

- 4) Przestrzeganie zasad przechowywania oraz przekazywania materiałów niejawnych (*nie stwierdzono naruszenia zasad przechowywania oraz przekazywania dokumentów zawierającymi informacje niejawne stanowiące tajemnicę państwową — 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 rocznej.
- 2) Wyszczególnienie numerów materiałów niejawnych, które nie zostały podszyte do właściwych teczek akt oraz przerejestrowane na rok następny.
- 3) Oświadczenie pełnomocnika ochrony o sprawdzeniu stanu faktycznego Akt Postępowań Sprawdzających.

4 Podpisy członków komisji (podkomisji).

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

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

„Z protokołem z kontroli rocznej stanu ochrony informacji niejawnych za rok (**wpisać rok**) zapoznałem się”:

(stopień wojskowy, imię i nazwisko)

(data)

* — tylko w Ministerstwie Obrony Narodowej.

Załącznik Nr 7

SZCZEGÓŁOWY ZAKRES

przedmiotowy kontroli problemowej stanu ochrony informacji niejawnych

1. OCHRONA INFORMACJI NIEJAWNYCH

1.1. 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) plan postępowania z materiałami zawierającymi informacje stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego,
- e) szczegółowe wymagania w zakresie ochrony w jednostce organizacyjnej informacji oznaczonych klauzulą „Zastrzeżone”,
- f) wykaz podstawowych materiałów niejawnych, wytwarzanych w jednostce organizacyjnej zawierających informacje niejawne stanowiące tajemnicę służbową z przeznaczeniem dla celów szkoleniowych.

1.2. Dostęp do informacji niejawnych.

- a) opracowanie spisu stanowisk, z którymi wiąże się dostęp do informacji niejawnych oraz ujęcie w rozkazie dziennym (decyzji) kierownika jednostki organizacyjnej,
- b) prowadzenie wykazu stanowisk i prac zleconych, z którymi wiąże się dostęp do informacji niejawnych oraz osób dopuszczonych do pracy lub służby na tych stanowiskach,
- c) ewidencja, przechowywanie i archiwizowanie akt postępowań sprawdzających,
- d) przestrzeganie przepisów w zakresie upoważniania osób do dostępu do informacji niejawnych.

Załącznik Nr 7 (cd.)

- 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) programy szkolenia oraz prowadzenie ewidencji szkoleniowej.
- 1.4. Sprawowanie nadzoru nad ochroną informacji niejawnych.
 - a) realizacja zaleceń pokontrolnych z kontroli stanu ochrony informacji niejawnych przeprowadzonych w jednostce organizacyjnej,
 - b) prowadzenie nadzoru służbowego w zakresie ochrony informacji niejawnych oraz dokumentowanie jego wyników. Kontrole doraźne, półroczne, roczne oraz problemowe,
 - c) wartość merytoryczna przeprowadzonych w jednostce organizacyjnej ocen stanu ochrony informacji niejawnych.
- 1.5. Znajomość przepisów o ochronie informacji niejawnych — test.
- 1.6. Działalność kancelarii tajnej oraz tajnej - zagranicznej.
 - 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) skuteczność nadzoru kierownika kancelarii nad wytwarzaniem i ewidencjonowaniem dokumentów niejawnych przez wykonawców technicznych,
 - g) przestrzeganie zasad wydawania, rozliczania i obiegu dokumentów niejawnych, a także adresowania, zabezpieczania i ekspedycji przesyłek,
 - h) prowadzenie wykazu osób upoważnionych do dostępu do informacji niejawnych oraz jego bieżąca aktualizacja,
 - i) przestrzeganie zasad kompletowania i brakowania akt oraz niszczenia dokumentów niejawnych,
 - j) dokonywanie zmian klauzul tajności na materiałach niejawnych oraz w urządzeniach ewidencyjnych,
 - k) organizowanie kancelarii ćwiczebnej, ewidencjonowanie, obieg i rozliczanie dokumentów ćwiczebnych,
 - ~~l) przygotowanie kancelarii tajnej do realizacji zadań na czas „W”~~
 - m) prowadzenie przeglądów materiałów zawierających informacje niejawne stanowiących tajemnicę służbową, wytworzonych w jednostce organizacyjnej, w celu ewentualnego przedłużenia terminu ich ochrony.
- 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 informacje 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 pobranych 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,
- 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.

Załącznik Nr 7 (cd.)

