403

ZARZĄDZENIE Nr 58/MON MINISTRA OBRONY NARODOWEJ

z dnia 22 grudnia 2011 r.

w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) zarządza się, co następuje:

Rozdział 1

Postanowienia ogólne

§ 1.1. Zarządzenie określa:

1) organizację, funkcjonowanie kancelarii kryptograficznych oraz organów nadzorujących ich pracę;
2) środki bezpieczeństwa fizycznego;
3) organizację, funkcjonowanie i zabezpieczenie kancelarii kryptograficznych na okrętach i pomocniczych jednostkach pływających Marynarki Wojennej;
4) organizację pracy kancelarii kryptograficznych, ich ochronę oraz obieg materiałów kryptograficznych podczas ćwiczeń, wojny, a także w czasie realizacji zadań poza granicami kraju;
5) zasady rejestrowania, kompletowania i niszczenia materiałów kryptograficznych;
6) sprawowanie nadzoru nad kancelariami kryptograficznymi;
7) wzory urządzeń ewidencyjnych.

2. Przepisów zarządzenia nie stosuje się do materiałów kryptograficznych wykorzystywanych przez uprawnione jednostki organizacyjne w trakcie realizacji czynności operacyjno-rozpoznawczych.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) akta — zbiór dokumentów ułożonych według rzeczowego wykazu akt, podszytych do teczek akt oznaczonych właściwą kategorią archiwalną i symbolem klasyfikacyjnym;
2) akta kryptograficzne — odpowiednio opracowane i zabezpieczone zbiory materiałów kryptograficznych, o których mowa w pkt 20 lit. d-f, pogrupowanych według wyciągu z jednolitego rzeczowego wykazu akt, oznaczone właściwą kategorią archiwalną i symbolem klasyfikacyjnym;
3) archiwista — żołnierz, funkcjonariusz lub pracownik zatrudniony w kancelarii kryptograficznej, podlegający bezpośrednio kierownikowi kancelarii kryptograficznej;
4) archiwum — wyodrębnione archiwum jednostki organizacyjnej, w rozumieniu przepisów zarządzenia Ministra Obrony Narodowej wydanego na podstawie art. 29 ust. 3 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698 i Nr 171, poz. 1016);
5) CUK — certyfikat upoważnienia kryptograficznego, dokument potwierdzający zgodę kierownika jednostki organizacyjnej na dostęp do materiałów kryptograficznych;
6) dokument kryptograficzny — każdy ciąg danych utrwalony na dowolnym nośniku, a w szczególności w banku danych kryptograficznych, na nośniku optycznym lub magnetycznym, papierze, posiadający cechy identyfikacyjne w postaci nazwy, klauzuli, numeru egzemplarza, numeru serii oraz innych danych pomocniczych, który wykorzystywany jest do kryptograficznego zabezpieczenia informacji przed jej ujawnieniem modyfikacją oraz realizacji procesu potwierdzenia autentyczności tej informacji przez produkt kryptograficzny;
7) dokument kryptograficzny bieżącej edycji — dokument kryptograficzny wykorzystywany w danym momencie do czasu zakończenia jego obowiązywania;
8) dokument kryptograficzny przyszłej edycji — dokument kryptograficzny przeznaczony do przyszłego zabezpieczenia informacji przez produkt kryptograficzny;
9) elektroniczny obieg dokumentów — proces rejestrowania, przechowywania, obiegu i udostępniania dokumentów w postaci elektronicznej, realizowany w jednostce organizacyjnej przy wykorzystaniu specjalistycznego systemu informatycznego;
10) ewidencja — służące do rejestrowania materiałów kryptograficznych księgi, dzienniki, wykazy, spisy, rejestry lub kartoteki oraz elektroniczne bazy danych o ustalonych wzorach i formach;
11) GKK — Główna Kancelaria Kryptograficzna — kancelaria kryptograficzna umiejscowiona w SKW będąca Główną Kancelarią Kryptograficzną dla jednostek organizacyjnych resortu

obrony narodowej, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, instytucji nadzorowanych przez Ministra Obrony Narodowej;

