Departament Ochrony Informacji Niejawnych

127

DECYZJA Nr 165/MON MINISTRA OBRONY NARODOWEJ

z dnia 29 kwietnia 2011 r.

w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej

Na podstawie § 2 pkt 6, 13 i 14 rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426) ustala się, co następuje:

Rozdział 1

Postanowienia ogólne

1. Decyzja określa organizację, warunki oraz tryb sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej.

2. Przepisy decyzji stosuje się do działalności kontrolnej w zakresie ochrony informacji niejawnych wykonywanej przez:
1) Ministra Obrony Narodowej;
2) osoby zajmujące kierownicze stanowiska w Ministerstwie Obrony Narodowej;
3) kierowników jednostek organizacyjnych resortu obrony narodowej;
4) kierowników komórek organizacyjnych Ministerstwa Obrony Narodowej;
5) Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych — Dyrektora Departamentu Ochrony Informacji Niejawnych;
6) pełnomocników do spraw ochrony informacji niejawnych w jednostkach organizacyjnych resortu obrony narodowej.

3. Użyte w decyzji określenia oznaczają:
1) ustawa — ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
2) resort obrony narodowej — dział administracji rządowej, w skład którego wchodzą: Minister Obrony Narodowej, jako kierownik działu administracji rządowej — obrona narodowa, Ministerstwo Obrony Narodowej, jako urząd, jednostki organizacyjne podległe lub nadzorowane przez Ministra Obrony Narodowej, oraz jednostki organizacyjne Sił Zbrojnych Rzeczypospolitej Polskiej;
3) jednostka organizacyjna — Ministerstwo Obrony Narodowej, jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną, w tym przedsiębiorstwo państwowe, dla którego jest on organem założycielskim;
4) komórka organizacyjna — Sekretariat Ministra Obrony Narodowej, departament, zarząd, biuro — wchodzące w skład Ministerstwa;
5) komórka wewnętrzna — część organizacyjną w strukturze jednostki organizacyjnej resortu obrony narodowej (komórki organizacyjnej Ministerstwa Obrony Narodowej);
6) kierownik jednostki organizacyjnej — dowódcę, szefa, dyrektora, komendanta, prezesa lub inną osobę stojącą na czele jednostki organizacyjnej resortu obrony narodowej, która kieruje całokształtem działalności tej jednostki, w tym również osobę czasowo pełniącą jego obowiązki;
7) kierownik komórki organizacyjnej — dyrektora, szefa, lub inną osobę stojącą na czele komórki organizacyjnej Ministerstwa Obrony Narodowej, która kieruje całokształtem działalności tej komórki, w tym również osobę czasowo pełniącą jego obowiązki;
8) pełnomocnik ochrony — pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych;
9) pion ochrony — wyodrębnioną komórkę organizacyjną do spraw ochrony informacji niejawnych, podległą pełnomocnikowi ochrony, wykonującą zadania określone w ustawie;
10) system ochrony informacji niejawnych — zespół przedsięwzięć organizacyjno-technicznych obejmujących: bezpieczeństwo osobowe, ochronę fizyczną i techniczną informacji niejawnych, obieg informacji niejawnych oraz bezpieczeństwo teleinformatyczne w jednostce organizacyjnej;
11) ryzyko — kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
12) szacowanie ryzyka — całościowy proces analizy i oceny ryzyka;
13) zarządzanie ryzykiem — skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;
14) działalność kontrolna — planowanie, organizowanie, koordynowanie i przeprowadzanie

kontroli, jej dokumentowanie i przedstawianie wyników właściwym organom, a także postępowanie pokontrolne;
15) kontrola (czynności kontrolne) — celową i zorganizowaną działalność zespołu (komisji, grupy, kontrolera, inspektora) prowadzoną w jednostce kontrolowanej, na podstawie planu i upoważnienia do jej przeprowadzenia;
16) książka kontroli — wyodrębnioną, prowadzoną w formie papierowej, książkę, za prowadzenie której jest odpowiedzialny kierownik jednostki (komórki) organizacyjnej. Przeznaczona jest do dokonywania przez kontrolującego wpisów dotyczących przedmiotu i zakresu kontroli, a także czasu jej trwania;
17) akta kontroli — zbiór dokumentów obejmujących w szczególności: zawiadomienie o zamiarze przeprowadzenia kontroli, upoważnienia do przeprowadzenia kontroli, protokół z kontroli, notatki i inne dokumenty — odpisy, wyciągi z rozkazów, informacje od kierownika jednostki kontrolowanej dotyczące usunięcia nieprawidłowości stwierdzonych podczas kontroli problemowej;
18) przełożony — żołnierz lub inna osoba niebędąca żołnierzem, której na mocy przepisów prawa, dokumentów kompetencyjnych lub decyzji podporządkowano podwładnych i nadano prawo kierowania ich czynnościami służbowymi.

4. Nadzór nad ochroną informacji niejawnych realizuje się w formie:
1) kontroli stanu zabezpieczenia informacji niejawnych;
2) oceny stanu zabezpieczenia informacji niejawnych;
3) decyzji wynikających z kontroli i oceny, o których mowa w ppkt 1 i 2.

5. Kontrole stanu zabezpieczenia informacji niejawnych w jednostkach i komórkach organizacyjnych realizuje się w celu:
1) ustalenia stanu faktycznego realizacji zadań w zakresie ochrony informacji niejawnych oraz oceny przestrzegania przepisów wydanych w tym zakresie;
2) określenia przyczyn i skutków ewentualnych naruszeń przepisów o ochronie informacji niejawnych oraz wskazania osób za to odpowiedzialnych;
3) wskazania sposobów umożliwiających usunięcie stwierdzonych nieprawidłowości;
4) sformułowania i przedłożenia przełożonym wniosków oraz zaleceń dotyczących doskonalenia systemu ochrony informacji niejawnych.

6. Kontrole, o których mowa w pkt 5, realizuje się, jako:
1) kontrole doraźne;
2) kontrole okresowe;
3) kontrole problemowe.

7. Do przeprowadzenia kontroli, o których mowa w pkt 6 ppkt 1 i 3, uprawnia imienne upoważnienie, wystawione przez zarządzającego kontrolę, wraz z legitymacją służbową lub dowodem osobistym. Wzór upoważnienia określa załącznik Nr 1 do decyzji. Upoważnienia nie wystawia się przełożonemu prowadzącemu kontrolę doraźną wobec podwładnych.

8. Kontrolujący musi posiadać poświadczenie bezpieczeństwa lub certyfikat bezpieczeństwa upoważniające do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej lub innych organizacji międzynarodowych o klauzuli co najmniej równej klauzuli materiałów podlegających kontroli, ważne do dnia zakończenia kontroli (w tym brakowania materiałów niejawnych) lub po ustaniu trybu odwoławczego od protokołu z kontroli problemowej. W przypadku kontroli materiałów kryptograficznych dodatkowo wymagane jest posiadanie przez kontrolującego właściwego upoważnienia wydanego na podstawie odrębnych przepisów dotyczących prowadzenia kontroli problemowych w zakresie funkcjonowania kancelarii kryptograficznych.

9. Kontrolowany ma obowiązek przedstawić do kontroli posiadane materiały niejawne, udzielać wyczerpujących ustnych i pisemnych wyjaśnień, udostępniać do wglądu prowadzone przez siebie urządzenia ewidencyjne, pomieszczenia i urządzenia techniczne przeznaczone do przetwarzania informacji niejawnych.

