Warszawa, dnia 9 lutego 2012 r.

Poz. 8

Departament Ochrony Informacji Niejawnych

DECYZJA Nr 7/MON MINISTRA OBRONY NARODOWEJ

z dnia 20 stycznia 2012 r.

w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych 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. Nr 94, poz. 426), w celu właściwej organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej ustala się, co następuje:

Rozdział 1
Postanowienia ogólne

1. Użyte w decyzji określenia oznaczają:
   1) administrator systemu – administratora systemu teleinformatycznego w rozumieniu przepisu art. 52 ust. 1 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), zwanej dalej „ustawą”;
   2) jednostka organizacyjna – Ministerstwo Obrony Narodowej, jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną;
   3) komórka organizacyjna – komórkę organizacyjną Ministerstwa Obrony Narodowej w rozumieniu statutu Ministerstwa Obrony Narodowej stanowiącego załącznik do zarządzenia Nr 160 Prezesa Rady Ministrów z dnia 24 października 2006 r. w sprawie nadania statutu Ministerstwu Obrony Narodowej (M. P. Nr 76, poz. 768, z późn. zm.[1)]);
   4) kierownik jednostki (komórki) organizacyjnej – dowódcę, szefa, dyrektora, komendanta lub inną osobę kierującą działalnością jednostki (komórki) organizacyjnej, w tym osobę czasowo pełniącą obowiązki;
   5) lokalny system teleinformatyczny – system teleinformatyczny funkcjonujący w jednej jednostce organizacyjnej;

[1)] Zmiany wymienionego zarządzenia zostały ogłoszone w M. P. z 2007 r. Nr 57, poz. 647 i Nr 97, poz. 1073, z 2008 r. Nr 68, poz. 611 oraz z 2010 r. Nr 99, poz. 1168.

6) oficer bezpieczeństwa systemów łączności i informatyki – funkcję sprawowaną w celu nadzoru nad bezpieczeństwem materiałów kryptograficznych;
7) ogólnosystemowa dokumentacja bezpieczeństwa – dokumentację bezpieczeństwa rozległego systemu teleinformatycznego;
8) organizator systemu – kierownika jednostki organizacyjnej organizującej system teleinformatyczny lub upoważnionego przez niego kierownika komórki organizacyjnej;
9) pełnomocnik ochrony – pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych w rozumieniu przepisu art. 14 ust. 2 ustawy;
10) rozległy system teleinformatyczny – system teleinformatyczny funkcjonujący w więcej niż jednej jednostce organizacyjnej.

Rozdział 2
Organizacja bezpieczeństwa teleinformatycznego

2. Zadania w zakresie bezpieczeństwa teleinformatycznego realizują:
   1) w jednostce organizacyjnej:
      a) kierownik jednostki organizacyjnej,
      b) kierownik komórki organizacyjnej,
      c) pełnomocnik ochrony,
      d) inspektor bezpieczeństwa teleinformatycznego,
      e) administrator systemu,
      f) oficer bezpieczeństwa systemów łączności i informatyki;
   2) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych Dyrektor Departamentu Ochrony Informacji Niejawnych, zwany dalej „Pełnomocnikiem Ministra”;
   3) Komendant Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych;
   4) Służba Kontrwywiadu Wojskowego.
3. Szczegółowy wykaz zadań w zakresie bezpieczeństwa teleinformatycznego dla osób funkcyjnych i instytucji wymienionych w pkt 2 zawiera załącznik Nr 1 do decyzji.
4. Sposób powoływania oraz kwalifikacje wymagane do pełnienia funkcji inspektora bezpieczeństwa teleinformatycznego i administratora systemu określa załącznik Nr 2 do decyzji.