12) inspekcja kryptograficzna — kontrola ochrony materiałów kryptograficznych oraz funkcjonowania kancelarii (stacji) kryptograficznej realizowana przez OBSŁiI, wykonywana w ramach nadzoru nad ochroną informacji niejawnych;

13) jednostka organizacyjna — komórki organizacyjne Ministerstwa Obrony Narodowej i jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym przedsiębiorstwo państwowe, dla którego jest on organem założycielskim, jednostka organizacyjna lub związek organizacyjny wchodzące w skład Sił Zbrojnych — w rozumieniu przepisów o powszechnym obowiązku obrony Rzeczypospolitej Polskiej;

14) kancelaria kryptograficzna — etatowa komórka organizacyjna funkcjonująca w jednostce organizacyjnej, odpowiedzialna za rejestrowanie, przyjmowanie, przechowywanie, udostępnianie, dystrybucję, przygotowanie materiałów do archiwizacji i niszczenie materiałów kryptograficznych, która może realizować zadania związane z ochroną kryptograficzną, takie jak: szyfrowanie i deszyfrowanie informacji niejawnych z wykorzystaniem certyfikowanych urządzeń i narzędzi kryptograficznych;

15) kierownik jednostki organizacyjnej — dowódca, szef, dyrektor, komendant, prezes lub inna osoba stojąca na czele jednostki organizacyjnej, która kieruje całokształtem działalności tej jednostki, w tym również osoba czasowo pełniąca jego obowiązki;

16) kierownik kancelarii kryptograficznej (w relacjach międzynarodowych — Crypto Custodian) — wyznaczony żołnierz, funkcjonariusz lub pracownik zajmujący etatowe stanowisko kierownika kancelarii kryptograficznej i kierujący jej pracą podlegający Oficerowi Bezpieczeństwa Systemów Łączności i Informatyki;

17) klasa systemu lub urządzenia alarmowego — kategoria jakości według Normy Obronnej NO-04-A004 „Obiekty Wojskowe. Systemy Alarmowe. Wymagania dotyczące urządzeń";

18) KOGD — Krajowy Organ Generacji i Dystrybucji — Organ Bezpieczeństwa Systemów Łączności i Informatyki, sprawujący nadzór nad bezpieczeństwem materiałów kryptograficznych w jednostkach organizacyjnych oraz instytucjach cywilnych realizujących zadania na rzecz resortu obrony narodowej i odpowiedzialny za:
   a) dystrybucję sojuszniczych i narodowych materiałów kryptograficznych,
   b) generację, wytwarzanie dokumentów kryptograficznych służących do zabezpieczenia narodowych potrzeb w zakresie ochrony systemów teleinformatycznych przetwarzających niejawne informacje narodowe i sojusznicze,
   c) nadzór nad zarządzaniem materiałami kryptograficznymi,
   d) określanie sposobu organizacji i funkcjonowania kancelarii kryptograficznej,
   e) powoływanie i odwoływanie kancelarii kryptograficznej,
   f) udzielanie zgody na generację i wytwarzanie dokumentów kryptograficznych poza KOGD,
   g) nadzór nad prowadzonymi szkoleniami specjalistycznymi personelu BSŁiI,
   h) nadzór nad prawidłowością funkcjonowania OBSŁiI oraz przestrzegania przez nich przepisów i procedur;

19) kurier — żołnierz, funkcjonariusz lub pracownik pełniący obowiązki w kancelarii kryptograficznej, podlegający bezpośrednio kierownikowi tej kancelarii;

20) materiał kryptograficzny to:
   a) dokument kryptograficzny,
   b) element systemu kryptograficznego, a w szczególności moduł, blok, podzespół, pomocnicze urządzenie kryptograficzne,
   c) produkt kryptograficzny lub jego część,
   d) publikacja i wydawnictwo kryptograficzne,
   e) dokumentacja techniczna systemów i produktów kryptograficznych,
   f) dokumentacja, pismo dotyczące tematyki kryptograficznej, ewidencji, przechowywania, wykorzystania i niszczenia materiałów kryptograficznych,
   g) formularz i inne urządzenia ewidencyjne przeznaczone do ewidencji materiałów kryptograficznych,
   h) inny dokument związany z tematyką kryptograficzną;

