionu ochrony
Nr .....

Stwierdza się, że Pan(i):

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

odbył(a) specjalistyczne przeszkolenie z zakresu obowiązków pracownika pionu ochrony 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. Nr 11, poz. 95) przeprowadzone przez Wojskowe Służby Informacyjne.

Nazwa systemu (sieci) teleinformatycznej .....
.....
.....

.....
(miejscowość i data)

m. p.

.....
(pieczęć imienna i podpis
upoważnionego przedstawiciela WSI)

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

(tekst ujednolicony DECYZJĄ NR 342/MON z dnia 9 grudnia 2002 r. zmieniającą decyzję 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 stanem ochrony 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 podporządkowanych lub nadzorowanych przez Ministra Obrony Narodowej albo przedsiębiorstwach państwowych, dla których jest on organem założycielskim, zwanych dalej „jednostkami organizacyjnymi", realizuje się w formie: kontroli, oceny stanu ochrony informacji niejawnych i decyzji wynikających z tej oceny.

§ 2

W jednostkach organizacyjnych przeprowadza się kontrole stanu ochrony informacji niejawnych, w celu:

1) sprawdzenia i oceny stanu przestrzegania przepisów o ochronie informacji niejawnych;
2) ustalenia przyczyn ujawnionych naruszeń zasad ochrony informacji niejawnych;
3) sformułowania wniosków i zaleceń w sprawie doskonalenia systemu ochrony informacji niejawnych.

W jednostkach organizacyjnych kontroluje się stan ochrony informacji niejawnych, w formie kontroli wewnętrznych lub zewnętrznych:

1) bieżących;
2) wyrywkowych;
3) półrocznych;
4) rocznych;
5) problemowych.

§ 4

1. Kontrola bieżąca służy sprawowaniu ciągłego nadzoru nad przestrzeganiem przez wykonawców i wykonawców technicznych zasad postępowania z materiałami zawierającymi informacje niejawne.
2. Kontrolę bieżącą prowadzą bezpośredni przełożeni oraz pion ochrony jednostki organizacyjnej.

3. 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.

§ 5
1. Kontrola wyrywkowa obejmuje w szczególności sprawdzenie:

1) zgodności ze stanem ewidencyjnym nośników informacji stanowiących tajemnicę państwową oraz uzyskanych z wymiany międzynarodowej, posiadanych przez wykonawców;
2) przestrzegania przepisów o ochronie informacji niejawnych w zakresie ewidencji i obiegu dokumentów.

2. Kontrola wyrywkowa jest realizowana przez pion ochrony w stosunku do komórek organizacyjnych, komórek wewnętrznych i samodzielnych stanowisk danej jednostki organizacyjnej, według planu (harmonogramu) kontroli zatwierdzonego przez kierownika jednostki organizacyjnej.
3. Z przebiegu kontroli wyrywkowej sporządza się notatkę. Wzór notatki o wynikach kontroli wyrywkowej obiegu i stanu faktycznego dokumentów u wykonawców przeprowadzanej przez pion ochrony określa załącznik Nr 1 do decyzji.

§ 6
1. Kontrola półroczna jest formą sprawdzenia:

1) zgodności ze stanem ewidencyjnym nośników informacji niejawnych, posiadanych przez wykonawców;
2) przestrzegania przepisów o ochronie informacji niejawnych w zakresie wytwarzania, ewidencji, przechowywania i niszczenia nośników informacji niejawnych;
3) wykonania zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli stanu ochrony informacji niejawnych.

2. Kontrolę półroczną prowadzą przełożeni w stosunku do podległych wykonawców i wykonawców technicznych.
3. Kierownicy kancelarii tajnych i zagranicznych oraz ich filii, a także innych komórek ewidencyjnych sporządzają dla osób prowadzących kontrolę półroczną wykazy materiałów niejawnych pobranych przez poszczególnych wykonawców i wykonawców technicznych.
4. Kontrolę półroczną przeprowadza się w terminie do dnia 30 czerwca każdego roku kalendarzowego.
5. Kierownik jednostki organizacyjnej może w uzasadnionych przypadkach przedłużyć rozkazem (decyzją) termin zakończenia kontroli półrocznej określonej w ust. 4, nie więcej jednak niż o 30 dni.
6. W razie nieobecności wykonawcy i wykonawcy technicznego w czasie przeprowadzania kontroli półrocznej, kontrolę w stosunku do tej osoby przeprowadza się bezpośrednio po jej powrocie do jednostki organizacyjnej.
7. Wyniki kontroli półrocznej stanu ochrony informacji niejawnych, przełożeni o których mowa w ust. 2, dokumentują w notatce. Wzór notatki o wynikach kontroli półrocznej stanu faktycznego i obiegu dokumentów u wykonawców określa załącznik Nr 2 do decyzji.
8. Kopię notatki o wynikach kontroli półrocznej stanu ochrony informacji niejawnych, opracowanej na podstawie notatek, o których mowa w ust. 7, dyrektorzy (szefowie) komórek organizacyjnych Ministerstwa Obrony Narodowej przekazują Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

§ 7
1. Kontrola roczna jest podstawową formą sprawdzenia realizacji zadań w zakresie ochrony i formacji niejawnych przez jednostkę organizacyjną.
2. Zakres oraz procedurę organizowania, prowadzenia i dokumentowania wyników kontroli rocznej stanu ochrony informacji niejawnych określa załącznik Nr 3 do decyzji.
3. Kontrolę roczną przeprowadza komisja, wyznaczona rozkazem (decyzją) kierownika jednostki organizacyjnej.
4. W jednostce organizacyjnej, w której kancelaria tajna ma filię tej kancelarii, mogą być powoływane podkomisje przeprowadzające kontrolę roczną komórek organizacyjnych lub komórek wewnętrznych obsługiwanych przez tę filię. Przepis ust. 3 stosuje się odpowiednio.
5. Kontrolę roczną w komórkach organizacyjnych Ministerstwa Obrony Narodowej przeprowadzają podkomisje wchodzące w skład komisji wyznaczonej decyzją Ministra Obrony Narodowej.
6. Pełnomocnik ochrony jest obowiązany do:

1) opracowania projektu rozkazu (decyzji), o którym mowa w ust. 3-5 przedstawienia go kierownikowi jednostki organizacyjnej;
2) prowadzenia szkoleń przewodniczących komisji i podkomisji wyznaczonych do prowadzenia kontroli rocznej.

§ 8
1. Meldunek o wyniku kontroli rocznej stanu ochrony informacji niejawnych w danym roku kalendarzowym przeprowadzonej w jednostce organizacyjnej, jej kierownik składa przełożonemu, w terminie do końca lutego następnego roku kalendarzowego. Wzór meldunku o wynikach kontroli rocznej stanu ochrony informacji niejawnych określa załącznik Nr 4 do decyzji.
2. Meldunek o wynikach kontroli rocznej stanu ochrony informacji niejawnych w danym roku kalendarzowym, przeprowadzonych w komórkach organizacyjnych Ministerstwa Obrony Narodowej, przewodniczący komisji kontroli rocznej przedkłada Ministrowi Obrony Narodowej, poprzez Pełnomocnika Ministra do Spraw Ochrony Informacji Niejawnych - w terminie do dnia 15 marca następnego roku kalendarzowego.
3. Meldunki zbiorcze o wynikach kontroli rocznych stanu ochrony informacji niejawnych według wzoru określonego w załączniku Nr 5, przesyłają do Szefa Wojskowych Służb Informacyjnych w terminie do dnia 15 kwietnia następnego roku kalendarzowego:

1) osoby zajmujące kierownicze stanowiska Ministerstwa - za bezpośrednio podległe jednostki organizacyjne;
2) Pełnomocnik Ministra do Spraw Ochrony Informacji Niejawnych - za Urząd Ministra Obrony Narodowej;
3) dowódcy rodzajów Sił Zbrojnych i Dowódca Garnizonu Warszawa - za podległe jednostki organizacyjne;
4) Kierownicy jednostek organizacyjnych bezpośrednio podległych Ministrowi Obrony Narodowej lub bezpośrednio przez niego nadzorowanych;
5) kierownicy komórek organizacyjnych Ministerstwa Obrony Narodowej - za podległe jednostki organizacyjne.

§ 9
1. Kontrole problemowe są zasadniczą formą sprawdzania stanu ochrony informacji niejawnych.
2. Do zarządzania i prowadzenia kontroli problemowej w zakresie ochrony informacji

niejawnych są uprawnieni: Szef Wojskowych Służb Informacyjnych oraz Dyrektor Departamentu Kontroli, a ponadto:

1) Sekretarz Stanu - I Zastępca Ministra Obrony Narodowej i podsekretarze stanu – w przyporządkowanych komórkach organizacyjnych oraz bezpośrednio podległych jednostkach organizacyjnych;
1a) Dyrektor Generalny - w komórkach organizacyjnych ministerstwa
2) Szef Sztabu Generalnego WP - w podległych komórkach organizacyjnych oraz bezpośrednio podległych jednostkach organizacyjnych, a także jednostkach organizacyjnych podległych dowódcom rodzajów Sił Zbrojnych i Dowódcy Garnizonu Warszawa;
3) dowódcy rodzajów Sił Zbrojnych, dowódcy okręgów wojskowych, dowódcy korpusów, Dowódca Garnizonu Warszawa, Komendant Główny Żandarmerii Wojskowej - w podległych jednostkach organizacyjnych;
4) kierownicy komórek organizacyjnych Ministerstwa Obrony Narodowej - w bezpośrednio podległych jednostkach organizacyjnych.

3. Zakres przedmiotowy kontroli problemowej stanu ochrony informacji niejawnych obejmuje:

1) wykonanie zaleceń z wcześniej przeprowadzonych kontroli stanu ochrony informacji niejawnych;
2) realizację zadań w zakresie ochrony informacji niejawnych jednostki organizacyjnej;
3) działalność pionu ochrony, a zwłaszcza kancelarii tajnej i zagranicznej oraz ich filii;
4) postępowanie z informacjami niejawnymi w innych komórkach ewidencyjnych, a w szczególności: hali maszyn, /kreślarni, powielarni, magazynie map, bibliotece, drukarni, taśmotece i wideotece;
5) postępowanie wykonawców i wykonawców technicznych z informacjami niejawnymi i ich nośnikami;
6) ochronę informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych;
7) realizację zadań w zakresie ochrony fizycznej jednostki organizacyjnej w części związanej z ochroną informacji niejawnych.

4. Szczegółowy zakres przedmiotowy kontroli problemowej stanu ochrony informacji niejawnych określa załącznik Nr 6 do decyzji.
5. W uzasadnionych przypadkach osoby zarządzające kontrolę mogą ograniczyć zakres przedmiotowy kontroli problemowej oraz czas jej trwania.
6. Kontrole problemowe stanu ochrony informacji niejawnych przeprowadza się w jednostkach organizacyjnych stosownie do potrzeb, nie rzadziej jednak niż raz na pięć lat.
7. Pełnomocnik ochrony jednostki organizacyjnej prowadzącej kontrolę problemową zobowiązany jest do prowadzenia szkoleń osób biorących udział w czynnościach kontrolnych.

§ 10
W zakresie nieuregulowanym w decyzji, do planowania, koordynacji i przeprowadzenia kontroli problemowych stanu ochrony informacji niejawnych oraz dokumentowania ich wyników i postępowania pokontrolnego stosuje się przepisy decyzji Nr 191/MON Ministra Obrony Narodowej z dnia I2 października 1999 r. w sprawie działalności kontrolnej w resorcie Obrony Narodowej (Dz. Rozk. MON poz. 89).

§ 11
1. Kierownicy jednostek organizacyjnych opracowują, co najmniej raz w roku, 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.
2. Ocenę stanu ochrony informacji niejawnych, o której mowa w ust. 1, w komórkach organizacyjnych Ministerstwa Obrony Narodowej opracowuje Pełnomocnik Ministra do praw Ochrony Informacji Niejawnych.
3. Ocenę stanu ochrony informacji niejawnych opracowuje się na podstawie:

1) wyników kontroli stanu ochrony informacji niejawnych;
2) meldunków lub zawiadomień o ujawnieniu informacji niejawnych osobom nieupoważnionym lub naruszeniu przepisów o ochronie informacji niejawnych;
3) wystąpień lub orzeczeń prokuratorów wojskowych oraz sądów wojskowych;
4) ocen stanu ochrony informacji niejawnych nadesłanych przez podległe jednostki organizacyjne;
5) Informacji uzyskanych z Wojskowych Służb Informacyjnych.

4. Ocena stanu ochrony informacji niejawnych obejmuje

1) zagrożenia występujące dla bezpieczeństwa informacji niejawnych:

a) ze strony obcych służb wywiadowczych,
b) ze strony przestępczości zorganizowanej i terroryzmu;

2) organizację systemu ochrony informacji niejawnych, w tym:

a) działalność pionu ochrony,
b) wydawanie aktów normatywnych,

c) sprawowanie nadzoru,
d) działalność organizacyjną,
e) działalność szkoleniową;

3) Funkcjonowanie systemu ochrony informacji niejawnych, w tym:

a) przestrzeganie przepisów o ochronie informacji niejawnych,
b) ochronę informacji niejawnych w systemach i sieciach teleinformatycznych,
c) ochronę informacji niejawnych w kontaktach zagranicznych;

4) wnioski ocenowe i decyzyjne.

5. Ocenę stanu ochrony informacji niejawnych przedstawia się na posiedzeniu organu kolegialnego jednostki organizacyjnej oraz przesyła się ją przełożonemu w terminie przez niego ustalonym.
6. Wnioski zawarte w ocenie stanu ochrony informacji niejawnych winny stanowić podstawę do planowania budżetowego wydatków związanych z ochroną informacji niejawnych.

§ 12
1. Zbiorczą ocenę stanu ochrony informacji niejawnych w danym roku kalendarzowym

opracowują osoby wymienione § 8 ust. 3 i przesyłają Szefowi Wojskowych Służb I formacyjnych w terminie do dnia 15 maja następnego roku kalendarzowego.
2. Szef Wojskowych Służb Informacyjnych przygotowuje zbiorczą ocenę stanu ochrony informacji niejawnych w resorcie Obrony Narodowej w danym roku kalendarzowym i przedstawia ją Ministrowi Obrony Narodowej w terminie do dnia 15 czerwca następnego roku kalendarzowego.

Decyzja wchodzi w życie po upływie 7 dni od dnia podpisania.

Minister Obrony Narodowej: /-/ Bronisław KOMOROWSKI

ZAŁĄCZNIKI DO DECYZJI:

Załącznik nr 1

Wzór

NOTATKA

o wynikach kontroli wyrywkowej stanu faktycznego i obiegu dokumentów u wykonawców przeprowadzonej przez pion ochrony w dniach .....

1. Kontrolę przeprowadzono w komórkach organizacyjnych (wewnętrznych)

.....

2. Kontrolą nie objęto niżej wymienionych wykonawców:

..... z powodu .....

..... z powodu .....

3. W wyniku przeprowadzonej kontroli nie stwierdzono braku dokumentów (w razie stwierdzenia braku dokumentów należy podać nazwę dokumentów, klauzulę, numer ewidencyjny, osobę odpowiedzialną za zagubienie, okoliczności zagubienia).
4. Stwierdzono u wykonawców następujące niedociągnięcia w zakresie przestrzegania przepisów o ochronie informacji niejawnych: (wyszczególnienie wykonawców oraz stwierdzonych u nich niedociągnięć).
5. Wnioski i propozycje mające na celu usunięcie stwierdzonych braków i niedociągnięć lub podjęte w tym zakresie przedsięwzięcia .....

.....

.....

.....

.....
(stanowisko służbowe, imię i nazwisko
data i podpis prowadzącego kontrolę)

Załącznik nr 2

Wzór

NOTATKA

o wynikach kontroli półrocznej stanu faktycznego i obiegu dokumentów u wykonawców przeprowadzonej w dniach .....

6. Kontrolę przeprowadzono w komórkach organizacyjnych (wewnętrznych)
.....
7. Kontrolą nie objęto niżej wymienionych wykonawców:
..... z powodu .....
..... z powodu .....
8. W wyniku przeprowadzonej kontroli nie stwierdzono braku dokumentów (w razie stwierdzenia braku dokumentów należy podać nazwę dokumentów, klauzulę, numer ewidencyjny, osobę odpowiedzialną za zagubienie, okoliczności zagubienia).
9. Stwierdzono u wykonawców następujące niedociągnięcia w zakresie przestrzegania przepisów o ochronie informacji niejawnych: (wyszczególnienie wykonawców oraz stwierdzonych u nich niedociągnięć).
10. Wnioski i propozycje mające na celu usunięcie stwierdzonych braków i niedociągnięć lub podjęte w tym zakresie przedsięwzięcia .....

.....

.....

.....

.....
(stanowisko służbowe, imię i nazwisko
data i podpis prowadzącego kontrolę)

Załącznik nr 3

Wzór

ZAKRES
oraz procedura organizowania, prowadzenia i dokumentowania wyników kontroli rocznej stanu ochrony informacji niejawnych

I. Cel kontroli:

1. Sprawdzenie przestrzegania w jednostce organizacyjnej /wojskowej/ przepisów o ochronie informacji niejawnych, ze szczególnym uwzględnieniem postanowień przepisów regulujących postępowanie z informacjami stanowiącymi tajemnicę państwową.
2. Sprawdzenie zgodności stanu faktycznego materiałów niejawnych ze stanem ewidencyjnym.
3. Sprawdzenie prawidłowości wydzielenia materiałów niejawnych posiadających wartość archiwalną.
4. Niszczenie materiałów niejawnych nie posiadających wartości archiwalnych.

II. Organizacja kontroli:

1. Kontrolę przeprowadza komisja wyznaczona rozkazem (decyzją) zawierającymi następujące dane:

1) skład osobowy komisji (co najmniej 3 osoby), z uwzględnieniem numerów poświadczeń bezpieczeństwa, ich klauzuli i terminów ważności;
2) termin rozliczenia wykonawców z materiałów niejawnych;
3) termin przygotowania do kontroli komórek organizacyjnych (wewnętrznych) prowadzących ewidencję materiałów niejawnych;
4) termin przygotowania do kontroli kancelarii /filii/;
5) termin rozpoczęcia i zakończenia kontroli.

2. W skład komisji wyznacza się osoby posiadające poświadczenia bezpieczeństwa o klauzulach równych lub wyższych niż materiały podlegające kontroli.
3. W skład komisji nie wyznacza się osób prowadzących ewidencję materiałów niejawnych w kontrolowanych komórkach organizacyjnych (wewnętrznych).
4. Członkowie komisji powinni być zapoznani z celem i zakresem kontroli wynikającymi z ustaleń kierownika jednostki organizacyjnej.
5. Pełnomocnik ochrony zobowiązany jest do przeprowadzenia szkolenia przewodniczącego komisji w zakresie metodyki prowadzenia kontroli.

III. Zakres kontroli:

1. Postępowanie z materiałami niejawnymi w kancelariach /filiach/ oraz innych komórkach prowadzących ewidencję:

1) szczegółowe sprawdzenie stanu faktycznego i porównanie ze stanem ewidencyjnym;
2) przestrzeganie zasad ewidencjonowania wytwarzanych materiałów niejawnych;

3) przestrzeganie zasad wytwarzania, przechowywania, udostępniania i niszczenia materiałów niejawnych.

2. Postępowanie z materiałami niejawnymi przez wykonawców:

1) przestrzeganie zasad wytwarzania materiałów niejawnych w tym również sporządzania notatek, odpisów, wyciągów i kopii;
2) przestrzeganie zasady selektywnego udostępniania informacji i dokumentowanie faktu zapoznawania się z informacjami stanowiącymi tajemnicę państwową oraz z informacjami uzyskanymi w ramach wymiany między państwami i organizacjami międzynarodowymi bez względu na klauzulę tajności;
3) przestrzeganie zasad przechowywania, przekazywania i niszczenia materiałów niejawnych.

3. Sposób realizacji zadań związanych z ochroną fizyczną informacji niejawnych.
4. Przestrzeganie zasad ochrony informacji niejawnych w systemach i sieciach teleinformatycznych.

IV. Dokumentowanie wyników kontroli:

Protokół z przeprowadzonej kontroli rocznej powinien zawierać następujące dane:

A. w części ogólnej:

1) numer i datę rozkazu (decyzji), będący podstawą działania komisji;
2) imiona, nazwiska, stopnie wojskowe, numery, klauzule i terminy ważności poświadczeń bezpieczeństwa przewodniczącego i członków komisji;
3) datę rozpoczęcia i zakończenia kontroli;
4) wykaz komórek organizacyjnych (wewnętrznych) objętych kontrolą;
5) podpisy członków komisji;
6) podpis zarządzającego kontrolę stwierdzającego zapoznanie się z treścią protokołu.