2. ORGANIZACJA I PRZYGOTOWANIE ORAZ FUNKCJONOWANIE SYSTEMU OCHRONY FIZYCZNEJ JEDNOSTKI ORGANIZACYJNEJ

- 2.1. Planowanie systemu ochrony obiektów.
 - a) organizacja ochrony jednostki na podstawie planu ochrony,
 - b) opracowanie „Rozkazu (decyzji) dowódcy do organizacji i funkcjonowania systemu ochrony obiektów wojskowych”,
 - c) opracowanie dokumentacji dla sił ochronnych i służb dyżurnych,
 - d) opracowywanie analiz zagrożeń,
 - e) organizacja współdziałania w zakresie ochrony jednostki organizacyjnej z organami Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, Policji i organami właściwego samorządu terytorialnego.
- 2.2. Organizacja ochrony konwojowanego mienia.
 - a) opracowanie instrukcji konwojowania,
 - b) opracowanie planu przeprowadzenia konwoju.
- 2.3. Szkolenia z zakresu problematyki ochrony obiektów.
 - a) stan wyszkolenia sił przewidzianych do wykonywania zadań ochronnych,
 - b) szkolenie z zakresu problematyki ochrony obiektów,
 - c) prowadzenie szkolenia z pozorowanym naruszeniem systemu ochrony obiektu,
 - d) przeszkolenie sił ochronnych, służb dyżurnych, administratorów systemów alarmowych i użytkowników systemów oraz urządzeń alarmowych z obsługi tych urządzeń,
 - e) szkolenie służb dyżurnych, ochronnych, wart oraz osób funkcyjnych,
 - f) dokumentacja szkoleniowa z zakresu ochrony obiektów.
- 2.4. Funkcjonowanie ochrony fizycznej, poziom wyszkolenia sił ochronnych.
 - a) pełnienie służby wartowniczej (ochronnej), wewnętrznej lub garnizonowej, portierów i dozorców,
 - b) wyposażenie sił ochronnych i służb dyżurnych w należyły sprzęt oraz uzbrojenie,
 - c) organizacja systemu ochrony w godzinach służbowych i po godzinach służbowych oraz w dniach wolnych od zajęć służbowych,
 - d) stan ogrodzeń, umocnień inżynierskich oraz sprawność oświetlenia,
 - e) zabezpieczenie stref bezpieczeństwa oraz pomieszczeń, w których jest przechowywany sprzęt i mienie wojskowe,
 - f) poziom wyszkolenia sił ochronnych, służb dyżurnych, wart oraz osób funkcyjnych,
 - g) oznakowanie obiektów znakami drogowymi i tablicami ostrzegawczymi.
- 2.5. Funkcjonowanie technicznych środków wspomagających ochronę w tym ich ilość i stan techniczny.
 - a) ilość, stan techniczny i zgodność urządzeń oraz 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 oraz służb dyżurnych.
- 2.6. Funkcjonowanie systemu przepustkowego i kontroli dostępu, przechowywanie, wydawanie i zdawanie kluczy.
 - a) funkcjonowanie systemu przepustkowego i kontroli dostępu,
 - b) określenie stref: administracyjnej i bezpieczeństwa, a także sposób ich ochrony,
 - c) sposób przechowywania i zabezpieczenia kluczy użytku bieżącego oraz zapasowych.
- 2.7. Ochrona obiektów i pomieszczeń podlegających szczególnej ochronie oraz przestrzeganie zasad używania urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w specjalnych strefach bezpieczeństwa oraz w strefach bezpieczeństwa.
 - a) sposób przechowywania i zabezpieczenia kluczy użytku bieżącego oraz zapasowych, kodów do zamków szyfrowych i kodów systemów alarmowych do pomieszczeń oraz obiektów podlegających szczególnej ochronie, a także znajdujących się w nich urządzeń do przechowywania dokumentów niejawnych,
 - b) określenie pomieszczeń, obiektów i rejonów podlegających szczególnej ochronie, a także sposób ich ochrony
 - c) przestrzeganie zasad używania urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku.
- 2.8. Działalność sprawozdawcza, prowadzenie analiz zagrożeń, kontroli i nadzorów służbowych oraz ich dokumentowanie.
 - a) opracowanie sprawozdania ze stanu ochrony obiektów jednostki organizacyjnej,
 - b) opracowywanie analiz zagrożeń,
 - c) kontrole stanu ochrony jednostki organizacyjnej (realizowane przez osoby funkcyjne tej jednostki) oraz ich dokumentowanie.

3. BEZPIECZEŃSTWO TELEINFORMATYCZNE

- 3.1. Organizacja systemu bezpieczeństwa teleinformatycznego.
 - a) posiadanie certyfikatów akredytacji bezpieczeństwa teleinformatycznego dla systemów, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę państwową,
 - b) akceptacja przez Służbę Kontrwywiadu Wojskowego dokumentacji bezpieczeństwa systemów i sieci teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych stanowiących tajemnicę służbową.
- 3.2. Bezpieczeństwo osobowe użytkowników systemów teleinformatycznych.
 - a) posiadanie stosownych poświadczeń bezpieczeństwa przez 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,
 - b) dokumentacja inspektora bezpieczeństwa teleinformatycznego, planowanie i dokumentowanie wyników kontroli zgodności funkcjonowania systemów teleinformatycznych z ich Szczególnymi Wymaganiami Bezpieczeństwa i Procedurami Bezpiecznej Eksploatacji.