Rozdział 3
Dokumentacja bezpieczeństwa teleinformatycznego

5. Dla systemów teleinformatycznych, w których mają być przetwarzane informacje niejawne, opracowuje się dokumentację bezpieczeństwa teleinformatycznego składającą się ze szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.
6. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa przetwarzanych w systemie teleinformatycznym informacji niejawnych oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a w przypadku systemów, w których przewiduje się wykorzystanie urządzeń lub narzędzi kryptograficznych, dodatkowo ich zabezpieczenie w dokumenty kryptograficzne.
7. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.
8. Za opracowanie dokumentacji bezpieczeństwa systemu teleinformatycznego i za przesłanie jej do podmiotu udzielającego akredytacji odpowiada organizator systemu.

9. Dokumentację bezpieczeństwa wykonuje się, z zastrzeżeniem pkt 10, w dwóch egzemplarzach, po jednym dla administratora systemu teleinformatycznego i podmiotu udzielającego akredytacji, chyba że podmiot udzielający akredytacji postanowi inaczej.
10. W przypadku systemów teleinformatycznych, dla których organizatorami są kierownicy komórek organizacyjnych, wykonywany jest dodatkowy egzemplarz dokumentacji bezpieczeństwa z przeznaczeniem dla Pełnomocnika Ministra.
11. W przypadku rozległych systemów teleinformatycznych opracowuje się ogólnosystemową dokumentację bezpieczeństwa teleinformatycznego i wynikające z niej załączniki dla poszczególnych lokalizacji lub usług uruchamianych w ramach tego systemu.
12. W ogólnosystemowej dokumentacji bezpieczeństwa organizator systemu teleinformatycznego opisuje minimalne wymagania bezpieczeństwa, w tym szczegółowe warunki i zasady dołączania nowych lokalizacji oraz uruchamiania nowych usług, a także określa niezbędne do wyznaczenia w poszczególnych lokalizacjach osoby funkcyjne i zakres ich zadań.
13. Kierownicy jednostek (komórek) organizacyjnych odpowiedzialni za poszczególne lokalizacje lub wdrażane usługi w rozległym systemie teleinformatycznym odpowiadają za opracowanie załączników wymienionych w pkt 11 i udostępniają organizatorowi systemu niezbędne informacje pozwalające na przeprowadzenie procesu szacowania ryzyka dla systemu, chyba że dokumentacja ogólnosystemowa stanowi inaczej.
14. Zmiany w dokumentacji bezpieczeństwa mogą być wprowadzane aneksami.
15. Za akceptację wyników procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych i za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada, z zastrzeżeniem pkt 16, organizator systemu.
16. Dla organizowanych w komórkach organizacyjnych systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych:
    1) dokumentacja bezpieczeństwa przesyłana jest do organu udzielającego akredytacji przez Pełnomocnika Ministra;
    2) wyniki szacowania ryzyka dla informacji niejawnych akceptuje Pełnomocnik Ministra.
17. Przed przedłożeniem do akredytacji, dokumentacja bezpieczeństwa systemu podlega uzgodnieniu z:
    1) właściwym oficerem bezpieczeństwa systemów łączności i informatyki, w przypadku stosowania urządzeń lub narzędzi kryptograficznych, w zakresie ich doboru i sposobu użycia oraz zabezpieczenia w dokumenty kryptograficzne;
    2) Resortowym Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych pod względem doboru oraz stosowania urządzeń lub narzędzi kryptograficznych stosowanych w rozległych systemach teleinformatycznych;
    3) właściwym pełnomocnikiem ochrony – w zakresie poprawności przeprowadzenia szacowania ryzyka dla informacji niejawnych oraz zgodności zapisów dokumentacji z przepisami i procedurami z zakresu ochrony informacji niejawnych;
    4) innym kierownikiem jednostki organizacyjnej – w razie potrzeby.