Rozdział 2

Kontrola doraźna

10. Kontrolę doraźną prowadzi się w celu niezwłocznego sprawdzenia stanu zabezpieczenia informacji niejawnych, w szczególności:
1) zgodności stanu faktycznego materiałów niejawnych oraz pieczęci urzędowych posiadanych przez wykonawców ze stanem ewidencyjnym;
2) stanu przestrzegania przez osoby kontrolowane przepisów o ochronie informacji niejawnych w zakresie przetwarzania informacji niejawnych;
3) innych zagadnień w zakresie stanu zabezpieczenia informacji niejawnych określonych przez zarządzającego kontrolę.

11. Kontrolę doraźną zarządzają i prowadzą według potrzeb lub niezwłocznie po uzyskaniu informacji mających istotny wpływ na stan zabezpieczenia informacji niejawnych, a także w związku z koniecznością uzyskania informacji o aktualnym stanie realizacji zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli problemowych:

1) pełnomocnik Ministra Obrony Narodowej do spraw ochrony informacji niejawnych w jednostkach i komórkach organizacyjnych z wyłączeniem uczelni wojskowych;
2) pełnomocnik ochrony w jednostce organizacyjnej;
3) kierownicy jednostek w podległych im jednostkach organizacyjnych;
4) przełożeni wobec podwładnych.

12. Z przeprowadzonej kontroli doraźnej kontrolujący sporządza meldunek, który przedkłada przełożonemu. Wzór meldunku określa załącznik Nr 2 do decyzji. W przypadku gdy kierownik jednostki organizacyjnej zarządzi kontrolę doraźną w podległej jednostce, nie ma obowiązku składania meldunku swojemu przełożonemu z przeprowadzonej kontroli.

13. O wynikach kontroli doraźnych, prowadzonych przez pion ochrony, powiadamia się przełożonych osób kontrolowanych zapoznając ich z meldunkiem z kontroli.

Rozdział 3

Kontrola okresowa

14. Kontrola okresowa jest zasadniczą formą sprawdzenia ewidencji, materiałów i obiegu dokumentów niejawnych w jednostce organizacyjnej. Zakres przedmiotowy kontroli okresowej określa załącznik Nr 3 do decyzji.

15. Kontrolę okresową ewidencji, materiałów i obiegu dokumentów niejawnych za rok poprzedni prowadzi się raz w roku od połowy grudnia tego roku do końca lutego roku następnego, za której przeprowadzenie odpowiada pełnomocnik ochrony.

16. W czasie trwania kontroli okresowej w jednostce organizacyjnej nie prowadzi się innych kontroli stanu zabezpieczenia informacji niejawnych.

17. Kontrolę okresową przeprowadza komisja wyznaczona w rozkazie dziennym lub decyzji kierownika jednostki organizacyjnej, z uwzględnieniem następujących zasad:
1) skład osobowy komisji powinien wynosić co najmniej trzy osoby, a w przypadkach uzasadnionych względami organizacyjnymi komisja może składać się z co najmniej dwuosobowych podkomisji;
2) osoby wchodzące w skład komisji muszą spełniać wymagania zawarte w pkt 8;
3) ostateczne zniszczenie wcześniej wydzielonych podczas brakowania materiałów powinno być realizowane przez co najmniej trzech członków komisji (podkomisji);
4) zasady brakowania i zniszczenia materiałów niejawnych określają odrębne przepisy;
5) do składu komisji nie wyznacza się osób odpowiedzialnych za prowadzenie ewidencji materiałów niejawnych w jednostkach organizacyjnych objętych kontrolą, z zastrzeżeniem ppkt 6;
6) przepisy ppkt 5 nie dotyczą dokumentów niejawnych Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i innych organizacji międzynarodowych oznaczonych kategoriami specjalnymi.

18. Kontrolę okresową w Ministerstwie Obrony Narodowej przeprowadza komisja wyznaczona decyzją Ministra Obrony Narodowej.

19. Decyzja albo rozkaz, o których mowa w pkt 17 i 18 powinny zawierać w szczególności następujące dane:
1) imienny skład osobowy komisji z uwzględnieniem numerów poświadczeń bezpieczeństwa, poświadczeń bezpieczeństwa lub certyfikatów bezpieczeństwa w zakresie dostępu do informacji Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej lub innych organizacji międzynarodowych, ich klauzul oraz terminów ważności, imiennych upoważnień do informacji niejawnych o klauzuli „zastrzeżone”;
2) termin rozliczenia wykonawców z materiałów niejawnych;
3) termin przygotowania do kontroli okresowej kancelarii tajnych, oraz innych komórek przechowujących i prowadzących ewidencję materiałów niejawnych;
4) termin rozpoczęcia i zakończenia kontroli okresowej.

20. Pełnomocnik do spraw ochrony informacji niejawnych odpowiada za organizację i przebieg kontroli okresowej w jednostce organizacyjnej, a w szczególności za:
1) opracowanie projektu rozkazu albo decyzji, o których mowa w pkt 17 i 18;
2) na podstawie opracowanego konspektu, zatwierdzonego przez kierownika jednostki organizacyjnej przeprowadzenie szkolenia członków komisji kontroli okresowej w zakresie metodyki prowadzenia kontroli; a także kierowników kancelarii tajnych oraz innych komórek przechowujących i prowadzących ewidencję materiałów niejawnych, w zakresie przygotowania tych komórek do kontroli okresowej;
3) sprawowanie nadzoru służbowego nad realizacją czynności kontrolnych wykonywanych przez komisję.

21. Wyniki kontroli okresowej komisje oraz podkomisje, o których mowa w pkt 17 i 18, dokumentują w protokole, którego układ przedstawia załącznik Nr 4 do decyzji. Kierownik jednostki lub komórki organizacyjnej, potwierdza swoim podpisem na protokole fakt zapoznania się z jego treścią.

22. Wyniki kontroli okresowej stanu zabezpieczenia informacji niejawnych przeprowadzonej w jednostce organizacyjnej jej kierownik przedkłada do dnia 15 marca swojemu bezpośredniemu przełożonemu w formie meldunku. Meldunek winien zawierać informacje o zgodności lub niezgodności stanu faktycznego materiałów niejawnych i pieczęci ze stanem ewidencyjnym oraz zasadnicze uwagi stwierdzone przez komisję w czasie kontroli.

23. Kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej oraz przewodniczący komisji, o której mowa w pkt 18, przedkładają Ministrowi Obrony Narodowej meldunki o wynikach kontroli okresowej stanu zabezpieczenia informacji niejawnych za pośrednictwem Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

24. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych przedkłada Ministrowi Obrony Narodowej do dnia 1 kwietnia meldunek zbiorczy o wynikach kontroli okresowej stanu zabezpieczenia informacji niejawnych, przeprowadzonej w Ministerstwie Obrony Narodowej oraz jednostkach organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej.

Rozdział 4

Kontrola problemowa

25. Kontrola problemowa jest podstawową formą sprawdzania stanu zabezpieczenia informacji niejawnych w jednostkach i komórkach organizacyjnych.

26. Minister Obrony Narodowej zarządza przeprowadzenie kontroli problemowych stanu zabezpieczenia informacji niejawnych w jednostkach i komórkach organizacyjnych resortu obrony narodowej. Do zarządzania i przeprowadzania kontroli problemowych są uprawnieni ponadto:

1) Szef Sztabu Generalnego Wojska Polskiego w jednostkach organizacyjnych jemu podporządkowanych;
2) Dowódcy rodzajów Sił Zbrojnych, Dowódca Operacyjny Sił Zbrojnych, Szef Inspektoratu Wsparcia Sił Zbrojnych, Szef Inspektoratu Wojskowej Służby Zdrowia, Szef Inspektoratu Uzbrojenia, Dowódca Garnizonu Warszawa, Komendant Główny Żandarmerii Wojskowej, dowódcy okręgów wojskowych, korpusów, dywizji (równorzędnych) — w podległych jednostkach organizacyjnych;
3) Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych — w jednostkach i komórkach organizacyjnych resortu obrony narodowej, z wyłączeniem uczelni wojskowych.