B. w części merytorycznej:

1) wyszczególnienie urządzeń ewidencyjnych oraz pozycji zapisów w tych urządzeniach, na podstawie których sprawdzono stan faktyczny materiałów niejawnych;
2) dane dotyczące stanu faktycznego poszczególnych rodzajów materiałów niejawnych:

a) zgodność lub niezgodność ze stanem ewidencyjnym,
b) wyszczególnienie materiałów brakujących (nie przedstawionych do kontroli) z podaniem ich klauzul i numerów ewidencyjnych oraz osób, które je pokwitowały,
c) wyszczególnienie materiałów brakujących (utraconych lub uznanych za utracone) z podaniem ich klauzul, numerów ewidencyjnych, okoliczności zagubienia, osób odpowiedzialnych za utratę oraz wykonanych przez komisję przedsięwzięć poszukiwawczych,
d) wyszczególnienie w załączniku numerów ewidencyjnych dokumentów niejawnych za rok kontrolowany i lata ubiegłe, które zostały przez komisję sprawdzone lecz nie zostały podszyte do właściwych teczek lub przerejestrowane,
e) fakty ujawnienia informacji niejawnych osobom nieupoważnionym,
f) okoliczności wskazujące na możliwość naruszenia przepisów o ochronie informacji niejawnych mogące spowodować ujawnienie informacji niejawnych,

g) ocenę przestrzegania przepisów o ochronie informacji niejawnych,
h) propozycje dotyczące osób zasługujących na wyróżnienie lub ukaranie,
i) propozycje dotyczące wniosków w sprawie przeprowadzenia postępowania sprawdzającego z pominięciem terminów i obowiązku wypełniania nowej ankiety bezpieczeństwa osobowego przez osobę sprawdzaną, o których mowa w art. 45 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 z późn. zm.)

Załącznik nr 4

Wzór

NOTATKA

o wynikach kontroli rocznej stanu ochrony
informacji niejawnych za rok .....

11. Kontrolę przeprowadzono w komórki organizacyjne (wewnętrznych)
.....
12. Dotychczas kontroli nie zakończono (nie przeprowadzono) w komórkach organizacyjnych (wewnętrznych) .....
13. Kontrole te zostaną przeprowadzone do .....
14. Meldunek o ich przeprowadzeniu zostanie przedstawiony w terminie do:
.....
15. Kontrole wykazały (ogólna ocena stanu ochrony informacji niejawnych)
.....
16. Stwierdzono następujące nieprawidłowości (informacje o utraconych dokumentach niejawnych, przypadki naruszenia przepisów .....
.....
17. Wnioski: .....

.....
(podpis)

Załącznik nr 5

.....
(pieczęć nagłówkowa)

Wzór

MELDUNEK ZBIORCZY

o wynikach kontroli rocznej stanu ochrony
informacji niejawnych za rok .....

18. Kontrolą jednostki (komórki) organizacyjne (bezpośrednio podległe i podległe) .....
19. Dotychczas kontroli nie zakończono (nie przeprowadzono) w jednostkach (komórkach)organizacyjnych: .....
    z następujących przyczyn .....
20. Kontrole te zostaną przeprowadzone do .....
21. Meldunek o ich przeprowadzeniu zostanie przedstawiony w terminie do:
.....
22. Kontrole wykazały (ogólna ocena stanu ochrony informacji niejawnych)
.....
23. Stwierdzono następujące nieprawidłowości (informacje o utraconych dokumentach niejawnych, przypadki naruszenia przepisów .....
.....
24. Wnioski: .....

.....
(podpis)

Załącznik nr 6

Wzór

SZCZEGÓŁOWY
zakres przedmiotowy kontroli problemowej stanu ochrony informacji niejawnych

1. Działalność normatywna i organizatorska:

1) kierownika jednostki organizacyjnej obejmuje:

a) spójność ustaleń normatywnych kontrolowanej jednostki z aktami prawnymi oraz normatywnymi szczebli nadrzędnych,
b) prowadzenie nadzoru służbowego w zakresie ochrony informacji niejawnych,
c) wartość merytoryczna prowadzonej w jednostce organizacyjnej oceny stanu ochrony informacji niejawnych,
d) reagowanie na fakty naruszania przepisów, utraty dokumentów niejawnych oraz ujawnienia tajemnicy,
e) przestrzeganie przepisów w zakresie upoważniania osób do dostępu do informacji niejawnych, a w tym zwłaszcza w stosunku do pracowników pionu ochrony;

2) pełnomocnika do spraw ochrony informacji niejawnych obejmuje:

a) ewidencję wydanych poświadczeń bezpieczeństwa,
b) realizację procedur sprawdzeniowych w zakresie zwykłego postępowania sprawdzającego w tym:

- podstawę wszczęcia postępowania,
- sposób dokumentowania informacji uzyskanych w wyniku sprawdzeń w kartotekach niedostępnych powszechnie,
- zgodność z zasadami ustawowymi podjętych decyzji o wydawaniu lub odmowy wydania poświadczeń bezpieczeństwa,
- ewidencję akt postępowania sprawdzającego (APS),
- przechowywanie i archiwizowanie APS;

c) plan ochrony jednostki i nadzorowanie jego realizacji,
d) systematyczność kontroli podległego pionu ochrony i działalności kancelarii tajnej,
e) szkolenie pracowników w zakresie ochrony informacji niejawnych,
f) plan postępowania z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego,
g) prowadzenie i dokumentowanie działań zmierzających do wyjaśnienia okoliczności naruszenia przepisów o ochronie informacji niejawnych.
h) współpracę w zakresie swoich zadań z właściwą komórką (jednostką) organizacyjną WSI.

2.Działalność kancelarii (filii) obejmuje:

1) urządzenie kancelarii oraz stan zabezpieczenia pomieszczeń kancelaryjnych;
2) przygotowanie fachowe kancelistów;

3) organizację pracy;
4) sposób prowadzenia ewidencji kancelaryjnej;
5) skuteczność nadzoru kierownika nad wytwarzaniem, ewidencjonowaniem, przechowywaniem i zabezpieczeniem dokumentów w halach maszyn, powielarniach itp.;
6) przestrzeganie zasad wydawania, rozliczania i obiegu dokumentów niejawnych, a także zasad kopertowania, adresowania i ekspedycji przesyłek;
7) prowadzenie kontroli bieżących wykonawców;
8) prowadzenie wykazów osób upoważnionych do dostępu do wiadomości niejawnych oraz ich bieżąca aktualizacja;
9) przygotowywanie przełożonym materiałów do prowadzenia kontroli półrocznej;
10) przestrzeganie zasad niszczenia dokumentów niejawnych oraz przechowywania makulatury niejawnej;
11) organizowanie kancelarii ćwiczebnej oraz rozliczanie dokumentów ćwiczebnych;
12) przygotowanie kancelarii do realizacji zadań na czas „W".

3. Postępowanie z dokumentami niejawnymi w innych komórkach ewidencjonujących dokumenty niejawne:

1) w hali maszyn /kreślarni, powielarni/ obejmuje:

a) sposób przyjęcia od zleceniodawcy dokumentów niejawnych,
b) zgodność klauzul dokumentów przekazanych do technicznego opracowania (brudnopisów) z dokumentami wytworzonymi,
c) ewidencjonowanie dokumentów wytworzonych i ich przekazywanie;

2) w magazynie map obejmuje:

a) urządzenie i zabezpieczenie magazynu,
b) sposób prowadzenia ewidencji,
c) sposób rozliczania wykonawców z pobranych materiałów,
d) przestrzeganie zasad dokonywania zmian klauzul tajności (terminowości i sposobu) oraz niszczenia wydawnictw służby topograficznej;

3) w bibliotece obejmuje:

a) urządzenie i zabezpieczenie pomieszczeń bibliotecznych,
b) prowadzenie ewidencji bibliotecznej,
c) przestrzeganie zasad udostępniania niejawnych wydawnictw,
d) wycofywanie oraz przeklasyfikowywanie wydawnictw,
e) postępowanie z niejawnymi dokumentami zdjęciowymi (negatywami, przeźroczami, odbitkami, fotoszkicami, fotomapami, fotoplanami, foliami na rzutnik itp.);

4) w drukarni obejmuje:

a) urządzenie i zabezpieczenie pomieszczeń produkcyjnych, w których wykonywane są dokumenty niejawne,
b) prowadzenie ewidencji dokumentów niejawnych oraz wytwarzanych w procesie produkcji materiałów dodatkowych (matryce, klisze, makulatura itp./,
c) przestrzeganie zasad przechowywania i przekazywania wydawnictw oraz niszczenia powstałej w toku produkcji makulatury i materiałów niejawnych;

5) w taśmotece i wideotece obejmuje:

a) urządzenie i zabezpieczenie pomieszczeń,
b) prowadzenie ewidencji taśm (metryczek),
c) prawidłowość oznakowania kaset,
d) przestrzeganie zasad kasowania i niszczenia taśm i kaset.

4. Postępowanie wykonawców z informacjami niejawnymi obejmuje:

1) znajomość przepisów o ochronie informacji niejawnych;
2) przestrzeganie zasad kwalifikowania informacji i oznaczania ich klauzulami;
3) przestrzeganie przepisów w zakresie opracowywania, przekazywania i udostępniania informacji niejawnych;
4) prawidłowość dokonywania weryfikacji klauzul informacji niejawnych;
5) zabezpieczenie informacji niejawnych w czasie pracy i po godzinach pracy.

5. Ochrona informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych obejmuje:

1) zabezpieczenie pomieszczeń i sprzętu komputerowego, w którym przetwarzane są informacje niejawne, a w szczególności zgodność stanu faktycznego ze szczególnymi wymaganiami bezpieczeństwa;
2) efektywność stosowanych rozwiązań technicznych i programowych w zakresie zabezpieczenia przetwarzanych informacji niejawnych przed dostępem osób nieupoważnionych;
3) ewidencjonowanie, przechowywanie i niszczenie nośników informacji niejawnych.

DECYZJA Nr 16/MON

MINISTRA OBRONY NARODOWEJ

z dnia 25 stycznia 2001 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) oraz w związku z art. 18 ust. 4 pkt 7, art. 22 i art. 54 ust. 1 i 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. Nr 11, poz. 95 oraz z 2000 r. Nr 12, poz. 136 i Nr 39, poz. 462), w celu realizacji zamierzeń związanych ze szkoleniem w zakresie ochrony informacji niejawnych ustala się, co następuje:

§ 1.
Decyzja określa szczegółowe zasady organizacji i prowadzenia szkolenia w zakresie ochrony informacji niejawnych w resorcie Obrony Narodowej.

§ 2.
W zakresie ochrony informacji niejawnych w resorcie Obrony Narodowej prowadzi się następujące rodzaje szkolenia:

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

§ 3.
1. Szkoleniem podstawowym obejmuje się osoby, po uzyskaniu przez nie po raz pierwszy poświadczenia bezpieczeństwa o danej klauzuli tajności, przed dopuszczeniem do pracy lub pełnienia służby na stanowisku, z którym może łączyć się dostęp do informacji niejawnych.

2. W uzasadnionych przypadkach szkoleniem podstawowym mogą być objęte osoby przed wydaniem poświadczenia bezpieczeństwa.

3. Celem szkolenia podstawowego jest zapoznanie osób, o których mowa w ust. 1, z:

1) zasadami i sposobami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania obowiązków służbowych na zajmowanym stanowisku;
2) zagrożeniami dla jednostki organizacyjnej ze strony obcych służb specjalnych, organizacji terrorystycznych i grup przestępczych, a także sposobami ich działania;
3) trybem postępowania w sytuacjach zagrożenia dla informacji niejawnych lub ich ujawnienia;
4) klasyfikowaniem informacji niejawnych oraz stosowaniem właściwych klauzul tajności, a także procedurami ich zmiany i znoszenia;
5) odpowiedzialnością karną, dyscyplinarną i służbową za naruszenie przepisów o ochronie informacji niejawnych.

4. Szkolenie podstawowe organizuje pełnomocnik do spraw ochrony informacji niejawnych, zgodnie z programem szkolenia zatwierdzonym przez kierownika jednostki organizacyjnej.

5. Pełnomocnik do spraw ochrony informacji niejawnych potwierdza odbycie szkolenia podstawowego wydaniem zaświadczenia, według wzoru określonego w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 23 lutego 1999 r. w sprawie wzoru zaświadczenia stwierdzającego odbycie przeszkolenia w zakresie informacji niejawnych (Dz. U. Nr 18, poz. 166).

6. Dodatkowo, w przypadku zmiany zakresu obowiązków służbowych, osoba może być objęta szkoleniem z zakresu określonego w ust. 3 pkt 1 i 4.

§ 4.
1. Dla osiągnięcia celu szkoleniowego, o którym mowa w § 3 ust. 3 pkt 4:

1) osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej oraz kierownicy komórek organizacyjnych bezpośrednio podległych Ministrowi Obrony Narodowej, opracowują wykazy typowych materiałów niejawnych wytwarzanych w podległych komórkach (jednostkach) organizacyjnych, które powinny być oznaczone odpowiednio Klauzulami tajności „ściśle tajne", „tajne" lub „poufne";
2) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych przygotuje, w porozumieniu z osobami, o których mowa w pkt 1, zbiorczy wykaz typowych materiałów niejawnych, które mogą być wytwarzane w komórkach organizacyjnych Ministerstwa Obrony Narodowej;
3) dowódcy rodzajów Sił Zbrojnych oraz Dowódca Garnizonu Warszawa, a także kierownicy jednostek organizacyjnych bezpośrednio podległych Ministrowi Obrony Narodowej, przygotują wykazy typowych materiałów niejawnych, wytwarzane we wszystkich podległych, podporządkowanych lub nadzorowanych jednostkach organizacyjnych, które powinny być oznaczone odpowiednio klauzulami tajności „ściśle tajne", „tajne" lub „poufne".

2. Wykazy, o których mowa w ust. 1 pkt 1, oraz ich zmiany poddaje się ocenie Szefa Wojskowych Służb Informacyjnych.

§ 5.
1. Szkoleniem uzupełniającym obejmuje się wszystkie osoby, które posiadają poświadczenie bezpieczeństwa.

2. Celem szkolenia uzupełniającego jest podtrzymanie i doskonalenie wiedzy u osób, o których mowa w ust. 1, uzyskanej podczas szkolenia podstawowego w zakresie ochrony informacji niejawnych.

3. Szkolenie uzupełniające organizuje pełnomocnik do spraw ochrony informacji niejawnych raz w roku lub częściej oraz w przypadku zmiany przepisów o ochronie informacji niejawnych.

4. Szkolenie uzupełniające prowadzi się na podstawie programu zatwierdzonego przez kierownika jednostki organizacyjnej.

§ 6.
Pełnomocnik do spraw ochrony informacji niejawnych odpowiada za:

1) opracowywanie szczegółowych programów szkolenia, uwzględniających zakres dostępu do informacji niejawnych osób szkolonych i specyfiki jednostki organizacyjnej;

2) wydanie zaświadczenia o ukończeniu szkolenia;

3) prowadzenie dokumentacji szkoleniowej, a w szczególności:

a) szczegółowych programów szkolenia,
b) dzienników lekcyjnych,
c) wyników sprawdzianów z opanowanej wiedzy,
d) rejestru wydanych zaświadczeń.

§ 7.
1. Szkoleniem specjalistycznym obejmuje się osoby przewidziane do objęcia stanowiska lub pełnienia funkcji:

1) pełnomocnika do spraw ochrony informacji niejawnych;
2) kierownika i zastępcy kierownika kancelarii tajnej oraz zagranicznej;
3) kancelisty kancelarii tajnej;
4) administratora systemów i sieci teleinformatycznych;
5) pracownika pionu ochrony odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa;
6) osoby odpowiedzialnej za nadzór, kontrolę, szkolenie i doradztwo w zakresie bezpieczeństwa przemysłowego.

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

3. Programy szkoleń specjalistycznych opracowuje Szef Wojskowych Służb Informacyjnych.

4. Potrzeby w zakresie szkolenia osób, o których mowa w ust. 1, zgłaszają drogą służbową do dnia 31 marca na następny rok do Dyrektora Departamentu Kadr:

1) osoby uprawnione do wyznaczania na stanowiska osób, o których mowa w ust. 1;
2) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych - w stosunku do osób zatrudnionych (pełniących służbę) w Ministerstwie Obrony Narodowej.

5. Dyrektor Departamentu Nauki i Szkolnictwa Wojskowego na podstawie potrzeb zgłoszonych przez Dyrektora Departamentu Kadr i w porozumieniu z Szefem Wojskowych Służb Informacyjnych oraz dowódcami rodzajów Sił Zbrojnych wyznaczy ośrodki realizujące szkolenie specjalistyczne z tym, że szkolenie osób, o których mowa w ust. 1 pkt 1 i 4 - 6, prowadzą w tych ośrodkach żołnierze lub pracownicy Wojskowych Służb Informacyjnych.

6. Wydatki na szkolenie specjalistyczne planują i realizują właściwi dysponenci, na których zaopatrzeniu pozostają osoby objęte szkoleniem.

7. Szkoleniem specjalistycznym w ośrodkach, o których mowa w ust. 5, mogą być objęte odpłatnie osoby zatrudnione u przedsiębiorcy, w jednostce naukowej lub badawczo - rozwojowej starającej się o zawarcie umowy lub wykonującej umowę na rzecz resortu Obrony Narodowej, z wykonaniem której łączy się dostęp do informacji niejawnych.

8. Ukończenie szkolenia specjalistycznego dokumentuje się zaświadczeniem.

§ 8.
1. W sprawie uzyskiwania klas kwalifikacyjnych przez personel kancelarii tajnych mają zastosowanie warunki określone w decyzji Nr 29/MON Ministra Obrony Narodowej z dnia 2 marca 1995 roku w sprawie uzyskiwania klas kwalifikacyjnych przez specjalistów wojskowych i instruktorów spadochronowych w Siłach Zbrojnych (Dz. Rozk. MON poz. 24 oraz z 1997 r. poz. 84).

2. Uzyskiwanie oraz potwierdzanie klas kwalifikacyjnych przez personel kancelarii tajnych organizują:

1) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych - w stosunku do żołnierzy pełniących służbę w Ministerstwie Obrony Narodowej;
2) pełnomocnicy do spraw ochrony informacji niejawnych dowódców rodzajów Sił Zbrojnych, okręgów wojskowych, Korpusu Powietrzno-zmechanizowanego, Inspektoratu Wojskowych Służb Informacyjnych, Komendy Głównej Żandarmerii Wojskowej i Dowódcy Garnizonu Warszawa - w stosunku do podległych, podporządkowanych i nadzorowanych komórek (jednostek) organizacyjnych.

§ 9.
Decyzja wchodzi w życie po upływie 14 dni od dnia jej ogłoszenia.

Minister Obrony Narodowej: /-/ B. KOMOROWSKI

DECYZJA Nr 29/MON

MINISTRA OBRONY NARODOWEJ

z dnia 22 lutego 2001 r.

w sprawie trybu certyfikacji 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

Na podstawie art. 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) oraz w związku z art. 14 ust. 1, pkt 1 i 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 oraz z 2000 r. Nr 12, poz. 136 i Nr 39, poz. 462), ustalam:

§ 1.
Szef Wojskowych Służb Informacyjnych, ze składu osobowego podległych jednostek, powoła stałą komisję do certyfikacji i kontroli, zwaną dalej „Komisją":

1) kancelarii zagranicznych;

2) punktów obsługi dokumentów zagranicznych, tworzonych na bazie kancelarii tajnych;

3) kancelarii środków i materiałów kryptograficznych;

4) stacji łączności kryptograficznej;

5) pomieszczeń wydzielonych (terminali) teleinformatycznych.

§ 2.
Szef Wojskowych Służb Informacyjnych:

1) określa zakres działania Komisji oraz nadzoruje jej pracę;

2) wskazuje pomieszczenia, o których mowa w § 1 pkt 5, wymagające certyfikacji;

3) wydaje certyfikaty bezpieczeństwa dla pomieszczeń, o których mowa w § 1;

4) zorganizuje system powiadamiania odpowiednio Biura Bezpieczeństwa Organizacji Traktatu Północnoatlantyckiego lub innej organizacji międzynarodowej, której Rzeczpospolita Polska jest stroną albo krajową władzę bezpieczeństwa państwa od którego uzyskano wiadomość niejawną w ramach realizacji porozumień międzynarodowych, stosownie do postanowień tych porozumień o ujawnieniu bądź naruszeniu bezpieczeństwa uzyskanych wiadomości niejawnych w resorcie Obrony Narodowej;

5) określi sposoby prowadzenia ewidencji i przechowywania certyfikatów bezpieczeństwa pomieszczeń, o których mowa w § 1;

6) określi i wprowadzi do użytku wytyczne dotyczące stosowania środków bezpieczeństwa fizycznego i zasad organizacji pomieszczeń wymienionych w §1 pkt 3-5.

