

Warszawa, dnia 27 sierpnia 2015 r.

Poz. 252

Departament Ochrony Informacji Niejawnych

**DECYZJA Nr 345/MON
MINISTRA OBRONY NARODOWEJ**

z dnia 27 sierpnia 2015 r.

w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa 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 oraz z 2014 r. poz. 933), w związku z § 3 ust. 2 pkt 9, § 4 ust. 1 pkt 4 oraz § 5 ust. 1 pkt 3 rozporządzenia Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. U. poz. 1660 oraz z 2015 r. poz. 236), ustala się, co następuje:

Rozdział 1

Postanowienia ogólne

1. Decyzja określa organizację, warunki i tryb sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, zwanych dalej „jednostkami organizacyjnymi”, oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej, zwanych dalej „komórkami organizacyjnymi”.
2. Przepisy decyzji stosuje się do działalności kontrolnej w zakresie stanu zabezpieczenia informacji niejawnych wykonywanej przez:
 - 1) Ministra Obrony Narodowej;
 - 2) osoby zajmujące kierownicze stanowiska Ministerstwa Obrony Narodowej;

- 3) kierowników jednostek organizacyjnych;
- 4) Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych - Dyrektora Departamentu Ochrony Informacji Niejawnych, zwanego dalej „Pełnomocnikiem Ministra”;
- 5) pełnomocników kierowników jednostek organizacyjnych do spraw ochrony informacji niejawnych w jednostkach organizacyjnych.

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 oraz z 2015 r. poz. 21);
- 2) komórka wewnętrzna - wyodrębnioną w jednostce lub komórce organizacyjnej strukturę organizacyjną powołaną do wykonywania określonych zadań wynikających z zakresu działania tej jednostki lub komórki organizacyjnej;
- 3) kierownik jednostki organizacyjnej - dowódcę, szefa, dyrektora, komendanta, prezesa, kierownika lub inną osobę stojącą na czele jednostki organizacyjnej, która kieruje całokształtem jej działalności, w tym również osobę czasowo pełniącą jego obowiązki;
- 4) kierownik komórki organizacyjnej - dyrektora, szefa, lub inną osobę stojącą na czele komórki organizacyjnej, która kieruje całokształtem jej działalności, w tym również osobę czasowo pełniącą jego obowiązki;
- 5) pełnomocnik ochrony - pełnomocnika kierownika jednostki organizacyjnej do spraw ochrony informacji niejawnych;
- 6) pion ochrony - wyodrębnioną komórkę wewnętrzną, podległą pełnomocnikowi ochrony, wykonującą zadania określone w ustawie;
- 7) 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;
- 8) działalność kontrolna - planowanie, organizowanie, koordynowanie i przeprowadzanie kontroli, jej dokumentowanie oraz przedstawianie wyników właściwym organom, a także postępowanie pokontrolne;
- 9) kontrola (czynności kontrolne) - celową i zorganizowaną działalność zespołu (komisji, grupy, kontrolera, inspektora) prowadzoną w jednostce kontrolowanej, na podstawie planu i upoważnienia do jej przeprowadzenia;
- 10) książka kontroli - wyodrębnioną, prowadzoną w jednostce lub komórce organizacyjnej w formie papierowej, książkę przeznaczoną do dokonywania przez kontrolującego wpisów dotyczących przedmiotu i zakresu kontroli, a także czasu jej trwania;
- 11) akta kontroli - zbiór dokumentów obejmujących w szczególności: zawiadomienie o zamiarze przeprowadzenia kontroli, upoważnienia do przeprowadzenia kontroli, wyniki kontroli, notatki i inne dokumenty - odpisy, wyciągi z rozkazów i informacje od kierownika jednostki kontrolowanej dotyczące usunięcia nieprawidłowości stwierdzonych podczas kontroli;

- 12) przełożony - żołnierz lub inną osobę niebędącą żołnierzem, której na mocy przepisów prawa, dokumentów kompetencyjnych lub decyzji podporządkowano podwładnych i nadano prawo kierowania ich czynnościami służbowymi;
 - 13) kancelaria tajna międzynarodowa - komórkę wewnętrzną, o której mowa w § 2 pkt 3 rozporządzenia Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.
4. Nadzór nad ochroną informacji niejawnych realizuje się w formie:
 - 1) kontroli ochrony informacji niejawnych i przestrzegania przepisów o ochronie tych informacji;
 - 2) oceny stanu zabezpieczenia informacji niejawnych;
 - 3) decyzji wynikających z kontroli i oceny, o których mowa w ppkt 1 i 2.
 5. Kontrole ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji w jednostkach i komórkach organizacyjnych realizuje się w celu:
 - 1) ustalenia stanu faktycznego realizacji zadań w zakresie ochrony informacji niejawnych i 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 bieżące;
 - 2) kontrole okresowe ewidencji, materiałów i obiegu dokumentów, zwane dalej „kontrolami okresowymi”;
 - 3) kontrole stanu zabezpieczenia informacji niejawnych.
 7. Do przeprowadzenia kontroli, o których mowa w pkt 6 ppkt 3, uprawnia pisemne imienne upoważnienie wystawione przez zarządzającego kontrolę, wraz z legitymacją służbową lub dowodem osobistym. Wzór upoważnienia określa załącznik Nr 1 do decyzji.
 8. Kontrolujący musi posiadać poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli, co najmniej równej klauzuli materiałów podlegających kontroli, ważne nie krócej niż do dnia zakończenia kontroli albo pisemne upoważnienie, o którym mowa w art. 21 ust. 4 pkt 1 ustawy, w przypadku, gdy przedmiotem kontroli są materiały o klauzuli „zastrzeżone”. W przypadku kontroli materiałów kryptograficznych dodatkowo wymagane jest posiadanie przez kontrolującego właściwego upoważnienia wydanego na podstawie przepisów określających zasady dostępu do materiałów kryptograficznych.
 9. Kontrolowany ma obowiązek przedstawić do kontroli posiadane materiały niejawne,

udzielać wyczerpujących ustnych i pisemnych wyjaśnień, udostępniać do wglądu prowadzone urządzenia ewidencyjne, pomieszczenia oraz urządzenia techniczne przeznaczone do przetwarzania informacji niejawnych.