21) Oficer BSŁiI — Oficer Bezpieczeństwa Systemów Łączności i Informatyki (w relacjach międzynarodowych Oficer INFOSEC), funkcja sprawowana w celu nadzoru nad bezpieczeństwem materiałów kryptograficznych;

22) OBSŁiI — Organ Bezpieczeństwa Systemów Łączności i Informatyki, wyspecjalizowana jednostka organizacyjna lub wewnętrzna komórka jednostki organizacyjnej, lub osoba odpowiedzialna za zapewnienie organizacyjnych, technicznych i programowych aspektów kryptograficznej ochrony informacji niejawnych oraz sprawowanie nadzoru nad funkcjonowaniem systemów kryptograficznych i teleinformatycznych, w których przetwarzane są niejawne materiały kryptograficzne, jak również za sprawowanie nadzoru nad zarządzaniem tymi materiałami.

23) pełnomocnik ochrony — pełnomocnik do spraw ochrony informacji niejawnych, o którym mowa w art. 14 ustawy z dnia 5 sierpnia 2010 r.

o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), zwanej dalej „ustawą".

24) personel BSŁiI — żołnierze, funkcjonariusze lub pracownicy jednostki organizacyjnej, wchodzący w skład i wykonujący zadania na rzecz OBSŁiI;
25) pomocnicze urządzenie ewidencyjne — urządzenie ewidencyjne nie podlegające zdaniu do archiwum stosowane w zależności od potrzeb wynikających z funkcjonowania kancelarii kryptograficznej;
26) potwierdzenie odbioru — fizyczne przekazywanie przez kierownika kancelarii kryptograficznej materiałów kryptograficznych, po złożeniu podpisu przez upoważnionego do odbioru użytkownika z danej jednostki organizacyjnej;
27) pracownik — osoba pozostająca w stosunku pracy z jednostką organizacyjną;
28) produkt kryptograficzny — urządzenie lub narzędzie zawierające co najmniej jeden mechanizm kryptograficzny wykorzystywany w celu zapewnienia wymaganego poziomu bezpieczeństwa przetwarzanych informacji;
29) przesyłka — materiały w postaci odpowiednio zabezpieczonych, zaadresowanych i oznaczonych paczek lub listów;
30) przesyłka kryptograficzna — materiały kryptograficzne w postaci zabezpieczonych, zaadresowanych i odpowiednio oznaczonych paczek lub listów;
31) raport posiadania — wypełniony formularz AF 21 PL określający stan ewidencyjny posiadanych materiałów kryptograficznych będących na ewidencji kancelarii kryptograficznej;
32) RCZBSiUT — Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych;
33) rejestr wzorów podpisów — formularz opisujący umiejscowienie kancelarii kryptograficznej w hierarchii, zawierający jej dane teleadresowe oraz dane osobowe, wzory podpisów personelu tej kancelarii i Oficera BSŁiI;
34) SKW — Służba Kontrwywiadu Wojskowego;
