Biuro Ochrony Informacji Niejawnych

19

DECYZJA Nr 24/MON MINISTRA OBRONY NARODOWEJ

z dnia 31 stycznia 2006 r.

w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej

Na podstawie § 2 pkt 6 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. z 1996 r., Nr 94, poz. 426), w celu poddania szczególnej ochronie systemów i sieci teleinformatycznych, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, ustala się, co następuje:

1. Użyte w decyzji określenia oznaczają:
1) ustawa — ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631);
2) jednostka organizacyjna:
   a) Ministerstwo Obrony Narodowej jako urząd Ministra Obrony Narodowej,
   b) jednostkę nie wchodzącą w skład ministerstwa, podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną,
   c) przedsiębiorcę, jednostkę naukową lub badawczo-rozwojową, zamierzających ubiegać się o zawarcie lub wykonujących umowę związaną z dostępem do informacji niejawnych, albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych;
3) komórka organizacyjna — Sekretariat Ministra Obrony Narodowej, departament, generalny zarząd, samodzielny zarząd, szefostwo, biuro;
4) kierownik jednostki (komórki) organizacyjnej — dowódcę, dyrektora, szefa, komendanta, prezesa;
5) pełnomocnik ochrony — pełnomocnika do spraw ochrony informacji niejawnych;
6) system lub sieć teleinformatyczna— system lub sieć teleinformatyczną (w rozumieniu ustawy) przeznaczoną do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych;
7) bezpieczeństwo teleinformatyczne — całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych oraz ochrony informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w tych systemach i sieciach przed przypadkowym lub celowym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania poprzez zastosowanie w sposób kompleksowy technicznych, programowych, kryptograficznych oraz organizacyjnych środków i metod;
8) dokumentacja bezpieczeństwa teleinformatycznego — szczególne wymagania bezpieczeństwa i procedury bezpiecznej eksploatacji systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie;
9) wyroby o przeznaczeniu specjalnym, służące do ochrony informacji niejawnych — wszelkie wyroby zaprojektowane i wykonane do ochrony informacji niejawnych oraz technologie związane z produkcją lub używaniem tych wyrobów, w szczególności:
   a) urządzenia i narzędzia kryptograficzne,
   b) pomocniczy sprzęt kryptograficzny, nie będący urządzeniem kryptograficznym, wykorzystywany do zabezpieczenia funkcjonowania systemu kryptograficznego, który wymaga specjalnej obsługi lub kontroli, w celu ochrony specjalnych elementów i układów kontrolnych,
   c) urządzenia w wykonaniu specjalnym, przeznaczone do zobrazowania, wytwarzania, przetwarzania, przechowywania i przekazywania informacji niejawnych,
   d) urządzenia ochrony elektromagnetycznej, w tym kabiny ekranujące, indywidualne osłony ekranujące, urządzenia do maskowania emisji ujawniającej,
   e) aparatownie łączności i informatyki, mobilne kancelarie kryptograficzne, zautomatyzowane wozy dowodzenia.

2. Zadania w zakresie ochrony systemów i sieci teleinformatycznych realizują:
1) w jednostce (komórce) organizacyjnej:
   a) kierownik jednostki (komórki) organizacyjnej,
   b) pełnomocnik ochrony,
   c) administrator systemu,
   d) inspektor bezpieczeństwa teleinformatycznego;
2) Centrum Bezpieczeństwa Teleinformacyjnego;
3) Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki;
4) organy bezpieczeństwa systemów łączności i informatyki jednostek organizacyjnych wszystkich szczebli dowodzenia;

5) Centrum Zarządzania Systemami Teleinformatycznymi;
6) Wojskowe Służby Informacyjne.