Rozdział 2

Kontrola bieżąca

10. Kontrolę bieżącą prowadzi się w celu sprawdzenia:
 - 1) stanu przestrzegania przez osoby kontrolowane przepisów o ochronie informacji niejawnych w zakresie przetwarzania informacji niejawnych;
 - 2) zgodności stanu faktycznego materiałów niejawnych posiadanych przez osoby kontrolowane ze stanem ewidencyjnym.
11. Kontrolę bieżącą w jednostce organizacyjnej prowadzą stosownie do potrzeb:
 - 1) pełnomocnik ochrony i upoważnieni przez niego pracownicy pionu ochrony;
 - 2) przełożeni wobec podwładnych.
12. Z przeprowadzonej kontroli bieżącej sporządza się notatkę służbową, w której wymienia się stwierdzone nieprawidłowości, nazwiska osób, u których występują i określa terminy usunięcia nieprawidłowości.
13. Z wynikami kontroli bieżącej przeprowadzonej przez osoby, o których mowa w pkt 11 ppkt 1, zapoznaje się przełożonych osób kontrolowanych.

Rozdział 3

Kontrola okresowa

14. Kontrola okresowa jest podstawową formą sprawdzenia ewidencji, materiałów i obiegu dokumentów niejawnych w jednostce organizacyjnej. Zakres przedmiotowy kontroli okresowej określa załącznik Nr 2 do decyzji.
15. Kontrolę okresową za rok kalendarzowy prowadzi się w pierwszym kwartale roku następnego.
16. W czasie trwania kontroli okresowej w jednostce organizacyjnej nie prowadzi się kontroli stanu zabezpieczenia informacji niejawnych.
17. Kontrolę okresową przeprowadza komisja wyznaczona rozkazem dziennym lub decyzją kierownika jednostki organizacyjnej, z uwzględnieniem następujących zasad:
 - 1) skład komisji powinien wynosić co najmniej trzy osoby; w przypadkach uzasadnionych względami organizacyjnymi komisja może składać się z podkomisji liczących nie mniej niż trzy osoby;
 - 2) osoby wchodzące w skład komisji muszą spełniać wymagania określone w pkt 8;
 - 3) ostateczne zniszczenie materiałów niejawnych powinno być realizowane przez co najmniej trzech członków komisji (podkomisji);

- 4) zasady niszczenia materiałów niejawnych określają przepisy zarządzenia Ministra Obrony Narodowej wydanego na podstawie art. 47 ust. 3 ustawy;
 - 5) do składu komisji nie wyznacza się osób odpowiedzialnych za prowadzenie ewidencji materiałów niejawnych w jednostkach organizacyjnych objętych kontrolą, z zastrzeżeniem ppkt 6;
 - 6) przepis ppkt 5 nie dotyczy dokumentów niejawnych NATO, UE i innych organizacji międzynarodowych oznaczonych kategoriami specjalnymi.
18. Kontrolę okresową w Ministerstwie Obrony Narodowej przeprowadza komisja powołana 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 NATO, UE lub innych organizacji międzynarodowych, ich klauzul i terminów ważności oraz pisemnych upoważnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone”;
 - 2) termin rozliczenia wykonawców z materiałów niejawnych;
 - 3) termin przygotowania do kontroli okresowej kancelarii tajnych, kancelarii tajnych międzynarodowych i komórek, o których mowa w art. 44 ust. 1 ustawy;
 - 4) termin rozpoczęcia i zakończenia oraz przedstawienia wyników kontroli okresowej.
20. Sposób oraz terminy prowadzenia kontroli okresowej dokumentów operacyjnych w jednostkach organizacyjnych Żandarmerii Wojskowej określa Komendant Główny Żandarmerii Wojskowej.
21. Pełnomocnik ochrony odpowiada za przygotowanie organizacyjne i nadzorowanie przebiegu kontroli okresowej w jednostce organizacyjnej, a w szczególności za:
- 1) opracowanie projektu rozkazu albo decyzji, o których mowa w pkt 17 i 18;
 - 2) przeprowadzenie, na podstawie konspektu zatwierdzonego przez kierownika jednostki organizacyjnej, szkolenia członków komisji kontroli okresowej w zakresie metodyki prowadzenia kontroli oraz kierowników kancelarii tajnych i innych komórek wymienionych w pkt 19 ppkt 3, w zakresie przygotowania tych komórek do kontroli okresowej.
22. Wyniki kontroli okresowej komisje oraz podkomisje, o których mowa w pkt 17 i 18, dokumentują w protokole, którego układ przedstawia załącznik Nr 3 do decyzji. Kierownik jednostki lub komórki organizacyjnej, potwierdza podpisem na protokole fakt zapoznania się z jego treścią.
23. Wyniki kontroli okresowej przeprowadzonej w jednostce organizacyjnej jej kierownik przedkłada do dnia 15 marca bezpośrednio przełożonemu w formie meldunku, z zastrzeżeniem pkt 24. Meldunek winien zawierać informacje dotyczące zgodności lub niezgodności stanu faktycznego materiałów niejawnych ze stanem ewidencyjnym i zasadnicze uwagi stwierdzone przez komisję w czasie kontroli.