Rozdział 4
Akredytacja systemów teleinformatycznych

18. Akredytacji bezpieczeństwa teleinformatycznego dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej i systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych udziela Służba Kontrwywiadu Wojskowego.
19. Akredytacji bezpieczeństwa teleinformatycznego dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” udziela organizator systemu.
20. W przypadku systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone”, w których zakłada się przetwarzanie

informacji niejawnych międzynarodowych, warunkiem dopuszczenia do ich przetwarzania jest wcześniejsze udzielenie przez organizatora systemu akredytacji bezpieczeństwa w trybie art. 48 ust. 9 lub 10 ustawy. Rozpoczęcie przetwarzania informacji niejawnych możliwe jest:

1) w odniesieniu do informacji oznaczonych klauzulą „zastrzeżone" – po zatwierdzeniu przez organizatora systemu stosownej dokumentacji bezpieczeństwa;
2) w odniesieniu do informacji niejawnych międzynarodowych – po otrzymaniu pisemnego potwierdzenia dopuszczenia przez Służbę Kontrwywiadu Wojskowego możliwości przetwarzania w danym systemie informacji niejawnych międzynarodowych, stanowiącego potwierdzenie spełnienia przez system wymagań wynikających z regulacji lub umów międzynarodowych.

Rozdział 5
Uruchamianie i wycofywanie systemów teleinformatycznych z eksploatacji

21. Informacje o uruchomieniu i wycofaniu z eksploatacji systemu teleinformatycznego umieszcza się w decyzji lub rozkazie właściwego kierownika jednostki (komórki) organizacyjnej.
22. O wyłączeniu z eksploatacji systemu teleinformatycznego organizator systemu powiadamia Służbę Kontrwywiadu Wojskowego.
23. W przypadku wyłączenia z eksploatacji systemu przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej, organizator systemu dodatkowo zwraca do organu, który udzielił akredytacji, świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.
24. W przypadku systemów organizowanych w komórkach organizacyjnych, informacja, o której mowa w pkt 22, przesyłana jest przez Pełnomocnika Ministra.

Rozdział 6
Postanowienia końcowe

25. W decyzji Nr 122/MON Ministra Obrony Narodowej z dnia 18 marca 2008 r. w sprawie powoływania w resorcie obrony narodowej pełnomocników i zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów oraz inspektorów bezpieczeństwa teleinformatycznego (Dz. Urz. MON Nr 6, poz. 61) uchyla się pkt 12-29.
26. Traci moc 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 (Dz. Urz. MON Nr 2, poz. 19 oraz z 2007 r. Nr 23, poz. 241).
27. W przypadku systemów teleinformatycznych, które uzyskały akredytację przed wejściem w życie niniejszej decyzji, nie wymagane jest formalne upoważnienie wynikające z zapisów definicji zawartej w pkt 1 ppkt 8.
28. Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Obrony Narodowej: *T. Siemoniak*

Załączniki do
decyzji Ministra Obrony Narodowej
z dnia 20 stycznia 2012 r. (poz. 8)