27. Kontrole problemowe stanu zabezpieczenia informacji niejawnych przeprowadzają zespoły, jako organy kontroli upoważnione przez osoby, o których mowa w pkt 26.

28. Kontrola problemowa stanu zabezpieczenia informacji niejawnych jest prowadzona w celu dokonania oceny:

1) stanu realizacji zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli stanu zabezpieczenia informacji niejawnych;
2) stanu zabezpieczenia informacji niejawnych;
3) organizacji i funkcjonowania systemu ochrony fizycznej informacji niejawnych jednostki organizacyjnej;
4) bezpieczeństwa teleinformatycznego;
5) przestrzegania przepisów o ochronie informacji niejawnych.

29. Szczegółowy zakres przedmiotowy kontroli problemowej stanu zabezpieczenia informacji niejawnych określa załącznik Nr 5 do decyzji. W uzasadnionych przypadkach, osoby zarządzające kontrolę mogą ograniczyć jej zakres.

30. Kontrolę problemową przeprowadza się zgodnie z rocznym planem kontroli. W przypadkach wskazujących na występowanie istotnych zagrożeń dla systemu ochrony informacji niejawnych, osoby wymienione w pkt 26 mogą zarządzić kontrolę nieujętą w planie.

31. Planowanie kontroli problemowych stanu zabezpieczenia informacji niejawnych koordynuje Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

32. Pełnomocnicy do spraw ochrony informacji niejawnych dowódców rodzajów Sił Zbrojnych, Dowódcy Operacyjnego Sił Zbrojnych, Szefa Inspektoratu Wsparcia Sił Zbrojnych, Szefa Inspektoratu Wojskowej Służby Zdrowia, Szef Inspektoratu Uzbrojenia, Dowódcy Garnizonu Warszawa, Komendanta Głównego Żandarmerii Wojskowej informują do dnia 1 września Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych o planowanych w następnym roku kalendarzowym, we wszystkich podległych jednostkach organizacyjnych kontrolach problemowych stanu zabezpieczenia informacji niejawnych.

33. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, jako koordynator zamierzeń kontrolnych, ma prawo dokonywania zmian terminów planowanych przedsięwzięć kontrolnych, po uzgodnieniu z osobami, o których

mowa w pkt 32. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych informuje Służbę Kontrwywiadu Wojskowego do dnia 1 października o planowanych w następnym roku kalendarzowym kontrolach stanu zabezpieczenia informacji niejawnych.

34. Czas trwania kontroli problemowej ustala każdorazowo zarządzający kontrolę — w zależności od potrzeb.

35. Podstawę do przeprowadzenia kontroli problemowej stanu ochrony informacji niejawnych stanowi plan jej przeprowadzenia, zatwierdzony przez osobę, o której mowa w pkt 26.

36. Kierownik kontrolowanej jednostki (komórki) organizacyjnej zapewnia kontrolującym warunki i środki niezbędne do sprawnego przeprowadzenia kontroli problemowej.

37. Kontrola problemowa kończy się omówieniem, którego czas i tryb prowadzenia oraz uczestników ustala przewodniczący zespołu kontrolującego.

38. Przewodniczący zespołu kontrolującego dokonuje wpisu w książce kontroli kontrolowanej jednostki (komórki) organizacyjnej.

39. Wyniki kontroli dokumentuje się w protokole, który powinien zawierać:
1) podstawę prawną przeprowadzenia kontroli problemowej;
2) imienny skład zespołu kontrolującego wraz z numerami i datą ważności upoważnień do przeprowadzenia kontroli problemowej;
3) termin rozpoczęcia i zakończenia kontroli;
4) zakres przedmiotowy kontroli;
5) oznaczenie kontrolowanej jednostki (komórki) organizacyjnej, jej siedzibę i adres, a także nazwę nadrzędnej jednostki organizacyjnej;
6) stopień, imię i nazwisko, nazwę stanowiska kierownika jednostki (komórki) kontrolowanej, datę objęcia stanowiska z podstawą prawną, zakres dostępu do informacji niejawnych — Nr i daty ważności wydanych poświadczeń bezpieczeństwa;
7) stopień, imię i nazwisko, nazwę stanowiska poprzedniego kierownika jednostki (komórki) kontrolowanej — okres pełnienia obowiązków — jeżeli nieprawidłowości w zakresie stanu zabezpieczenia informacji niejawnych zaistniały w tym czasie;
8) stopień, imię i nazwisko, nazwę stanowiska pełnomocnika ochrony i pozostałych osób pionu ochrony jednostki kontrolowanej, datę objęcia stanowiska z podstawą prawną, zakres dostępu do informacji niejawnych — numer i datę ważności wydanych poświadczeń bezpieczeństwa, a także zaświadczeń o przeszkoleniu w zakresie ochrony informacji niejawnych;
9) stan realizacji zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli stanu zabezpieczenia informacji niejawnych;
10) opis stanu faktycznego stwierdzonego w czasie kontroli, w tym ustalone nieprawidłowości i przyczyny ich powstania, osoby za to odpowiedzialne, wnioski oraz zalecenia pokontrolne;
11) pouczenie o prawie, sposobie i terminie zgłoszenia zastrzeżeń do ustaleń zawartych w protokole kontroli;
12) parafy umieszczone na każdej stronie protokołu przewodniczącego zespołu kontrolującego i kierownika kontrolowanej jednostki (komórki) organizacyjnej, a w razie jego nieobecności osoby czasowo pełniącej jego obowiązki;
13) podpisy na ostatniej stronie protokołu przewodniczącego zespołu kontrolującego i kierownika kontrolowanej jednostki (komórki) organizacyjnej, a w razie jego nieobecności osoby pełniącej jego obowiązki oraz miejsce i datę podpisania protokołu kontroli.

40. W przypadku gdy protokół kontroli zawiera informacje niejawne, protokół oznacza się odpowiednią klauzulą tajności, o nadaniu której decyduje przewodniczący zespołu kontrolującego.

41. Protokół, o którym mowa w pkt 39, sporządza się w trzech jednobrzmiących egzemplarzach, z przeznaczeniem dla:
1) zarządzającego kontrolę;
2) kierownika kontrolowanej jednostki (komórki) organizacyjnej;
3) przełożonego kierownika kontrolowanej jednostki (komórki) organizacyjnej;
4) w przypadku gdy zarządzającym kontrolę jest przełożony kierownika jednostki kontrolowanej, protokół sporządza się w dwóch jednobrzmiących egzemplarzach.

42. Termin przekazania protokołu kierownikowi kontrolowanej jednostki (komórki) organizacyjnej nie powinien być dłuższy niż 30 dni od dnia zakończenia czynności kontrolnych.

43. Kierownik kontrolowanej jednostki (komórki) organizacyjnej w terminie do 30 dni od daty otrzymania protokołu, lub po ustaniu trybu odwoławczego od protokołu z kontroli problemowej, zawiadamia w formie pisemnej jednostkę nadrzędną oraz informuje organ prowadzący kontrolę o sposobie wykorzystania uwag i wniosków w działalności służbowej, a także usunięcia nieprawidłowości i podjęciu działań zmierzających do zapobieżenia ich występowania, a także przyczynach ewentualnego niewykonania zaleceń z kontroli.