24. Kierownicy jednostek organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej i przewodniczący komisji, o której mowa w pkt 18, przedkładają Ministrowi Obrony Narodowej meldunki o wynikach kontroli okresowej za pośrednictwem Pełnomocnika Ministra.
25. Pełnomocnik Ministra przedkłada Ministrowi Obrony Narodowej do dnia 1 kwietnia meldunek zbiorczy o wynikach kontroli okresowej przeprowadzonej w Ministerstwie Obrony Narodowej i jednostkach organizacyjnych bezpośrednio podporządkowanych Ministrowi Obrony Narodowej.

Rozdział 4

Kontrola stanu zabezpieczenia informacji niejawnych

26. Kontrola stanu zabezpieczenia informacji niejawnych jest podstawową formą sprawdzania ochrony informacji niejawnych i przestrzegania przepisów o ochronie tych informacji w jednostkach organizacyjnych.
27. Minister Obrony Narodowej zarządza przeprowadzenie kontroli stanu zabezpieczenia informacji niejawnych we wszystkich jednostkach organizacyjnych. Do zarządzania kontroli stanu zabezpieczenia informacji niejawnych są uprawnieni ponadto:
 - 1) Pełnomocnik Ministra - we wszystkich jednostkach organizacyjnych, z wyłączeniem uczelni wojskowych;
 - 2) osoby, o których mowa w pkt 3 ppkt 3, którym podporządkowano jednostki organizacyjne – w podległych jednostkach organizacyjnych.
28. Kontrole stanu zabezpieczenia informacji niejawnych przeprowadzają zespoły z pionów ochrony jednostek organizacyjnych, jako organy kontroli upoważnione przez osoby, o których mowa w pkt 27. Zarządzający kontrolę może w uzasadnionych przypadkach uzupełnić skład zespołu kontrolującego o inne osoby pełniące służbę lub zatrudnione w kierowanej przez niego jednostce organizacyjnej.
29. Kontrola stanu zabezpieczenia informacji niejawnych jest prowadzona w celu dokonania oceny:
 - 1) stanu realizacji zaleceń pokontrolnych z wcześniej przeprowadzonych kontroli stanu zabezpieczenia informacji niejawnych;
 - 2) organizacji systemu ochrony informacji niejawnych w jednostce organizacyjnej;
 - 3) bezpieczeństwa osobowego;
 - 4) organizacji i funkcjonowania systemu ochrony fizycznej informacji niejawnych jednostki organizacyjnej;
 - 5) obiegu informacji niejawnych w jednostce organizacyjnej;
 - 6) bezpieczeństwa teleinformatycznego;
 - 7) bezpieczeństwa przemysłowego;
 - 8) przestrzegania przepisów o ochronie informacji niejawnych.

30. Szczegółowy zakres przedmiotowy kontroli stanu zabezpieczenia informacji niejawnych określa załącznik Nr 4 do decyzji; w uzasadnionych przypadkach osoby zarządzające kontrolę mogą zmienić jej zakres.
31. W czasie kontroli stanu zabezpieczenia informacji niejawnych nie sprawdza się ewidencji operacyjnej oraz dokumentów operacyjnych Żandarmerii Wojskowej.
32. W trakcie kontroli stanu zabezpieczenia informacji niejawnych zarządzonych przez Ministra Obrony Narodowej, Pełnomocnika Ministra oraz dowódców rodzajów sił zbrojnych, prowadzonych przez zespoły kontrolujące wyłonione z etatowych komórek kontrolnych wchodzących w skład pionów ochrony Ministerstwa Obrony Narodowej albo dowództw rodzajów sił zbrojnych, można sprawdzać działalność kancelarii tajnej międzynarodowej w zakresie określonym w załączniku Nr 4 pkt 1.6 lit. c-k.
33. Kontrolę stanu zabezpieczenia informacji niejawnych przeprowadza się zgodnie z rocznym planem kontroli; w przypadkach wskazujących na występowanie istotnych zagrożeń dla systemu ochrony informacji niejawnych, osoby wymienione w pkt 27 mogą zarządzić kontrolę nieujęłą w planie.
34. Planowanie kontroli stanu zabezpieczenia informacji niejawnych koordynuje Pełnomocnik Ministra.
35. Pełnomocnicy ochrony: Dowódcy Generalnego Rodzajów Sił Zbrojnych, Dowódcy Operacyjnego Rodzajów Sił Zbrojnych, Dowódcy Garnizonu Warszawa, Komendanta Głównego Żandarmerii Wojskowej oraz Dyrektora Narodowego Centrum Kryptologii informują do dnia 1 września Pełnomocnika Ministra o planowanych do przeprowadzenia w następnym roku kalendarzowym, w podległych jednostkach organizacyjnych, kontrolach stanu zabezpieczenia informacji niejawnych.
36. Pełnomocnik Ministra, jako koordynator zamierzeń kontrolnych, po uzgodnieniu z osobami, o których mowa w pkt 35, ma prawo dokonywania zmian terminów planowanych przedsięwzięć kontrolnych. Pełnomocnik Ministra informuje Służbę Kontrwywiadu Wojskowego do dnia 1 października o planowanych do przeprowadzenia w następnym roku kalendarzowym kontrolach stanu zabezpieczenia informacji niejawnych.
37. Czas trwania kontroli stanu zabezpieczenia informacji niejawnych ustala, w zależności od potrzeb, zarządzający kontrolę.
38. Podstawę do przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych stanowi plan jej przeprowadzenia, zatwierdzony przez osobę, o której mowa w pkt 27.
39. Kierownik kontrolowanej jednostki organizacyjnej zapewnia kontrolującemu warunki i środki niezbędne do sprawnego przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych.
40. Kontrola stanu zabezpieczenia informacji niejawnych kończy się omówieniem, którego czas, miejsce, tryb prowadzenia i uczestników ustala przewodniczący zespołu kontrolującego.
41. Przewodniczący zespołu kontrolującego dokonuje wpisu o przeprowadzeniu kontroli w książce kontroli kontrolowanej jednostki organizacyjnej.