35) stacja kryptograficzna — etatowa komórka organizacyjna funkcjonująca w jednostce organizacyjnej realizująca zadania związane z ochroną kryptograficzną (szyfrowanie, deszyfrowanie) informacji niejawnych z wykorzystaniem urządzeń i narzędzi kryptograficznych, nie pełniąca funkcji kancelarii kryptograficznej;
36) system kryptograficzny — część systemu teleinformatycznego realizującego kryptograficzne zabezpieczenie informacji przy pomocy jednego lub więcej produktów kryptograficznych (mechanizmów, urządzeń i narzędzi) oraz procedur i metod postępowania stosowanych przez personel BSŁiI);
37) Szef KOGD (w relacjach międzynarodowych — National Distribution Authority) — Szef Krajowego Organu Generacji i Dystrybucji, to jest Dyrektor Biura Łączności i Informatyki SKW kierujący KOGD z upoważnienia i w imieniu Szefa Służby Kontrwywiadu Wojskowego;
38) trwałe urządzenie ewidencyjne — urządzenie ewidencyjne podlegające archiwizacji;
39) urządzenie ewidencyjne — księga, dziennik, wykaz, spis, rejestr, formularz lub kartoteka o ustalonych rubrykach, prowadzone w formie papierowej lub elektronicznej, służący do rejestrowania materiałów kryptograficznych oraz umożliwiające kontrolę ich stanu i obiegu;
40) urządzenie kryptograficzne — certyfikowane urządzenie wykorzystywane do zabezpieczenia informacji przekazywanej w dowolnej sieci telekomunikacyjnej, przed jej ujawnieniem, modyfikacją oraz realizacji procesu potwierdzenia autentyczności tej informacji;
41) WSK RP — Wojskowa Służba Kurierska Rzeczypospolitej Polskiej, to jest żołnierze, funkcjonariusze lub pracownicy SKW oraz Centrum Wsparcia Teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polskiej, zwanego dalej „CWT SZ RP", realizujący dystrybucję materiałów kryptograficznych na szczeblu centralnym;
42) wykonawca — żołnierz, funkcjonariusz lub pracownik zajmujący określone stanowisko służbowe, wykonujący zadania zgodnie z zakresem obowiązków, posiadający stosowne poświadczenia bezpieczeństwa i przeszkolenie w zakresie ochrony informacji niejawnych oraz upoważnienie do dostępu do materiałów kryptograficznych;
43) wytyczne — Wytyczne SKW w sprawie powoływania i odwoływania kancelarii kryptograficznych;
44) zarządzanie materiałem kryptograficznym — całokształt przedsięwzięć związany z ochroną (bezpieczeństwem) materiałów kryptograficznych, od złożenia zapotrzebowania na dokumenty kryptograficzne, generację, wytwarzanie, ewidencję, dystrybuowanie oraz ich niszczenie;
45) zasada wiedzy niezbędnej — udostępnianie określonej informacji wyłącznie osobom, którym jest to niezbędne do realizacji czynności służbowych;
46) zastępca kierownika kancelarii kryptograficznej (w relacjach międzynarodowych — Alternate Crypto Custodian) — wyznaczony żołnierz, funkcjonariusz lub pracownik zajmujący etatowe stanowisko zastępcy kierownika tej kancelarii.