3. Kierownik komórki organizacyjnej odpowiada za organizację, eksploatację i bezpieczeństwo systemów i sieci teleinformatycznych, funkcjonujących w komórce organizacyjnej, w szczególności za:
1) wyznaczenie administratorów systemów lub sieci teleinformatycznych;
2) opracowanie i przekazanie do Wojskowych Służb Informacyjnych dokumentacji bezpieczeństwa teleinformatycznego, uzgodnionej w trybie określonym w pkt 5-7;
3) informowanie Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych o stanie realizacji prac związanych z opracowywaniem dokumentacji bezpieczeństwa teleinformatycznego oraz jej przygotowaniem do wdrożenia;
4) przekazanie Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych informacji o potrzebach w zakresie wyposażenia w sprzęt informatyczny i urządzenia, w tym wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, o których mowa w pkt 1 ppkt 9 lit. c i d;
5) występowanie do Wojskowych Służb Informacyjnych poprzez Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, z wnioskami o:
   a) dokonanie pomiarów i określenie Poziomu Zabezpieczenia Miejsca oraz Poziomu Zabezpieczenia Urządzenia,
   b) przeprowadzenie akredytacji bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych,
   c) przeprowadzenie certyfikacji lub ponownej certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, wymienionych w pkt 1 ppkt 9 lit. c i d,
   d) przeprowadzenie certyfikacji pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnych.

4. Kierownik jednostki organizacyjnej odpowiada za organizację, eksploatację i bezpieczeństwo systemów i sieci teleinformatycznych, funkcjonujących w jednostce organizacyjnej, w szczególności za:
1) wyznaczenie osób funkcyjnych, zgodnie z art. 64 ustawy;
2) opracowanie i przekazanie do Wojskowych Służb Informacyjnych dokumentacji bezpieczeństwa teleinformatycznego, uzgodnionej w trybie, o którym mowa w pkt 5-7;
3) określenie warunków i sposobu przydzielenia uprawnień użytkownikom systemów lub sieci teleinformatycznych;
4) występowanie do Wojskowych Służb Informacyjnych z wnioskami o:
   a) dokonanie pomiarów i określenie Poziomu Zabezpieczenia Miejsca oraz Poziomu Zabezpieczenia Urządzenia,
   b) przeprowadzenie akredytacji bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych,
   c) przeprowadzenie certyfikacji lub ponownej certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, o których mowa w pkt 1 ppkt 9 lit. c i d,
   d) przeprowadzenie certyfikacji lub ponownej certyfikacji: kancelarii kryptograficznych, stacji kryptograficznych, kabin kryptograficznych, pomieszczeń wydzielonych przeznaczonych do przetwarzania informacji niejawnych, kancelarii zagranicznych i punktów obsługi dokumentów zagranicznych.

5. Dokumentacja bezpieczeństwa teleinformatycznego przed przekazaniem do Wojskowych Służb Informacyjnych podlega uzgodnieniu z:
1) pełnomocnikiem ochrony jednostki organizacyjnej, w której będzie eksploatowany system lub sieć teleinformatyczna, oraz
2) Wojskowym Biurem Bezpieczeństwa Łączności i Informatyki lub organem bezpieczeństwa systemów łączności i informatyki dowództwa rodzaju Sił Zbrojnych, Dowództwa Garnizonu Warszawa, Dowództwa Operacyjnego, w przypadku gdy:
   a) w systemie lub sieci teleinformatycznej jest planowane stosowanie środków ochrony kryptograficznej, lub
   b) zasięg systemu lub sieci teleinformatycznej wykracza poza obręb strefy bezpieczeństwa jednostki (komórki) organizacyjnej.

6. Dokumentacja bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych, o których mowa w pkt 5 ppkt 2, podlega uzgodnieniu z:
1) Wojskowym Biurem Bezpieczeństwa Łączności i Informatyki w stosunku do systemów i sieci teleinformatycznych obejmujących swoim zasięgiem:
   a) komórkę organizacyjną,
   b) jednostkę organizacyjną, z zastrzeżeniem ppkt 2,
   c) rodzaj Sił Zbrojnych lub dowództwo rodzaju Sił Zbrojnych, Dowództwo Garnizonu Warszawa, Dowództwo Operacyjne,
   d) resort obrony narodowej lub wykraczających poza niego na podstawie umów, porozumień, aktów prawnych;
2) organem bezpieczeństwa systemów łączności i informatyki dowództwa rodzaju Sił Zbrojnych, Dowództwa Garnizonu Warszawa, Dowództwa Operacyjnego, w stosunku do systemów i sieci teleinformatycznych obejmujących swoim

zasięgiem jednostkę organizacyjną podległą właściwemu dowódcy.