42. Wyniki kontroli stanu zabezpieczenia informacji niejawnych dokumentuje się w protokole, który powinien zawierać:
- 1) podstawę prawną przeprowadzenia kontroli;
 - 2) imienny skład zespołu kontrolującego wraz z numerami i datą ważności upoważnień do przeprowadzenia kontroli;
 - 3) termin rozpoczęcia i zakończenia kontroli;
 - 4) zakres przedmiotowy kontroli;
 - 5) oznaczenie kontrolowanej jednostki organizacyjnej, jej siedzibę i adres, a także nazwę nadrzędnej jednostki organizacyjnej;
 - 6) stopień wojskowy, imię i nazwisko, nazwę stanowiska służbowego kierownika kontrolowanej jednostki organizacyjnej, datę objęcia stanowiska służbowego z podstawą prawną, zakres dostępu do informacji niejawnych - numer i datę ważności wydanych poświadczeń bezpieczeństwa;
 - 7) stopień wojskowy, imię i nazwisko, nazwę stanowiska służbowego poprzedniego kierownika kontrolowanej jednostki organizacyjnej i okres pełnienia przez niego obowiązków - w przypadku gdy nieprawidłowości w zakresie stanu zabezpieczenia informacji niejawnych zaistniały w tym czasie;
 - 8) stopień wojskowy, imię i nazwisko, nazwę stanowiska służbowego pełnomocnika ochrony i pozostałych osób z pionu ochrony jednostki kontrolowanej, datę objęcia stanowiska służbowego 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;
 - 12) parafy przewodniczącego zespołu kontrolującego umieszczone na każdej stronie protokołu;
 - 13) podpisy przewodniczącego zespołu kontrolującego i kierownika jednostki kontrolowanej zamieszczone na ostatniej stronie oraz miejsce i datę podpisania protokołu kontroli.
43. Protokół sporządza się w trzech jednobrzmiących egzemplarzach, z przeznaczeniem dla:
- 1) zarządzającego kontrolę;
 - 2) kierownika kontrolowanej jednostki organizacyjnej;
 - 3) przełożonego kierownika kontrolowanej jednostki lub komórki organizacyjnej.
44. W przypadku, gdy protokół kontroli zawiera informacje niejawne, przewodniczący zespołu

kontrolującego nadaje mu stosowną klauzulę tajności.

45. Termin przekazania protokołu kierownikowi kontrolowanej jednostki organizacyjnej nie powinien być dłuższy niż 30 dni od dnia zakończenia czynności kontrolnych.
46. Kierownik kontrolowanej jednostki lub komórki organizacyjnej ma prawo zgłoszenia osobie zarządzającej kontrolę, w terminie siedmiu dni roboczych od dnia otrzymania protokołu, umotywowanych pisemnych zastrzeżeń do jego treści.
47. Osoba zarządzająca kontrolę:
 - 1) odrzuca zastrzeżenia, jeżeli zostały zgłoszone przez osobę nieuprawnioną do ich wniesienia lub wniesione po terminie określonym w pkt 46 albo
 - 2) uwzględnia zastrzeżenia w całości lub w części albo je oddala
 - 3) o podjętej decyzji zawiadamia na piśmie zgłaszającego zastrzeżenia.
48. W przypadku stwierdzenia zasadności zgłoszonych zastrzeżeń dokonuje się zmiany treści protokołu kontroli i dołącza do niego wykaz uwzględnionych zastrzeżeń.
49. Kierownik kontrolowanej jednostki organizacyjnej w terminie 30 dni od dnia otrzymania protokołu lub zakończenia procedury odwoławczej zawiadamia jednostkę nadrzędną oraz informuje organ, który przeprowadził kontrolę, o sposobie wykorzystania uwag i wniosków, a także usunięciu nieprawidłowości wymienionych w protokole.
50. Zarządzający kontrolę dokonuje analizy zebranych wyników przeprowadzonych kontroli stanu zabezpieczenia informacji niejawnych, w celu określenia ewentualnych zmian koniecznych do wprowadzenia w obowiązujących przepisach i wypracowania rozwiązań zmierzających do poprawy organizacji oraz systemu ochrony informacji niejawnych w podległych i nadzorowanych jednostkach organizacyjnych.

