Biuro Ochrony Informacji Niejawnych

20

DECYZJA Nr 25/MON MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach i komórkach organizacyjnych resortu obrony narodowej

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. z 1996 r. Nr 94, poz. 426), w związku z art. 14 ust. 1 pkt 1 i 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631), w celu zapewnienia szczególnej ochrony informacjom niejawnym pochodzącym z wymiany zagranicznej oraz materiałom i narzędziom kryptograficznym, stanowiącym tajemnicę państwową i służbową, przed ich nieuprawnionym ujawnieniem, ustala się, co następuje:

1. Ilekroć w decyzji jest mowa o:
1) pomieszczeniu wydzielonym — należy przez to rozumieć pomieszczenie, w którym:
   a) zainstalowano serwery sieciowe, terminale sieci teleinformatycznych, autonomiczne stanowiska komputerowe, a także ich elementy aktywne lub pasywne, w szczególności routery, switche, modemy, panele światłowodowe, służące do ochrony informacji niejawnych wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w komórce organizacyjnej Ministerstwa Obrony Narodowej i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, z wykorzystaniem materiałów i narzędzi kryptograficznych,
   b) prowadzi się projektowanie, produkcję, montaż, naprawę lub serwisowanie urządzeń ochrony kryptograficznej lub innych wyrobów o przeznaczeniu specjalnym służących do ochrony informacji niejawnych, wchodzące w skład zespołu pomieszczeń kancelarii kryptograficznej;
2) certyfikacie bezpieczeństwa dla pomieszczenia — należy przez to rozumieć formalny dokument, potwierdzający zdolność personelu i pomieszczenia lub zespołu pomieszczeń do zapewnienia wymaganej ochrony informacjom niejawnym pochodzącym z wymiany zagranicznej oraz materiałom i narzędziom kryptograficznym, stanowiącym tajemnicę państwową i służbową, wytwarzanym, przechowywanym, przetwarzanym lub przekazywanym w tych pomieszczeniach, przed ich nieuprawnionym ujawnieniem.

2. Szef Wojskowych Służb Informacyjnych powoła, ze składu osobowego podległych komórek i jednostek organizacyjnych, Stałą Komisję do Certyfikacji i Kontroli, zwaną dalej „Komisją".

3. W skład Komisji wchodzi:
1) przewodniczący;
2) sekretarz;
3) członkowie (audytorzy wiodący, audytorzy techniczni).

4. Komisja przeprowadza audyty certyfikacyjne, recertyfikacyjne oraz kontrole okresowe:
1) kancelarii zagranicznych;
2) punktów obsługi dokumentów zagranicznych, tworzonych na bazie kancelarii tajnych;
3) kancelarii kryptograficznych;
4) stacji łączności kryptograficznej;
5) kabin kryptograficznych;
6) pomieszczeń wydzielonych, organizowanych lub funkcjonujących w komórkach organizacyjnych Ministerstwa Obrony Narodowej i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, innych jednostkach organizacyjnych realizujących produkcję lub usługi, stanowiące tajemnicę państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa i potrzeby Sił Zbrojnych Rzeczypospolitej Polskiej, zwanych dalej „Siłami Zbrojnymi" a także przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa, jeśli uczestnikami tego obrotu są jednostki organizacyjne Sił Zbrojnych lub inne jednostki podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.

5. Komisja przeprowadza audyty certyfikacyjne, recertyfikacyjne oraz kontrole okresowe pomieszczeń, o których mowa w pkt 4, na podstawie pisemnego upoważnienia, wydanego przez Szefa Wojskowych

Służb Informacyjnych. Wzór upoważnienia określa załącznik Nr 1 do decyzji.

6. Nadzór nad pracami Komisji, z upoważnienia i w imieniu Szefa Wojskowych Służb Informacyjnych, sprawuje Szef Zarządu Ochrony Informacji Niejawnych Inspektoratu Wojskowych Służb Informacyjnych.

7. Szef Wojskowych Służb Informacyjnych:
1) decyduje o przeprowadzeniu audytu certyfikacyjnego lub recertyfikacyjnego pomieszczeń, o których mowa w pkt 4, na podstawie wniosków w sprawie przeprowadzenia audytu certyfikacyjnego lub recertyfikacyjnego, złożonych przez właściwych kierowników komórek lub jednostek organizacyjnych;
2) wydaje certyfikaty bezpieczeństwa dla pomieszczeń, o których mowa w pkt 4, których wzór określa załącznik Nr 2 do decyzji;
3) określi sposoby prowadzenia ewidencji i przechowywania certyfikatów bezpieczeństwa pomieszczeń, o których mowa w pkt 4;
4) wyda i wprowadzi do użytku służbowego, w resorcie obrony narodowej, wytyczne w zakresie stosowania środków bezpieczeństwa fizycznego i zasad organizacji pomieszczeń, wymienionych w pkt 4 ppkt 3-6.