§ 3.
Do podstawowych obowiązków Komisji należy:

1) sprawdzanie pomieszczeń, o których mowa w § 1, pod względem spełnienia wymagań bezpieczeństwa fizycznego oraz sporządzanie protokołów z przebiegu wykonanych sprawdzeń według wzoru określonego w załączniku nr 1 do decyzji;

2) występowanie z wnioskiem do Szefa Wojskowych Służb Informacyjnych o wydanie certyfikatów bezpieczeństwa dla pomieszczeń spełniających warunki bezpieczeństwa fizycznego według określonego w załączniku nr 2 do decyzji;

3) formułowanie zaleceń (w przypadku negatywnej oceny sprawdzanego pomieszczenia), które będą przedkładane właściwemu dowódcy (szefowi, komendantowi, dyrektorowi) do realizacji;

4) dokonywanie okresowych kontroli pomieszczeń, o których mowa w § 1. zgodnie z planem zatwierdzonym przez Szefa Wojskowych Służb Informacyjnych.

§ 4.
Dokumenty wykonane przez Komisję przechowuje się:

1) protokoły komisyjnego sprawdzenia - w Inspektoracie Wojskowych Służb Informacyjnych;

2) certyfikaty bezpieczeństwa kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych:

a) egz. nr 1 -w Inspektoracie Wojskowych Służb Informacyjnych,
b) egz. nr 2 - w Kancelarii Głównej Zagranicznej Ministerstwa Obrony Narodowej,
c) egz. nr 3- w sprawdzonej kancelarii zagranicznej lub w punkcie obsługi dokumentów zagranicznych;

3) certyfikaty bezpieczeństwa kancelarii środków i materiałów kryptograficznych, stacji łączności kryptograficznej oraz niektórych pomieszczeń terminali teleinformatycznych:

a) egz. Nr 1 -w Inspektoracie Wojskowych Służb Informacyjnych,
b) egz. nr 2 - w Głównej Kancelarii Środków i Materiałów Kryptograficznych,
c) egz. nr 3 - w sprawdzonej kancelarii, w stacji łączności, w pomieszczeniu terminala teleinformatycznego.

§ 5.
Dysponenci środków budżetowych, każdy w swoim zakresie, wydzielają środki na utworzenie lub przygotowanie pomieszczeń, o których mowa w § 1, w podległych (zaopatrywanych) jednostkach organizacyjnych.

§ 6.
Dowódca Garnizonu Warszawa, w porozumieniu z Dyrektorem Generalnym Ministerstwa

Obrony Narodowej, zapewni wyposażenie w niezbędny sprzęt biurowy, kwaterunkowy i informatyczny oraz środki łączności dla tworzonych pomieszczeń określonych w § 1 w komórkach organizacyjnych Ministerstwa Obrony Narodowej.

§ 7.
Dyrektor Biura Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej zapewni:

1) prowadzenie w Kancelarii Głównej Zagranicznej Ministerstwa Obrony Narodowej ewidencji kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych uruchamianych w jednostkach organizacyjnych resortu Obrony Narodowej;

2) przechowywanie w Kancelarii Głównej Zagranicznych Ministerstwa Obrony Narodowej certyfikatów bezpieczeństwa, o których mowa w § 4 pkt 2.

§ 8.
Dowódców (szefów, komendantów, dyrektorów) jednostek organizacyjnych resortu Obrony Narodowej, w których utworzono pomieszczenia, określone w § 1 pkt 1 I 2, zobowiązuje się do:

1) zapewnienia funkcjonowania utworzonych komórek organizacyjnych zgodnie z ustaleniami zawartymi w przepisach o ochronie informacji niejawnych;

2) zorganizowania ciągłego nadzoru służbowego ich pracy oraz reagowania na stwierdzone naruszenia przepisów, o których mowa w pkt 1;

3) informowania Szefa Wojskowych Służb Informacyjnych w przypadkach naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne" lub wyższą;

4) pisemnego zgłaszania do Szefa Wojskowych Służb Informacyjnych wniosków dotyczących komisyjnego sprawdzenia:

a) kancelarii zagranicznych lub punktów obsługi dokumentów zagranicznych, w przypadkach wprowadzenia jakichkolwiek zmian w ich organizacji, wyposażeniu lub funkcjonowaniu,
b) kancelarii tajnych, które mają pełnić funkcje punktów obsługi dokumentów zagranicznych,
-w celu wydania im certyfikatów bezpieczeństwa;

5) ogłoszenia w rozkazie (decyzji) wewnętrznym faktu uruchomienia kancelarii zagranicznej lub punktu obsługi dokumentów zagranicznych oraz przesłania odpowiedniego wyciągu do Kancelarii Głównej Zagranicznej Ministerstwa Obrony Narodowej;

6) objęcia kancelarii zagranicznej lub punktu obsługi dokumentów zagranicznych kontrolą oraz nadzorem realizowanym przez podległy pion ochrony.

§ 9.
Dowódców (szefów, komendantów, dyrektorów) jednostek organizacyjnych resortu Obrony Narodowej, w których utworzono pomieszczenia, określone w § 1 pkt 3-5, zobowiązuje się do pisemnego zgłaszania do Szefa Wojskowych Służb Informacyjnych wniosków dotyczących komisyjnego ich sprawdzenia, w celu wydania im certyfikatów bezpieczeństwa.

§ 10.
Dowódców (szefów, komendantów, dyrektorów) jednostek organizacyjnych resortu Obrony Narodowej, jako zleceniodawców, zobowiązują do określania przedsiębiorcom, jednostkom naukowym lub badawczo-rozwojowym w „Instrukcji bezpieczeństwa przemysłowego" warunków przewidzianych decyzją, w przypadku realizacji umów na rzecz resortu Obrony Narodowej, związanych z dostępem do informacji niejawnych pochodzących z wymiany międzynarodowej.

§ 11.
Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Obrony Narodowej: /-/ B. KOMOROWSKI

Załącznik nr 1

PROTOKÓŁ

Komisyjnego sprawdzenia .....
w .....
Komisja stała w składzie:
Przewodniczący: .....
Członkowie: .....
.....
.....

powołana rozkazem Nr ..... z dnia ..... szefa Wojskowych Służb Informacyjnych, na podstawie § 1 decyzji Nr 29/MON 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, po dokonaniu sprawdzenia pomieszczenia .....

..... stwierdza co następuje:

Sprawdzane pomieszczenie jest:

1. Zorganizowane w sposób zapewniający wymagany poziom bezpieczeństwa ochrony informacji niejawnych, do klauzuli .....** włącznie*.
2. Zorganizowane w sposób niezapewniający zgodnego z wymaganiami poziomu bezpieczeństwa ochrony informacji niejawnych do klauzuli .....** włącznie*.

WNIOSKI:

3. Komisja wystąpi o wystawienie certyfikatu bezpieczeństwa dla sprawdzonego pomieszczenia, ważnego do dnia .....*
4. Komisja zaleca wykonanie niżej wymienionych przedsięwzięć:*
   a) .....
   b) .....
   c) .....
   d) .....
5. Termin wykonania przedsięwzięć, o których mowa w pkt 4, ustalono na dzień .....*
6. Po wykonaniu przedsięwzięć, o których mowa w pkt 4. komisja dokona ponownego sprawdzenia pomieszczenia.*

Podpisy członków komisji:
Przewodniczący: .....
Członkowie: .....
.....
.....

---

* niepotrzebne skreślić
** podać właściwą klauzulę np.: TAJNE

Załącznik nr 2

CERTYFIKAT BEZPIECZEŃSTWA

dla pomieszczenia .....

w .....

Zaświadcza się, że Stała Komisja, działająca na podstawie § 1 decyzji Nr 29/MON Ministra Obrony Narodowej z dnia 22 lutego 2001r. 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, w dniach ..... przeprowadziła kontrolę pomieszczenia .....

w .....

Komisja stwierdziła, że kontrolowane pomieszczenie jest zorganizowane w sposób zapewniający wymagany poziom bezpieczeństwa i ochrony informacji niejawnych, do klauzuli .....* włącznie.

W związku z powyższym potwierdzam, że wymienione pomieszczenie zapewnia wymagany poziom bezpieczeństwa i ochrony informacji niejawnych, do klauzuli ..... * włącznie.

Certyfikat ważny jest do: .....

Data: .....

(pieczęć urzędowa)

(imię i nazwisko, stopień, stanowisko służbowe, podpis)

---

* podać właściwą klauzulę np.: TAJNE

DECYZJA NR 278/MON

MINISTRA OBRONY NARODOWEJ

z dnia 15 października 2003 r.

w sprawie sprawdzenia prawidłowości oznaczenia klauzulami tajności dokumentów zawierających informacje niejawne stanowiące tajemnicę państwową, wytworzonych przed dniem 10 maja 1990r.

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996r. W sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (dz. U. Nr 94, poz. 426) ustalam co następuje:

1. Kierownicy (dyrektorzy, szefowie, dowódcy, komendanci) jednostek i komórek organizacyjnych resortu obrony narodowej, zwani dalej „kierownikami".

1) powołają w podległych sobie jednostkach i komórkach organizacyjnych zespoły robocze, pod przewodnictwem pełnomocników do spraw ochrony informacji niejawnych, które dokonają sprawdzenia przechowywanych dokumentów zawierających informacje niejawne stanowiące tajemnicę państwową, wytworzonych przed dniem 10 maja 1990 roku, zwanych dalej „dokumentami";

2) na podstawie przedstawionych przez zespoły robocze wykazów:

a) dokonają oceny prawidłowości oznaczenia klauzulami tajności wytworzonych w jednostce organizacyjnej dokumentów, zgodnie z przepisami rozporządzenia Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999r. W sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach (Dz. U. Nr 18, poz. 167 oraz z 2001r. Nr 121, poz. 305),

b) w odniesieniu do dokumentów, które zostały wytworzone w innych jednostkach i komórkach organizacyjnych – zwrócą się do właściwych kierowników lub ich następców prawnych o przekazania informacji dotyczących aktualnych klauzul tych dokumentów;

3) spowodują:

a) naniesienia klauzul tajności na dokumentach, stosowanie do „Wykazu rodzajów informacji niejawnych stanowiących tajemnicę państwową", stanowiącego załącznik Nr 1 do ustawy z dnia 22 stycznia 1999r. O ochronie informacji niejawnych (Dz. U. Nr 11, poz. Z późn. Zm.),

b) niezwłoczne przekazanie dokumentów, do właściwego archiwum wojskowego, jeżeli posiadają wartość archiwalną, albo ich zniszczenie, jeżeli zostały zakwalifikowane do właściwej kategorii;

4) złożą – w terminie do dnia 28 lutego 2004r. – swoim bezpośrednim przełożonym meldunek o realizacji zadań nałożonych niniejszą decyzją.

2. Członkowie zespołów roboczych powinni posiadać poświadczenia bezpieczeństwa odpowiednie do klauzul sprawdzanych dokumentów.

3. Kierownicy jednostek i komórek organizacyjnych wymienieni z 1 8 ust. 3 decyzji 182/MON Ministra Obrony Narodowej z dnia 6 października 2000r. W sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (Dz. Rozk. MON z 2000r., poz. 112 oraz Dz. Urz. MON z 2002r. Nr 25, poz. 219) – w terminie do dnia 15 marca 2004r. – złożą Ministrowi Obrony Narodowej, za pośrednictwem Szefa Wojskowych Służb Informacyjnych, zbiorcze meldunki o wykonaniu niniejszej decyzji.

4. Decyzja wchodzi w życie z dniem podpisania.

DECYZJA NR 40/MON

MINISTRA OBRONY NARODOWEJ

z dnia 9 lutego 2004 r.

w sprawie szczegółowych zasad i trybu przeprowadzania postępowań sprawdzających, wydawania certyfikatów bezpieczeństwa NATO i UE oraz ich dokumentowania

Na podstawie § 2 pkt. 6 i pkt. 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) oraz w związku z art. 29 i 30 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 z późn. zm.) zwanej dalej „ustawą", ustalam 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" - ustalają dla kierowanych komórek (jednostek) „Wykaz stanowisk i prac zleconych, z którymi wiąże się dostęp do informacji niejawnych oraz osób dopuszczonych do pracy lub służby na tych stanowiskach", zwany dalej -"wykazem stanowisk"; dla każdej klauzuli informacji niejawnej sporządza się oddzielny wykaz stanowisk. Wzór wykazu stanowisk określa załącznik Nr 1 do decyzji.

2. Wykaz stanowisk dotyczący komórek organizacyjnych Ministerstwa Obrony Narodowej sporządza się z uwzględnieniem stanowisk i rodzajów prac zleconych, o których mowa w przepisach rozporządzenia Rady Ministrów z dnia 9 lutego 1999 r. w sprawie stanowisk i rodzajów prac zleconych w organach administracji rządowej, których wykonywanie może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwowa.

§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 Wojskowych Służb Informacyjnych, na polecenie Ministra Obrony Narodowej.

2. Z wnioskami w sprawie przeprowadzenia poszerzonego lub specjalnego postępowania sprawdzającego wobec innych osób niż wymienione w ust. 1, opracowanymi stosownie do wykazu stanowisk, występują:

1) do Szefa Wojskowych Służb Informacyjnych:

a) osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej - wobec kierowników bezpośrednio przyporządkowanych komórek organizacyjnych MON,
b) Dyrektor Departamentu Kadr i Szkolnictwa Wojskowego - wobec żołnierzy zawodowych

planowanych do wyznaczenia na stanowiska służbowe, o których mowa w § 48 rozporządzenia Ministra Obrony Narodowej z dnia 19 grudnia 1996 r. w sprawie służby wojskowej żołnierzy zawodowych (Dz. U. z 1997r. Nr 7, poz. 38 z późn. zm.), zwanego dalej „rozporządzeniem", w przypadkach, gdy obsada stanowiska wiąże się z dostępem do informacji niejawnych o wyższej klauzuli tajności niż posiadane przez kandydata poświadczenie bezpieczeństwa,
c) Szef Generalnego Zarządu Zasobów Osobowych - P1 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,
e) kierownicy przedsiębiorstw, jednostek naukowych lub badawczo -rozwojowych oraz innych jednostek organizacyjnych spoza resortu Obrony Narodowej - wobec pracowników wykonujących prace związane z realizacją produkcji lub usług stanowiących tajemnicę państwową ze względu na obronność państwa i potrzeby Sił Zbrojnych albo prace związane z obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową ze względu na obronność państwa jeżeli uczestnikami tego obrotu są Siły Zbrojne lub inne jednostki organizacyjne resortu Obrony Narodowej,

2) do kierowników właściwych jednostek organizacyjnych Wojskowych Służb Informacyjnych, zwanych dalej „jednostkami organizacyjnymi WSI":

a) kierownicy komórek organizacyjnych MON wobec podległych żołnierzy i pracowników wojska, planowanych do wyznaczenia lub wyznaczonych na stanowiska albo do prac zleconych objętych wykazem stanowisk w przyporządkowanych (podległych) im komórkach organizacyjnych MON,
b) dowódcy (komendanci), o których mowa w § 49 ust. 2-6 rozporządzenia, 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 osób o których mowa w ust. 2 pkt. 2 lit. a) i c) kierownicy komórek organizacyjnych MON występują poprzez Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

4. W przypadkach o których mowa w art. 44 ust. 1 pkt. 2 i 3 ustawy, przepisy ust. 2 pkt. 1 lit. a, c, d i e oraz pkt. 2 stosuje się odpowiednio.

5. Wzory „Wniosku o wszczęcie postępowania sprawdzającego" i „Polecenia wszczęcia postępowania sprawdzającego", określają załączniki Nr 2 i Nr 3 do decyzji.

§ 3.
1. Czynności postępowania sprawdzającego dokumentowane są w formie akt postępowania sprawdzającego.

2. Akta każdego postępowania sprawdzającego (nowego i kolejnego) 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 wszelką korespondencję i dokumenty sporządzone w toku tego postępowania, a w szczególności dokumenty stanowiące załączniki Nr 5-9 do decyzji.

§ 4.
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 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 postępowania sprawdzające", zwanym dalej „wykazem osób"; wzór wykazu osób określa załącznik Nr 10 do decyzji,
b) dokonuje sprawdzenia danych zawartych w ankiecie bezpieczeństwa osobowego poprzez wysłanie wniosków do:

- Krajowego Rejestru Karnego Ministerstwa Sprawiedliwości, na formularzu jak załącznik Nr 5 do decyzji;
- Biura Informacji i Statystyki Centralnego Zarządu Służby Więziennej, na formularzu jak załącznik Nr 6 do decyzji;
- właściwego Urzędu Stanu Cywilnego, na formularzu jak załącznik Nr 7 do decyzji.
- właściwej jednostki organizacyjnej WSI (wyłącznie przy postępowaniu dotyczącym dostępu do informacji oznaczonych klauzula POUFNE) o sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie; wzór wniosku określa załącznik Nr 8 do decyzji.

c) opracowuje notatkę dotyczącą wyników przeprowadzonego postępowania sprawdzającego, według układu merytorycznego określonego w załączniku Nr 9 do decyzji.
d) wydaje osobie sprawdzanej poświadczenie bezpieczeństwa lub odmawia wydania poświadczenia bezpieczeństwa.

§ 5.
1. Poświadczenie bezpieczeństwa przekazuje się osobie sprawdzanej za pokwitowaniem na kserokopii poświadczenia bezpieczeństwa (czytelny podpis z datą odbioru). W przypadku braku możliwości osobistego przekazania poświadczenia bezpieczeństwa osobie sprawdzanej, należy:

1) doręczyć poświadczenie bezpieczeństwa osobie sprawdzanej za pokwitowaniem przez pocztę; zwrotne potwierdzenie odbioru wtacza się do akt postępowania sprawdzającego;
2) przesłać poświadczenie bezpieczeństwa kierownikowi jednostki organizacyjnej, w której osoba sprawdzana pełni służbę (pracuje); drugi egzemplarz pisma przewodniego, za którym przesłano poświadczenie bezpieczeństwa włącza się do akt postępowania sprawdzającego.

2. O wyniku przeprowadzonego postępowania sprawdzającego należy zawiadomić pisemnie kierownika jednostki organizacyjnej, który wnioskował lub polecił jego przeprowadzenie, załączając do pisma kopię poświadczenia bezpieczeństwa lub odmowy wydania poświadczenia bezpieczeństwa, w celu włączenia do akt personalnych osoby sprawdzanej.

3. Drugi egzemplarz pisma, o którym mowa w ust. 2. wraz z kopią poświadczenia bezpieczeństwa lub odmowy wydania poświadczenia bezpieczeństwa, włącza się do akt postępowania sprawdzającego; do akt włącza się również pokwitowanie doręczenia odmowy wydania poświadczenia bezpieczeństwa.

4. Pełnomocnik ochrony po zakończeniu postępowania sprawdzającego dotyczącego dostępu do informacji oznaczonych klauzulą „POUFNE", przesyła w terminie 7 dni kartę ewidencyjną (KE) do właściwej jednostki organizacyjnej WSI; wzór karty ewidencyjnej (KE) określa załącznik Nr 11 do decyzji.

§ 6.
1. W przypadku zagubienia (utraty) poświadczenia bezpieczeństwa, jednostka organizacyjna WSI lub pełnomocnik ochrony na pisemny wniosek osoby sprawdzanej, wydają jego duplikat. Duplikat poświadczenia bezpieczeństwa oznacza się dodatkowo napisem DUPLIKAT umieszczonym w środku dolnej części dokumentu, pod okrągłą pieczęcią jednostki organizacyjnej. Wniosek oraz kopię wydanego duplikatu poświadczenia włącza się do akt postępowania sprawdzającego.

2. W przypadku zmiany danych personalnych zawartych w poświadczeniu bezpieczeństwa, jednostka organizacyjna WSI 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, osoba wnioskująca dołącza oryginał dokumentu potwierdzającego zmianę danych personalnych. Dokumenty te wpina 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 (KE) do właściwej jednostki organizacyjnej WSI oraz zawiadamia kierownika jednostki organizacyjnej; przepis § 5 ust. 3 stosuje się odpowiednio.