Rozdział 5

Ocena stanu zabezpieczenia informacji niejawnych

51. Pełnomocnik ochrony opracowuje ocenę stanu zabezpieczenia informacji niejawnych w jednostce organizacyjnej za poprzedni rok kalendarzowy, która stanowi zasadniczą formę rozliczenia się z realizacji zadań i przestrzegania przepisów o ochronie informacji niejawnych oraz podstawę do doskonalenia systemu ochrony informacji niejawnych w tej jednostce.
52. Ocenę, o której mowa w pkt 51, opracowuje się na podstawie:
 - 1) wyników kontroli okresowych i stanu zabezpieczenia informacji niejawnych przeprowadzonych w jednostkach lub komórkach organizacyjnych;
 - 2) meldunków o naruszeniu przepisów o ochronie informacji niejawnych.
53. Ocena stanu zabezpieczenia informacji niejawnych powinna obejmować:
 - 1) zastosowane w jednostce organizacyjnej rozwiązania systemowe mające na celu obniżenie prawdopodobieństwa wystąpienia 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) przyczyny niezrealizowania niektórych zadań;
 - 5) wnioski i propozycje oraz potrzeby.
54. Układ i szczegółową treść oceny określa załącznik Nr 5 do decyzji.
55. Z oceną zapoznaje się kierownika jednostki organizacyjnej i przesyła do dnia 31 marca pełnomocnikowi ochrony bezpośrednio nadrzędnej jednostki organizacyjnej.
56. Pełnomocnicy ochrony kierowników jednostek organizacyjnych bezpośrednio podporządkowanych:
- 1) Ministrowi Obrony Narodowej;
 - 2) Sekretarzowi Stanu w Ministerstwie Obrony Narodowej, Szefowi Sztabu Generalnego Wojska Polskiego, podsekretarzom stanu w Ministerstwie Obrony Narodowej i Dyrektorowi Generalnemu Ministerstwa Obrony Narodowej;
 - 3) kierownikom (szefom) komórek organizacyjnych
- przesyłają do dnia 30 kwietnia Szefowi Służby Kontrwywiadu Wojskowego i Pełnomocnikowi Ministra ocenę za swoją jednostkę organizacyjną oraz oceny zebrane z podległych jednostek organizacyjnych.
57. Pełnomocnik Ministra do dnia 15 maja przedstawia Szefowi Służby Kontrwywiadu Wojskowego ocenę stanu zabezpieczenia informacji niejawnych w Ministerstwie Obrony Narodowej.
58. 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 7

Postanowienia końcowe

56. Traci moc decyzja Nr 61/MON Ministra Obrony Narodowej z dnia 5 marca 2012 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej (Dz. Urz. Min. Obr. Nar. poz. 86 oraz z 2013 r. poz. 373).
57. Decyzja wchodzi w życie z dniem ogłoszenia.

Minister Obrony Narodowej: *T. Siemoniak*

ZAŁĄCZNIK Nr 1

WZÓR

.....
(nazwa organu zarządzającego kontrolę)

dnia

Upoważnienie Nr ...

Na podstawie pkt decyzji Nr /MON Ministra Obrony Narodowej z dnia 2015 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz w komórkach organizacyjnych Ministerstwa Obrony Narodowej (Dz. Urz. Min. Obr. Nar. poz.)

upoważniam:

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

do przeprowadzania 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 służbowe, stopień wojskowy, imię i nazwisko,
organu zarządzającego kontrolę)

Ważność upoważnienia przedłuża się do dnia

(m.p)
pieczęć okrągła
organu zarządzającego kontrolę

.....
(stanowisko służbowe, stopień wojskowy, imię i nazwisko
zarządzającego kontrolę)

ZAKRES PRZEDMIOTOWY KONTROLI OKRESOWEJ¹⁾

1. Sprawdzenie stanu przestrzegania zasad postępowania z materiałami niejawnymi w kancelariach tajnych, tajnych międzynarodowych i innych komórkach, w których są przechowywane, ewidencjonowane i udostępniane materiały niejawne, polega na:
 - 1.1. Szczegółowym sprawdzeniu stanu faktycznego materiałów niejawnych przechowywanych w kancelariach tajnych i innych komórkach, w których są przetwarzane materiały niejawne oraz porównaniu ze stanem ewidencyjnym z wyłączeniem teczek akt postępowań sprawdzających.
 - 1.2. Sprawdzeniu przestrzegania zasad przetwarzania materiałów niejawnych.
 - 1.3. Sprawdzeniu przestrzegania 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, polega na szczegółowym sprawdzeniu i porównaniu ze stanem ewidencyjnym materiałów niejawnych pobranych przez wykonawców.
3. Zniszczenie uprzednio zakwalifikowanych przez uprawnione osoby materiałów niejawnych.

¹⁾ W zakresie przedmiotowym kontroli okresowej uwzględnia się ponadto zadania wynikające z decyzji Nr 377/MON Ministra Obrony Narodowej z dnia 12 października 2011 r. w sprawie wprowadzenia do użytku „Instrukcji o pieczęciach używanych w resorcie obrony narodowej” (Dz. Urz. Min. Obr. Nar. Nr 21, poz. 315 oraz z 2013 r. poz. 364).

WZÓR

PROTOKÓŁ

Z KONTROLI OKRESOWEJ¹⁾

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 NATO, UE lub innych organizacji międzynarodowych, a także pisemnych upoważnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone”)

przeprowadziła w dniach (wpisać datę rozpoczęcia, datę zakończenia) kontrolę okresową **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 (wewnętrzne) sprawdzono na podstawie nw. dzienników ewidencyjnych kancelarii tajnej (nazwa kancelarii): (wyszczególnienie nazw dzienników ewidencyjnych oraz pozycji zapisów w tych dziennikach, na podstawie których sprawdzono stan faktyczny materiałów niejawnych przetwarzanych lub przekazanych przez jednostkę organizacyjną);
- 2) dane dotyczące stanu faktycznego materiałów niejawnych:
 - a) stan faktyczny materiałów niejawnych w (nazwa kontrolowanej jednostki lub komórki organizacyjnej) jest zgodny (niezgodny) 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 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 i przekazywania materiałów niejawnych (nie stwierdzono naruszenia zasad przechowywania oraz przekazywania dokumentów zawierających 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 zniszczonych przez komisję kontroli okresowej;
- 2) wyszczególnienie numerów materiałów niejawnych, które nie zostały podszyte do właściwych teczek akt i nie zostały przerejestrowane na rok następnny.