7. Do Wojskowych Służb Informacyjnych przekazuje dokumentację bezpieczeństwa teleinformatycznego systemów lub sieci teleinformatycznych, obejmujących swoim zasięgiem:
1) komórkę organizacyjną — jej kierownik;
2) jednostkę organizacyjną — jej kierownik, z zastrzeżeniem ppkt 3-6;
3) rodzaj Sił Zbrojnych lub dowództwo rodzaju Sił Zbrojnych — dowódca rodzaju Sił Zbrojnych;
4) Dowództwo Garnizonu Warszawa lub jednostki organizacyjne podległe dowódcy Garnizonu Warszawa — dowódca Garnizonu Warszawa;
5) Dowództwo Operacyjne lub jednostki organizacyjne podległe dowódcy Dowództwa Operacyjnego — dowódca Dowództwa Operacyjnego;
6) resort obrony narodowej lub wykraczających poza niego, na podstawie umów, porozumień, aktów prawnych, a także w innych przypadkach nie określonych w ppkt 3-5 — kierownik jednostki (komórki) organizacyjnej, będący organizatorem systemu lub sieci.

8. Pełnomocnik ochrony:
1) odpowiada za zapewnienie ochrony systemów i sieci teleinformatycznych funkcjonujących w jednostce organizacyjnej z wyłączeniem organizacyjnych, technicznych, programowych i eksploatacyjnych aspektów ochrony kryptograficznej, o których mowa w pkt 11-15, w szczególności za:
   a) zapewnienie przestrzegania zasad ochrony informacji niejawnych w systemie lub sieci teleinformatycznej, w tym właściwego i bezpiecznego obiegu dokumentów oraz elektronicznych nośników informacji,
   b) zapewnienie bezpieczeństwa fizycznego obszaru, w którym usytuowany jest system lub sieć teleinformatyczna,
   c) planowanie potrzeb rzeczowo-finansowych na zabezpieczenie, zgodnie z wymaganymi standardami, funkcjonowania systemów i sieci teleinformatycznych,
   d) zapewnienie dostępu do systemu lub sieci teleinformatycznej wyłącznie upoważnionym osobom, posiadającym odpowiednie i ważne poświadczenia bezpieczeństwa oraz uprawnienia,
   e) organizację i prowadzenie szkolenia użytkowników w zakresie bezpieczeństwa systemów i sieci teleinformatycznych funkcjonujących w jednostce (komórce) organizacyjnej oraz ochrony informacji niejawnych w tych systemach i sieciach,
   f) kontrolę znajomości i przestrzegania procedur bezpiecznej eksploatacji przez użytkowników systemu lub sieci teleinformatycznej,
   g) nadzór nad konfiguracją systemu lub sieci teleinformatycznej oraz przemieszczaniem ich elementów składowych,
   h) prowadzenie ewidencji systemów i sieci teleinformatycznych, w tym wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych, o których mowa w pkt 1 ppkt 9 lit. c i d,
   i) nadzór nad bezpieczną eksploatacją systemów i sieci teleinformatycznych oraz wyrobów o przeznaczeniu specjalnym, o których mowa w pkt 1 ppkt 9 lit. c i d;
2) uczestniczy w opracowywaniu projektów dokumentów normatywnych regulujących w jednostce (komórce) organizacyjnej problematykę ochrony informacji niejawnych wytwarzanych, przechowywanych, przetwarzanych lub przekazywanych w systemach i sieciach teleinformatycznych, w tym:
   a) programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów i sieci teleinformatycznych,
   b) dokumentacji bezpieczeństwa teleinformatycznego;
3) uzgadnia dokumentację bezpieczeństwa systemów i sieci teleinformatycznych:
   a) w jednostce (komórce) organizacyjnej,
   b) obejmujących swoim zasięgiem dwie albo więcej bezpośrednio podległe jednostki organizacyjne;
4) w przypadku stwierdzenia naruszeń bezpieczeństwa lub rozbieżności pomiędzy stanem faktycznym, a zapisami zawartymi w dokumentacji bezpieczeństwa teleinformatycznego, informuje o powyższym Szefa Wojskowych Służb Informacyjnych oraz właściwy organ bezpieczeństwa systemów łączności i informatyki, jeżeli uczestniczył w opiniowaniu dokumentacji bezpieczeństwa teleinformatycznego.