44. Bezpośredni przełożony jednostki, w której prowadzona była kontrola problemowa zobowiązany jest, w terminie do 30 dni od daty otrzymania meldunku o usunięciu nieprawidłowości, do podjęcia decyzji w sprawie przeprowadzenia w niej kontroli doraźnej w celu sprawdzenia usunięcia nieprawidłowości stwierdzonych podczas kontroli problemowej, a o jej wynikach informuje zarządzającego tą kontrolę.

45. Wszystkie dokumenty dotyczące kontroli problemowej włącza się do akt kontroli, którym nadaje klauzulę tajności przewodniczący zespołu kontrolnego, zgodnie z obowiązującymi w tym zakresie przepisami.

46. Zarządzający kontrolę, na podstawie zebranych wyników z przeprowadzonych kontroli problemowych, dokonuje analizy w celu określenia zmian w regulacjach prawnych, a także w zakresie poprawy organizacji i sytemu ochrony informacji niejawnych w podległych jednostkach organizacyjnych lub przez nich nadzorowanych.

47. W zakresie nieuregulowanym w decyzji, do planowania, koordynowania, przeprowadzania i dokumentowania wyników kontroli problemowych stanu ochrony informacji niejawnych oraz postępowania pokontrolnego stosuje się przepisy decyzji Ministra Obrony Narodowej w sprawie działalności kontrolnej w resorcie obrony narodowej.

Rozdział 5

Ocena stanu zabezpieczenia informacji niejawnych

48. Kierownicy jednostek organizacyjnych opracowują ocenę stanu zabezpieczenia 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.

49. Ocenę stanu zabezpieczenia informacji niejawnych w Ministerstwie Obrony Narodowej opracowuje Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

50. Ocenę, o której mowa w pkt 48 i 49, opracowuje się na podstawie:
1) wyników kontroli stanu zabezpieczenia informacji niejawnych przeprowadzonych w jednostkach lub komórkach organizacyjnych;
2) meldunków o naruszeniu przepisów o ochronie informacji niejawnych.

51. Ocena stanu zabezpieczenia informacji niejawnych powinna obejmować:
1) rozwiązania systemowe w jednostce organizacyjnej, dotyczące działań, przy udziale jednostek nadrzędnych, a także innych instytucji wspomagających, zaniechania ewentualnych — realnych zagrożeń lub ich wykluczenia, wynikających między innymi z oceny zarządzania ryzykiem bezpieczeństwa informacji niejawnych;
2) organizację systemu ochrony informacji niejawnych;
3) funkcjonowanie systemu ochrony informacji niejawnych;
4) wnioski i propozycje, potrzeby, przyczyny nie realizowania niektórych zadań;
5) układ i szczegółową treść oceny określa załącznik Nr 6 do decyzji.

52. Klauzulę tajności ocenie stanu zabezpieczenia informacji niejawnych nadaje osoba, która jest uprawniona do jej podpisania.

53. Ocenę stanu zabezpieczenia informacji niejawnych za poprzedni rok kalendarzowy omawia się na posiedzeniu kierownictwa jednostki organizacyjnej oraz przesyła do dnia 31 marca bezpośredniemu przełożonemu.

54. Kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych:
1) Ministrowi Obrony Narodowej;
2) Sekretarzowi Stanu w Ministerstwie Obrony Narodowej, podsekretarzom stanu w Ministerstwie Obrony Narodowej, Dyrektorowi Generalnemu Ministerstwa Obrony Narodowej, Szefowi Sztabu Generalnego Wojska Polskiego;
3) dyrektorom (szefom) komórek organizacyjnych Ministerstwa Obrony Narodowej;
4) szefom komórek organizacyjnych tworzących Sztab Generalny Wojska Polskiego,

przesyłają do dnia 30 kwietnia ocenę za poprzedni rok kalendarzowy za swoją jednostkę organizacyjną wraz z ocenami zebranymi ze wszystkich podległych jednostek organizacyjnych Szefowi Służby Kontrwywiadu Wojskowego i Pełnomocnikowi Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych.

55. Pełnomocnik Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych do dnia 15 maja przedstawia Ministrowi Obrony Narodowej i Szefowi Służby Kontrwywiadu Wojskowego ocenę, o której mowa w pkt 48.

56. Szef Służby Kontrwywiadu Wojskowego, corocznie do dnia 15 czerwca, przygotowuje informację o stanie zabezpieczenia informacji niejawnych w resorcie obrony narodowej za poprzedni rok kalendarzowy i przedstawia ją Ministrowi Obrony Narodowej.

Rozdział 6

Postanowienia końcowe

57. Traci moc decyzja Nr 20/MON Ministra Obrony Narodowej z dnia 21 stycznia 2010 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (Dz. Urz. MON Nr 1, poz. 7).

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

Minister Obrony Narodowej:

wz. Sekretarz Stanu
do Spraw Społecznych i Profesjonalizacji: *Cz. Piątas*

Załączniki do decyzji Nr 165/MON
Ministra Obrony Narodowej
z dnia 29 kwietnia 2011 r. (poz. 127)

Załącznik Nr 1

WZÓR

.....
(nazwa organu zarządzającego kontrolę)

dnia .....

Upoważnienie Nr .....

Na podstawie pkt ..decyzji Nr ../MON Ministra Obrony Narodowej z dnia …… 2011 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (Dz. Urz. MON Nr …, poz. ….)

upoważniam:

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

do przeprowadzania kontroli (*tu wpisać rodzaj kontroli*) stanu zabezpieczenia informacji niejawnych w:

.....
(nazwa i adres kontrolowanej jednostki/komórki organizacyjnej)

Upoważnienie ważne jest za okazaniem legitymacji służbowej (dowodu osobistego).

Ważność upoważnienia upływa z dniem ……

(m.p)

pieczęć okrągła
organu zarządzającego kontrolę

.....
(stanowisko, stopień, imię i nazwisko,
podpis osoby wydającej upoważnienie)

Ważność upoważnienia przedłuża się do dnia ……..

(m.p)

pieczęć okrągła
organu zarządzającego kontrolę

.....
(stanowisko, stopień, imię i nazwisko,
podpis osoby wydającej upoważnienie)

Załącznik Nr 2

WZÓR

Miejscowość, data

NAZWA STANOWISKA ADRESATA

MELDUNEK

w sprawie kontroli doraźnej stanu zabezpieczenia informacji niejawnych

Melduję, że na podstawie pkt … ppkt … decyzji Nr …./MON Ministra Obrony Narodowej z dnia ……. 2011 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (Dz. Urz. MON Nr …, poz. ….) przeprowadziłem(am) w dniach ..... kontrolę doraźną stanu zabezpieczenia informacji niejawnych w:

.....
(nazwa komórki (jednostki) organizacyjnej)

Kontrolą objęto następujące zagadnienia:
- (*wymienić zagadnienia poddane kontroli- opcjonalnie, jeśli polecono sprawdzenie innych niż kontrola stanu faktycznego materiałów niejawnych oraz pieczęci*),
- stan faktyczny materiałów niejawnych oraz pieczęci,
- wykonanie zaleceń pokontrolnych poprzednich kontroli (*wpisać, jakich*),

oraz następujące osoby:
- (*wymienić nazwiska osób, które skontrolowano*);
- .....