§ 7.
1. Akta zakończonych zwykłych postępowań sprawdzających są przechowywane przez 10 lat przez pełnomocników ochrony jednostki organizacyjnej, w której przeprowadzono postępowanie.

2. W przypadku zmiany miejsca służby (pracy) przez osobę sprawdzaną, akta postępowania sprawdzającego przesyłane są z urzędu do właściwego pełnomocnika ochrony w jednostce organizacyjnej, w której osoba ta wykonuje obowiązki służbowe.

3. Akta postępowania sprawdzającego archiwizuje się na zasadach określonych w odrębnych przepisach.

4. O przekazaniu akt postępowania sprawdzającego do archiwum lub innej jednostki organizacyjnej, pełnomocnik ochrony informuje właściwą jednostkę WSI poprzez przesłanie w ciągu 7 dni karty ewidencyjnej (KE) oraz odnotowuje ten fakt w rubryce 14 wykazu osób.

5. W przypadku przekazania zakończonych 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 (KE) do właściwej jednostki organizacyjnej WSI. podając w pkt. 10 karty (KE) aktualne miejsce przechowywania akt postępowania.

§ 8.
1. Pełnomocnik ochrony prowadzi ewidencję osób, którym wydano poświadczenie i certyfikat bezpieczeństwa albo odmówiono wydania poświadczenia bezpieczeństwa, wykorzystując karty ewidencyjne (KE) oraz wykaz osób i wykaz stanowisk.

2. Wykaz osób, o którym mowa w § 4 pkt. 2 lit. a, stanowi książkę ewidencyjną akt postępowań sprawdzających i podlega zarejestrowaniu w rejestrze teczek dokumentów niejawnych, dzienników i książek ewidencyjnych w kancelarii tajnej jednostki organizacyjnej.

3. W wykazie stanowisk, o którym mowa w § 1 ust. 1, pełnomocnik ochrony ewidencjonuje osoby, którym wydano poświadczenia i certyfikaty bezpieczeństwa albo odmówiono wydania poświadczeń bezpieczeństwa.

§ 9.
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 w poczet stanu zmiennego akademii (szkoły, ośrodka), komendanci, o których mowa w ust. 1. występują z pisemnym wnioskiem do właściwej jednostki organizacyjnej WSI lub polecają pełnomocnikom ochrony

przeprowadzenie stosownego postępowania sprawdzającego, jeżeli osoby te nie posiadają aktualnego odpowiedniego poświadczenia bezpieczeństwa.

§ 10.
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 wypełnionych ankiet bezpieczeństwa osobowego, jeżeli nie posiadają oni aktualnego odpowiedniego poświadczenia bezpieczeństwa wydanego przez służbę ochrony państwa (pełnomocnika ochrony).

4. W odniesieniu do żołnierzy rezerwy postępowania sprawdzające prowadzą:

1) zwykłe - pełnomocnicy ochrony mobilizujących jednostek organizacyjnych;
2) poszerzone i specjalne -właściwe jednostki organizacyjne WSI.

§ 11.
1. Kierownicy jednostek organizacyjnych oraz kierownicy komórek organizacyjnych uprawnieni do występowania z wnioskami o przeprowadzenie postępowania sprawdzającego, występują do Szefa Wojskowych Służb Informacyjnych o wydanie:

1) certyfikatu bezpieczeństwa NATO (NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE) - osobom, o których mowa w art. 29 pkt. 1 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 NATO zgodnie z przydzielonym etatem dla przedstawicieli Sił Zbrojnych RP;
b) pełniącym służbę lub zatrudnionym w następujących komórkach bezpośrednio dokonujących wymiany dokumentów i informacji niejawnych NATO:

- kancelariach zagranicznych,
- punktach obsługi dokumentów zagranicznych,
- kancelariach środków i materiałów kryptograficznych,
- stacjach łączności kryptograficznej,
- w służbie kurierskiej;

2) certyfikatu potwierdzającego sprawdzenie osoby (CERTIFICATE OF SECURITY CLEARANCE) - osobom przewidzianym do uczestniczenia w konferencjach 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,

3) certyfikatu bezpieczeństwa UE (FU PERSONNEL SECURITY CLEARANCE CERTIFICATE) - osobom, o których mowa w art. 29 pkt. 1 ustawy, których praca wymaga dostępu do informacji niejawnych UE.

2. Szef Wojskowych Służb Informacyjnych wydaje certyfikaty, o których mowa w ust. 1, w terminie 30 dni od złożenia wniosku, wyłącznie:

1) osobom posiadającym ważne poświadczenie bezpieczeństwa;
2) po przeszkoleniu zainteresowanej osoby we właściwej jednostce organizacyjnej WSI w zakresie przepisów bezpieczeństwa NATO lub UE i odebraniu stosownego oświadczenia o przeszkoleniu.

3. Wzór wniosków o wydanie certyfikatów, o których mowa w:

1) ust. 1-pkt. 1 - określa załącznik Nr 12 do decyzji;
2) ust. 1 pkt. 2 - określa załącznik Nr 13 do decyzji;
3) ust. 1 pkt. 3 - określa załącznik Nr 14 do decyzji.

4. W przypadku zagubienia (utraty) certyfikatów bezpieczeństwa o których mowa w ust. 1, Szef WSI na pisemny wniosek osoby sprawdzonej, wydaje jego duplikat.

§ 12.
1. W przypadku zgłoszenia przez partnera zagranicznego wymogu potwierdzenia uprawnień do dostępu do informacji niejawnych w formie „Request for Visit" (RFV) dla osób wyjeżdżających za granicę, pełnomocnik ochrony przedstawia Szefowi Wojskowych Służb Informacyjnych wniosek, wypełniony według zasad określonych na str. 1 - 8 instrukcji stanowiącej załącznik Nr 15 do decyzji.

2. Wniosek, o którym mowa w ust. 1 przesyła się do Szefa WSI, co najmniej na 5 dni roboczych przed upływem terminu jego złożenia do Krajowej Władzy Bezpieczeństwa wizytowanego kraju.

3. Formularz wniosku (RFV), określony w odrębnych przepisach, stanowi załącznik Nr 16 do decyzji.

4. Tabelaryczne zestawienie terminów składania wniosków określa załącznik Nr 17 do decyzji.

§ 13.
Przepisy niniejszej decyzji, z wyłączeniem §11 i 12, stosuje się odpowiednio do postępowań sprawdzających prowadzonych przez Żandarmerię Wojskową.

§ 14.
1. Do czasu wyczerpania zapasów, zezwala się na korzystanie z dotychczasowego wzoru karty ewidencyjnej (KE).

2. Karta ewidencyjna (KE), o której mowa w ust. 1, powinna zawierać w pozycji „adnotacje" uzupełnienie informacji przewidzianych w pkt. 13-15 nowego wzoru karty ewidencyjnej (KE), określonego w załączniku Nr 11 do decyzji.

§ 15.
Traci moc decyzja Nr 29/MON Ministra Obrony Narodowej z dnia 8 marca 2000r. w sprawie szczegółowych zasad i trybu przeprowadzania postępowań sprawdzających, dokumentowania i archiwizacji materiałów dotyczących postępowań (Dz. Rozk. MON, poz. 74).

§ 16.
Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER OBRONY NARODOWEJ
/-/ Jerzy SZMAJDZIŃSKI

ZAŁĄCZNIKI DO DECYZJI:

Załącznik nr 1

WYKAZ STANOWISK I PRAC ZLECONYCH, Z KTÓRYMI WIĄŻE SIĘ DOSTĘP DO INFORMACJI NIEJAWNYCH

ORAZ OSÓB DOPUSZCZONYCH DO PRACY LUB SŁUŻBY NA TYCH STANOWISKACH

NAZWA STANOWISKA /RODZAJ PRACY ZLECONEJ/

.....

KLAUZULA TAJNOŚCI .....

Lp.	Stopień wojskowy	**Imię i nazwisko** numer PESEL	Okres pełnienia służby				**Klauzula tajności**	Data szkolenia, ***numer*** zaświadczenia	Uwagi
			od	do	poświadczenia /odmowy/	certyfikatu			

Uwaga! Niniejszy wykaz należy prowadzić w oparciu o dołączony spis stanowisk (zleconych prac), zakładając oddzielnie karty tego wykazu dla każdego stanowiska, pracy zleconej. Dopuszcza się dodatkowe prowadzenie wykazu w formie elektronicznej oraz w przypadku znacznej liczby stanowisk, oddzielnie dla każdej komórki organizacyjnej jednostki.

Załącznik nr 2

..... (miejscowość i data)

(nazwa jednostki organizacyjnej)

POUFNE
(po wypełnieniu)

Egz. pojedynczy

.....

.....
(nazwa organu realizującego postępowanie sprawdzające)

WNIOSEK

o wszczęcie postępowania sprawdzającego

Na podstawie art. 38 ust. 1 / art. 39 ust. 1* w związku z art. 44* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 1999 r. Nr 11, poz. 95 z późn. zm.) 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 Pf - ..... – 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

*** wypełnić jeżeli postępowanie takie było prowadzone

Załącznik nr 3

.....

(nazwa jednostki organizacyjnej)

(miejscowość i data)

POUFNE
(po wypełnieniu)

Egz. pojedynczy

.....

.....
(nazwa organu realizującego postępowanie sprawdzające)

POLECENIE

wszczęcia postępowania sprawdzającego

Na podstawie art. 37 ust. 1 / art. 38 ust. 1 / art. 39 ust. 1* w związku z art. 44* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 1999 r. Nr 11, poz. 95 z późn. zm.) 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 Pf - ..... – 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

MINISTERSTWO OBRONY NARODOWEJ

.....

(nazwa organu realizującego postępowanie sprawdzające)

.....

(klauzula tajności)

Egz. pojedynczy

AKTA

POSTĘPOWANIA SPRAWDZAJĄCEGO

.....

(nr akt / PS (Z, P lub S) / rok)

.....

(stopień wojskowy, nazwisko i imię, imię ojca, rok urodzenia)

ROZPOCZĘTO .....

ZAKOŃCZONO .....

ILOŚĆ ARKUSZY .....

PRZECHOWYWAĆ LAT .....

KATEGORIA ARCHIWALNA .....

Załącznik nr 4

str. 2

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 2, 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.
9) Drugi egzemplarz informacji przesłanej do kierownika właściwej jednostki organizacyjnej dotyczącej sposobu zakończenia postępowania wraz z kserokopią poświadczenia bezpieczeństwa bądź odmowy poświadczenia bezpieczeństwa.

Załącznik nr 4

(nr akt)

SPIS DOKUMENTÓW

Nr dokumentów		Skąd lub dokąd przesłany	Nazwa dokumentu	Numer strony	*Uwagi*
Wych.	Wch.				
1	2	3	4	5	6

Załącznik nr 4

(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

Załącznik nr 4

(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

Data wystawienia .....

znak opłaty

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:
WSI – art. 6 pkt. 7 ustawy o KRK;
Pełnomocnicy ochrony –art. 37 ust. 2 pkt. 2 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 37a
00-975 Warszawa 12 skr. poczt. 200

Na postawie art. 37 ust. 2 pkt. 2*/ art. 38 ust. 1 pkt. 1*/ art. 39 ust. 1* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. Nr 11 poz. 95), 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.

Załącznik nr 7

.....
(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. 2 pkt 4*/ art. 38 ust. 1 pkt. 1*/ art. 39 ust. 1* ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych 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 / państwową*.

Pieczęć pełnomocnika ochrony/ żołnierza służby ochrony państwa*

.....
(data i podpis)

* niepotrzebne skreślić

Załącznik nr 8

.....

(nazwa jednostki organizacyjnej)

.....

(klauzula tajności)

Egz. pojedynczy

.....

.....

(nazwa właściwej terytorialnie jednostki organizacyjnej realizującej sprawdzenia)

WNIOSEK

o przeprowadzenie sprawdzeń zgodnie z art. 37 ust. 2 pkt. 3 w związku z art. 18 ust. 7 ustawy z 22.01.1999 r. Dz. U. nr 11 poz. 95 z p. zm.

Proszę o dokonanie sprawdzeń w ewidencjach i kartotekach niedostępnych powszechnie wobec:

.....

(stopień, imię i nazwisko, imię ojca, imię i nazwisko panieńskie matki)

.....

(data urodzenia, dokładny adres zamieszkania, PESEL)

Podstawa sprawdzenia:.....

.....

(powód sprawdzenia, nr akt postępowania)

Załączniki: dokumenty potwierdzające zasadność wszczęcia postępowania*).

Pieczęć pełnomocnika ochrony

.....

(data i podpis)

*) dotyczy realizacji postępowań wobec osób spoza resortu ON.

Załącznik nr 9

....
(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 (szczególnie w przypadku odmowy wydania poświadczenia bezpieczeństwa).

(stanowisko, stopień, imię i nazwisko sporządzającego)

.....
(podpis)

Załącznik nr 10

.....
(klauzula tajności)
Egz. pojedynczy

WYKAZ OSÓB, WOBEC KTÓRYCH PRZEPROWADZONO POSTĘPOWANIA SPRAWDZAJĄCE*)

Układ strony lewej.

Lp. data wszczęcia	Stopień wojskowy	Imię i nazwisko, imię ojca	Data i miejsce urodzenia	Miejsce zamieszkania (kod, miejscowość, ulica, nr domu i mieszkania)	Miejsce pracy, służby, stanowisko	Sygnatura akt postępowania sprawdzającego (np.: nr kolejny akt/rodzaj postępowania/rok) ..... /PS/...../.....
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 adres właściwej jednostki WSI do której przesłano kartę ewidencyjną (KE)*	UWAGI
	wydanego poświadczenia bezpieczeństwa	odmowy wydania poświadczenia bezpieczeństwa				
8	9	10	11	12	13	14

UWAGA!

* Dopuszcza się prowadzenie wykazu oddzielnie na każdą klauzulę tajności.

**) W pozycji nr 8 należy wpisać nazwę jednostki organizacyjnej, w której realizowano postępowanie sprawdzające. Natomiast w pozycji nr 13 wpisuje się „Dowódca J.W. .....” .

Załącznik nr 11

KARTA EWIDENCYJNA

POUFNE
(po wypełnieniu)

1. .....
Nazwisko (wypełnić drukowanymi literami)

2. .....
Nazwisko poprzednie (wypełnić drukowanymi literami)

3. .....
Imię, imiona (wypełnić drukowanymi literami)

4. .....
Imię ojca

5. .....
Imię i nazwisko panieńskie matki

6. .....
Nr PESEL, miejsce urodzenia

7. .....
Miejsce zamieszkania (kod i miejscowość, ulica, nr domu, nr mieszkania)

8. .....
Nazwa i adres jednostki organizacyjnej

9. .....
Nazwa komórki organizacyjnej zajmowane stanowisko

.....

10. .....
Sygnatura akt postępowania sprawdzającego i miejsce ich przechowywania

11. .....
Zakres dostępu do informacji (zastrzeżone poufne, tajne, ściśle tajne)

12. .....
Data wydania poświadczenia bezpieczeństwa/odmowy

13. .....
Data ważności poświadczenia bezpieczeństwa

14. .....
Numer poświadczenia bezpieczeństwa/odmowy

15. .....
Data wydania i numer zaświadczenia o przeszkoleniu w zakresie ochrony informacji niejawnych

.....
(imienna pieczęć i podpis upoważnionego żołnierza WSI lub pełnomocnika ochrony)

16. .....
Nazwa jednostki WSI (wypełnia właściwa jednostka terytorialna)
adnotacje

.....

.....

.....

.....

Załącznik nr 12

.....

(nazwa jednostki organizacyjnej)

.....

(miejscowość, data)

.....

(klauzula tajności)

Egz. nr .....

SZEF

WOJSKOWYCH SŁUŻB INFORMACYJNYCH

w Warszawie

WNIOSEK

o wydanie certyfikatu bezpieczeństwa NATO

Wnoszę o wydanie certyfikatu bezpieczeństwa NATO (NATO Personnel Security Clearance Certificate) uprawniającego do dostępu do wiadomości oznaczonych klauzulą:

- COSMIC TOP SECRET,*
- COSMIC TOP SECRET ATOMAL,*
- NATO SECRET,*
- NATO SECRET ATOMAL,*
- NATO CONFIDENTIAL,*
- NATO CONFIDENTIAL ATOMAL,*

dla.....

(stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia, PESEL)

z datą ważności do ..... .

Nadmieniam, że ww. posiada poświadczenie bezpieczeństwa nr ..... ważne do dnia ....., upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą ..... .

Załączniki: potwierdzone kserokopie dokumentów dających podstawę wydania certyfikatu bezpieczeństwa NATO.

Stanowisko, stopień, imię i nazwisko

kierownika jednostki organizacyjnej(wnioskodawcy)

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 13

.....

(nazwa jednostki organizacyjnej)

.....

(miejscowość, data)

.....

(klauzula tajności)

Egz. nr .....

SZEF

WOJSKOWYCH SŁUŻB INFORMACYJNYCH

w Warszawie

WNIOSEK

o wydanie certyfikatu potwierdzającego sprawdzenie osoby

Wnoszę o wydanie certyfikatu potwierdzającego sprawdzenie osoby (Certificate of Security Clearance) uprawniającego do dostępu do wiadomości oznaczonych klauzulą:

- COSMIC TOP SECRET,*
- COSMIC TOP SECRET ATOMAL,*
- NATO SECRET,*
- NATO SECRET ATOMAL,*
- NATO CONFIDENTIAL,*
- NATO CONFIDENTIAL ATOMAL,*

dla.....

(stopień, imię i nazwisko, imię ojca)

.....

(data i miejsce urodzenia, 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: potwierdzone kserokopie dokumentów o udziale osoby w konferencji, wizycie za granicą.

Stanowisko, stopień, imię i nazwisko

kierownika jednostki organizacyjnej.(wnioskodawcy)

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 14

.....

(nazwa jednostki organizacyjnej)

.....

(miejscowość, data)

.....

(klauzula tajności)

Egz. nr .....

SZEF

WOJSKOWYCH SŁUŻB INFORMACYJNYCH

w Warszawie

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: potwierdzone kserokopie dokumentów dających podstawę wydania certyfikatu bezpieczeństwa UE.

Stanowisko, stopień, imię i nazwisko

kierownika jednostki organizacyjnej(wnioskodawcy)

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 15

Zasady wypełniania formularza „Wniosek o Złożenie Wizyty" Requestfor 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.

1.	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 SECURITY CLEARANCE	**Do not fill in** (to be completed by government certifying authority). Note for the certifying 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.
12.	REQUESTING NATIONAL SECURITY AUTHORITY	**Do not fill in**. Note for the requesting NSA: a. Mention name, address and telephone number (can be pre-printed); b. Sign and eventually stamp this item.
13.	REMARKS	This item can be used for certain administrative requirements (e.g., proposed itinerary, request for hotel and/or transportation. This space is also available for the receiving NSA for processing, e.g., "no security objections", etc. ID number amendment.

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 NATO UNCLASSIFIED

NATO UNCLASSIFIED

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:
SIGNATURE:TE
LEPHONE No:

11. CERTIFICATION OF SECURITY CLEARANCE

NAME:

ADDRESS: STAMP

TELEPHONE:

SIGNATURE:

12. REOUESTING NATIONAL SECURITY AUTHORITY

NAME:
ADDRESS:
TELEPHONE
SIGNATURE:

STAMP

13. REMA

NATO UNCLASSIFIED

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 16

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:

Załącznik 16

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:

Załącznik nr 16

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:

Załącznik nr 17

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

Dziennik Urzędowy MON Nr 15, Poz. 149

ZARZĄDZENIE NR 49/MON

MINISTRA OBRONY NARODOWEJ

z dnia 5 sierpnia 2002r.

w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych

Na podstawie art. 53 ust. 2 ustawy z dnia 22 stycznia 1999r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z 2000 r. Nr 12, poz. 136 i Nr 39, poz.462 oraz z 2001r. 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) zarządza się, co następuje:

Rozdział 1

Postanowienia ogólne

§ 1.
Zarządzenie określa szczególne zasady organizacji kancelarii tajnych w resorcie Obrony Narodowej, stosowania środków ochrony fizycznej, tryb obiegu informacji niejawnych oraz wzory urządzeń ewidencyjnych.