9. Administrator systemu realizuje zadania w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad bezpieczeństwa systemu lub sieci teleinformatycznej, w szczególności:
1) opracowuje dokumentację bezpieczeństwa teleinformatycznego oraz propozycje jej uaktualniania;
2) przechowuje oryginały zatwierdzonej (zaakceptowanej) dokumentacji bezpieczeństwa teleinformatycznego;
3) wdraża procedury bezpiecznej eksploatacji systemu lub sieci teleinformatycznej;
4) współuczestniczy w szkoleniu użytkowników systemu lub sieci teleinformatycznej z zakresu ich bezpiecznej eksploatacji;
5) utrzymuje zgodność konfiguracji i parametrów systemu lub sieci teleinformatycznej z dokumentacją bezpieczeństwa teleinformatycznego oraz innymi dokumentami normatywnymi;
6) systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń oraz poprawność działania systemu lub sieci teleinformatycznej;

7) informuje pełnomocnika ochrony oraz Centrum Wsparcia Technicznego funkcjonującego w Centrum Zarządzania Systemami Teleinformatycznymi resortu obrony narodowej o stwierdzonych naruszeniach bezpieczeństwa systemu lub sieci teleinformatycznej;
8) zgłasza pełnomocnikowi ochrony potrzeby w zakresie serwisowania i ponownej certyfikacji wyrobów o przeznaczeniu specjalnym, o których mowa w pkt 1 ppkt 9 lit. c i d;
9) analizuje i archiwizuje rejestr zdarzeń w systemie lub sieci teleinformatycznej, prawidłowość dokumentowania i archiwizowania zdarzeń;
10) prowadzi na bieżąco wykaz osób mających dostęp do systemu lub sieci teleinformatycznej oraz przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki (komórki) organizacyjnej.

10. Inspektor bezpieczeństwa teleinformatycznego realizuje zadania w zakresie bieżącej kontroli zgodności funkcjonowania systemu lub sieci teleinformatycznej z dokumentacją bezpieczeństwa teleinformatycznego z wyłączeniem organizacyjnych, technicznych, programowych i eksploatacyjnych aspektów ochrony kryptograficznej, o których mowa w pkt 11-15, w szczególności kontroluje:
1) przestrzeganie zasad ochrony informacji niejawnych w systemie lub sieci teleinformatycznej;
2) stan zabezpieczeń fizycznych, elektromagnetycznych i elektronicznych pomieszczeń lub obszarów, w których usytuowane są systemy lub sieci teleinformatyczne;
3) aktualność wykazów osób mających dostęp do systemu lub sieci teleinformatycznej, przydzielanie kont użytkownikom, zakres nadanych im uprawnień oraz prawidłowość zabezpieczeń zastosowanych w systemie lub sieci;
4) znajomość i przestrzeganie przez użytkowników procedur bezpiecznej eksploatacji systemu lub sieci teleinformatycznej;
5) przestrzeganie zasad i wymagań w zakresie oznaczania, ewidencjonowania, przechowywania i przekazywania wytworzonych dokumentów niejawnych oraz ich terminowe rozliczanie;
6) zgodność konfiguracji systemu lub sieci teleinformatycznej z dokumentacją bezpieczeństwa teleinformatycznego;

a ponadto:
7) analizuje rejestr zdarzeń w systemie lub sieci teleinformatycznej, prawidłowość dokumentowania i archiwizowania zdarzeń;
8) informuje pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu lub sieci teleinformatycznej;
9) prowadzi szkolenia użytkowników w zakresie ochrony informacji niejawnych oraz przestrzegania zasad bezpieczeństwa w systemie lub sieci teleinformatycznej;
10) uczestniczy w opracowywaniu:
a) programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów i sieci teleinformatycznych,
b) dokumentacji bezpieczeństwa teleinformatycznego.

11. Organy wymienione, o których mowa w pkt 2 ppkt 2- 4, odpowiadają za kryptograficzną ochronę informacji w systemach i sieciach teleinformatycznych oraz sprawowanie nadzoru nad eksploatacją technicznych i programowych środków ochrony tych systemów i sieci.