Na podstawie wyników kontroli stwierdzono, iż:

1. (*opis ustaleń kontroli zgodny z celami i zakresem kontroli)*
2. Stan faktyczny materiałów niejawnych oraz pieczęci pobranych przez kontrolowane osoby jest zgodny ze stanem ewidencyjnym (*w razie stwierdzenia braku dokumentów należy podać ich klauzulę, numery ewidencyjne, nazwy dokumentów lub, czego dotyczą, przez kogo zostały pobrane, datę pobrania oraz okoliczności utraty*).
3. Występują następujące niedociągnięcia w zakresie przestrzegania przepisów o ochronie informacji niejawnych dotyczących przetwarzania dokumentów niejawnych (*wymienić niedociągnięcia, nazwiska osób komórek, u których występują, przyczyny ich powstania, skutki oraz określić osoby odpowiedzialne*):
   - .....
   - .....
4. Wnioski i zalecenia pokontrolne.

nazwa stanowiska służbowego osoby funkcyjnej

.....
(podpis osoby kontrolującej)

Opcjonalnie*: „Z meldunkiem zapoznałem się”:

data i podpis przełożonego osoby kontrolowanej

*- w przypadku kontroli prowadzonej przez pełnomocnika ochrony

Załącznik Nr 3

ZAKRES
przedmiotowy kontroli okresowej ewidencji, materiałów i obiegu dokumentów niejawnych

1. Sprawdzenie stanu przestrzegania zasad postępowania z materiałami niejawnymi w kancelariach tajnych i innych komórkach, w których są przechowywane, ewidencjonowane i udostępniane materiały niejawne:

1.1. szczegółowe sprawdzenie stanu faktycznego materiałów niejawnych przechowywanych w kancelariach tajnych i innych komórkach, w których są przetwarzane materiały niejawne oraz porównanie ze stanem ewidencyjnym z wyłączeniem teczek akt postępowań sprawdzających, w tym:
   a) materiałów niejawnych ujętych w RTD za lata poprzednie, w których prowadzono kontrolę roczną lub okresową,
   b) materiałów niejawnych ujętych we wszystkich urządzeniach ewidencyjnych w ostatnim roku.

1.2. przestrzeganie zasad przetwarzania materiałów niejawnych.

1.3. przestrzeganie obowiązku dokumentowania faktu zapoznania się z informacjami niejawnymi oznaczonymi klauzulą „ściśle tajne” i „tajne”.

2. Sprawdzenie stanu przestrzegania zasad postępowania z materiałami niejawnymi przez wykonawców:

— szczegółowe sprawdzenie i porównanie ze stanem ewidencyjnym materiałów niejawnych pobranych przez wykonawców.

3. Zniszczenie uprzednio zakwalifikowanych przez uprawnione osoby materiałów niejawnych.

4. Sprawdzenie stanu faktycznego pieczęci jednostki organizacyjnej oraz porównanie go ze stanem ewidencyjnym.

Załącznik Nr 4

WZÓR

PROTOKÓŁ

z kontroli okresowej ewidencji, materiałów i obiegu dokumentów niejawnych

1. Część ogólna:

Powołana rozkazem (*decyzją*) Nr (*numer i data wydania rozkazu dziennego albo decyzji kierownika jednostki organizacyjnej)* w sprawie przeprowadzenia kontroli okresowej **ewidencji, materiałów i obiegu dokumentów niejawnych** za rok …….... w (*nazwa jednostki organizacyjnej*) komisja w składzie:

(*stopnie wojskowe, imiona, nazwiska członków komisji (podkomisji), numery, klauzule tajności oraz terminy ważności poświadczeń bezpieczeństwa, poświadczeń bezpieczeństwa lub certyfikatów bezpieczeństwa w zakresie dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej lub innych organizacji międzynarodowych, a także imiennych upoważnień do informacji niejawnych o klauzuli „zastrzeżone";*

przeprowadziła w dniach *(wpisać datę rozpoczęcia ÷ datę zakończenia)* kontrolę **ewidencji, materiałów i obiegu dokumentów niejawnych**

Kontrolą objęto następujące komórki organizacyjne *(komórki wewnętrzne)*:

(*wymienić komórki organizacyjne (komórki wewnętrzne) objęte kontrolą*).

2. Część merytoryczna:

1) Stan faktyczny materiałów niejawnych przetwarzanych lub przekazanych przez kontrolowane komórki organizacyjne sprawdzono na podstawie nw. dokumentów Kancelarii Tajnej (*nazwa kancelarii*): (*wyszczególnienie nazw urządzeń ewidencyjnych oraz pozycji zapisów w tych urządzeniach, na podstawie, których sprawdzono stan faktyczny materiałów niejawnych przetwarzanych lub przekazanych przez jednostkę organizacyjną*)
   a) Rejestr teczek dokumentów niejawnych, dzienników i książek ewidencyjnych:
      – za rok ….. poz. (*od pozycji pierwszej do ostatniej*),
      – za rok ….. poz. (*od pozycji pierwszej do ostatniej*),
   b) Dziennik korespondencji Nr wg RTD ……. – poz. (*od pozycji pierwszej do ostatniej*),
   c) Skorowidz rejestru wydanych dokumentów Nr wg RTD ……. – poz. (*od pozycji pierwszej do ostatniej*),
   d) Dzienniki ewidencji wykonanych dokumentów Nr wg RTD…… – poz. (*od pozycji pierwszej do ostatniej za ostatni rok kalendarzowy*),
   e) Książka ewidencji pieczęci Nr wg RTD …….. ,
   f) Książka ewidencji wydawnictw i inne urządzenia ewidencyjne;

2) Dane dotyczące stanu faktycznego materiałów niejawnych:
   a) Stan faktyczny materiałów niejawnych oraz pieczęci w (*nazwy wewnętrznych komórek organizacyjnych)* jest zgodny ze stanem ewidencyjnym. (*zgodność lub niezgodność stanu faktycznego materiałów niejawnych oraz pieczęci ze stanem ewidencyjnym)*,
   b) W (*nazwy wewnętrznych komórek organizacyjnych*) nie okazano do kontroli następujących materiałów niejawnych:
      (wyszczególnienie brakujących materiałów / nieprzedstawionych do kontroli, utraconych lub uznanych za utracone), z podaniem ich klauzuli tajności, tytułu lub czego dotyczą, numerów ewidencyjnych oraz nazwisk osób, które

Załącznik Nr 4 (cd.)

je pobrały ze wskazaniem przyczyn, okoliczności i skutków utraty oraz czynności podjętych przez komisję w celu ich odszukania);

3) Przestrzeganie zasady selektywnego udostępniania informacji niejawnych oraz dokumentowania faktu zapoznania się z materiałami zawierającymi informacje niejawne oznaczone klauzulą „ściśle tajne" i „tajne*" (nie stwierdzono naruszenia zasad postępowania z dokumentami zawierającymi takie informacje niejawne – w innym przypadku opisać stwierdzone naruszenia zasad);*
4) Przestrzeganie zasad przechowywania oraz przekazywania materiałów niejawnych*(nie stwierdzono naruszenia zasad przechowywania oraz przekazywania dokumentów zawierającymi informacje niejawne oznaczone klauzulą „ściśle tajne" i „tajne" – w innym przypadku opisać stwierdzone naruszenia zasad);*
5) Ogólna ocena przestrzegania przepisów o ochronie informacji niejawnych w jednostce albo komórce organizacyjnej (*opisowo przedstawić, na jakim poziomie przestrzega się przepisów o ochronie informacji niejawnych*);
6) Wnioski i zalecenia pokontrolne.

3 W załącznikach:

1) Wykaz materiałów niejawnych i pieczęci zniszczonych przez komisję kontroli okresowej;
2) Wyszczególnienie numerów materiałów niejawnych, które nie zostały podszyte do właściwych teczek akt oraz nie zostały przerejestrowane na rok następny.