§2.
Określenia użyte w zarządzeniu, oznaczają:
1) ustawa - ustawę z dnia 22 stycznia 1999r. o ochronie informacji niejawnych;
2) jednostka organizacyjna - jednostkę nie wchodzącą w skład Ministerstwa, podległą Ministrowi lub przez niego nadzorowaną;
3) komórka organizacyjna Ministerstwa Obrony Narodowej - Sekretariat Ministra, departament, generalny zarząd, samodzielny zarząd, biuro;
4) kancelaria tajna - komórkę podległą bezpośrednio pełnomocnikowi ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, kompletowanie i obieg dokumentów niejawnych;
5) filia kancelarii tajnej - komórkę wchodzącą w skład kancelarii tajnej jednostki organizacyjnej, odpowiedzialną za właściwe rejestrowanie, przechowywanie, kompletowanie i obieg dokumentów niejawnych;
6) kancelaria zagraniczna - komórkę podległą bezpośrednio pełnomocnikowi ochrony, odpowiedzialną za rejestrowanie, przechowywanie, kompletowanie i obieg dokumentów niejawnych wymienianych z innymi państwami i organizacjami międzynarodowymi;
7) kancelaria ćwiczebna - komórkę tworzoną w jednostce organizacyjnej na czas ćwiczeń i treningów sztabowych, odpowiedzialną za rejestrowanie, przechowywanie i obieg dokumentów otrzymywanych, wytwarzanych i przetwarzanych w czasie ćwiczeń oraz treningów sztabowych, zawierających informacje niejawne;
8) kancelaria wojenna - komórkę tworzoną w jednostce organizacyjnej na czas wojny, odpowiedzialną za rejestrowanie, przechowywanie i obieg dokumentów bojowych zawierających informacje niejawne;
9) kierownik kancelarii - żołnierza zawodowego lub pracownika wojska kierującego pracą kancelarii tajnej lub zagranicznej, podlegającego pełnomocnikowi ochrony;

10)zastępca kierownika kancelarii - żołnierza zawodowego lub pracownika wojska zajmującego etatowe stanowisko zastępcy kierownika, podlegającego bezpośrednio kierownikowi kancelarii;
11)kancelista - żołnierza zawodowego lub pracownika wojska pełniącego służbę wojskową albo zatrudnionego w kancelarii tajnej lub zagranicznej, podlegającego bezpośrednio kierownikowi kancelarii;
12)punkt obsługi dokumentów zagranicznych - wydzieloną część kancelarii lub filii kancelarii tajnej odpowiedzialna za rejestrowanie, przechowywanie i obieg dokumentów wymienianych z innymi państwami i organizacjami międzynarodowymi;
13) żołnierz - osobę pełniącą czynną służbę wojskową w jednostce organizacyjnej;
14) pracownik wojska - osobę pozostającą w stosunku pracy z jednostką organizacyjną;
15) wykonawca - żołnierza lub pracownika wojska zajmującego określone stanowisko służbowe, wykonującego zadania zgodnie z zakresem obowiązków, posiadającego stosowne poświadczenie bezpieczeństwa osobowego;
16)wykonawca techniczny - wykonawcę odpowiedzialnego za utrwalenie informacji niejawnych w sposób określony w art. 2 pkt 5 ustawy;
17) urządzenie ewidencyjne - księgę, dziennik, wykaz, spis, rejestr i kartotekę o ustalonych rubrykach, służącą do rejestrowania dokumentów zawierających informacje niejawne oraz umożliwiającą kontrolę ich stanu i obiegu;
18) trwałe urządzenie ewidencyjne - urządzenie ewidencyjne, które:

a) nie podlega niszczeniu i jest przekazywane do archiwum,
b) nadaje dokumentom niezmienne numery ewidencyjne, powiązane w sposób trwały z danym urządzeniem, umożliwiające włączenie dokumentów do obiegu zewnętrznego,
c) umożliwia jednoznaczne określenie stanu ewidencyjnego dokumentów;

19) pomocnicze urządzenie ewidencyjne - urządzenie ewidencyjne, które:

a) stosuje się wyłącznie w obiegu wewnętrznym dokumentów,
b) podlega niszczeniu w jednostce organizacyjnej,
c) nadaje dokumentowi zmienne numery ewidencyjne,
d) umożliwia określenie zasięgu obiegu dokumentów oraz ułatwia ustalenie ich stanu ewidencyjnego w okresie istnienia danego urządzenia ewidencyjnego;

20) dokumenty ćwiczebne - dokumenty zawierające utrwalone informacje niejawne, otrzymane lub wytworzone w jednostce organizacyjnej podczas ćwiczeń;
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 przedmiotowych oznaczonych właściwą kategorią archiwalną;
23) strefa bezpieczeństwa - obszar, obiekt, fragment budynku, jedno lub kilka pomieszczeń, posiadające ściśle określone, oznaczone i strzeżone granice, w których są przechowywane, przetwarzane lub wytwarzane informacje niejawne o klauzuli „Poufne" lub wyższej. Wejście osób do strefy lub wyjście z niej może nastąpić wyłącznie po okazaniu przepustki, identyfikatora lub po akceptacji przez system kontroli dostępu.
W zależności od sposobu przechowywania informacji niejawnych rozróżnia się następujące klasy strefy bezpieczeństwa:

a) ***strefa bezpieczeństwa klasy I*** - obszar, w którym są przetwarzane i przechowywane informacje niejawne o klauzuli „Poufne" lub wyższej w taki sposób, że wejście do tego obszaru praktycznie oznacza dostęp do tych informacji. W strefie mogą być zatrudnione wyłącznie osoby posiadające poświadczenia bezpieczeństwa osobowego, upoważniające do dostępu do informacji niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyżej sklasyfikowanej informacji
przechowywanej, przetwarzanej lub wytwarzanej w tym obszarze. Wstęp osób nie będących żołnierzami albo pracownikami komórki organizacyjnej objętej strefą (interesanci, personel sprzątający i techniczny) 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 przypadkowe ujawnienie ich treści,

b) ***strefa bezpieczeństwa klasy II*** - obszar, w którym są wytwarzane, przetwarzane i przechowywane informacje niejawne o klauzuli „Poufne" lub wyższej w taki sposób, że wejście do niego nie jest równoznaczne z dostępem do tych informacji. Żołnierze i pracownicy wojska komórek organizacyjnych objętych strefą oraz personel sprzątający i techniczny powinni posiadać poświadczenia bezpieczeństwa osobowego uprawniające co najmniej do dostępu do informacji niejawnych oznaczonych klauzulą „Poufne". Osoby nie będące żołnierzami albo pracownikami jednostki organizacyjnej (interesanci) mogą w niej przebywać za zgodą kierownika komórki organizacyjnej objętej tą strefą lub upoważnionych przez niego osób i pod nadzorem żołnierza lub pracownika tej komórki;

24) ***strefa administracyjna*** - obszar, obiekt, fragment budynku przylegający do I lub II strefy bezpieczeństwa, w którym zapewniona jest kontrola ruchu osób i pojazdów;
25) klasa systemów lub urządzeń alarmowych - kategoria jakości według Normy Obronnej NO-04-A004 Obiekty Wojskowe. Systemy Alarmowe. Wymagania dotyczące urządzeń;
26) szafa - szafę, sejf, skarbczyk, skrzynię, kontener lub inne urządzenie służące do przechowywania materiałów zawierających informacje niejawne;
27) klasa szafy - oznaczenie szafy określające stopień zapewnienia bezpieczeństwa przechowywanym w niej materiałom niejawnym;
28) pełnomocnik ochrony - pełnomocnika do spraw ochrony informacji niejawnych.

Rozdział 2
Organizacja i funkcjonowanie kancelarii tajnej i zagranicznej

§3.
1. Kancelarie tajne i zagraniczne, zwane dalej „kancelariami", tworzy się w jednostkach organizacyjnych, w których występują dokumenty zawierające informacje niejawne oznaczone klauzulą „POUFNE" lub stanowiące tajemnicę państwową.
2. Kancelarią kieruje kierownik kancelarii, wyznaczony przez kierownika jednostki organizacyjnej.
3. W uzasadnionych przypadkach w jednostce organizacyjnej można tworzyć filie kancelarii, których pracę koordynuje kierownik kancelarii.
4. W Ministerstwie Obrony Narodowej oraz dowództwach rodzajów sił zbrojnych dopuszcza się tworzenie więcej niż jednej kancelarii.
5. Na stanowisko kierownika kancelarii, zastępcy kierownika kancelarii, kierownika filii i kancelisty wyznacza się żołnierza zawodowego lub pracownika wojska, który posiada poświadczenie bezpieczeństwa odpowiednie dla klauzuli otrzymywanych, wytwarzanych, przetwarzanych, przekazywanych i przechowywanych w kancelarii dokumentów niejawnych

oraz odbył szkolenie podstawowe i specjalistyczne, potwierdzone stosownym zaświadczeniem.

§4.
1. Do obowiązków kierownika kancelarii lub kierownika filii należy w szczególności:

1) rejestrowanie dokumentów niejawnych otrzymywanych, wysyłanych oraz wytworzonych na potrzeby wewnętrzne jednostki organizacyjnej, według zasad ustalonych w zarządzeniu;
2) prowadzenie ewidencji pieczęci urzędowych oraz służbowych posiadanych przez jednostkę lub komórkę organizacyjną;
3) wysyłanie dokumentów wytworzonych w jednostce organizacyjnej do adresatów;
4) prowadzenie wykazów osób upoważnionych do dostępu do informacji niejawnych, posiadających stosowne poświadczenia bezpieczeństwa;
5) udostępnianie dokumentów niejawnych osobom, o których mowa w pkt 4;
6) prowadzenie bieżącej kontroli sposobu wytwarzania dokumentów niejawnych przez wykonawców i wykonawców technicznych;
7) rozliczanie wykonawców z powierzonych im dokumentów niejawnych;
8) kompletowanie dokumentów oraz przygotowywanie akt do archiwizacji;
9) wykonywanie poleceń pełnomocnika ochrony.

2. Kierownicy kancelarii zagranicznych oraz kancelarii, w których zorganizowano punkty obsługi dokumentów zagranicznych, mają obowiązek prowadzenia wykazu kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych w resorcie Obrony Narodowej, na podstawie informacji otrzymywanych z Kancelarii Głównej Zagranicznej Ministerstwa Obrony Narodowej.

3. Szczegółowe obowiązki kierownika kancelarii oraz kierowników filii ustala pełnomocnik ochrony, a zastępcy kierownika kancelarii i kancelistów kierownik kancelarii.

§5.
1. Przekazanie obowiązków na stanowisku kierownika kancelarii następuje na podstawie protokołu zdawczo-odbiorczego, w obecności pełnomocnika ochrony, osoby zdającej oraz przyjmującej obowiązki.

2. 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 oraz pozycje zapisów w tych urządzeniach;
2) informacje dotyczące zgodności lub niezgodności stanu faktycznego dokumentów niejawnych znajdujących się w kancelarii tajnej ze stanem ewidencyjnym;
3) ewentualne uwagi osoby przyjmującej obowiązki kierownika kancelarii, dotyczące nieprawidłowości ujawnionych w zakresie ewidencjonowania i obiegu dokumentów.

3. Protokół, o którym mowa w ust. 1, podpisuje osoba przekazująca obowiązki kierownika kancelarii oraz osoba przyjmująca, a zatwierdza pełnomocnik ochrony. Jeden egzemplarz protokołu jest przechowywany w kancelarii, drugi przez pełnomocnika ochrony.

4. Dodatkowy egzemplarz protokołu może być wydany przekazującemu obowiązki kierownika kancelarii, na jego żądanie.
5. Na czas okresowej nieobecności (urlop, choroba, wyjazd służbowy) kierownika kancelarii

zastępuje jego zastępca lub kancelista, a w razie ich braku, osoba posiadająca stosowne poświadczenie bezpieczeństwa oraz odbyte przeszkolenia, o których mowa w § 3 ust. 5, wyznaczona rozkazem dziennym lub innym dokumentem decyzyjnym przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony.

6. Kierownik kancelarii przekazuje protokolarnie zastępującej go osobie, nie będącej zastępcą kierownika kancelarii lub kancelista, wyłącznie urządzenia ewidencyjne i materiały niezbędne do bieżącej pracy kancelarii. Szafy z pozostałymi dokumentami niejawnymi zamyka i oznakowuje swoją pieczęcią numerową.

7. Jeżeli kierownik kancelarii nie może uczestniczyć w czynnościach, o których mowa w ust. 1 i 6, kierownik jednostki organizacyjnej powołuje komisję w celu przekazania jego obowiązków.

8. Przewodniczący komisji, o której mowa w ust. 7, 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. Kancelarię organizuje się w pomieszczeniach spełniających następujące warunki bezpieczeństwa:

1) zlokalizowanych, z zastrzeżeniem ust. 2, w budynku o konstrukcji murowanej lub betonowej, 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, pozbawionych zbędnych otworów;
3) w przypadku, gdy ściany zewnętrzne lub strop 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;
4) wyposażonych w drzwi wejściowe stalowe lub drewniane pełne wzmocnione o grubości co najmniej 2 cm, obustronnie obite blachą stalową o grubości co najmniej 2mm, zabezpieczone przed wyłamaniem od strony zawiasów, wyposażone w dwa zamki, w tym jeden mechaniczny szyfrowy, o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skoku nastawień nie większym niż jedna działka, posiadający co najmniej 100 podziałek na tarczy;
5) z oknami zabezpieczonymi w sposób uniemożliwiający ich otwarcie przez osobę, nieupoważnioną oraz wgląd z zewnątrz; w otworach okiennych, z zastrzeżeniem pkt 6, instaluje się kratę wykonaną w ramie 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, wzmocnioną płaskownikami stalowymi o przekroju nie mniejszym niż 45x6 mm, usytuowanymi w poziomie, w rozstawie nie większym niż 500 mm;
6) otwory okienne, których dolna krawędź znajduje się na wysokości powyżej 5,5 m od poziomu otaczającego terenu wyposaża się w jedno z następujących zabezpieczeń:
a) siatkę stalową z drutu o grubości nie mniejszej niż 2 mm, o oczkach nie większych niż 20x20 mm,

b) folię antywłamaniową,
c) szyby o podwyższonej odporności na stłuczenie;

7) otwory wentylacyjne zabezpiecza się na poziomie stropów siatką stalowa o średnicy oczka 10 mm oraz wyposaża od wewnątrz w otwory rewizyjne umożliwiające kontrolę przewodów wentylacyjnych.

2. Nie dopuszcza się lokalizacji kancelarii na poddaszach.

3. W kancelarii wydziela się pomieszczenie lub miejsce przeznaczone do udostępniania wykonawcom dokumentów niejawnych.

4. Pomieszczenia kancelarii zalicza się do I strefy bezpieczeństwa.

5. W kancelarii instaluje się przeciwpożarowy system alarmowy, systemy sygnalizujące próby siłowego otwarcia drzwi wejściowych i okien, ruch w pomieszczeniach oraz system sygnalizacji napadu; zaleca się instalowanie telewizyjnych systemów nadzoru do prowadzenia ciągłej obserwacji zewnętrznej drzwi wejściowych i okien.

6. Instalowane systemy i urządzenia alarmowe powinny odpowiadać następującym klasom:

1) SA4 i S - w przypadku przechowywania dokumentów zawierających informacje niejawne oznaczone klauzulą „Ściśle Tajne",
2) SA3 i C - w przypadku przechowywania dokumentów zawierających informacje niejawne oznaczone klauzulą „Tajne" i „Poufne".

7. Kancelarię wyposaża się w:

1) urządzenia do przechowywania dokumentów niejawnych:

a) szafy stalowe klasy A do przechowywania dokumentów zawierających informacje niejawne stanowiące tajemnicą 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 C do przechowywania dokumentów zawierających informacje niejawne stanowiące tajemnicę służbową, oznaczonych klauzulą „Zastrzeżone";

2) sprzęt kwaterunkowy zgodnie z obowiązującą normą należności;
3) barierkę uniemożliwiającą wstęp osobom nieupoważnionym do pomieszczeń kancelaryjnych;
4) urządzenia do niszczenia dokumentów na miał papierowy lub tnące na paski o maksymalnych wymiarach 1,5x25 mm.

8. Warunki techniczne jakim powinny odpowiadać szafy, o których mowa w ust. 7 pkt 1 określa załącznik nr 1 do zarządzenia.

9. Na drzwiach urządzeń, o których mowa w ust. 7 pkt 1, nakleja się kartę informacyjną, której wzór określa załącznik nr 2 do zarządzenia.
10. Zaleca się wyposażanie kancelarii w sprzęt informatyczny przystosowany do przetwarzania informacji niejawnych zapisanych na elektronicznych nośnikach informacji.

11. W szczególnie uzasadnionych przypadkach, uniemożliwiających spełnienie któregokolwiek warunków, o których mowa w ust. 1, zgody na zastosowanie alternatywnych środków bezpieczeństwa udziela szef Wojskowych Służb Informacyjnych.

§7.
1. Dokumenty zawierające informacje niejawne będące na ewidencji kancelarii przechowuje się w urządzeniach do przechowywania dokumentów odrębnych dla każdej klauzuli, państwa i organizacji międzynarodowej.
2. Zezwala się przechowywać dokumenty o różnych klauzulach tajności w jednym urządzeniu, pod warunkiem, że jego konstrukcja pozwala na ich rozdzielenie i zamknięcie w odrębnych skrytkach.
3. Dokumenty o różnych klauzulach tajności, a także dokumenty jawne mogą być przechowywane wspólnie, jeżeli ich treść łączy się bezpośrednio z określoną sprawą.
4. Teczki akt, segregatory, schematy oraz inne materiały niejawne o dużych rozmiarach, przechowuje się w kancelarii w obudowanych, zamykanych i opieczętowanych regałach lub przystosowanych do tego celu meblach.
5. Przedmioty, urządzenia o dużych wymiarach, tablice poglądowe, schematy, mapy, oraz wojskowe wydawnictwa specjalistyczne zawierające informacje niejawne, przechowuje się w pomieszczeniach zabezpieczonych w sposób określony w § 6 ust 1, 2, 5 i 6.
6. W pomieszczeniach służbowych nie spełniających standardów bezpieczeństwa, określonych w § 6 ust. 1, 2, 5 i 6, materiały zawierające informacje niejawne należy przechowywać wyłącznie w urządzeniach, o których mowa w § 6 ust. 7 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 może odbywać się wyłącznie w obecności co najmniej jednej osoby z jej etatowego personelu.
2. Na czas sprzątania personel kancelarii zabezpiecza dokumenty niejawne w sposób uniemożliwiający przypadkowe ujawnienie ich treści osobom nieupoważnionym.

§9.
Zabrania się wnoszenia do pomieszczeń kancelarii urządzeń służących do rejestrowania informacji, w tym dźwięku i obrazu oraz telefonów komórkowych.

§10.
1. Po zakończeniu pracy kierownik kancelarii zamyka i plombuje urządzenia do przechowywania dokumentów niejawnych oraz zabezpiecza pomieszczenia kancelarii.
2. Zasady zdawania, przechowywania i wydawania kluczy użytku bieżącego do pomieszczeń i urządzeń, o których mowa w ust. 1, oraz kluczy zapasowych do pomieszczeń kancelarii, ustala kierownik jednostki organizacyjnej w planie ochrony.
3. Klucze zapasowe oraz kody dostępu do urządzeń, o których mowa w ust. 1, 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. Formularze oraz koperty, o których mowa w ust. 3, oznacza się klauzulą tajności odpowiadającą klauzuli najwyżej sklasyfikowanej informacji, przechowywanej w danym urządzeniu.
5. Zabrania się zapisywania przez użytkowników kodów dostępu oraz wynoszenia poza teren jednostki (komórki) organizacyjnej kluczy, o których mowa w ust. 2.

6. Kody, o których mowa w ust. 3, zmienia się:

1) w urządzeniach nowo instalowanych oraz w odstępach czasowych nie przekraczających 6 miesięcy;
2) po każdej naprawie lub konserwacji zamka;
3) po przekazaniu obowiązków na stanowisku kierownika kancelarii, jego zastępcy lub kancelisty;
4) w przypadku ujawnienia kodu osobie nieupoważnionej.

7. W przypadku utraty (zagubienia) kluczy od pomieszczeń i urządzeń, o których mowa w ust. 1, należy bezwzględnie wymienić zamki.