załącznik Nr 1

Szczegółowy wykaz zadań w zakresie bezpieczeństwa teleinformatycznego

1. Kierownik jednostki organizacyjnej odpowiada za organizację, eksploatację i bezpieczeństwo systemów teleinformatycznych funkcjonujących w jednostce organizacyjnej, w szczególności za:
   1) nadzór nad opracowaniem dokumentacji bezpieczeństwa dla organizowanych przez siebie systemów teleinformatycznych;
   2) akceptację wyników procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w organizowanych przez siebie systemach teleinformatycznych;
   3) udzielanie akredytacji bezpieczeństwa teleinformatycznego dla organizowanych przez siebie systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone";
   4) wyznaczanie, zgodnie z art. 52 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), zwanej dalej „ustawą", osób funkcyjnych dla organizowanych przez siebie systemów teleinformatycznych;
   5) wyznaczanie osób funkcyjnych przewidzianych w dokumentacji bezpieczeństwa dla eksploatowanych w jednostce organizacyjnej systemów teleinformatycznych;
   6) występowanie do Służby Kontrwywiadu Wojskowego z wnioskami o:
      a) weryfikację w trybie art. 48 ust. 11 i 12 ustawy poprawności akredytacji bezpieczeństwa teleinformatycznego udzielonej dla systemów teleinformatycznych przetwarzających informacje niejawne oznaczone klauzulą „zastrzeżone",
      b) udzielenie akredytacji bezpieczeństwa teleinformatycznego dla organizowanych przez siebie systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej,
      c) udzielenie akredytacji bezpieczeństwa teleinformatycznego dla organizowanych przez siebie systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych,
      d) określenie poziomu zabezpieczenia miejsca, technicznego poziomu zabezpieczenia urządzenia lub klasy urządzenia,
      e) przeprowadzenie certyfikacji środków ochrony elektromagnetycznej przeznaczonych do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej,
      f) dopuszczenie do stosowania w organizowanym przez siebie systemie przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", urządzeń lub narzędzi kryptograficznych w trybie art. 50 ust. 7 ustawy.
2. Kierownik komórki organizacyjnej odpowiada za eksploatację i bezpieczeństwo systemów teleinformatycznych funkcjonujących w komórce organizacyjnej, w szczególności za wyznaczanie osób funkcyjnych przewidzianych w dokumentacji bezpieczeństwa dla tych systemów. Ponadto w przypadku, kiedy kierownik komórki organizacyjnej został upoważniony przez kierownika jednostki organizacyjnej do pełnienia funkcji organizatora systemów teleinformatycznych, dodatkowo odpowiada za ich organizację, w szczególności za:
   1) nadzór nad opracowaniem dokumentacji bezpieczeństwa dla organizowanych przez siebie systemów teleinformatycznych;
   2) występowanie o wyznaczenie, zgodnie z art. 52 ust. 1 pkt 2 ustawy, osób funkcyjnych dla organizowanych przez siebie systemów teleinformatycznych;
   3) udzielanie akredytacji bezpieczeństwa teleinformatycznego dla organizowanych przez siebie

systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”;

4) występowanie do Służby Kontrwywiadu Wojskowego przez Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych Dyrektora Departamentu Ochrony Informacji Niejawnych, zwanego dalej „Pełnomocnikiem Ministra”, z wnioskami o:
   a) weryfikację w trybie art. 48 ust. 11 i 12 ustawy poprawności akredytacji bezpieczeństwa teleinformatycznego udzielonej dla systemów teleinformatycznych przetwarzających informacje niejawne oznaczone klauzulą „zastrzeżone”,
   b) udzielenie akredytacji bezpieczeństwa teleinformatycznego dla organizowanych przez siebie systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej,
   c) udzielenie akredytacji bezpieczeństwa teleinformatycznego dla organizowanych przez siebie systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych,
   d) określenie poziomu zabezpieczenia miejsca, technicznego poziomu zabezpieczenia urządzenia lub klasy urządzenia;
   e) przeprowadzenie certyfikacji środków ochrony elektromagnetycznej przeznaczonych do ochrony informacji niejawnych o klauzuli „poufne” lub wyższej,
   f) dopuszczenie do stosowania w organizowanym przez siebie systemie przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, urządzeń lub narzędzi kryptograficznych w trybie art. 50 ust. 7 ustawy;
5) informowanie Pełnomocnika Ministra o stanie realizacji prac związanych z opracowywaniem dokumentacji bezpieczeństwa systemów teleinformatycznych i jej przygotowaniem do wdrożenia;
6) przekazywanie Pełnomocnikowi Ministra informacji o potrzebach w zakresie wyposażenia w środki ochrony elektromagnetycznej przeznaczone do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej.