4 Podpisy członków komisji (podkomisji).

(stopień, imię i nazwisko) ……

(stopień, imię i nazwisko) ……

(stopień, imię i nazwisko) ……

5 Podpis kierownika jednostki organizacyjnej (*kierowników komórek organizacyjnych****), potwierdzający fakt zapoznania się z protokołem z kontroli okresowej stanu ochrony informacji niejawnych**.

„Z protokołem zapoznałem się":

(*stopień, imię i nazwisko)* *(data)* ……

*- tylko w Ministerstwie Obrony Narodowej.

Załącznik Nr 5

SZCZEGÓŁOWY ZAKRES

przedmiotowy kontroli problemowej stanu zabezpieczenia informacji niejawnych

1. OCHRONA INFORMACJI NIEJAWNYCH.

1.1. Planowanie i organizacja systemu ochrony informacji niejawnych.

a) spójność dokumentów normatywnych wydanych przez kierownika kontrolowanej jednostki organizacyjnej z aktami prawnymi oraz normatywnymi szczebli nadrzędnych,
b) sprecyzowanie zadań, dotyczących ochrony informacji niejawnych, w zakresach zadań oraz zakresach obowiązków osób funkcyjnych,
c) reagowanie na fakty naruszania przepisów o ochronie informacji niejawnych, utraty dokumentów niejawnych oraz ujawnienia informacji niejawnych osobom nieupoważnionym,
d) instrukcja „Sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone” oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony”,
e) określenie sposobu i trybu przetwarzania informacji niejawnych o klauzuli „poufne” w podległych komórkach organizacyjnych,
f) dokumentacja określająca poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą,
g) zatwierdzony przez kierownika jednostki organizacyjnej plan ochrony informacji niejawnych, w tym postępowanie z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego, a także sposób ich realizacji,
h) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka,
i) ujęcie w planie zasadniczych przedsięwzięć jednostki organizacyjnej zadań pionu ochrony,
j) sporządzenie przez pełnomocnika ochrony planu kontroli problemowych w zakresie stanu zabezpieczenia informacji niejawnych w jednostkach organizacyjnych wyszczególnionych w rozdziale 4 pkt 26.

1.2. Dostęp do informacji niejawnych.

a) prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto,
b) prowadzenie wykazu osób, które uzyskały pisemne upoważnienie wydane przez kierownika jednostki organizacyjnej na udostępnienie informacji niejawnych o klauzuli „zastrzeżone”,
c) przestrzeganie terminu informowania organu, który wydał poświadczenie bezpieczeństwa oraz Służby Kontrwywiadu Wojskowego o zatrudnieniu na stanowisku osoby legitymującej się odpowiednim poświadczeniem bezpieczeństwa,
d) ewidencja, przechowywanie i archiwizowanie akt postępowań sprawdzających,
e) przestrzeganie przepisów w zakresie upoważniania osób do dostępu do informacji niejawnych.

1.3. Planowanie i realizacja szkolenia z zakresu ochrony informacji niejawnych.

a) szkolenie podstawowe i uzupełniające kadry i pracowników oraz specjalistyczne w zakresie ochrony informacji niejawnych,
b) rejestr wydanych zaświadczeń o przeszkoleniu,

Załącznik Nr 5 (cd.)

c) programy szkolenia oraz prowadzenie ewidencji szkoleniowej,
d) plan szkolenia uzupełniającego.

1.4. Sprawowanie nadzoru nad ochroną informacji niejawnych.
a) realizacja zaleceń pokontrolnych z kontroli stanu zabezpieczenia informacji niejawnych przeprowadzonych w jednostce organizacyjnej,
b) prowadzenie nadzoru służbowego w zakresie stanu zabezpieczenia informacji niejawnych oraz dokumentowanie jego wyników,
c) wartość merytoryczna przeprowadzonych w jednostce organizacyjnej ocen stanu zabezpieczenia informacji niejawnych.

1.5. Znajomość przepisów o ochronie informacji niejawnych — test.

1.6. Działalność kancelarii tajnej oraz tajnej zagranicznej (międzynarodowej).
a) stan zabezpieczenia oraz wyposażenie pomieszczeń kancelaryjnych,
b) fizyczne oddzielenie materiałów o różnych klauzulach tajności oraz przestrzeganie zasady przechowywania dokumentów uzyskanych w ramach realizacji porozumień międzynarodowych odrębnie dla każdego państwa i organizacji międzynarodowej,
c) przygotowanie specjalistyczne kierownika, jego zastępcy oraz pracowników kancelarii tajnej,
d) organizacja pracy kancelarii, zakresy działania osób funkcyjnych,
e) przestrzeganie zasad ewidencjonowania dokumentów,
f) przestrzeganie zasad wydawania, rozliczania i obiegu dokumentów niejawnych, a także adresowania, zabezpieczania i ekspedycji przesyłek,
g) prowadzenie wykazu osób upoważnionych do dostępu do informacji niejawnych oraz jego bieżąca aktualizacja,
h) przestrzeganie zasad kompletowania i brakowania akt oraz niszczenia dokumentów niejawnych,
i) dokonywanie zmian klauzul tajności na materiałach niejawnych oraz w urządzeniach ewidencyjnych,
j) organizowanie kancelarii ćwiczebnej, ewidencjonowanie, obieg i rozliczanie dokumentów ćwiczebnych,
k) przygotowanie kancelarii tajnej do realizacji zadań na czas „W".

1.7. Postępowanie z materiałami niejawnymi w innych komórkach przechowujących oraz prowadzących ewidencję materiałów niejawnych. Postępowanie wykonawców z informacjami niejawnymi.
a) zabezpieczenie i wyposażenie pomieszczeń, w których są przechowywane materiały niejawne,
b) przeszkolenie specjalistyczne personelu,
c) prowadzenie ewidencji materiałów niejawnych,
d) prowadzenie oraz bieżąca aktualizacja wykazu osób upoważnionych do dostępu do informacji niejawnych,
e) przestrzeganie zasad przechowywania, udostępniania i niszczenia materiałów niejawnych,
f) przestrzeganie przepisów w zakresie przechowywania i przekazywania informacji niejawnych,
g) terminowość rozliczania się wykonawców z wytworzonych materiałów niejawnych.

1.8. Klasyfikowanie materiałów niejawnych, w tym sposób ich wytwarzania, przetwarzania, ewidencji, oznaczania i niszczenia.
a) przestrzeganie zasad klasyfikowania informacji niejawnych oraz oznaczania dokumentów, w tym klauzulami tajności,
b) niszczenie materiałów niejawnych,
c) aktualizacja klauzul tajności na materiałach niejawnych oraz w urządzeniach ewidencyjnych.

Załącznik Nr 5 (cd.)

1.9. Bezpieczeństwo przemysłowe.
   a) prowadzenie ewidencji przedsiębiorców realizujących na rzecz jednostki organizacyjnej umowy lub zadania związane z dostępem do informacji niejawnych,
   b) opracowanie Instrukcji Bezpieczeństwa Przemysłowego — jako integralnej części umowy,
   c) sprawowanie nadzoru nad realizacją umowy, z wykonaniem której wiąże się dostęp do informacji niejawnych.

2. ORGANIZACJA I PRZYGOTOWANIE ORAZ FUNKCJONOWANIE SYSTEMU OCHRONY FIZYCZNEJ INFORMACJI NIEJAWNYCH.

2.1. Planowanie systemu ochrony fizycznej informacji niejawnych.
   a) organizacja ochrony informacji niejawnych na podstawie planu ochrony informacji niejawnych jednostki organizacyjnej,
   b) opracowanie decyzji (rozkazu) w sprawie organizacji systemu przepustkowego w jednostce organizacyjnej,
   c) opracowanie dokumentacji dla sił ochronnych i służb dyżurnych,
   d) opracowywanie analiz zagrożeń,
   e) organizacja współdziałania w zakresie ochrony informacji niejawnych z organami Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, Policji oraz innymi organami porządkowymi.