Rozdział 4
Zasady organizacji, funkcjonowania i zabezpieczenia kancelarii tajnych na okrętach i jednostkach pływających Marynarki Wojennej

§11.
1. Kancelarię na okręcie organizuje się w pomieszczeniach spełniających następujące warunki bezpieczeństwa:

1) zlokalizowanych pod pokładem głównym okrętu, przy czym ściany zewnętrzne nie powinny być burtami;
2) oddzielonych od innych pomieszczeń trwałymi ścianami bez otworów konstrukcyjnych; konstrukcja ścian powinna uniemożliwiać przedostanie się do wewnątrz przy użyciu narzędzi ręcznych;
3) nie posiadających okien (bulajów), a gdy jest to niemożliwe bulaje powinny być nieotwieralne, wykonane z hartowanego szkła i zabezpieczone w sposób uniemożliwiający wgląd z zewnątrz;
4) posiadających otwory wentylacyjne i inne otwory w ścianach, podłogach lub sufitach zabezpieczone przed penetracją siatką stalową o średnicy oczka 10 mm; jeżeli otwory przekraczają 600 cm 2, przegrody powinny być wzmocnione prętami stalowymi lub wyposażone w system detekcji obecności osób;
5) wyposażonych w drzwi wejściowe wykonane ze stali, zabezpieczone przed włamaniem od strony zawiasów i ryglowane na trzech pozostałych płaszczyznach, zamykane na dwa zamki, w tym jeden mechaniczny szyfrowy, o zmiennym nastawieniu szyfrowym, co najmniej trzytarczowy, o cichym przesuwie, skoku nastawień nie większym niż jedna działka, posiadający co najmniej 100 podziałek na tarczy.

2. Pomieszczenia kancelarii zalicza się do I strefy bezpieczeństwa.
3. Pomieszczenia kancelarii powinny być chronione ogólnookrętową instalacją przeciwpożarową.
4. W kancelarii instaluje się systemy sygnalizujące próby siłowego otwarcia drzwi wejściowych, ruch w pomieszczeniach oraz system sygnalizacji napadu.
5. Instalowane systemy i urządzenia powinny spełniać warunki, o których mowa w § 6 ust. 6.
6. Kancelarię wyposaża się w szafę stalową klasy A, wyposażoną w zamykane skrytki umożliwiające odrębne przechowywanie dokumentów o różnych klauzulach tajności oraz urządzenia, o których mowa w § 6 ust. 7 pkt 3 i 4.
7. Podczas postoju w porcie, dokumenty niejawne przechowuje się w kancelarii okrętu.
8. Na okrętach wyposażonych w kancelarię kryptograficzną nie organizuje się dodatkowej kancelarii.
9. Na okrętach, na których nie ma możliwości zorganizowania kancelarii, dokumenty

niejawne przechowuje się w kabinie dowódcy okrętu, wyposażonej zgodnie z § 6 ust. 7 pkt 1.
10. 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 § 18 ust. 8; dokument musi pozostawać pod stałą kontrolą służby wachtowej.
11. Fakt przekazania dokumentów niejawnych, o których mowa w ust. 10, podlega odnotowaniu w dzienniku wachtowym.

Rozdział 5
Zasady rejestrowania i niszczenia dokumentów niejawnych

§12.
1. Kancelaria przyjmuje, rejestruje, przechowuje, przekazuje i wysyła dokumenty zawierające informacje niejawne.

2. Stan ewidencyjny dokumentów oraz ich obieg obrazują trwałe i pomocnicze urządzenia ewidencyjne.

3. Trwałymi urządzeniami ewidencyjnymi są:

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) „Książka ewidencji wydawnictw, dokumentacji technicznej oraz materiałów filmowych", zwana dalej „Książką ewidencji wydawnictw", której wzór określa załącznik nr 6 do zarządzenia;
4) „Książka ewidencji pieczęci", której wzór określają odrębne przepisy.

4. Pomocniczymi urządzeniami ewidencyjnymi są:

1) „Wykaz osób upoważnionych do dostępu do informacji niejawnych", którego wzór określa załącznik nr 7 do zarządzenia;
2) „Kartoteka 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;

3) „Dziennik ewidencji wykonanych dokumentów", którego wzór określa załącznik nr 10 do zarządzenia;
4) „Wykaz przesyłek nadanych" oraz „Wykaz przesyłek wydanych", których wzór określają odrębne przepisy;
5) „Książka doręczeń", której wzór określa załącznik nr 11 do zarządzenia;
6) „Karta zapoznania się z dokumentem niejawnym", której wzór określają odrębne przepisy;
7) „Metryka elektronicznego nośnika informacji", której wzór określa załącznik nr 12 do zarządzenia;
8) „Rozdzielnik stały", którego wzór określa załącznik nr 13 do zarządzenia.

5. Kancelaria tajna prowadzi trwałe urządzenia ewidencyjne, o których mowa w ust. 3 oraz urządzenia pomocnicze wymienione w ust. 4 pkt 1, 2 i 4-8;

6. „Dziennik ewidencji wykonanych dokumentów", o którym mowa w ust. 4 pkt 3, prowadzi wykonawca techniczny lub osoba wyznaczona przez kierownika jednostki albo komórki organizacyjnej wytwarzającej dokumenty niejawne.

§13.
1. Karty urządzeń ewidencyjnych w formie broszur numeruje, przeszywa, opisuje i opieczętowuje kancelaria jednostki organizacyjnej w sposób, którego wzór określa załącznik nr 14 do zarządzenia.
2. W urządzeniach ewidencyjnych, o których mowa w ust. 1, z wyłączeniem urządzeń wskazanych w § 12 ust. 3 pkt 3 i 4, ust. 4 pkt 2, § 15 ust. 5 pkt l i § 37 ust. 1, zaznacza się początek i koniec roku kalendarzowego oraz po zakończeniu roku sporządza się adnotację na jakiej pozycji zapisu zakończono ewidencję, potwierdzoną podpisem kierownika kancelarii i pieczęcią „Do pakietów".

§14.
1. „Rejestr dokumentacji" jest nadrzędnym urządzeniem ewidencyjnym w stosunku do innych urządzeń ewidencyjnych, w którym rejestruje się:

1) trwałe urządzenia ewidencyjne kancelarii oraz pomocnicze urządzenia ewidencyjne, o których mowa w § 12 ust. 4 pkt 2 lit b i pkt 8;
2) teczki akt (przedmiotowe);
3) książki rozkazów dziennych, meldunków, protokołów finansowych, materiałowych, uzbrojenia i sprzętu wojskowego oraz inne, prowadzone przez poszczególne komórki organizacyjne jednostki organizacyjnej, jeżeli podlegają przekazaniu do archiwum.

2. Każdy tom urządzenia, teczki akt lub dokumentu, o którym mowa w ust. 1, rejestruje się pod odrębną pozycją.

3. „Rejestru dokumentacji" nie rejestruje się, z zastrzeżeniem ust. 4.

4. „Rejestr dokumentacji" filii kancelarii rejestruje się w „Rejestrze dokumentacji" kancelarii.

5. „Rejestr dokumentacji" opatruje się adnotacją o ilości stron, poświadczoną podpisem pełnomocnika ochrony jednostki organizacyjnej oraz pieczęcią urzędową jednostki organizacyjnej.

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 materiałów zaewidencjonowanych w latach poprzednich.

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 oznaczenie roku (np. RWD Pf-7/2002).
9. Po likwidacji (rozformowaniu) jednostki organizacyjnej „Rejestr dokumentacji" podlega przekazaniu do archiwum.

§15.
1. W „Dzienniku korespondencji" rejestruje się dokumenty niejawne, otrzymane oraz wytworzone w jednostce organizacyjnej.

2. W „Dzienniku korespondencji" nie rejestruje się:

1) dowodów materiałowo-finansowych (rachunki, faktury, itp.), które przekazuje się za pokwitowaniem w „Książce doręczeń" właściwej komórce organizacyjnej, w której podlegają ewidencji stosownie do odrębnych przepisów;
2) dokumentów przesłanych omyłkowo.

3. Kancelaria prowadzi odrębne „Dzienniki korespondencji" dla poszczególnych klauzul tajności; dopuszcza się rejestrowanie w jednym „Dzienniku korespondencji" dokumentów otrzymywanych i wysyłanych.
4. Przepis ust. 3 nie dotyczy „Dzienników korespondencji", o których mowa w ust. 5 pkt 1, 2 i 4 oraz & 37 ust. 1.
5. W odrębnych „Dziennikach korespondencji" rejestruje się:

1) dokumenty planowania mobilizacyjnego, operacyjnego oraz osiągania wyższych stanów gotowości bojowej i obronnej, zachowując ciągłość pozycji zapisów przez okres obowiązywania danego planu;
2) dokumenty decyzyjne wydawane przez kierownika jednostki organizacyjnej, których ewidencję prowadzi kancelaria, przy czym:

a) liczba porządkowa, pod którą wpisano dokument decyzyjny w dzienniku jest równocześnie jego numerem ewidencyjnym,
b) numerację dokumentów rozpoczyna się w każdym roku kalendarzowym od liczby „1",
c) jeżeli kierownik jednostki organizacyjnej wydaje dokumenty decyzyjne w różnych formach (np. zarządzenia i decyzje), to rejestruje się je w odrębnych „Dziennikach korespondencji",
d) „Dziennik korespondencji prowadzi się do całkowitego wykorzystania kart;

3) dokumenty uzyskane od innych państw oraz organizacji międzynarodowych w ramach realizacji umów międzynarodowych;
4) „Karty zapoznania się z dokumentem", z uwzględnieniem pkt 2 lit. b i d.

6. Po wykorzystaniu wszystkich stron „Dziennika korespondencji", zakłada się następny tom i zachowuje ciągłość dotychczasowej numeracji.

7. Zarejestrowanie korespondencji otrzymanej polega na:

1) opatrzeniu otrzymanego dokumentu pieczęcią wpływu oraz odciśnięciu pieczęci formularzowej na załącznikach;
2) wpisaniu w kolejnej pozycji „Dziennika korespondencji":

a) numeru porządkowego, który jest jednocześnie numerem ewidencyjnym,
b) danych ewidencyjnych dokumentu, nadanych przez nadawcę (numer wychodzący i data wysłania),
c) ilości stron dokumentu wraz z załącznikami,
d) ilości załączników i ich stron lub nazwy i liczby elektronicznych nośników informacji, jeżeli załączniki zostały wykonane na tych nośnikach;

3) wpisaniu danych wymienionych w pkt 2 lit. a, c i d na dokumencie w odpowiednich polach odcisków pieczęci.

8. Szczegółowe zasady oznaczania dokumentów niejawnych regulują odrębne przepisy.

9. Korespondencję opatrzoną adnotacją „Do rąk własnych" rejestruje się bez otwierania wewnętrznego opakowania przesyłki, poprzez wpisanie w odpowiednich rubrykach „Dziennika korespondencji" zapisów umieszczonych na opakowaniu wewnętrznym, zamieszczenie w rubryce „Uwagi" adnotacji „Do rąk własnych", odciśnięcie na opakowaniu pieczęci wpływu i wpisaniu numeru ewidencyjnego według „Dziennika korespondencji" oraz daty wpływu przesyłki.
10. Jeżeli przesyłka opatrzona adnotacją „Do rak własnych" zawiera kilka dokumentów, to każdy z nich rejestruje się pod odrębną pozycją „Dziennika korespondencji", a na opakowaniu przesyłki zamieszcza się numery ewidencyjne poszczególnych dokumentów.
11. Przesyłkę opatrzoną adnotacją „Do rąk własnych" przekazuje się bezpośrednio adresatowi, a w razie jego nieobecności osobie przez niego upoważnionej.
12. Przesyłkę opatrzoną adnotacją „Do rąk własnych" można zwrócić do kancelarii w stanie otwartym lub zamkniętym.
13. W przypadku, gdy przesyłka oznaczona adnotacją „Do rąk własnych" zostanie zwrócona do kancelarii w otwartym opakowaniu, podlega zarejestrowaniu na zasadach określonych w ust. 7, z tym, że zachowuje się numer ewidencyjny wpisany na opakowaniu i uzupełnia nie zapisane rubryki „Dziennika korespondencji".
14. 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";

2) w przypadku zauważenia nieprawidłowości lub podejrzeń co do zawartości przesyłki, kierownik kancelarii odmawia jej przyjęcia powiadamiając o tym pełnomocnika ochrony.

15. Zarejestrowanie korespondencji wysyłanej odbywa się na zasadach określonych w ust. 7, z tym, że używa się pieczęci nagłówkowej, a w odpowiednich rubrykach „Dziennika korespondencji" wpisuje się ilość stron dokumentu wraz z załącznikami, ilość załączników oraz stron załączników pozostających w aktach lub nazwę i liczbę elektronicznych nośników informacji, jeżeli załączniki zostały wykonane na tych nośnikach, numer ewidencyjny według „Dziennika ewidencji wykonanych dokumentów" oraz wykonawcę.
16. W rubryce „Uwagi" „Dziennika korespondencji" wpisuje się datę wysłania dokumentu, numer i pozycję zapisu w „Książce doręczeń" albo numer i pozycję zapisu w „Wykazie przesyłek nadanych", za którym dokument przekazano przewoźnikowi.
17. Jeżeli w kancelarii nie pozostawia się żadnego egzemplarza dokumentu, w rubryce „Uwagi" zamieszcza się dodatkowo adnotację „tylko adresat".
18. Przed zarejestrowaniem w „Dzienniku korespondencji" dokumentu przekazanego do wysłania, w kancelarii sprawdza się czy dokument:
1) został właściwie wykonany i oznaczony;
2) wytworzono w ilości podanej w rozdzielniku;
3) zawiera dane określające faktyczną ilość załączników i stron załączników przesyłanych do adresata oraz pozostawianych w aktach;
4) został podpisany przez osobę uprawnioną.

19. W razie niespełnienia jednego z warunków, o których mowa w ust. 18, kierownik kancelarii zwraca dokument wykonawcy do poprawienia lub uzupełnienia.

§16.
1. W „Książce ewidencji wydawnictw" rejestruje się dokumenty niejawne wytwarzane na potrzeby jednostki organizacyjnej lub otrzymane, które są:

1) wojskowymi wydawnictwami specjalistycznymi;
2) materiałami szkoleniowymi i informacyjnymi;
3) dokumentacją techniczną (schematy, rysunki);
4) gotowymi materiałami filmowymi.

2. Kancelaria prowadzi odrębne „Książki ewidencji wydawnictw" dla każdej klauzuli tajności.
3. Kancelaria rejestruje w „Książce ewidencji wydawnictw" dokumenty, o których mowa w ust. 1, wpisując do niej:

1) pod odrębną pozycją tytuł każdego z otrzymanych dokumentów, według kolejności ich wpływu;
2) ilość i numery egzemplarzy danego tytułu dokumentu;
3) numer i datę faktury, asygnaty lub pisma przewodniego, za którymi je przekazano.

4. Liczba porządkowa pozycji, o której mowa w ust. 3 pkt 1, jest jednocześnie numerem ewidencyjnym wszystkich egzemplarzy danego tytułu dokumentu.
5. 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" i wpisuje numer ewidencyjny.
6. Asygnaty, faktury i pisma przewodnie, za którymi przesłano dokumenty, wskazane w ust. 1, opatruje się numerem, pod którym zarejestrowano pierwszy wymieniony w nich materiał.
7. Dokumentację techniczna oraz gotowe materiały filmowe, o których mowa w ust. 1 pkt 3 i 4, ewidencjonuje się w oddzielnych „Książkach ewidencji wydawnictw"; w razie otrzymywania niewielu tytułów w ciągu roku kalendarzowego, ich ewidencję można prowadzić łącznie z wojskowymi wydawnictwami specjalistycznymi.
8. Negatywy filmów oraz pozytywy zawierające informacje niejawne ewidencjonuje się oddzielnie; w razie dodatkowego wytwarzania pozytywów, ewidencjonuje się je pod odrębną pozycją.

§17.
1. W wykazie, o którym mowa § 12 ust. 4 pkt 1, wpisuje się imiona i nazwiska osób upoważnionych do dostępu do informacji niejawnych, z wyszczególnieniem klauzuli tajności tych informacji oraz terminów ważności poświadczeń bezpieczeństwa.
2. „Wykaz osób upoważnionych do dostępu do informacji niejawnych" wykonuje się w układzie alfabetycznym, z uwzględnieniem struktury organizacyjnej jednostki organizacyjnej.
§18.
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 blankietów szyfrogramów i telegramów,
b) kalki i taśmy maszynowe, taśmy karbonizowane (jednorazowego użytku),

c) elektroniczne nośniki informacji, w szczególności dyski twarde, płyty CD, CD-R, CD-RW, DVD, dyskietki, taśmy magnetyczne oraz kasety taśmowe;

2) pomocnicze urządzenia ewidencyjne wymienione w § 12 ust. 4 pkt 1, 3, 5 i 7;
3) załączniki odłączone od pism przewodnich, nie podlegające ewidencji w innych urządzeniach.

2. W „RWD" ewidencjonuje się również udostępnienie wykonawcom dokumentów niejawnych:

1) zarejestrowanych we właściwych 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, map, teczek akt i innych dokumentów, których urządzenia ewidencyjne nie przewidują możliwości kwitowania w nich pobrania i zwrotu dokumentu.

3. „RWD" rejestruje się. w „Skorowidzu RWD" według:

1) układu alfabetycznego, jeżeli jest prowadzony imiennie dla wykonawców albo komórki organizacyjnej;
2) numerów ewidencyjnych lub sygnatur, jeżeli jest prowadzony dla poszczególnych dokumentów albo wydawnictw.

4. Numerem ewidencyjnym karty „RWD" jest numer porządkowy, pod którym została ona zarejestrowana w „Skorowidzu RWD".

5. Na dokumentach zarejestrowanych w „RWD" nanosi się i poświadcza pieczęcią „Do pakietów" numer ewidencyjny, który składa się z nazwy urządzenia, numeru karty, o którym mowa w ust. 4, łamanego przez liczbę porządkową pozycji, pod którą zarejestrowano 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 numeru ewidencyjnego dokumentu lub sygnatury wydawnictwa, bez wpisywania w kolumnie 1 numeru porządkowego.

7. Dokumenty zarejestrowane w „RWD", po zwróceniu ich do kancelarii, podlegają zniszczeniu lub przerejestrowaniu do „RWD" innego wykonawcy.
8. „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.

9. Po wykorzystaniu wszystkich pozycji w „RWD", dołącza się nową kartę zachowując ciągłość numeracji.

10. „RWD" wykonawców niszczy się komisyjnie po upływie jednego roku od daty zwrotu wszystkich zarejestrowanych w nich dokumentów.

11. „RWD" przeznaczone do wypożyczania dokumentów lub wydawnictw niszczy się komisyjnie bezpośrednio po ich rozliczeniu.

§19.
1. „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.
2. Dla każdej techniki wytwarzania dokumentów prowadzi się odrębny „Dziennik ewidencji wykonanych dokumentów".
3. „Dziennik ewidencji wykonanych dokumentów" rejestruje się w „RWD" osób, o których mowa w § 12 ust. 6, i niszczy komisyjnie po upływie roku od rozliczenia zaewidencjonowanych w nim dokumentów.
4. Dokumenty niejawne przeznaczone dla adresatów zagranicznych rejestruje się w „Dziennikach ewidencji wykonanych dokumentów", ujętych w ewidencji kancelarii zagranicznej.
5. 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 jest numerem ewidencyjnym dokumentu.
6. Dodatkowo wytworzony dokument zawierający informacje niejawne, w szczególności odpis, kopię lub reprodukcję rejestruje się każdorazowo pod odrębną pozycją „Dziennika ewidencji wykonanych dokumentów".
7. Kierownik kancelarii co najmniej raz w miesiącu rozlicza „Dziennik ewidencji wykonanych dokumentów" poprzez wpisanie w odpowiedniej rubryce dziennika numerów pod jakimi wytworzone dokumenty zarejestrowano w urządzeniach ewidencyjnych kancelarii.

§20.
1. W „Wykazie przesyłek nadanych" rejestruje się wojskowe przesyłki pocztowe przekazywane przewoźnikowi lub adresatowi, jeżeli są dostarczane bezpośrednio przez przedstawiciela nadawcy albo adresata.
2. 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.
3. 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.
4. 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.
5. Kierownik kancelarii wpisuje w rubryce „Uwagi" wykazu, o którym mowa w ust. 4, numery ewidencyjne pod jakimi poszczególne przesyłki zostały zarejestrowane w „Dzienniku korespondencji".
6. Kancelaria przechowuje wykazy, o których mowa w ust. 1, 3 i 4, w specjalnie przeznaczonych do tego celu segregatorach, wykazy niszczy się komisyjnie po przeprowadzeniu kontroli rocznej stanu ochrony informacji niejawnych.
7. Szczegółowe zasady stosowania „Wykazu przesyłek nadanych" oraz „Wykazu przesyłek wydanych" określają odrębne przepisy.

§21.
1. W „Książce doręczeń" rejestruje się dokumenty doręczane adresatom bezpośrednio przez personel kancelarii.
2. „Książkę doręczeń" wykorzystuje się do czasu wykorzystania wszystkich pozycji i niszczy komisyjnie po przeprowadzeniu kontroli rocznej.
3. „Książka doręczeń" nie może służyć do ewidencjonowania obiegu dokumentów przekazywanych poza jednostkę organizacyjną.