3. Pełnomocnik ochrony odpowiada za zapewnienie ochrony systemów teleinformatycznych funkcjonujących w jednostce organizacyjnej (z wyłączeniem organizacyjnych, technicznych, programowych i eksploatacyjnych aspektów ochrony kryptograficznej), w szczególności za:
   1) zapewnienie przestrzegania zasad ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych, w tym właściwego i bezpiecznego obiegu dokumentów oraz informatycznych nośników danych;
   2) zapewnienie bezpieczeństwa fizycznego obszarów, w których usytuowane są systemy teleinformatyczne;
   3) organizację i prowadzenie szkoleń użytkowników w zakresie bezpieczeństwa teleinformatycznego;
   4) nadzór nad konfiguracją systemów teleinformatycznych i przemieszczaniem ich elementów składowych;
   5) prowadzenie ewidencji systemów teleinformatycznych – ewidencja systemów może być prowadzona w postaci elektronicznej i powinna zawierać co najmniej: nazwę systemu, klauzule przetwarzanych w nim informacji, nazwę komórki, w której uruchomiono system, lokalizację, imię i nazwisko administratora, datę uruchomienia oraz datę upływu ważności akredytacji;
   6) prowadzenie ewidencji środków ochrony elektromagnetycznej – ewidencja tych środków może być prowadzona w postaci elektronicznej i powinna zawierać co najmniej: nazwę i numer seryjny środka ochrony elektromagnetycznej, numer wydanego certyfikatu i Techniczny Poziom Zabezpieczenia Urządzenia oraz termin ważności wydanego certyfikatu;
   7) prowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych.

   Ponadto pełnomocnik ochrony:

1) uczestniczy w opracowywaniu projektów dokumentów regulujących w danej jednostce organizacyjnej problematykę ochrony przetwarzanych w systemach teleinformatycznych informacji niejawnych, w tym:
   a) programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów teleinformatycznych,
   b) dokumentacji bezpieczeństwa systemów teleinformatycznych;
2) uzgadnia dokumentację bezpieczeństwa:
   a) organizowanych w danej jednostce organizacyjnej systemów teleinformatycznych,
   b) dla elementów rozległych systemów teleinformatycznych funkcjonujących w danej jednostce organizacyjnej.

4. Inspektor bezpieczeństwa teleinformatycznego realizuje zadania w zakresie weryfikacji i bieżącej kontroli zgodności funkcjonowania eksploatowanego w danej jednostce organizacyjnej systemu teleinformatycznego z jego dokumentacją bezpieczeństwa, a w szczególności kontroluje:
   1) przestrzeganie zasad ochrony przetwarzanych w systemie teleinformatycznym informacji niejawnych;
   2) poprawność realizacji zadań wykonywanych przez administratora;
   3) zgodność konfiguracji systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu teleinformatycznego;
   4) stan środków bezpieczeństwa fizycznego i ochrony elektromagnetycznej;
   5) aktualność wykazów osób mających dostęp do systemu teleinformatycznego, prawidłowość przydzielania kont użytkownikom, zakres nadanych im uprawnień i prawidłowość zabezpieczeń zastosowanych w systemie teleinformatycznym;
   6) znajomość i przestrzeganie przez użytkowników procedur bezpiecznej eksploatacji systemu teleinformatycznego.

   Ponadto inspektor bezpieczeństwa teleinformatycznego:
   1) analizuje rejestry zdarzeń w systemie teleinformatycznym i prawidłowość ich archiwizowania;
   2) informuje pełnomocnika ochrony o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo systemu teleinformatycznego;
   3) uczestniczy w opracowywaniu programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych planowanych do budowy systemów teleinformatycznych.
5. Administrator systemu realizuje zadania w zakresie odpowiedzialności za funkcjonowanie systemu teleinformatycznego oraz odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, w szczególności:
   1) opracowuje i uaktualniania dokumentację bezpieczeństwa systemu teleinformatycznego;
   2) przechowuje oryginały zatwierdzonej dokumentacji bezpieczeństwa teleinformatycznego systemu teleinformatycznego;
   3) uczestniczy w procesie szacowania ryzyka;
   4) wdraża procedury bezpiecznej eksploatacji;
   5) szkoli użytkowników systemu teleinformatycznego z zakresu procedur bezpiecznej eksploatacji;
   6) utrzymuje zgodność konfiguracji i parametrów systemu teleinformatycznego z dokumentacją bezpieczeństwa systemu;
   7) systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń i poprawność działania systemu teleinformatycznego;
   8) informuje pełnomocnika ochrony o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego;
   9) zgłasza do pełnomocnika ochrony potrzeby w zakresie serwisowania i certyfikacji środków ochrony elektromagnetycznej;
   10) analizuje i archiwizuje rejestr zdarzeń w systemie teleinformatycznym;
   11) prowadzi wykaz osób mających dostęp do systemu teleinformatycznego zawierający co