12. Centrum Bezpieczeństwa Teleinformacyjnego, podporządkowane Szefowi Wojskowych Służb Informacyjnych, jest właściwe do:
1) opracowywania projektów dokumentów normatywnych dotyczących zasad bezpieczeństwa teleinformatycznego;
2) opiniowania projektów dokumentów normatywnych dotyczących organizacji, funkcjonowania i bezpieczeństwa systemów łączności i informatyki, systemów ochrony kryptograficznej oraz systemów i sieci teleinformatycznych chronionych kryptograficznie;
3) opiniowania dokumentacji bezpieczeństwa teleinformatycznego systemów i sieci chronionych kryptograficznie;
4) opiniowania programów szkoleń dotyczących bezpieczeństwa teleinformatycznego, w tym również eksploatacji urządzeń ochrony kryptograficznej;
5) dokonywania rocznej i doraźnych ocen stanu bezpieczeństwa systemów i sieci chronionych kryptograficznie;
6) badania i oceny systemów ochrony kryptograficznej oraz systemów i sieci chronionych kryptograficznie, w ramach prowadzonego procesu certyfikacyjnego lub akredytacyjnego;
7) wykonywania funkcji centralnego organu dystrybucji narodowych materiałów kryptograficznych oraz materiałów kryptograficznych pochodzących z wymiany międzynarodowej w resorcie obrony narodowej;
8) generacji i wytwarzania dokumentów kryptograficznych dla potrzeb narodowych systemów ochrony kryptograficznej;
9) sprawowania nadzoru nad bezpieczeństwem narodowych materiałów kryptograficznych i materiałów kryptograficznych pochodzących z wymiany międzynarodowej, eksploatowanych i wykorzystywanych w jednostkach (komórkach) organizacyjnych resortu obrony narodowej;
10) prowadzenia kontroli w zakresie bezpieczeństwa teleinformatycznego, zarządzanych przez Szefa Wojskowych Służb Informacyjnych;

11) dokonywania sprawdzeń zgodności stanu faktycznego systemów i sieci chronionych kryptograficznie z dokumentacją bezpieczeństwa teleinformatycznego;
12) szkolenia z zakresu ochrony informacji niejawnych osób dokonujących odbioru technicznego lub serwisowania urządzeń ochrony kryptograficznej, kończonego egzaminem i wydaniem zaświadczenia o odbyciu przeszkolenia oraz prowadzenie ewidencji tych zaświadczeń (wzór zaświadczenia o odbyciu przeszkolenia z zakresu ochrony informacji niejawnych w przedmiocie odbioru technicznego lub serwisowania urządzeń ochrony kryptograficznej określa załącznik Nr 1 do decyzji);
13) wydawania pozwoleń na dostęp do systemów ochrony kryptograficznej osobom spoza organów bezpieczeństwa teleinformacyjnego oraz nie będącym pracownikami w jednostce organizacyjnej;
14) pełnienia funkcji Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe.

13. Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki jest właściwe do:
1) opracowywania projektów dokumentów normatywnych dotyczących:
   a) organizacji, funkcjonowania i bezpieczeństwa systemów łączności specjalnej wykorzystujących materiały kryptograficzne (szyfrowe i kodowe),
   b) organizacji, funkcjonowania i bezpieczeństwa systemów ochrony kryptograficznej stosowanych w systemach i sieciach teleinformatycznych resortu obrony narodowej,
   c) gospodarki materiałowej i zasad eksploatacji urządzeń ochrony kryptograficznej;
2) koordynowania działalności organów bezpieczeństwa systemów łączności i informatyki rodzajów Sił Zbrojnych, Dowództwa Garnizonu Warszawa, Dowództwa Operacyjnego i Centrum Zarządzania Systemami Teleinformatycznymi;
3) planowania, organizowania, prognozowania rozwoju, eksploatacji i nadzoru nad funkcjonowaniem systemów łączności specjalnej, systemów ochrony kryptograficznej stosowanych w systemach i sieciach teleinformatycznych resortu obrony narodowej oraz podczas misji pokojowych i ćwiczeń, a także Wojennego Systemu Dowodzenia;
4) rozdziału, dystrybucji, ewidencji, wprowadzania, wycofywania oraz nadzoru nad niszczeniem materiałów kryptograficznych w Siłach Zbrojnych;
5) planowania i organizowania szkoleń i kursów specjalistycznych personelu stacji/aparatowni kryptograficznych i kancelarii kryptograficznych oraz żołnierzy i pracowników organów, o których mowa w pkt 2 ppkt 4, w zakresie organizacji, funkcjonowania i bezpieczeństwa systemów ochrony kryptograficznej, a także gospodarki materiałowej sprzętem ochrony kryptograficznej w Siłach Zbrojnych;
6) uzgadniania dokumentacji bezpieczeństwa teleinformatycznego;
7) opracowywania dokumentacji bezpieczeństwa teleinformatycznego dla systemów, o których mowa w ppkt 1 lit. a, oraz przekazywania jej do Wojskowych Służb Informacyjnych celem zatwierdzenia lub akceptacji;
8) współuczestniczenia w kontrolach systemów i sieci chronionych kryptograficznie;
9) prowadzenia kontroli problemowych, zarządzanych przez Szefa Generalnego Zarządu Dowodzenia i Łączności — P6, organów bezpieczeństwa, o których mowa w pkt 2 ppkt 4, w zakresie organizacji, funkcjonowania, bezpieczeństwa materiałów kryptograficznych oraz systemów i sieci chronionych kryptograficznie;
10) wydawania pozwoleń na eksploatację urządzeń ochrony kryptograficznej oraz prowadzenia ewidencji wydanych pozwoleń (wzory pozwoleń na eksploatację urządzeń określa załącznik Nr 2 do decyzji).