2.2. Organizacja ochrony konwojowanego mienia.
   a) opracowanie instrukcji konwojowania materiałów niejawnych,
   b) opracowanie planu przeprowadzenia konwoju;

2.3. Funkcjonowanie ochrony fizycznej informacji niejawnych, poziom wyszkolenia sił ochronnych.
   a) pełnienie służby wartowniczej (ochronnej), wewnętrznej lub garnizonowej, portierów i dozorców,
   b) wyposażenie sił ochronnych i służb dyżurnych w należny sprzęt i uzbrojenie,
   c) organizacja systemu ochrony fizycznej informacji niejawnych w godzinach służbowych i po godzinach służbowych oraz w dniach wolnych od zajęć służbowych,
   d) wyznaczenie i zabezpieczenie stref ochronnych,
   e) poziom wyszkolenia sił ochronnych, służb dyżurnych, wart oraz osób funkcyjnych.

2.4. Funkcjonowanie technicznych środków wspomagających ochronę informacji niejawnych w tym ich ilość i stan techniczny.
   a) ilość, stan techniczny i zgodność urządzeń i systemów alarmowych z parametrami określonymi w normie obronnej,
   b) sprawność urządzeń alarmowych.
   c) konserwacja systemów i urządzeń alarmowych,
   d) ilość i stan techniczny środków łączności sił ochronnych i służb dyżurnych.

2.5. Funkcjonowanie systemu przepustkowego i kontroli dostępu, przechowywanie, wydawanie i zdawanie kluczy i kodów oraz przestrzeganie zasad używania urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w strefach ochronnych.
   a) funkcjonowanie systemu przepustkowego i kontroli dostępu,
   b) określenie stref ochronnych, a także sposób ich ochrony,
   c) sposób przechowywania i zabezpieczenia kluczy użytku bieżącego i zapasowych, kodów do zamków szyfrowych oraz kodów systemów alarmowych do pomieszczeń usytuowanych w strefach ochronnych, a także znajdujących się w nich urządzeń do przechowywania dokumentów niejawnych,
   d) przestrzeganie zasad używania urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku.

Załącznik Nr 5 (cd.)

3. BEZPIECZEŃSTWO TELEINFORMATYCZNE.

3.1. Organizacja systemu bezpieczeństwa teleinformatycznego.
- a) posiadanie akredytacji bezpieczeństwa teleinformatycznego dla systemów, przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej,
- b) posiadanie zatwierdzonej przez kierownika jednostki organizacyjnej dokumentacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”.

3.2. Bezpieczeństwo osobowe użytkowników systemów teleinformatycznych.
- a) posiadanie stosownych poświadczeń bezpieczeństwa lub pisemnych upoważnień wydanych przez kierownika jednostki organizacyjnej dla użytkowników systemu,
- b) szkolenie użytkowników systemów i sieci teleinformatycznych.

3.3. Zgodność elementów systemu teleinformatycznego i realizowanych w nim czynności z ustaleniami Szczególnych Wymagań Bezpieczeństwa.
- a) oprogramowania systemowego, użytkowego i narzędziowego,
- b) konfiguracji sprzętu komputerowego,
- c) zabezpieczenia sprzętu przed nieuprawnionym dostępem,
- d) monitorowania i dokumentowania dostępu do systemu,
- e) zgodność ze Szczególnymi Wymaganiami Bezpieczeństwa zabezpieczeń oraz wyposażenia pomieszczenia systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych.

3.4. Przestrzeganie przez użytkowników przepisów o ochronie informacji przy użytkowaniu niejawnych i jawnych systemów teleinformatycznych.
- a) znajomość oraz przestrzeganie przez użytkowników postanowień Procedur Bezpiecznej Eksploatacji,
- b) wykonywanie i rozliczanie wydruków niejawnych dokumentów,
- c) przechowywanie, ewidencjonowanie, udostępnianie i niszczenie elektronicznych nośników informacji.

3.5. Sprawowanie nadzoru nad niejawnymi systemami teleinformatycznymi.
- a) wyznaczenie przez kierownika jednostki organizacyjnej administratora systemu teleinformatycznego oraz inspektora bezpieczeństwa teleinformatycznego, jak też ukończenie przez nich szkolenia specjalistycznego z zakresu bezpieczeństwa teleinformatycznego,
- b) dokumentacja inspektora bezpieczeństwa teleinformatycznego, planowanie oraz dokumentowanie kontroli zgodności funkcjonowania systemów teleinformatycznych z ich Szczególnymi Wymaganiami Bezpieczeństwa oraz Procedurami Bezpiecznej Eksploatacji.

Załącznik Nr 6

OCENA
STANU ZABEZPIECZENIA INFORMACJI NIEJAWNYCH
za rok ……

w .....
(nazwa i adres jednostki organizacyjnej)

podległej *(dowódcy/szefowi itp.)* .....
(nazwa i adres jednostki nadrzędnej)

1. Stopień, imię i nazwisko kierownika jednostki organizacyjnej, numer i klauzula posiadanego poświadczenia bezpieczeństwa – do kiedy ważne, telefon – służbowy, komórkowy – służbowy.
2. Telefon kontaktowy do służby dyżurnej jednostki organizacyjnej.
3. Nazwa inspektoratu lub ekspozytury Służby Kontrwywiadu Wojskowego wspomagających jednostkę organizacyjną.
4. Przedstawienie propozycji rozwiązań systemowych w jednostce organizacyjnej, dotyczących działań przy udziale jednostek nadrzędnych, a także innych instytucji wspomagających, zaniechania ewentualnych — realnych zagrożeń lub ich wykluczenia, wynikających między innymi z oceny zarządzania ryzykiem bezpieczeństwa informacji niejawnych.
5. Organizacja systemu ochrony informacji niejawnych, w tym:

   5.1. Struktura etatowa i stan ewidencyjny pionu ochrony, usytuowanie w strukturze jednostki organizacyjnej:

   a) Struktura pionu ochrony (w formie schematu strukturalnego),

   b) Stopień, imię i nazwisko pełnomocnika do spraw ochrony informacji niejawnych, numer i klauzula posiadanego poświadczenia bezpieczeństwa – do kiedy ważne, numer zaświadczenia o przeszkoleniu przez służbę ochrony państwa, telefon kontaktowy – służbowy, komórkowy – służbowy,

   c) Stopień, imię i nazwisko kierownika kancelarii tajnej, tajnej międzynarodowej, numer i klauzula posiadanego poświadczenia bezpieczeństwa, poświadczenia bezpieczeństwa w zakresie dostępu do informacji niejawnych NATO, UE lub innych organizacji międzynarodowych, (certyfikatów bezpieczeństwa) – do kiedy ważne, numer zaświadczenia o przeszkoleniu przez służbę ochrony państwa, telefon kontaktowy – służbowy, komórkowy – służbowy,

   d) Dane statystyczne:

Stanowisko etatowe pełnomocnika			Ilość stanowisk etatowych pionu ochrony (w tym pełnomocnik ochrony)														SUMA	UWAGI *jeżeli występują stanowiska nieetatowe, np. z planu zatrudnienia to należy wpisać w tej rubryce.
Samodzielne	Łączone z innym	Stopień etatowy	płk (kmdr)	ppłk (kmdr por.)	mjr (kmdr ppor.)	kpt. (kpt. mar.)	por. (por. mar.)	ppor. (ppor. mar.)	st. chor. szt.(st. chor. szt. mar.)	st. chor. (st. chor. mar.)	chor. (chor. mar.)	mł. chor. (mł. chor. mar.)	st. sierż. (st. bosm.)	sierż. (.bosm.)	plut. (bsmt)	stanowiska cywilne		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

   e) Czy jednostka posiada dostateczną ilość urządzeń do przechowywania materiałów niejawnych?