najmniej: imię i nazwisko, nazwę jednostki (komórki) organizacyjnej, posiadane poświadczenie bezpieczeństwa (jego numer, klauzulę i datę ważności) oraz przydziela użytkownikom konta, zgodnie z uprawnieniami nadanymi przez kierownika jednostki (komórki) organizacyjnej;

12) zapewnia dostęp do systemu teleinformatycznego wyłącznie użytkowników posiadających wymagane uprawnienia oraz odpowiednie i ważne poświadczenia bezpieczeństwa.

6. Oficer bezpieczeństwa systemów łączności i informatyki realizuje zadania w zakresie nadzoru nad bezpieczeństwem kryptograficznym, w szczególności:
   1) nadzoruje przekazywanie urządzeń i narzędzi kryptograficznych poza jednostkę (komórkę) organizacyjną;
   2) prowadzi kontrole urządzeń i narzędzi kryptograficznych stosowanych w systemach teleinformatycznych;
   3) w przypadku stosowania urządzeń lub narzędzi kryptograficznych – uzgadnia dokumentację bezpieczeństwa systemu teleinformatycznego pod kątem odpowiedniego doboru tych urządzeń i zabezpieczenia w dokumenty kryptograficzne.
7. Pełnomocnik Ministra oprócz zadań określonych w pkt 3 jest właściwy w zakresie:
   1) opracowywania projektów aktów normatywnych i projektów wytycznych normujących zasady ochrony systemów teleinformatycznych w resorcie obrony narodowej;
   2) akceptacji wyników szacowania ryzyka dla systemów teleinformatycznych, dla których kierownicy komórek organizacyjnych pełnią funkcję organizatora systemu.
8. Komendant Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych (RCZBSiUT) jest właściwy do:
   1) opracowywania projektów wytycznych i projektów innych dokumentów dotyczących:
      a) organizacji, funkcjonowania i bezpieczeństwa systemów ochrony kryptograficznej stosowanych w systemach teleinformatycznych resortu obrony narodowej,
      b) gospodarki materiałowej i zasad eksploatacji urządzeń ochrony kryptograficznej;
   2) koordynowania działalności organów bezpieczeństwa systemów łączności i informatyki rodzajów Sił Zbrojnych Rzeczypospolitej Polskiej, Dowództwa Operacyjnego Sił Zbrojnych, Inspektoratu Wsparcia Sił Zbrojnych, Dowództwa Garnizonu Warszawa i równorzędnych oraz Centrum Wsparcia Teleinformatycznego Sił Zbrojnych Ministerstwa Obrony Narodowej;
   3) planowania, organizowania, prognozowania rozwoju, eksploatacji i nadzoru nad funkcjonowaniem systemów ochrony kryptograficznej stosowanych w systemach teleinformatycznych resortu obrony narodowej;
   4) planowania, organizowania oraz sprawowania nadzoru nad szkoleniem specjalistycznym personelu organów bezpieczeństwa systemów łączności i informatyki;
   5) koordynacji działań podległego mu Centrum Wsparcia Technicznego Systemu Reagowania na Incydenty Komputerowe w stosunku do resortowych systemów teleinformatycznych;
   6) uzgadniania dokumentacji bezpieczeństwa teleinformatycznego dla systemów rozległych w przypadku stosowania urządzeń lub narzędzi kryptograficznych pod względem ich doboru i stosowania oraz zabezpieczenia w dokumenty kryptograficzne.