14. Organy bezpieczeństwa systemów łączności i informatyki danego szczebla organizacyjnego odpowiadają za realizację zadań, o których mowa w pkt 13 ppkt 1 i 3-8, stosownie do zakresu kompetencji na swoim szczeblu organizacyjnym, koordynują działalność organów bezpieczeństwa systemów łączności i informatyki jednostek podległych oraz uzgadniają dokumentację bezpieczeństwa teleinformatycznego, zgodnie z pkt 5 ppkt 2 i pkt 6 ppkt 2.

15. Personel organów bezpieczeństwa systemów łączności i informatyki, o których mowa w pkt 2 ppkt 4, współpracuje z pełnomocnikiem ochrony i inspektorem bezpieczeństwa teleinformatycznego w zakresie zapewnienia właściwej ochrony informacjom niejawnym w systemach i sieciach teleinformatycznych danej jednostki (komórki) organizacyjnej, a także udziela pełnomocnikowi ochrony niezbędnych konsultacji w zakresie opracowywania dokumentacji bezpieczeństwa teleinformatycznego oraz innych dokumentów dotyczących problematyki ochrony informacji niejawnych w systemach i sieciach teleinformatycznych.

16. Centrum Zarządzania Systemami Teleinformatycznymi realizuje zadania Centrum Wsparcia Technicznego Systemu Reagowania na Incydenty Komputerowe w stosunku do systemów i sieci teleinformatycznych w resorcie obrony narodowej.

17. 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 zabezpieczających, służących ochronie informacji niejawnych stanowiących tajemnicę państwową i służbową;
3) opiniowania przedstawianej do zatwierdzenia lub akceptacji dokumentacji bezpieczeństwa teleinformatycznego;
4) akceptowania dokumentacji bezpieczeństwa teleinformatycznego, opracowanej dla systemów lub sieci teleinformatycznych, dotyczących informacji niejawnych stanowiących tajemnicę służbową;
5) zatwierdzania dokumentacji bezpieczeństwa teleinformatycznego, opracowanej dla systemów lub sieci teleinformatycznych, dotyczących informacji niejawnych stanowiących tajemnicę państwową;
6) akredytacji systemów i sieci teleinformatycznych;
7) wydawania certyfikatów akredytacji bezpieczeństwa teleinformatycznego dla systemów i sieci teleinformatycznych, dotyczących informacji niejawnych stanowiących tajemnicę państwową;
8) prowadzenia badań i wydawania certyfikatów dla wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych;
9) określania Poziomu Zabezpieczenia Miejsca i Poziomu Zabezpieczenia Urządzenia;
10) planowania i prowadzenia specjalistycznych szkoleń administratorów systemów, zakończonych egzaminem i wydaniem zaświadczenia o odbyciu przeszkolenia (wzór zaświadczenia o odbyciu przeszkolenia z zakresu obowiązków administratora systemu określa załącznik Nr 3 do decyzji);
11) planowania i prowadzenia specjalistycznych szkoleń inspektorów bezpieczeństwa teleinformatycznego, zakończonych egzaminem i wydaniem zaświadczenia o odbyciu przeszkolenia (wzór zaświadczenia o odbyciu przeszkolenia z zakresu obowiązków pracownika pionu ochrony inspektora bezpieczeństwa teleinformatycznego określa załącznik Nr 4 do decyzji);
12) planowania i prowadzenia specjalistycznych szkoleń w zakresie serwisowania wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych;
13) kontroli systemów i sieci teleinformatycznych oraz przestrzegania obowiązujących w tym zakresie przepisów;
14) dokonywania rocznej i doraźnych ocen stanu ochrony informacji niejawnych w resorcie obrony narodowej, w zakresie bezpieczeństwa teleinformatycznego.