TAK	NIE*

*Jeżeli nie ma dostatecznej ilości urządzeń, to gdzie i w jaki sposób przechowywane są materiały niejawne.

Załącznik Nr 6 (cd.)

f) Czy pomieszczenia przeznaczone do przechowywania materiałów niejawnych (kancelaria tajna, biblioteka, kancelaria mobilizacyjna, itp.) spełniają wymagania określone w obowiązujących w tym zakresie przepisach

TAK	NIE	Jeśli NIE, to, czy szef SKW wyraził zgodę na zastosowanie alternatywnych środków bezpieczeństwa – podać Nr i datę pisma wchodzącego.

g) Sposób utylizowania odpadów uzyskanych po wstępnym niszczeniu materiałów niejawnych (gdzie, nazwa i adres podmiotu dokonującego utylizacji – posiadanie certyfikatu).

5.2. Organizacja obsługi kancelaryjnej oraz obieg dokumentów i materiałów niejawnych:

a) Obsługę kancelaryjną w zakresie materiałów niejawnych jednostki zapewnia:

Własna kancelaria tajna	Kancelaria innej jednostki	UWAGI

b) W jednostce zorganizowano (ilość): - etatowych

Kancelarie Tajne	Kancelarie Tajne Zagraniczne (Międzynarodowe)	Punkty Obsługi Dokumentów Zagranicznych (Międzynarodowych)	Biblioteki Niejawne	Inne komórki przechowujące oraz prowadzące ewidencję materiałów niejawnych (podać nazwy tych komórek wewnętrznych)

c) Łączny obieg materiałów niejawnych (w poprzednim roku kalendarzowym):

Materiały niejawne krajowe	Ściśle tajne	Tajne	Poufne	RAZEM
Wchodzące				
Wychodzące				
Materiały niejawne NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	RAZEM
Wchodzące				
Wychodzące				
Materiały niejawne UE	TOP SECRET	SECRET	CONFIDENTIAL	RAZEM
Wchodzące				
Wychodzące				
Materiały niejawne z innych państw lub organizacji międzynarodowych	Ściśle tajne*	Tajne*	Poufne*	RAZEM
Wchodzące				
Wychodzące				

* odpowiedniki klauzuli.

d) Dane statystyczne (łącznie) za jednostki organizacyjne obsługiwane w zakresie kancelaryjnym wg tabel jak wyżej z wyszczególnieniem nazw jednostek obsługiwanych– oraz z rozbiciem na poszczególne jednostki organizacyjne.

Załącznik Nr 6 (cd.)

5.3. Funkcjonowanie niejawnych systemów teleinformatycznych:

a) Czy jednostka posiada akredytowane systemy teleinformatyczne przeznaczone do przetwarzania informacji niejawnych – dotyczy to także MIL-WAN i innych systemów zastrzeżonych itp.

TAK	NIE

b) Jeśli jednostka nie posiada akredytowanych systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych, to gdzie je przetwarza?

Nie dotyczy	Użyczenie przez inną jednostkę (wpisać pełną nazwę)	Jednostka nie ma potrzeb w zakresie przetwarzania informacji niejawnych w systemach teleinformatycznych

c) Akredytowane systemy teleinformatyczne: - dotyczy to także MIL-WAN i innych systemów zastrzeżonych itp.

Lp.	Nazwa systemu	Klauzula	Data ważności akredytacji	Kto udzielił akredytacji	Ilość komputerów	UWAGI

5.4. Bezpieczeństwo przemysłowe:

a) Czy jednostka zlecała wykonanie umów lub zadań związanych z dostępem do informacji niejawnych?

TAK	NIE

b) Zawarte umowy (zadania, zlecenia) związane z dostępem do informacji niejawnych (w poprzednim roku kalendarzowym):

Lp.	Nazwa podmiotu	Klauzula przekazywanych informacji	Data zawarcia umowy	Data zakończenia umowy	Umowa dotyczy	UWAGI

6. Funkcjonowanie systemu ochrony informacji niejawnych, a zwłaszcza:

6.1. Przestrzeganie przepisów o ochronie informacji niejawnych:

a) Czy w jednostce, w poprzednim roku kalendarzowym, były incydenty zagubienia, ujawnienia lub nieuprawnionego dostępu do informacji niejawnych?

NIE	TAK	Jeśli TAK, to opisać czego incydenty dotyczyły oraz wypełnić pkt b.

b) Nieprawidłowości dotyczące zagubienia, ujawnienia lub nieuprawnionego dostępu do informacji niejawnych (ilość):

Nieprawidłowości (ilość przypadków):	Ściśle tajne	Tajne	Poufne	Zastrzeżone	Inne* międzynarodowe
Zagubienia					
Ujawnienia					
Nieuprawniony dostęp					
Inne*					

*opisać jakie.

Załącznik Nr 6 (cd.)

c) Postępowania wyjaśniające, postępowania karne i dyscyplinarne związane z naruszeniem przepisów o ochronie informacji niejawnych:

Postępowania (ilość przypadków):	Klauzula informacji, których dotyczy postępowanie					Organ prowadzący postępowanie
	Ściśle tajne	Tajne	Poufne	Zastrzeżone	Inne* międzynarodowe	
Wyjaśniające						
Dyscyplinarne						
Karne						

(Opisać wynik ww. postępowań)

6.2. Prowadzenie postępowań sprawdzających:

a) Postępowania sprawdzające w poprzednim roku kalendarzowym:

Postępowania sprawdzające	Wszczęte	Umorzenie postępowania	Zawieszenie	Zakończone	
				Wydaniem poświadczenia bezpieczeństwa	Wydaniem decyzji o odmowie wydania
Pełnomocnik					
SKW					

b) Kontrolne Postępowania sprawdzające w poprzednim roku kalendarzowym:

Kontrolne Postępowania sprawdzające	Wszczęte	Umorzenie postępowania	Zawieszenie	Zakończone	
				Cofnięciem poświadczenia bezpieczeństwa	Informacją o braku zastrzeżeń
Pełnomocnik					
SKW					

c) Stwierdzone problemy dotyczące realizacji prowadzenia postępowań sprawdzających (zwykłych i poszerzonych).

6.3. Sprawowanie nadzoru i kontroli w poprzednim roku kalendarzowym:

a) Kontrole spoza jednostki organizacyjnej (typ kontroli, organ kontrolujący, zalecenia pokontrolne i ich realizacja).

b) Przyczyny nie wykonania zaleceń pokontrolnych.

6.4. Działalność szkoleniowa:

a) Czy jednostka zgłaszała potrzeby szkoleniowe, których nie uwzględniono?

TAK	NIE	Jeśli TAK, to jakie potrzeby nie zostały uwzględnione?

b) Stwierdzone problemy dotyczące działalności szkoleniowej.

6.5. Ochrona informacji niejawnych w kontaktach zagranicznych:

a) Problemy zaistniałe podczas kontaktów zagranicznych związane z zapewnieniem ochrony informacji niejawnych.

7. Inne wnioski dotyczące zabezpieczenia informacji niejawnych w jednostce organizacyjnej.

stopień, imię, nazwisko i podpis

kierownika jednostki organizacyjnej