8. Do podstawowych zadań i obowiązków Komisji należy:
1) sprawdzanie, w trakcie prowadzonego audytu certyfikacyjnego lub recertyfikacyjnego stanu zabezpieczeń pomieszczeń, o których mowa w pkt 4, w zakresie spełniania wymagań bezpieczeństwa osobowego, fizycznego, technicznego oraz zastosowanych procedur organizacyjnych i prawnych;
2) sporządzanie raportów z wykonanych szczegółowych czynności sprawdzających w ramach prowadzonych audytów certyfikacyjnych lub recertyfikacyjnych;
3) występowanie z wnioskami do Szefa Wojskowych Służb Informacyjnych o wydanie certyfikatów bezpieczeństwa dla pomieszczeń, o których mowa w pkt 4, które zostały sprawdzone, a stan ich zabezpieczeń został zweryfikowany z obowiązującymi wymaganiami i pozytywnie oceniony przez Komisję, w trakcie prowadzonego audytu certyfikacyjnego lub recertyfikacyjnego;
4) formułowanie zaleceń (dotyczy tylko przypadków negatywnej oceny pomieszczenia lub pomieszczeń, o których mowa w pkt 4) przedkładanych do realizacji właściwemu kierownikowi komórki lub jednostki organizacyjnej;
5) prowadzenie kontroli okresowych certyfikowanych pomieszczeń, o których mowa w pkt 4, w zakresie spełniania wymagań dla pomieszczeń certyfikowanych, zgodnie z planem kontroli, zatwierdzonym przez Szefa Wojskowych Służb Informacyjnych.

9. Terminy ważności dokumentów z przeprowadzonego audytu certyfikacyjnego lub recertyfikacyjnego pomieszczeń , o których mowa w pkt 4:
1) raporty z przeprowadzonych audytów — zachowują ważność na czas ważności certyfikatów bezpieczeństwa pomieszczeń wydanych na ich podstawie;
2) certyfikaty bezpieczeństwa:
   a) 5 lat — dla pomieszczeń, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową o klauzuli ŚCIŚLE TAJNE,
   b) 7 lat — dla pomieszczeń, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową o klauzuli TAJNE,
   c) 10 lat — dla pomieszczeń, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę służbową o klauzuli POUFNE.

10. Dokumenty z przeprowadzonego audytu certyfikacyjnego lub recertyfikacyjnego, wykonane przez Komisję, przechowuje:
1) raporty z przeprowadzonych audytów — Stała Komisja do Certyfikacji i Kontroli Wojskowych Służb Informacyjnych;
2) certyfikaty bezpieczeństwa kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych:
   a) egz. nr 1 — Stała Komisja do Certyfikacji i Kontroli Wojskowych Służb Informacyjnych,
   b) egz. nr 2 — Główna Kancelaria Zagraniczna Ministerstwa Obrony Narodowej,
   c) egz. nr 3 — kancelaria zagraniczna lub punkt obsługi dokumentów zagranicznych, której dotyczył audyt certyfikacyjny lub recertyfikacyjny;
3) certyfikaty bezpieczeństwa kancelarii kryptograficznych i kabin kryptograficznych:
   a) egz. nr 1 — Stała Komisja do Certyfikacji i Kontroli Wojskowych Służb Informacyjnych,
   b) egz. nr 2 — Główna Kancelaria Kryptograficzna Centrum Bezpieczeństwa Teleinformacyjnego,
   c) egz. nr 3 — kancelaria kryptograficzna lub kabina kryptograficzna, których dotyczył audyt certyfikacyjny lub recertyfikacyjny;
4) certyfikaty bezpieczeństwa stacji łączności kryptograficznej oraz pomieszczeń wydzielonych:
   a) egz. nr 1 — Stała Komisja do Certyfikacji i Kontroli Wojskowych Służb Informacyjnych,
   b) egz. nr 2 — Centrum Bezpieczeństwa Teleinformacyjnego,
   c) egz. nr 3 — stacja łączności kryptograficznej lub pomieszczenie wydzielone, których dotyczył audyt certyfikacyjny lub recertyfikacyjny.