   Ponadto Komendant RCZBSiUT wyznacza, ze składu osobowego RCZBSiUT, osobę lub osoby pełniące funkcję oficera bezpieczeństwa łączności i informatyki dla komórek organizacyjnych Ministerstwa Obrony Narodowej.
9. Służba Kontrwywiadu Wojskowego jest właściwa w zakresie:
   1) określania ogólnych zasad bezpieczeństwa teleinformatycznego;
   2) weryfikacji poprawności akredytacji udzielonych dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone”;
   3) udzielania akredytacji bezpieczeństwa teleinformatycznego dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej;

4) udzielania akredytacji dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych;
5) wydawania świadectw akredytacji bezpieczeństwa teleinformatycznego;
6) badań i oceny bezpieczeństwa w ramach certyfikacji:
   a) środków ochrony elektromagnetycznej,
   b) urządzeń i narzędzi kryptograficznych,
   c) urządzeń i narzędzi służących do realizacji zabezpieczeń teleinformatycznych;
7) określania poziomu zabezpieczenia miejsca, technicznego poziomu zabezpieczenia urządzenia lub klasy urządzenia;
8) prowadzenia specjalistycznych szkoleń dla administratorów systemów i inspektorów bezpieczeństwa teleinformatycznego;
9) dokonywania okresowej i doraźnych ocen stanu zabezpieczenia informacji niejawnych w resorcie obrony narodowej, w zakresie bezpieczeństwa teleinformatycznego;
10) opiniowania projektów dokumentów normatywnych dotyczących organizacji, funkcjonowania i bezpieczeństwa systemów teleinformatycznych oraz projektów wytycznych i projektów innych dokumentów dotyczących:
    a) organizacji, funkcjonowania i bezpieczeństwa systemów ochrony kryptograficznej, stosowanych w systemach teleinformatycznych resortu obrony narodowej,
    b) gospodarki materiałowej i zasad eksploatacji urządzeń ochrony kryptograficznej,
    c) prognozowania rozwoju systemów ochrony kryptograficznej;
11) kontroli systemów teleinformatycznych i przestrzegania przepisów obowiązujących w tym zakresie;
12) nadzoru nad realizacją zadań określonych w pkt 3;
13) opiniowania programów szkoleń dotyczących eksploatacji urządzeń ochrony kryptograficznej;
14) wykonywania funkcji krajowego organu dystrybucji i generacji materiałów kryptograficznych na potrzeby jednostek oraz pełnienia funkcji National Distribution Authotrity (NDA) dla materiałów kryptograficznych wykorzystywanych w systemach teleinformatycznych przetwarzających informację NATO;
15) wydawania zaleceń w zakresie bezpieczeństwa teleinformatycznego do stosowania w resorcie obrony narodowej.

załącznik Nr 2

Sposób powoływania oraz kwalifikacje wymagane do pełnienia funkcji inspektora bezpieczeństwa teleinformatycznego i administratora systemu