18. Traci moc decyzja Nr 181/MON Ministra Obrony Narodowej z dnia 6 października 2000 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej (Dz. Rozk. MON z 2000 r., poz. 111).

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

Minister Obrony Narodowej: *R. Sikorski*

Załączniki do decyzji Nr 24/MON
Ministra Obrony Narodowej
z dnia 31 stycznia 2006 r. (poz. 19)

Załącznik Nr 1

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

ZAŚWIADCZENIE

o odbyciu przeszkolenia z zakresu ochrony informacji niejawnych w przedmiocie odbioru technicznego/serwisowania* urządzeń ochrony kryptograficznej

Nr .....

Stwierdza się, że Pan(i):

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

odbył(a) przeszkolenie z zakresu ochrony informacji niejawnych dla osób dokonujących odbioru technicznego/serwisowania* urządzeń ochrony kryptograficznej typu:

.....

.....

.....

przeprowadzone przez Wojskowe Służby Informacyjne.

.....
(miejscowość i data)

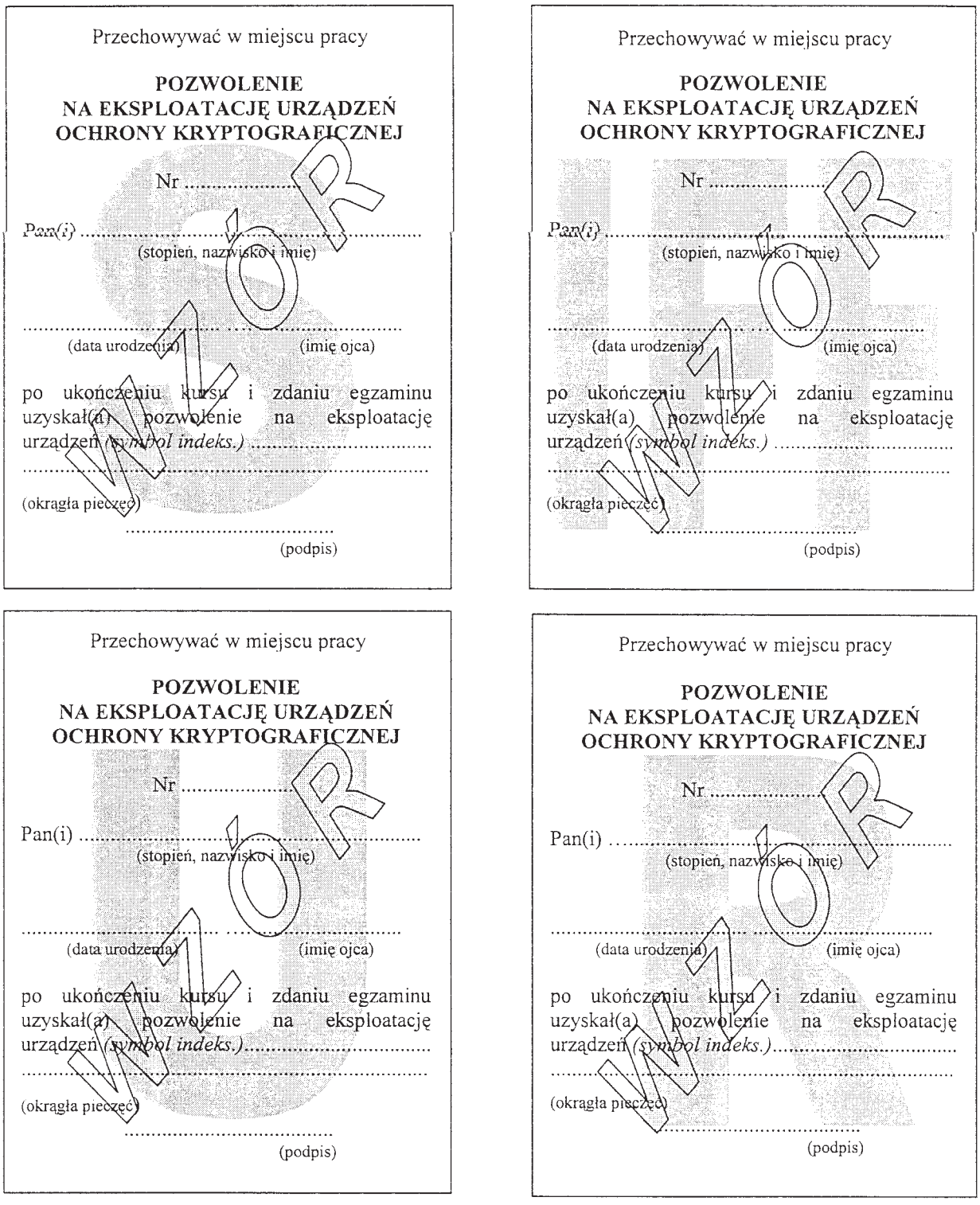
m.p.