11. Dysponenci środków budżetowych, każdy w swoim zakresie, wydzielają środki finansowe na

utworzenie pomieszczeń, o których mowa w pkt 4, ich zabezpieczenie i wyposażenie, w podległych sobie jednostkach i komórkach organizacyjnych.

12. Dyrektor Departamentu Administracyjnego, w porozumieniu z Dyrektorem Generalnym Ministerstwa Obrony Narodowej, zapewni wyposażenie w niezbędny sprzęt biurowy, kwaterunkowy i informatyczny oraz środki łączności tworzonych w komórkach organizacyjnych Ministerstwa Obrony Narodowej pomieszczeń, o których mowa w pkt 4.

13. Dyrektor Biura Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej zapewni:

1) prowadzenie w Głównej Kancelarii Zagranicznej Ministerstwa Obrony Narodowej szczegółowej ewidencji kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych tworzonych i certyfikowanych w:
   a) komórkach organizacyjnych Ministerstwa Obrony Narodowej,
   b) jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych,
   c) innych jednostkach organizacyjnych realizujących produkcję lub usługi, stanowiące tajemnicę państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa i potrzeby Sił Zbrojnych, a także przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową lub służbową o klauzuli POUFNE ze względu na obronność państwa, jeśli uczestnikami tego obrotu są Siły Zbrojne lub inne jednostki organizacyjne podległe Ministrowi Obrony Narodowej;
2) przechowywanie w Głównej Kancelarii Zagranicznej Ministerstwa Obrony Narodowej certyfikatów bezpieczeństwa, o których mowa w pkt 4 ppkt 1 i 2.

14. Kierownicy jednostek i komórek organizacyjnych resortu obrony narodowej, w których utworzono pomieszczenia, o których mowa w pkt 4 ppkt 1 i 2:

1) występują do Szefa Wojskowych Służb Informacyjnych z pisemnymi wnioskami o przeprowadzenie:
   a) audytu certyfikacyjnego — w przypadkach nowo utworzonych kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych lub kancelarii tajnych, które mają pełnić funkcje punktów obsługi dokumentów zagranicznych (przed ich uruchomieniem),
   b) audytu recertyfikacyjnego — w przypadkach wprowadzania w funkcjonujących kancelariach zagranicznych lub punktach obsługi dokumentów zagranicznych posiadających certyfikaty bezpieczeństwa, jakichkolwiek zmian w ich organizacji, funkcjonowaniu, zabezpieczeniu i wyposażeniu oraz na sześć miesięcy przed wygaśnięciem terminu obowiązywania certyfikatu bezpieczeństwa;
2) ogłaszają w rozkazie wewnętrznym fakt uruchomienia w jednostce lub komórce organizacyjnej resortu obrony narodowej, na podstawie certyfikatu bezpieczeństwa otrzymanego z Wojskowych Służb Informacyjnych, kancelarii zagranicznej lub punktu obsługi dokumentów zagranicznych;
3) obejmują kancelarię zagraniczną lub punkt obsługi dokumentów zagranicznych kontrolą i stałym nadzorem służbowym, realizowanym przez podległy kierownikowi jednostki lub komórki organizacyjnej pion ochrony informacji niejawnych;
4) zapewniają im warunki funkcjonowania, zgodnie z przepisami o ochronie informacji niejawnych;
5) informują Szefa Wojskowych Służb Informacyjnych o przypadkach naruszenia przepisów o ochronie informacji niejawnych;
6) informują Dyrektora Biura Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej o uruchomieniu w jednostce lub komórce organizacyjnej resortu obrony narodowej kancelarii zagranicznej lub punktu obsługi dokumentów zagranicznych oraz o ich likwidacji — dla celów, określonych w pkt 13.

15. Kierownicy jednostek i komórek organizacyjnych resortu obrony narodowej, w których utworzono pomieszczenia, określone w pkt 4 ppkt 3-6, występują do Szefa Wojskowych Służb Informacyjnych z pisemnymi wnioskami o przeprowadzenie:

1) audytu certyfikacyjnego — w przypadkach nowo utworzonych specjalistycznych komórek lub pomieszczeń (przed ich uruchomieniem);
2) audytu recertyfikacyjnego — w przypadkach wprowadzania w funkcjonujących pomieszczeniach posiadających certyfikaty bezpieczeństwa, jakichkolwiek zmian w ich organizacji, funkcjonowaniu, zabezpieczeniu i wyposażeniu oraz na sześć miesięcy przed wygaśnięciem terminu obowiązywania certyfikatu bezpieczeństwa.