1. Administratorów systemów teleinformatycznych, z zastrzeżeniem pkt 2, wyznaczają kierownicy jednostek organizacyjnych eksploatujących te systemy, zgodnie z dokumentacją bezpieczeństwa.
2. W przypadku systemów teleinformatycznych organizowanych lub eksploatowanych w komórkach organizacyjnych, administratorów wyznacza Dyrektor Generalny Ministerstwa Obrony Narodowej na wniosek kierowników właściwych komórek organizacyjnych przesłany przez Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych Dyrektora Departamentu Ochrony Informacji Niejawnych, zwanego dalej „Pełnomocnikiem Ministra".
3. Administratorem systemu nie może być pracownik pionu ochrony.
4. Przepis pkt 3 nie dotyczy systemów teleinformatycznych eksploatowanych w pionach ochrony jednostek organizacyjnych.
5. W przypadku, o którym mowa w pkt 4, nie można łączyć funkcji administratora systemu i inspektora bezpieczeństwa teleinformatycznego.
6. Do pełnienia funkcji administratora systemu zaleca się wyznaczać osoby posiadające wykształcenie informatyczne.
7. Do pełnienia funkcji administratora systemu, w którym przetwarzane są informacje niejawne o klauzuli „tajne" lub „ściśle tajne", wyznacza się osoby posiadające kwalifikacje w zakresie administrowania systemami teleinformatycznymi, potwierdzone ważnym świadectwem, certyfikatem lub zaświadczeniem.
8. Kierownicy jednostek (komórek) organizacyjnych kierują osoby wyznaczone do pełnienia funkcji administratora systemu, o którym mowa w pkt 7, na dodatkowe szkolenia, poza określonymi w art. 52 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), w celu podnoszenia ich kwalifikacji w zakresie administrowania systemami teleinformatycznymi.
9. Dodatkowe szkolenia kończące się wydaniem dokumentu, o którym mowa w pkt 8, potwierdzającego nabycie umiejętności w zakresie administrowania systemem użytkowanym w jednostce (komórce) organizacyjnej, są prowadzone:
   1) w ośrodkach kształcenia autoryzowanych przez producenta (producentów) sprzętu komputerowego, oprogramowania lub urządzeń wraz z oprogramowaniem, zapewniających bezpieczeństwo systemów teleinformatycznych;
   2) przez organy wojskowe pod warunkiem uzgodnienia programu oraz formy szkolenia przez Dyrektora Departamentu Informatyki i Telekomunikacji.
10. Na szkolenia, o których mowa w pkt 8, kierownicy jednostek (komórek) organizacyjnych mogą kierować (w miarę posiadanych środków) administratorów pozostałych systemów teleinformatycznych.
11. O wyznaczeniu do pełnienia funkcji administratora systemu, a także o odwołaniu z pełnienia tej funkcji, kierownicy jednostek (komórek) organizacyjnych informują właściwego pełnomocnika ochrony.
12. Inspektorów bezpieczeństwa teleinformatycznego wyznaczają:
   1) w jednostkach organizacyjnych – kierownicy tych jednostek, na wniosek pełnomocnika ochrony, spośród pracowników pionu ochrony;
   2) w Ministerstwie Obrony Narodowej – Dyrektor Generalny Ministerstwa Obrony Narodowej, na wniosek Pełnomocnika Ministra, spośród żołnierzy zawodowych i pracowników Departamentu Ochrony Informacji Niejawnych.

13. W stosunku do osób wyznaczonych do pełnienia funkcji inspektora bezpieczeństwa teleinformatycznego, przepisy pkt 6 -10 stosuje się odpowiednio.
14. Wyznaczenie i odwołanie administratora systemu lub inspektora bezpieczeństwa teleinformatycznego odbywa się w formie decyzji (rozkazu) osób wskazanych odpowiednio w pkt 1, 2 i 12. Decyzja (rozkaz) powinna zawierać co najmniej informacje określające:
    1) podstawę prawną wyznaczenia lub odwołania;
    2) imię i nazwisko osoby wyznaczanej lub odwoływanej oraz nazwę jednostki (komórki) organizacyjnej;
    3) w przypadku inspektora bezpieczeństwa teleinformatycznego – nazwę jednostki organizacyjnej, w której będzie wykonywał zadania;
    4) w przypadku administratora – nazwę, klauzulę i lokalizację systemu teleinformatycznego.
15. Żołnierzom zawodowym wyznaczonym do pełnienia funkcji administratora systemu lub inspektora bezpieczeństwa teleinformatycznego za realizację powierzonych im czynności wypłaca się dodatkowe wynagrodzenie na zasadach i w trybie określonym w przepisach o służbie wojskowej żołnierzy zawodowych, a pracownikom wyznaczonym do pełnienia tych funkcji – na zasadach określonych w przepisach o wynagrodzeniu pracowników.
16. W przypadkach uzasadnionych względami etatowymi, funkcję inspektora bezpieczeństwa teleinformatycznego może pełnić pełnomocnik ochrony.