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.

„Z protokołem zapoznałem się”:

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

¹⁾ W protokole uwzględnia się ponadto wyniki kontroli pieczęci, zgodnie z decyzją Nr 377/MON Ministra Obrony Narodowej z dnia 12 października 2011 r. w sprawie wprowadzenia do użytku „Instrukcji o pieczęciach używanych w resorcie obrony narodowej” (Dz. Urz. Min. Obr. Nar. Nr 21, poz. 315 oraz z 2013 r. poz. 364)

* - tylko w Ministerstwie Obrony Narodowej.

SZCZEGÓŁOWY ZAKRES PRZEDMIOTOWY KONTROLI STANU ZABEZPIECZENIA INFORMACJI NIEJAWNYCH

1. OCHRONA INFORMACJI NIEJAWNYCH.

1.1. Kontrola planowania i organizacji systemu ochrony informacji niejawnych uwzględniająca:

- a) spójność dokumentów normatywnych wydanych przez kierownika kontrolowanej jednostki organizacyjnej z aktami prawnymi i normatywnymi szczebli nadrzędnych,
- b) sprecyzowanie zadań, dotyczących ochrony informacji niejawnych, w zakresach zadań i zakresach obowiązków osób funkcyjnych,
- c) reagowanie na fakty naruszania przepisów o ochronie informacji niejawnych, utraty dokumentów niejawnych i ujawnienia informacji niejawnych osobom nieupoważnionym,
- d) instrukcję „Sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone” oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony”,
- e) dokumentację określającą sposób i tryb przetwarzania informacji niejawnych o klauzuli "poufne" w podległych komórkach organizacyjnych,
- f) dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą,
- g) plan ochrony informacji niejawnych w jednostce organizacyjnej, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego, a także sposób jego 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 stanu zabezpieczenia informacji niejawnych w jednostkach organizacyjnych wyszczególnionych w pkt 27.

1.2. Kontrola dostępu do informacji niejawnych uwzględniająca:

- 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 i Służby Kontrwywiadu Wojskowego o zatrudnieniu na stanowisku osoby legitymującej się odpowiednim poświadczeniem bezpieczeństwa,
 - d) ewidencję, przechowywanie i archiwizowanie akt postępowań sprawdzających,
 - e) przestrzeganie przepisów w zakresie upoważniania osób do dostępu do informacji niejawnych.
- 1.3. Kontrola planowania i realizacji szkolenia z zakresu ochrony informacji niejawnych obejmująca:
- a) szkolenie podstawowe oraz uzupełniające żołnierzy i pracowników oraz specjalistyczne w zakresie ochrony informacji niejawnych,
 - b) prowadzenie rejestru wydanych zaświadczeń o przeszkoleniu,
 - c) prowadzenie ewidencji szkoleniowej,
 - d) sporządzenie planów szkolenia podstawowego i uzupełniającego.
- 1.4. Kontrola sprawowania nadzoru nad ochroną informacji niejawnych obejmująca:
- a) realizację zaleceń pokontrolnych z kontroli stanu zabezpieczenia informacji niejawnych przeprowadzonych w jednostce organizacyjnej,
 - b) prowadzenie nadzoru służbowego w zakresie stanu zabezpieczenia informacji niejawnych i dokumentowanie jego wyników,
 - c) sprawdzenie wartości merytorycznej przeprowadzonych w jednostce organizacyjnej ocen stanu zabezpieczenia informacji niejawnych.
- 1.5. Sprawdzenie znajomości przepisów o ochronie informacji niejawnych na podstawie przeprowadzonego sprawdzianu wiedzy.
- 1.6. Kontrola działalności kancelarii tajnej obejmująca sprawdzenie:
- a) stanu zabezpieczenia i wyposażenia pomieszczeń kancelaryjnych,
 - b) fizycznego oddzielenia materiałów o różnych klauzulach tajności oraz przestrzegania zasady przechowywania dokumentów uzyskanych w ramach realizacji porozumień międzynarodowych odrębnie dla każdego państwa,
 - c) przygotowania specjalistycznego kierownika, jego zastępcy i pracowników kancelarii tajnej,
 - d) organizacji pracy kancelarii i zakresów działania osób funkcyjnych,
 - e) przestrzegania zasad ewidencjonowania dokumentów,
 - f) przestrzegania zasad wydawania, rozliczania i obiegu dokumentów niejawnych, a także adresowania, zabezpieczania i ekspedycji przesyłek,