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

* niepotrzebne skreślić

Załącznik Nr 2

Wzory
pozwoleń na eksploatację urządzeń ochrony kryptograficznej



Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY KRYPTOGRAFICZNEJ

Nr .....

Pan(i) .....
(stopień, nazwisko i imię)

.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu uzyskał(a) pozwolenie na eksploatację urządzeń *(symbol indeks.)* .....
.....

(okrągła pieczęć)

.....
(podpis)

Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY KRYPTOGRAFICZNEJ

Nr .....

Pan(i) .....
(stopień, nazwisko i imię)

.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu uzyskał(a) pozwolenie na eksploatację urządzeń *(symbol indeks.)* .....
.....

(okrągła pieczęć)

.....
(podpis)

Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY KRYPTOGRAFICZNEJ

Nr .....

Pan(i) .....
(stopień, nazwisko i imię)

.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu uzyskał(a) pozwolenie na eksploatację urządzeń *(symbol indeks.)* .....
.....

(okrągła pieczęć)

.....
(podpis)

Przechowywać w miejscu pracy

POZWOLENIE
NA EKSPLOATACJĘ URZĄDZEŃ
OCHRONY KRYPTOGRAFICZNEJ

Nr .....

Pan(i) .....
(stopień, nazwisko i imię)

.....
(data urodzenia) (imię ojca)

po ukończeniu kursu i zdaniu egzaminu uzyskał(a) pozwolenie na eksploatację urządzeń *(symbol indeks.)* .....
.....

(okrągła pieczęć)

.....
(podpis)

Duże litery: **S, IFF, U, R** – są koloru żółtego:

S - kryptograficzne urządzenia szyfrujące
IFF - kryptograficzne urządzenia identyfikacji obiektów
U - kryptograficzne urządzenia utajniające
R - kryptograficzne radiowe urządzenia utajniające

Załącznik Nr 3

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

ZAŚWIADCZENIE

o odbyciu przeszkolenia z zakresu obowiązków administratora systemu

Nr .....

Stwierdza się, że Pan(i):

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

odbył(a) specjalistyczne przeszkolenie z zakresu obowiązków „administratora systemu" w przedmiocie ochrony informacji niejawnych wymagane przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz. 1631), przeprowadzone przez Wojskowe Służby Informacyjne.

.....
(miejscowość i data)

m.p.

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

Załącznik Nr 4

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

ZAŚWIADCZENIE

o odbyciu przeszkolenia z zakresu obowiązków inspektora bezpieczeństwa teleinformatycznego

Nr .....

Stwierdza się, że Pan(i):

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

odbył(a) specjalistyczne przeszkolenie z zakresu obowiązków „pracownika pionu ochrony informacji niejawnych - inspektora bezpieczeństwa teleinformatycznego" odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania systemu lub sieci teleinformatycznej ze szczególnymi wymaganiami bezpieczeństwa w przedmiocie ochrony informacji niejawnych, wymagane przepisami ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 2005 r. Nr 196, poz. 1631), przeprowadzone przez Wojskowe Służby Informacyjne.

.....
(miejscowość i data)

m.p.

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