§22.
1. Kancelaria prowadzi ewidencją pieczęci urzędowych i służbowych jednostki organizacyjnej, kamieni, godeł i znaków do plombowania oraz pakietów z pieczęciami na okres wojny.
2. Wzory pieczęci stosowanych w kancelarii określa załącznik nr 15 do zarządzenia.
3. Pieczęcie, o których mowa w ust. 1, ewidencjonuje się w „Książce ewidencji pieczęci".
4. „Książkę ewidencji pieczęci" prowadzi się do czasu wykorzystania wszystkich kart i zdaje do archiwum po upływie 5 lat od jej zakończenia.

§23.
1. W „Karcie zapoznania się z dokumentem niejawnym" rejestruje się każdorazowy fakt udostępnienia dokumentów zawierających informacje niejawne stanowiące tajemnicę państwowa i uwierzytelnia podpisem osoby zapoznającej się z dokumentem.
2. Fakt zapoznania się z dokumentem niejawnym wchodzącym w skład zbioru dokumentów, rejestruje się w „Karcie zapoznania się z dokumentem" wystawionej dla całego zbioru.
3. Przepis ust. 2 stosuje się odpowiednio do teczek akt.
4. „Karty zapoznania się z dokumentem" nie zakłada się dla urządzeń ewidencyjnych oraz brudnopisów dokumentów, o których mowa w ust. 1.
5. „Kartę zapoznania się z dokumentem niejawnym":

1) podłącza się do dokumentu, o którym mowa w ust. 1;
2) przesyła lub archiwizuje wraz z dokumentem, którego dotyczy albo z protokołem jego zniszczenia.

§24.
1. W „Metryce elektronicznego nośnika informacji", zwanej dalej „metryką", rejestruje się dane dotyczące informacji niejawnych zapisanych na nośniku.
2. Metrykę zakłada kancelaria wydająca 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.
6. Metrykę niszczy się komisyjnie po upływie roku od chwili zniszczenia nośnika.

§25.
1. „Rozdzielnik stały" dokumentuje obieg dokumentów zawierających informacje niejawne, wysyłanych cyklicznie, w ciągu roku lub kilku lat, do stałych adresatów, a w szczególności:

1) decyzji, rozkazów i innych dokumentów decyzyjnych;
2) dokumentów informacyjno-sprawozdawczych i planistycznych;
3) biuletynów i innych wydawnictw periodycznych.

2. „Rozdzielnik stały" określa

1) adresatów;
2) numery egzemplarzy dokumentów przeznaczone dla poszczególnych adresatów oraz numery egzemplarzy dokumentów pozostające w aktach kancelarii.

3. „Rozdzielnik stały" podlega zatwierdzeniu przez kierownika jednostki organizacyjnej albo osobę, przez niego upoważnioną.

§26.
1. Zapisów w urządzeniach ewidencyjnych dokonuje się czarnym lub niebieskim atramentem albo tuszem.
2. Zmiany zapisów, o których mowa w ust. 1, nanosi się kolorem czerwonym poprzez skreślenie pierwotnego zapisu, umieszczenie nowego zapisu uwierzytelnionego podpisem kierownika kancelarii w rubryce „Uwagi" urządzenia ewidencyjnego, odciskiem pieczęci „Do pakietów" oraz wpisaniem daty wprowadzenia zmiany.
3. Zabrania się wycierania, zamazywania i zaklejania zapisów w urządzeniach ewidencyjnych.

§27.
1. Kancelaria przekazuje dokumenty zawierające informacje niejawne oznaczone klauzulą „Poufne" lub stanowiące tajemnicę państwową wyłącznie wykonawcom posiadającym stosowne poświadczenia bezpieczeństwa, których pomieszczenia są zlokalizowane w strefie bezpieczeństwa i wyposażone w urządzenia do przechowywania dokumentów, o których mowa w § 6 ust. 7 pkt 1, na podstawie dekretacji kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej, za pokwitowaniem w dzienniku korespondencji lub innym urządzeniu ewidencyjnym.
2. W sytuacjach szczególnych, za zgodą kierownika jednostki organizacyjnej, zezwala się na udostępnianie materiałów niejawnych oznaczonych klauzulą „Poufne" lub „Tajne" wykonawcom nie posiadającym urządzeń, o których mowa w § 6 ust.7 pkt 1, jeżeli spełniają pozostałe warunki określone w ust. 1.
3. Wykonawca, któremu udostępniono materiały niejawne na zasadach określonych w ust. 2, ma obowiązek zachowania środków bezpieczeństwa uniemożliwiających dostąp do tych materiałów przez osoby nieuprawnione oraz zwrócić je do kancelarii przed zakończeniem dnia pracy.
4. Wykonawcom, których pomieszczenia służbowe znajdują się poza strefą bezpieczeństwa, materiały niejawne oznaczone klauzulą „Poufne" oraz stanowiące tajemnicę państwową udostępnia się w pomieszczeniu lub miejscu pracy w kancelarii, o którym mowa w § 6 ust. 3.
5. Przesyłki opatrzone adnotacją „Pilne" przekazuje się adresatom bezzwłocznie.
6. O Udostępnianie materiałów niejawnych oznaczonych klauzulą „Zastrzeżone' odbywa się na zasadach określonych przez kierownika jednostki organizacyjnej.
7. Przekazywanie dokumentów niejawnych poza jednostkę organizacyjną odbywa się wyłącznie przez kancelarię i za zgodą kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej.
8. Zezwala się na czasowe przekazywanie dokumentów niejawnych, zawierających informacje stanowiące tajemnicę służbową, pomiędzy wykonawcami tej samej jednostki organizacyjnej, za pokwitowaniem w „Dzienniku wykonawcy". Wzór „Dziennika wykonawcy" określa załącznik nr 16 do zarządzenia.
9. Wykorzystane dokumenty zawierające informacje niejawne, otrzymane i wytworzone w jednostce organizacyjnej podlegają:

1) skompletowaniu przez ułożenie w segregatorach, według numerów ewidencyjnych lub spraw i podszyciu po zakończeniu roku kalendarzowego do odpowiednich teczek przedmiotowych o określonej kategorii archiwalnej, jeżeli stanowią wartość archiwalną lub użytkową, z zastrzeżeniem ust. 10;
2) zwrotowi do wydawcy, jeżeli określił on taki sposób postępowania;
3) bieżącemu niszczeniu.

10. Elektroniczne nośniki informacji, na których utrwalono informacje niejawne, kompletuje się przez ich ułożenie według numerów ewidencyjnych w pojemnikach oznaczonych jak teczki przedmiotowe, zawierających wykaz przechowywanych nośników, z zastosowaniem środków lub procedur zabezpieczających przed utratą możliwości zapisu danych.
11. Wykaz, o którym mowa w ust. 10, powinien zawierać numer ewidencyjny nośnika, numer ewidencyjny jego metryki oraz numer i stronę teczki przedmiotowej, do której metryka została wszyta.
12. Metryki elektronicznych nośników informacji kompletuje się w odrębnej teczce przedmiotowej, przeznaczonej wyłącznie do kompletowania tych urządzeń ewidencyjnych, teczce nadaje się numer odpowiadający numerowi pojemnika traktując ją jako kolejny tom tego samego urządzenia ewidencyjnego.
13. Segregatory, okładki teczek akt oraz pojemniki, o których mowa w ust. 9 i 10, w zależności od klauzuli przechowywanych w nich informacji powinny mieć następujące kolory:

1) „Ściśle tajne" - czerwony;
2) „Tajne" - niebieski;
3) „Poufne' - zielony;
4) „Zastrzeżone" - szary.

14. Dopuszcza się kompletowanie dokumentów niejawnych w segregatorach i pojemnikach innego koloru, pod warunkiem, że zostały one oznaczone w sposób wyraźny naklejkami odpowiadającymi kolorom, o których mowa w ust. 13.
15. Teczki akt oraz pojemniki z elektronicznymi nośnikami informacji, o których mowa w ust. 9 i 10, przechowuje się w kancelarii przez okres 5 lat, a po upływie tego czasu niszczy lub przekazuje do właściwego archiwum wojskowego.
16. Zasady archiwizowania i brakowania dokumentów reguluj ą odrębne przepisy.

§28.
1. Dokumenty, zawierające informacje niejawne, 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 kierownik kancelarii lub kancelista;
3) wykonawca i wykonawca techniczny.

2. Komisyjnemu niszczeniu podlegają:

1) dokumenty zawierające informacje niejawne stanowiące tajemnicę państwową;
2) wojskowe wydawnictwa specjalistyczne i dokumentacja techniczna;
3) teczki przedmiotowe kategorii „Bc", po upływie okresu ich przechowywania;
4) urządzenia ewidencyjne nie podlegające przekazaniu do archiwum;
5) elektroniczne nośniki informacji oznaczone klauzulą „Ściśle tajne" i „Tajne".

3. Niszczenie dokumentów zawierających informacje niejawne stanowiące tajemnicą służbową, nie wymienionych w ust. 2, oraz elektronicznych nośników informacji oznaczonych klauzulami „Zastrzeżone" i „Poufne", odbywa się w obecności osób, o których mowa w ust. 1 pkt 2 lub 3, a fakt zniszczenia dokumentuje się w rubryce „Uwagi" urządzenia ewidencyjnego adnotacją o treści: „Zniszczono dnia..", potwierdzoną czytelnymi podpisami osób niszczących dokumenty.

4. Komisyjne zniszczenie dokumentów potwierdza się w protokole zniszczenia, którego wzór określa załącznik nr 17 do zarządzenia.

5. Protokół zniszczenia stanowi dla kierownika kancelarii 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.., póz. nr .." oraz uwierzytelnienie wpisu podpisem i odciskiem pieczęci „Do pakietów".

6. Protokoły zniszczenia podlegają archiwizacji.

§29.
1. Dokumenty niejawne, o których mowa w § 28 ust. 2 i 3, wstępnie niszczy kierownik kancelarii przez kilkakrotne ich przedarcie, pod nadzorem członków komisji albo wykonawcy.
2. Dokumenty wstępnie zniszczone przechowuje się w zaplombowanych workach lub pojemnikach w kancelarii lub innym pomieszczeniu zabezpieczonym jak kancelaria.
3. Nie dokonuje się wstępnego niszczenia wojskowych wydawnictw specjalistycznych, dokumentacji technicznej, teczek akt i innych zbroszurowanych dokumentów, elektronicznych nośników danych oraz matryc metalowych, zawierających informacje niejawne, jeżeli byłoby to zbyt pracochłonne ze względu na ich liczbę, w szczególności w składnicach, drukarniach, bibliotekach, archiwach; do czasu ostatecznego zniszczenia należy je przechowywać w sposób określony w ust. 2.
4. Osoby, o których mowa w ust. 1, nadzorujące niszczenie dokumentów niejawnych, zapewniają zachowanie warunków uniemożliwiających wgląd do nich osobom nieupoważnionym.
5. Zabrania się wywożenia na wysypiska śmieci częściowo zniszczonych dokumentów niejawnych oraz kopert i innych opakowań, w których otrzymano dokumenty niejawne.

§30.
Dokument uważa się za ostatecznie zniszczony, jeżeli został pocięty na paski o wymiarach maksymalnych 1,5x25 mm lub zmielony na miał papierowy albo spalony w piecu, ewentualnie rozpuszczony w kadziach z ługiem w zakładach papierniczych pod nadzorem osób, o których mowa w § 29 ust. 1.

§31.
1. Sposoby i procedury niszczenia elektronicznych nośników informacji oraz informacji utrwalonych na tych nośnikach określają odrębne przepisy.
2. Zabrania się powtórnego wykorzystywania elektronicznych nośników informacji zakwalifikowanych i przeznaczonych do zniszczenia.

§32.
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 i archiwalnych oraz pieczęci i stempli;
2) zniszczenie dokumentów kategorii "Bc";
3) zwrot wydawnictw wojskowych, wojskowych map topograficznych oraz pieczęci i stempli do jednostki organizacyjnej, z której zostały przysłane;
4) przekazanie do właściwego archiwum pozostałych dokumentów po ich skompletowaniu i podszyciu do teczek przedmiotowych;
5) skompletowanie w jednej teczce przedmiotowej i przekazanie do właściwego archiwum wojskowego protokołów zniszczenia dokumentów niejawnych, wykazów dokumentów przekazanych do archiwum, protokołu z wynikami sprawdzenia stanu faktycznego dokumentów, o których mowa pkt 1, oraz protokołu likwidacyjnego jednostki organizacyjnej.

2. Kierownik kancelarii likwidowanej jednostki organizacyjnej może być przeniesiony na inne stanowisko służbowe dopiero po całkowitym rozliczeniu i przekazaniu wszystkich dokumentów zawierających informacje niejawne.

Rozdział 6
Organizacja pracy kancelarii tajnych, ich ochrona i obieg dokumentów podczas ćwiczeń, wojny oraz w czasie realizacji zadań w misjach organizacji międzynarodowych

§33.
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; wykaz powinien zawierać wyłącznie dokumenty niezbędne w działaniach bojowych lub do przeprowadzenia ćwiczenia.

§34.
Kierownik jednostki organizacyjnej zapewnia niezbędne środki transportu oraz ochronę do przewozu wyposażenia kancelarii i jej dokumentacji podczas ćwiczeń lub w warunkach bojowych.

§35.
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, spośród personelu kancelarii tajnej;
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. 5.

§36.
1. Kancelarię ćwiczebną rozmieszcza się:

1) jeżeli ćwiczenia odbywają się. w rejonie stałego zakwaterowania jednostki organizacyjnej - w osobnym pomieszczeniu, spełniającym warunki bezpieczeństwa określone w § 6 ust. 1 pkt 1 i 2 oraz ust. 7 pkt 1, 2 i 4, oddzielnie od pomieszczeń kancelarii tajnej;
2) jeżeli ćwiczenia odbywają się w warunkach polowych - w oddzielnych samochodach, budowlach, schronach lub kontenerach, rozmieszczonych w rejonie stanowiska dowodzenia, jak najbliżej „Centrum Dowodzenia", 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;

3) kancelaria powinna mieć zapewnioną całodobowa ochronę na czas ćwiczeń.

2. Zasady rozmieszczania i zabezpieczenia kancelarii, o których mowa w ust. 1, stosuje się odpowiednio dla kancelarii wojennych.

§37.
1. Kancelaria ćwiczebna rejestruje dokumenty ćwiczebne na zasadach określonych w rozdziale 5 w oddzielnie założonych w tym celu urządzeniach ewidencyjnych wymienionych w § 12 ust. 3 pkt 2 oraz ust. 4, z tym, że na dokumentach ćwiczebnych przed klauzulą tajności umieszcza się kryptonim ćwiczenia lub jeżeli ćwiczenie takiego kryptonimu nie posiada, wyraz „ĆWICZEBNE".
2. Urządzenia, o których mowa w ust. 1:

1) wykorzystuje się w kolejnych ćwiczeniach, aż do całkowitego wykorzystania wszystkich stron;
2) wypełnia się zapisami ewidencyjnymi od nowa dla każdego ćwiczenia, rozpoczynając zapis od liczby 1, po wpisaniu kryptonimu lub nazwy ćwiczenia;
3) niszczy się komisyjnie po upływie roku od wypełnienia ostatniej pozycji zapisu.

§38.
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) organizuje wszycie do odrębnych teczek dokumentów otrzymanych i wytworzonych w czasie ćwiczeń, stanowiących wartość szkoleniową lub archiwalną,
b) wydziela do zniszczenia dokumenty nie przedstawiające wartości szkoleniowej lub archiwalnej,
c) dokonuje adnotacji w urządzeniach ewidencyjnych kancelarii ćwiczebnej o wszyciu dokumentów do teczek lub ich zniszczeniu,
d) rozlicza się z dokumentów, urządzeń ewidencyjnych oraz pieczęci zabranych na ćwiczenia.

§39.
1. Przygotowanie kancelarii tajnej 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 szefów właściwych komórek organizacyjnych,
c) prowadzi ewidencję dokumentów i innych nośników zawierających informacje niejawne, wypożyczonych z kancelarii, a ujętych w wykazie, o którym mowa w § 33 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 funkcjonowanie kancelarii wojennej,
b) opieczętowuje urządzenia do przechowywania dokumentów, o których mowa w § 6 ust. 7 pkt 1 i pomieszczenia kancelarii oraz przekazuje służbie dyżurnej wykaz zabranych dokumentów niejawnych i urządzeń ewidencyjnych,
c) zapewnia rozwinięcie oraz przygotowanie kancelarii wojennej do pracy.

2. Przepisu ust. 1 pkt 2 nie stosuje się, jeżeli jednostka organizacyjna nie opuszcza miejsca stałego zakwaterowania.

3. Ilość 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.
§40.
1. Kancelaria wojenna jednostki organizacyjnej rejestruje dokumenty zawierające informacje niejawne na zasadach określonych w rozdziale 4, w urządzeniach ewidencyjnych wymienionych w § 12 ust. 3 pkt 1, 2 i 4 oraz ust. 4.
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 i utraconych przez jednostkę organizacyjną oraz ich obiegu;
2) odtworzenie stanu faktycznego dokumentów znajdujących się w jednostce organizacyjnej.

§41.
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.

§42.
1. Akta wytworzone i zdobyte w czasie działań bojowych kompletuje się na zasadach określonych w przepisach o postępowaniu z wojskowymi materiałami archiwalnymi.
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 oraz inne materiały zawierające informacje niejawne oznaczone klauzula „Ściśle tajne".

Rozdział 7
Postanowienia końcowe

§43.
1. Pomieszczenia kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych podlegają certyfikacji na zasadach określonych w odrębnych przepisach. 2. Ustalenia dotyczące kancelarii tajnej, określone w zarządzeniu, mają zastosowanie odpowiednio do filii kancelarii tajnej.
3. Do czasu wyposażenia jednostek organizacyjnych w urządzenia do przechowywania dokumentów spełniających wymagania techniczne, o których mowa w § 6 ust. 7 pkt 1, dopuszcza się przechowywanie dokumentów zawierających informacje niejawne stanowiące tajemnicę służbową w dotychczas użytkowanych sejfach i szafach stalowych, nie dłużej jednak niż **do dnia 31 grudnia 2008r**.
4. Zezwala się na wykorzystywanie, do chwili wyczerpania zapasów, druków (formularzy) urządzeń ewidencyjnych wprowadzonych zarządzeniem Nr 10/MON Ministra Obrony Narodowej z dnia 5 czerwca 2000r. w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Rozk. MON póz. 51), z wyłączeniem urządzeń, o których mowa w § 12 ust. 4 pkt 1, 6 i 7 niniejszego zarządzenia.

§44.
Traci moc zarządzenie Nr 10/MON Ministra Obrony Narodowej z dnia 5 czerwca 2000r. w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Rozk. MON, poz. 51).

§45.
Zarządzenie wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

MINISTER OBRONY NARODOWEJ
wz. Andrzej TOWPIK
Podsekretarz Stanu

Załącznik nr 1

KLASYFIKACJA I WYMAGANIA TECHNICZNE URZĄDZEŃ DO PRZECHOWYWANIA DOKUMENTÓW NIEJAWNYCH

I. SZAFA STALOWA KLASY A

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.
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 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.

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 A.
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 zanikami 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.

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) listą wszystkich zamków, które mogą być użyte zamiennie, z podaniem producenta i numeru modelu;
8) inne cechy charakteryzujące szafą.

11. Szafa powinna posiadać certyfikat wydany przez jednostką certyfikującą, potwierdzający zgodność wyrobu z wymaganiami klasy B.
12. Szafa powinna posiadać tabliczką, wydaną przez certyfikującą 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, rok produkcji, klasę wyrobu, numer certyfikatu;
4) masę.

III. SZAFA STALOWA KLASY C

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.

Załącznik nr 2

STRZEŻ TAJEMNICY PAŃSTWOWEJ I SŁUŻBOWEJ

SZAFA nr fabryczny .....

Odpowiedzialny: ..... nr pieczęci .....
..... nr pieczęci .....
..... nr pieczęci .....