- g) prowadzenia wykazu osób upoważnionych do dostępu do informacji niejawnych i jego bieżącej aktualizacji,
 - h) przestrzegania zasad kompletowania i brakowania akt oraz niszczenia dokumentów niejawnych,
 - i) dokonywania zmian klauzul tajności na materiałach niejawnych i w urządzeniach ewidencyjnych,
 - j) organizowania kancelarii ćwiczebnej, ewidencjonowania, obiegu i rozliczania dokumentów ćwiczebnych,
 - k) przygotowania kancelarii tajnej do realizacji zadań na czas „W”.
- 1.7. Kontrola postępowania z materiałami niejawnymi w innych komórkach przechowujących i prowadzących ewidencję materiałów niejawnych. Postępowanie wykonawców z informacjami niejawnymi obejmująca sprawdzenie:
- a) zabezpieczenia i wyposażenia pomieszczeń, w których są przechowywane materiały niejawne,
 - b) przeszkolenia specjalistycznego personelu,
 - c) prowadzenia ewidencji materiałów niejawnych,
 - d) prowadzenia i bieżącej aktualizacji wykazu osób upoważnionych do dostępu do informacji niejawnych,
 - e) przestrzegania zasad przechowywania, udostępniania i niszczenia materiałów niejawnych,
 - f) przestrzegania przepisów w zakresie przechowywania i przekazywania informacji niejawnych,
 - g) terminowości rozliczania się wykonawców z wytworzonych materiałów niejawnych.
- 1.8. Kontrola klasyfikowania materiałów niejawnych, w tym sposobu ich wytwarzania, przetwarzania, ewidencji, oznaczania i niszczenia obejmująca:
- a) przestrzeganie zasad klasyfikowania informacji niejawnych i oznaczania dokumentów, w tym klauzulami tajności,
 - b) niszczenie materiałów niejawnych,
 - c) aktualizację klauzul tajności na materiałach niejawnych i w urządzeniach ewidencyjnych.
- 1.9. Kontrola bezpieczeństwa przemysłowego obejmująca sprawdzenie:
- a) prowadzenia ewidencji przedsiębiorców realizujących na rzecz jednostki organizacyjnej umowy lub zadania związane z dostępem do informacji niejawnych,
 - b) opracowania Instrukcji Bezpieczeństwa Przemysłowego - jako integralnej części umowy,
 - c) sprawowania 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. Kontrola planowania systemu ochrony fizycznej informacji niejawnych obejmująca:
 - a) organizację ochrony informacji niejawnych na podstawie planu ochrony informacji niejawnych jednostki organizacyjnej, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne” w razie wprowadzenia stanu nadzwyczajnego i niezbędne elementy planu ochrony,
 - b) opracowanie decyzji (rozkazu) w sprawie organizacji systemu przepustkowego w jednostce organizacyjnej,
 - c) opracowywanie analiz zagrożeń,
 - d) organizację współdziałania w zakresie ochrony informacji niejawnych z organami Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, Policji i innymi organami porządkowymi.
- 2.2. Kontrola przewożenia materiałów niejawnych na podstawie opracowanych w jednostce organizacyjnej zasad postępowania z ochranianymi i przewożonymi przesyłkami niejawnymi.
- 2.3. Kontrola funkcjonowania ochrony fizycznej informacji niejawnych obejmująca:
 - a) zorganizowanie stref ochronnych oraz systemu wejść i wyjść z tych stref,
 - b) zabezpieczenie stref ochronnych,
 - c) oznaczanie stref ochronnych.
- 2.4. Kontrola funkcjonowania technicznych środków wspomagających ochronę informacji niejawnych w tym ich ilość i stan techniczny obejmująca:
 - a) ilość, stan techniczny i zgodność urządzeń oraz systemów alarmowych z parametrami określonymi w normie obronnej,
 - b) sprawność, konserwację systemów i urządzeń alarmowych.
- 2.5. Kontrola funkcjonowania systemu przepustkowego i kontroli dostępu, przechowywania, wydawania oraz zdawania kluczy i kodów oraz przestrzegania zasad używania urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w strefach ochronnych obejmująca:
 - a) funkcjonowanie systemu przepustkowego i kontroli dostępu,
 - b) nadawanie uprawnień do wstępu do stref ochronnych,
 - c) sposób przechowywania i zabezpieczenia kluczy użytku bieżącego oraz zapasowych, kodów do zamków szyfrowych i kodów systemów alarmowych do pomieszczeń, w których przetwarzane są informacje niejawne, a także znajdujących się w nich urządzeń do przechowywania dokumentów niejawnych,
 - d) przestrzeganie zasad używania urządzeń do rejestracji, kopiowania lub transmisji

obrazu i dźwięku.

3. BEZPIECZEŃSTWO TELEINFORMATYCZNE.

3.1. Kontrola organizacji bezpieczeństwa teleinformatycznego obejmująca:

- a) posiadanie zatwierdzonej przez kierownika jednostki organizacyjnej dokumentacji bezpieczeństwa systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone” i realizację czynności, o których mowa w art. 48 ust. 11 i 12 ustawy,
- b) posiadanie świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego dla systemów przeznaczonych do przetwarzania informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą,
- c) posiadanie zgody Agencji Bezpieczeństwa Wewnętrznego lub Służby Kontrwywiadu Wojskowego na przetwarzanie informacji niejawnych międzynarodowych.

3.2. Kontrola bezpieczeństwa osobowego użytkowników systemów teleinformatycznych obejmująca:

- a) zgodność poświadczeń bezpieczeństwa lub pisemnych upoważnień wydanych przez kierownika jednostki organizacyjnej dla użytkowników systemu teleinformatycznego z postanowieniami dokumentacji bezpieczeństwa,
- b) posiadanie zaświadczeń o odbyciu przez użytkowników systemów teleinformatycznych szkoleń, o których mowa w art. 19 ustawy.

3.3. Kontrola zgodności elementów systemu teleinformatycznego i realizowanych w nim czynności z ustaleniami szczególnych wymagań bezpieczeństwa, obejmująca:

- a) oprogramowanie systemowe, użytkowe i narzędziowe,
- b) konfigurację sprzętu komputerowego,
- c) zabezpieczenie sprzętu przed nieuprawnionym dostępem,
- d) monitorowanie i dokumentowanie dostępu do systemu,
- e) zgodność ze szczególnymi wymaganiami bezpieczeństwa zabezpieczeń i wyposażenia pomieszczenia systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych.