16. Kierownicy jednostek i komórek organizacyjnych resortu obrony narodowej, jako zleceniodawcy, określają przedsiębiorcom, jednostkom naukowym lub badawczo-rozwojowym w „Instrukcji bezpieczeństwa przemysłowego", warunki do spełnienia wymagane niniejszą decyzją, w przypadkach realizacji umów na rzecz resortu obrony narodowej, związanych z dostępem do informacji niejawnych, pochodzących z wymiany zagranicznej lub materiałów i narzędzi kryptograficznych.

17. Pomieszczenia, o których mowa w pkt 4, którym kończy się okres ważności wydanego certyfikatu bezpieczeństwa, należy zgłaszać do audytu recertyfikacyjnego, nie później niż sześć miesięcy przed wygaśnięciem ważności certyfikatu bezpieczeństwa.

18. Traci moc decyzja Nr 29/MON Ministra Obrony Narodowej z dnia 22 lutego 2001 r. w sprawie trybu certyfikacji i kontroli kancelarii zagranicznych, kancelarii środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji łączności kryptograficznej oraz pomieszczeń wydzielonych (terminali) teleinformatycznych w jednostkach organizacyjnych resortu Obrony Narodowej (Dz. Urz. MON Nr 3, poz. 32).

19. Decyzja wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Minister Obrony Narodowej: *R. Sikorski*

Załączniki do decyzji Nr 25/MON
Ministra Obrony Narodowej
z dnia 31 stycznia 2006 r. (poz. 20)

Załącznik Nr 1

Warszawa, ...

SZEF

WOJSKOWYCH SŁUŻB INFORMACYJNYCH
00-909 Warszawa 60, tel. 6 841 664

UPOWAŻNIENIE NR ..... / ..... /SKCiK

Na podstawie pkt 5 decyzji Nr ..... /MON Ministra Obrony Narodowej z dnia ..... 2006 roku w sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach organizacyjnych resortu obrony narodowej, upoważniam:

Pana

.....

(stopień, imię i nazwisko)

do przeprowadzenia sprawdzenia pomieszczenia / zespołu pomieszczeń * .... w ramach audytu certyfikacyjnego / recertyfikacyjnego / kontroli okresowej*, zgłoszonego(ych)* do audytu certyfikacyjnego / recertyfikacyjnego * przez ..... pismem nr ..... z dnia ....., znajdującego(ych)* się w:

.....

(nazwa i adres instytucji, jednostki wojskowej)

Upoważnienie niniejsze ważne jest za okazaniem legitymacji służbowej.

Ważność upoważnienia upływa z dniem .....

(pieczęć urzędowa)

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

Ważność upoważnienia przedłuża się do dnia .....

(pieczęć urzędowa)

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

* - w oryginale wybrać odpowiednią formę

Załącznik Nr 2

CERTYFIKAT BEZPIECZEŃSTWA

dla pomieszczenia / zespołu pomieszczeń *

.....

w .....
(nazwa jednostki wojskowej, jednostki, komórki organizacyjnej)

/ ..... /
(dokładny adres)

Zaświadcza się, że Stała Komisja do Certyfikacji i Kontroli, działając na podstawie pkt 2 decyzji Nr...../MON Ministra Obrony Narodowej z dnia ..... 2006 roku w sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach i komórkach organizacyjnych resortu obrony narodowej, w dniu ..... roku przeprowadziła audyt certyfikacyjny pomieszczenia / zespołu pomieszczeń * .....
w .....

Komisja stwierdziła, że skontrolowane(y)* pomieszczenie / zespół pomieszczeń * jest zorganizowane(y)* w sposób zapewniający wymagany poziom bezpieczeństwa i ochrony informacji niejawnych, do klauzuli ..... włącznie.

W związku z powyższym potwierdzam, że wymienione(y)* pomieszczenie / zespół pomieszczeń * zapewnia wymagany poziom bezpieczeństwa i ochrony informacji niejawnych, do klauzuli ..... włącznie.

Certyfikat ważny jest do: ..... roku.

SZEF
WOJSKOWYCH SŁUŻB INFORMACYJNCYH

m.p.

(podpis)

.....
(stopień, imię i nazwisko)

WARSZAWA, dnia .....

WSI/SKCiK – nr kolejny / typ pomieszczenia / rok kalendarzowy (nr egzemplarza)

* - w oryginale wybrać odpowiednią formę