PRZED OPUSZCZENIEM MIEJSCA PRACY SPRAWDŹ ZABEZPIECZENIE POWIERZONYCH CI DOKUMENTÓW

Załącznik Nr 3

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 */**

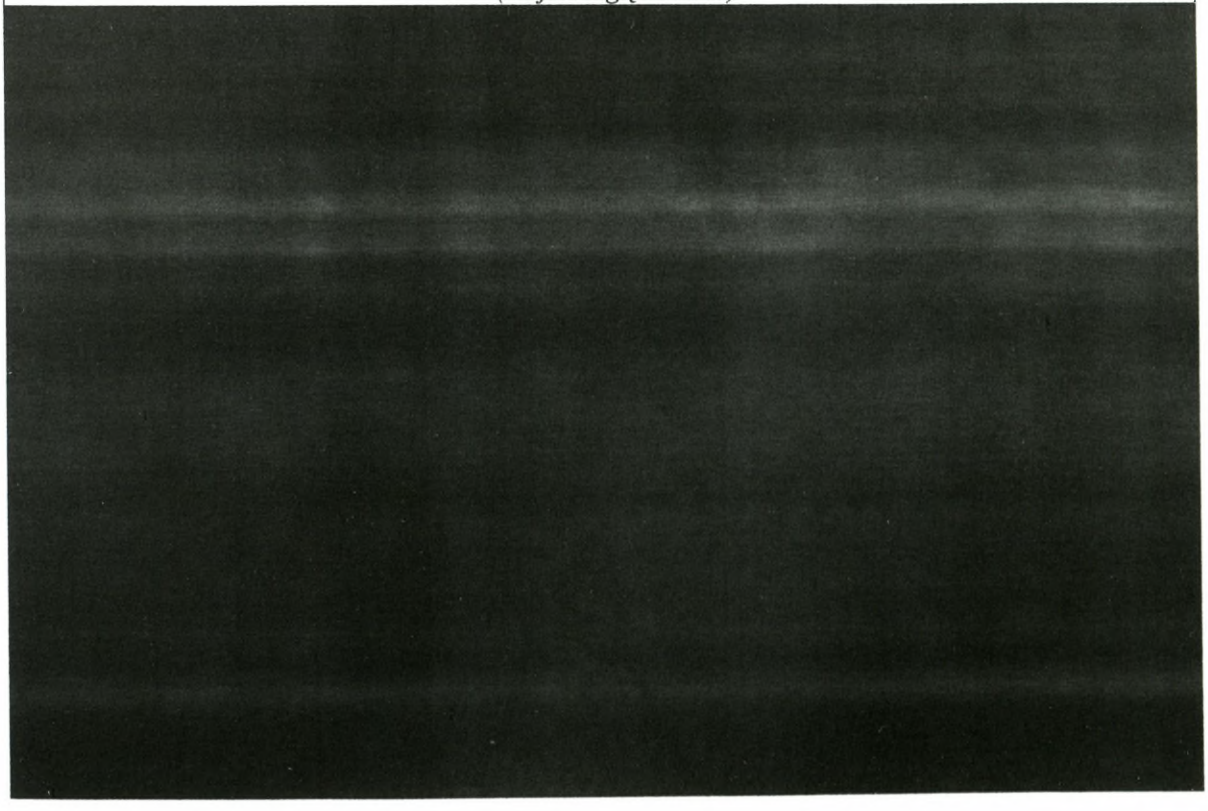
1. OBRÓT W LEWO ..... RAZY DO NUMERU.....
2. OBRÓT W PRAWO ..... RAZY DO NUMERU.....
3. OBRÓT W LEWO ..... RAZY DO NUMERU.....
4. OBRÓT W PRAWO ..... RAZY DO NUMERU.....
5. OBRÓT W LEWO ..... RAZY DO NUMERU.....

* JEŚLI KOMBINACJA ZACZYNA SIĘ. PRZEKRĘCANIEM POKRĘTŁA ZAMKA SZYFROWEGO W LEWO, ZACZYNAMY OPIS OD POZYCJI 1.

JEŚLI KOMBINACJA ZACZYNA SIĘ PRZEKRĘCANIEM POKRĘTŁA ZAMKA SZYFROWEGO WPRAWO, 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			
				Stron dok. wraz z załącznikami	Załącz-ników	Stron załączni-ków
1	2	3	4	5	6	7

Strona prawa

Numer wg dziennika ewidencji wykonanych dokumentów	Kto (wydział, stanowisko) wykonał dokument, komu przekazano, lub numer RWD	Pokwitowanie i data		Numer (symbol) akt, w których jest dokument przechowywany lub jego kopia	Uwagi
		Wykonawcy pobierającego dokument	pracownika kancelarii potwierdzającego zwrot dokumentu		
8	9	10	11	12	13

...Załącznik nr 6

KSIĄŻKA EWIDENCJI WYDAWNICTW, DOKUMENTACJI TECHNICZNEJ ORAZ MATERIAŁÓW FILMOWYCH

Strona lewa

....

Nr porządkowy Nazwa dokumentu

Lp.					
	Nr i data faktury (pisma)	S k ą d	Liczba egz.	Nr Nr egz.	Liczba załączników i ich stron

....

Nr porządkowy Nazwa dokumentu

Lp.	*Otrzymano*				
	Nr i data faktury (pisma)	S k ą d	Liczba egz.	Nr Nr egz.	Liczba załączników i ich stron

.....	.....	.....
Sygnatura	..Rok wydania	...Klauzula tajności

W y s ł a n o				Pozostało		Nr Nr teczki i stron podszytych faktur (pism)	Adnotacje o wysłaniu lub zniszczeniu dokumentu	Uwagi
Nr i data faktury (pisma)	D o k ą d	Liczba egz.	Nr Nr egz.	Liczba egz.	Nr Nr egz.			

.....	.....	.....
Sygnatura	Rok wydania	Klauzula tajności

W y s ł a n o				Pozostało		Nr Nr teczki i stron podszytych faktur (pism)	Adnotacje o wysłaniu lub zniszczeniu dokumentu	Uwagi
Nr i data faktury (pisma)	D o k ą d	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 wojsk.	Imię i nazwisko	Nazwa komórki organizacyjnej	Klauzula upoważnienia, /nr poświadczenia bezpieczeństwa/	Termin ważności upoważnienia /poświadczenia bezpieczeństwa/	Uwagi
1	2	3	4	5	6	7

Załącznik Nr 8

REJESTR WYDANYCH DOKUMENTÓW Nr .....

.....	.....	.....
stopień wojskowy	imię i nazwisko lub nazwa dokumentu	nazwa jednostki lub komórki organizacyjnej

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
243			

Strona prawa

Data zakończenia	Adnotacje o zniszczeniu	Uwagi

Załącznik Nr 10

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

Załącznik nr 11

KSIĄŻKA DORĘCZEŃ

Lp.	Data przyjęcia przesyłki (dzień miesiąc, godzina	Numer ewidencyjny dokumentu	Adresat	Potwierdzenie odbioru dokumentu	
				Stopień wojskowy, imię nazwisko	Pieczęć data i podpis
1	2	3	4	5	6

Załącznik nr 12

METRYKA ELEKTRONICZNEGO NOŚNIKA INFORMACJI

.....

(rodzaj i numer ewidencyjny nośnika)

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

Załącznik nr 13

ZATWIERDZAM

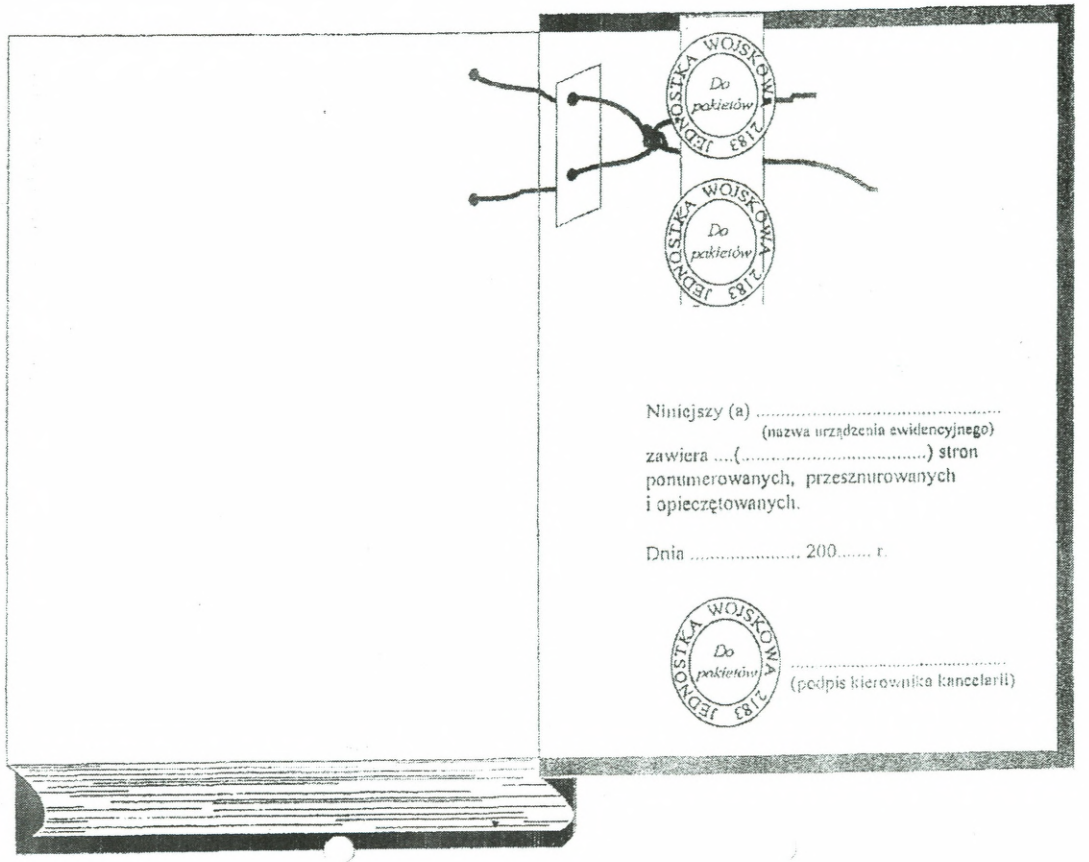
(stanowisko, stopień imię i nazwisko osoby zatwierdzającej)

„.....„ ..... 200 ..... r.

ROZDZIELNIK STAŁY NR .....

Lp.	Nazwa jednostki lub komórki organizacyjnej	Adres	Nr przesłanych egzemplarzy	Uwagi

WZÓR PRZESZYCIA, OPISANIA I OPIECZĘTOWANIA ZBROSZUROWANEGO URZĄDZENIA EWIDENCYJNEGO, ZESZYTU BRUDNOPISU, NOTATNIKA ITP.



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.	

2) dokumentów krajowych:

1	2	3	4
1.	 *..... 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 ..... (data) Zał. ..... Ark.	Pieczęć wpływu pism - prostokątna o długości 54 mm i szerokości 27 mm., wypukła do tuszu.	
3.		Pieczęć do pakietów o średnicy 30 mm wypukła 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 numer - dwie pieczęcie jeżeli jednostka posiada pełną nazwę i numer jednostki.
5.	ZASTRZEŻONE	Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości	
6.	POUFNE	Pieczęć informacyjna wypukła do tuszu o różnych wymiarach długości	
7.	TAJNE	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.	**POUFNE** RWD Nr	Pieczęć **formularzowa** wypukła do tuszu o długości 28 mm i szerokości 26 mm.	
14.	**TAJNE** 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 opieczętowanych. Dn. "....." 20..... r.** ..... **(kierownik kancelarii)**	Pieczęć formularzowa wypukła do tuszu o długości 70 mm i szerokości 26 mm.	
17.	Zał. Nr ..... Wchodz. Do pisma Nr ..... Wychodz.	**Pieczęć formularzowa wypukła do tuszu o długości 62 mm i szerokości 20 mm.**	

Załącznik nr 16

DZIENNIK WYKONAWCY

Lp.	Numery dokumentów			Ilość stron dokumentu	Skąd wpłynął lub dokąd wysłano dokument	Czego dokument dotyczy lub jego nazwa	Komu przekazano dokument		Nr teczki w której znajduje się pismo	Uwagi
	Wchodzący	Wychodzący	Według dziennika ewidencji wykonanych dokumentów				Stopień wojskowy imię i nazwisko	Data i podpis		
1	2	3	4	5	6	7	8	9	10	11

Załącznik nr 17

WZÓR

ZEZWALAM
na zniszczenie dokumentów
wyszczególnionych w protokole

.....
(stanowisko, stopień wojskowy, imię, nazwisko)

PROTOKÓŁ ZNISZCZENIA DOKUMENTÓW

Zgodnie z rozkazem dziennym 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	UWAGI
1	2	3	4	5	6	7	8

Dokumenty wymienione pod pozycją..... po zatwierdzeniu zostały zniszczone w dniu ..... r. przez .....
(pocięcie, spalenie, przemiał itp.)

- 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 Wojskowych Służb Informacyjnych 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 nadsyła n ej;

   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.	nalizy 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 i 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 i 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 z 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.	B50	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.	eldunki o wypadkach związanych z dyslokacją i obsługą sprzętu wojskowego	BE 15	Bc	
	4.	eldunki 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 roczne.	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 potrąceń.	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 wojskowych.	A	Bc	
	2.	Zbiorcze zestawienia, analizy i oceny wykorzystania obiektów koszarowych i zasobów mieszkaniowych wojska.	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 architektonicznych.	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)

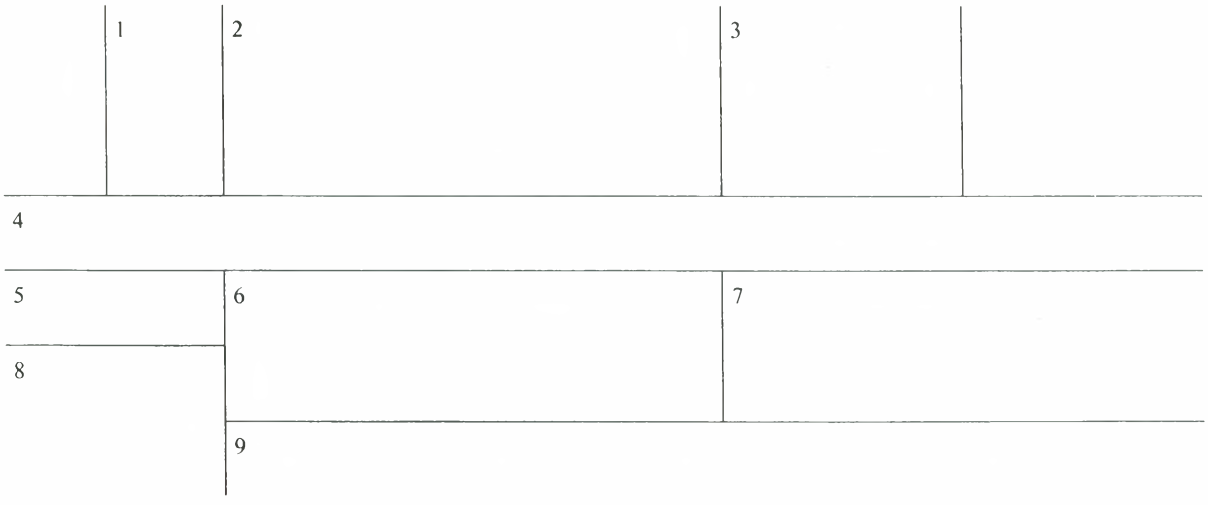
KATEGORIA .....

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

277

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. .....

.....

.....

.....

.....

Stwierdza się, że dokumentacja niearchiwalna wymieniona w spisie akt nr ..... / ..... została w naszej obecności zniszczona przez .....

(sposób zniszczenia)

w dniu ..... w .....

(nazwa instytucji niszczącej)

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

Art. 265.
§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje stanowiące tajemnicę państwową,
podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca
podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 266.
§ 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację stanowiącą tajemnicę służbową lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes,
podlega karze pozbawienia wolności do lat 3.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Art. 267.
§ 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268.
§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 269.
§ 1. Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji,
podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.

1)

Dz.U.02.171.1396
Dz.U.02.241.2074
Dz.U.04.202.2065
Dz.U.05.10.69

USTAWA

z dnia 14 lipca 1983 r.

o narodowym zasobie archiwalnym i archiwach

(tekst jednolity)

2)

U S T A W A

z dnia 29 sierpnia 1997 r.

o ochronie danych osobowych

(Dz.U.2002.101.926 - tekst jednolity)

3)

Dz.U.97.114.740

USTAWA

z dnia 22 sierpnia 1997 r.

o ochronie osób i mienia

(Dz. U. z dnia 26 września 1997 r.)

4)

Dz.U.99.53.549
Dz.U.03.52.451
Dz.U.03.199.1939
Dz.U.04.52.525

USTAWA

z dnia 21 maja 1999r.

o broni i amunicji

(Dz. U. z dnia 19 czerwca 1999r.)
(tekst jednolity)

5)

Dz.U.01.128.1402

USTAWA

z dnia 27 lipca 2001 r.

o ochronie baz danych

(Dz. U. z dnia 9 listopada 2001 r.)

6)

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.)

7)

Dz.U.03.139.1326
Dz.U.04.171.1800

USTAWA

z dnia 9 lipca 2003 r.

o Wojskowych Służbach Informacyjnych

(Dz. U. z dnia 8 sierpnia 2003 r.)

8)

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.)

9)

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.)

10)

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.)

11)

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.)

12)

Dz.U.99.18.160

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. z dnia 5 marca 1999 r.)

13)

Dz.U.99.18.161

ROZPORZĄDZENIE

PREZESA RADY MINISTRÓW

z dnia 25 lutego 1999r.

w sprawie sposobu i trybu udostępniania danych z ewidencji

(Dz. U. z dnia 5 marca 1999r.)

14)

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.)

15)

M.P.03.44.656

ZARZĄDZENIE Nr 79
PREZESA RADY MINISTRÓW

z dnia 12 września 2003 r.

w sprawie zasad, zakresu i trybu współdziałania oraz szczegółowego rozdziału kompetencji pomiędzy Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu i Wojskowe Służby Informacyjne

(M.P. z dnia 19 września 2003 r.)

16)

Dz.U.99.60.647
Dz.U.02.176.1446

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.)
(Dz. U. z dnia 23 października 2002 r.)
tekst ujednolicony

17)

Dz.U.99.58.619

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.)

18)

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

19)

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.)

20)

Dz.U.02.176.1446

ROZPORZĄDZENIE

MINISTRA OBRONY NARODOWEJ

z dnia 10 października 2002 r.

zmieniające rozporządzenie w sprawie ochrony przez specjalistyczne uzbrojone formacje ochronne terenów komórek i jednostek organizacyjnych resortu obrony narodowej

(Dz. U. z dnia 23 października 2002 r.)

21)

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"

22)

DECYZJA Nr 58/MON

MINISTRA OBRONY NARODOWEJ

z dnia 1 marca 2004 r.

w sprawie działalności Wojskowej Służby Kurierskiej Sił Zbrojnych Rzeczypospolitej Polskiej

23)

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

24)

Dz.U.98.80.521
Dz.U.01.121.1306

ROZPORZĄDZENIE

MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 3 czerwca 1998 r.

w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

(Dz. U. z dnia 30 czerwca 1998 r.)

25)

Dz.U.98.80.521
Dz.U.01.121.1306

ROZPORZĄDZENIE

MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 3 czerwca 1998 r.

w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

(Dz. U. z dnia 30 czerwca 1998 r.)

26)

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.)

27)

Dz.U.99.18.166

ROZPORZĄDZENIE

MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 23 lutego 1999 r.

w sprawie wzoru zaświadczenia stwierdzającego odbycie przeszkolenia w zakresie ochrony informacji niejawnych

(Dz. U. z dnia 5 marca 1999 r.)

28)

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.)

29)

Dz.U.04.193.1974

UMOWA

podpisana w Warszawie dnia 4 września 2001 r.

między Rządem Rzeczypospolitej Polskiej a Gabinetem Ministrów Ukrainy w sprawie wzajemnej ochrony informacji niejawnych

(Dz. U. z dnia 3 września 2004 r.)

30)

Dz.U.04.117.1214

UMOWA

podpisana w Starej Lubowni dnia 29 lipca 2002 r.

między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Słowackiej o wzajemnej ochronie informacji niejawnych

(Dz. U. z dnia 25 maja 2004 r.)

31)

Dz.U.04.221.2242

UMOWA

między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Łotewskiej o wzajemnej ochronie informacji niejawnych

podpisana w Warszawie dnia 26 lutego 2003 r.

(Dz. U. z dnia 12 października 2004 r.)

32)

W ZAKRESIE TELEINFORMATYKI

1. BTPO-701A

2. DBBT-301B

3. DBBT-801A

4. DBBT-802A

Druk AON zam. nr 734/WW

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 58198
II
Akademii Obrony Narodowej