3.4. Kontrola przestrzegania przez użytkowników przepisów o ochronie informacji przy użytkowaniu niejawnych i jawnych systemów teleinformatycznych, obejmująca:

- 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. Kontrola sprawowania nadzoru nad niejawnymi systemami teleinformatycznymi, obejmująca:

- a) wyznaczenie przez kierownika jednostki organizacyjnej administratora systemu teleinformatycznego i inspektora bezpieczeństwa teleinformatycznego, jak również ukończenie przez nich szkolenia specjalistycznego z zakresu bezpieczeństwa teleinformatycznego,
- b) sprawdzenie dokumentacji inspektora bezpieczeństwa teleinformatycznego, planowania i dokumentowania kontroli zgodności funkcjonowania systemów teleinformatycznych z ich szczególnymi wymaganiami bezpieczeństwa oraz procedurami bezpiecznej eksploatacji,
- c) prowadzenie przez administratora systemu teleinformatycznego dokumentacji eksploatacyjnej systemu teleinformatycznego i jej zgodność z postanowieniami stosownej dokumentacji bezpieczeństwa.

WZÓR

**OCENA
STANU ZABEZPIECZENIA INFORMACJI NIEJAWNYCH**

za rok.....

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

1. Stopień wojskowy, imię i nazwisko kierownika jednostki organizacyjnej, numer i klauzula tajności posiadanego poświadczenia bezpieczeństwa - do kiedy ważne, numer zaświadczenia o przeszkoleniu, o którym mowa w art. 19 ust. 2 pkt 2 ustawy (jeżeli w jednostce organizacyjnej są przetwarzane informacje o klauzuli „ściśle tajne” lub „tajne”), 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 mających na celu obniżenie prawdopodobieństwa wystąpienia 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 wojskowy, imię i nazwisko pełnomocnika do spraw ochrony informacji niejawnych, numer i klauzula tajności posiadanego poświadczenia bezpieczeństwa - do kiedy ważne, numer zaświadczenia o przeszkoleniu, o którym mowa w art. 19 ust. 2 pkt 1 ustawy, telefon kontaktowy - służbowy, komórkowy - służbowy,
 - c) stopień wojskowy, imię i nazwisko kierownika kancelarii tajnej, kancelarii tajnej międzynarodowej, numer i klauzula tajności 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, 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 | Łączony z innym | Stopień etatowy | plk (kmdr) | pplk (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.) | ml. chor. (ml. 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,

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 1 datę pisma wchodzącego. |
| | | |

g) sposób postępowania ze wstępnie zniszczonymi materiałami niejawnymi (gdzie, nazwa i adres podmiotu dokonującego ostatecznego zniszczenia, sposób zniszczenia, dane urządzenia, w którym ostatecznie zniszczono materiały); Sposób utylizacji odpadów powstałych w wyniku ostatecznego zniszczenia materiałów.

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 Międzynarodowe | Punkty Obsługi Dokumentów Międzynarodowych | Biblioteki Niejawne | Inne komórki przechowujące i prowadzące ewidencję materiałów niejawnych (podać nazwy tych komórek wewnętrznych) |
|------------------|---------------------------------|--|---------------------|---|
| | | | | |

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

| Materiały niejawne krajowe | Ścisłe tajne | Tajne | Poufne | Zastrzeżone | RAZEM |
|---|-------------------|-------------|-------------------|-----------------|-------|
| Wchodzące | | | | | |
| Wychodzące | | | | | |
| Materiały niejawne NATO | COSMIC TOP SECRET | NATO SECRET | NATO CONFIDENTIAL | NATO RESTRICTED | RAZEM |
| Wchodzące | | | | | |
| Wychodzące | | | | | |
| Materiały niejawne UE | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED | RAZEM |
| Wchodzące | | | | | |
| Wychodzące | | | | | |
| Materiały niejawne z innych państw lub organizacji międzynarodowych | Ścisłe tajne* | Tajne* | Poufne* | Zastrzeżone* | RAZEM |
| Wchodzące | | | | | |
| Wychodzące | | | | | |

* odpowiedniki klauzuli.

d) dane statystyczne (łącznie) za jednostki organizacyjne obsługiwane w zakresie kancelaryjnym według tabel jak wyżej z wyszczególnieniem nazw jednostek obsługiwanych - oraz z rozbiem na poszczególne jednostki organizacyjne.

5.3. Funkcjonowanie niejawnych systemów teleinformatycznych:

a) czy jednostka posiada akredytowane systemy teleinformatyczne przeznaczone do przetwarzania informacji niejawnych - dotyczy to także systemu MIL-WAN i innych systemów teleinformatycznych dopuszczonych do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone”,

| TAK | NIE |
|-----|-----|
| | |

b) jeżeli 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 systemu MIL-WAN i innych systemów teleinformatycznych dopuszczonych do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone”,

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

d) funkcje pełnione w jednostce organizacyjnej na podstawie zgody wyrażonej przez Służbę Kontrwywiadu Wojskowego zgodnie z przepisem art. 52 ust. 2 ustawy.

| Lp. | Funkcja - stanowisko (administrator/inspektor) | Imię i Nazwisko | Nazwa macierzystej jednostki organizacyjnej administratora/inspektora | Okres pełnienia funkcji (data rozpoczęcia i zakończenia) | Nr pisma (decyzji) SKW |
|-----|--|-----------------|---|--|------------------------|
| | | | | | |

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 tajności 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 lit. 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.

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

| Postępowania (ilość przypadków): | Klauzula tajności 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 wojskowy, imię, nazwisko i podpis
pełnomocnika ochrony