Rozdział 2

Organizacja, funkcjonowanie kancelarii kryptograficznej oraz organy nadzorujące ich pracę

§ 3.1. W jednostkach organizacyjnych, które wykorzystują lub planują wykorzystywać materiały

kryptograficzne utrzymuje się powołane lub powołuje się kancelarie kryptograficzne.

2. Obrót materiałami kryptograficznymi odbywa się wyłącznie pomiędzy jednostkami organizacyjnymi posiadającymi kancelarie kryptograficzne.

3. Sposób i tryb powoływania i odwoływania kancelarii kryptograficznych określają odrębne przepisy.

4. Kancelaria kryptograficzna może przyjmować, rejestrować, przechowywać i wysyłać tylko materiały kryptograficzne narodowe i pochodzące z wymiany międzynarodowej oraz inne dokumenty związane z tematyką kryptograficzną, pod warunkiem, że będą one fizycznie od siebie oddzielone i rejestrowane w odrębnych urządzeniach ewidencyjnych.

5. Kancelaria kryptograficzna jednostki organizacyjnej w szczególnie uzasadnionych przypadkach może za zgodą Szefa KOGD zaopatrywać w materiały kryptograficzne inne jednostki organizacyjne.

6. W przypadkach, o których mowa w ust. 5, kierownik jednostki organizacyjnej nie posiadający kancelarii kryptograficznej powinien:
1) wyznaczyć Oficera BSŁiI;
2) opracować (w trzech egzemplarzach, według wzoru określonego w załączniku Nr 1) we współdziałaniu z kierownikiem jednostki organizacyjnej, który ma obsługiwać tę jednostkę „Procedury zaopatrywania w materiały kryptograficzne ... (podać nazwę jednostki organizacyjnej) przez kancelarię kryptograficzną nr ... (podać nazwę jednostki organizacyjnej)";
3) przesłać, poprzez RCZBSiUT, zatwierdzone procedury do Szefa KOGD celem akceptacji;
4) przesłać zaakceptowany przez Szefa KOGD trzeci egzemplarz Procedur, o których mowa w pkt 3 do jednostki organizacyjnej zaopatrującej w materiały kryptograficzne.

7. Zgoda, o której mowa w ust. 5, jest wydawana na czas określony.

8. Szef KOGD może zalecać powołanie kancelarii kryptograficznej.

9. W przypadku uzasadnionym względami organizacyjnymi, w jednostce organizacyjnej można powołać więcej niż jedną kancelarię kryptograficzną (np. stacjonarną i polową lub mobilną).

§ 4.1. Obsługę kancelarii kryptograficznej stanowi wyznaczony rozkazem (decyzją) etatowy personel tej kancelarii w tym:
1) kierownik kancelarii kryptograficznej;
2) zastępca (zastępcy) kierownika kancelarii kryptograficznej;
3) w zależności od potrzeb szyfrant (szyfranci), archiwista (archiwiści), kurier (kurierzy).

2. Personel kancelarii kryptograficznej może pełnić jednocześnie funkcję personelu kancelarii kryptograficznej stacjonarnej oraz polowej lub mobilnej w ramach jednej jednostki organizacyjnej.

3. Na stanowiska etatowego personelu kancelarii kryptograficznej wyznacza się żołnierza, funkcjonariusza lub pracownika, który posiada poświadczenia bezpieczeństwa odpowiednie do klauzul tajności materiałów niejawnych otrzymywanych, wytwarzanych, przetwarzanych, przekazywanych i przechowywanych w kancelarii kryptograficznej posiada aktualne zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych oraz szkolenie/szkolenia specjalistyczne określone w odrębnych przepisach.

§ 5.1. Do obowiązków kierownika kancelarii kryptograficznej należy:
1) kierowanie pracą tej kancelarii;
2) przyjmowanie, rejestrowanie, przechowywanie oraz przekazywanie materiałów kryptograficznych otrzymywanych, wysyłanych oraz wytwarzanych na potrzeby wewnętrzne jednostki organizacyjnej oraz jednostek zaopatrywanych;
3) współudział w planowaniu i prowadzeniu inspekcji kryptograficznych w zaopatrywanych kancelariach kryptograficznych;
4) dokonywanie dystrybucji (redystrybucji) materiałów kryptograficznych do zaopatrywanych kancelarii kryptograficznych;
5) prowadzenie aktualnej ewidencji materiałów kryptograficznych;
6) dokonywanie sprawdzeń posiadanych materiałów kryptograficznych;
7) sprawdzanie poświadczeń bezpieczeństwa i CUK osób korzystających z zasobów kancelarii kryptograficznej, prowadzenie ich ewidencji oraz prowadzenie wykazów osób upoważnionych do dostępu do materiałów kryptograficznych, którego wzór określa załącznik Nr 2;
8) posiadanie aktualnych edycji publikacji kryptograficznych i poprawne wprowadzanie do nich zmian;
9) meldowanie oficerowi BSŁiI o każdym stwierdzonym naruszeniu bezpieczeństwa fizycznego i kryptograficznego oraz o możliwym lub rzeczywistym zagrożeniu bezpieczeństwa materiałów kryptograficznych;
10) udostępnianie i wydawanie materiałów kryptograficznych osobom, o których mowa w pkt 7;
11) kompletowanie materiałów kryptograficznych oraz przygotowywanie akt do archiwizacji;

12) przesyłanie do nadrzędnej kancelarii rocznych raportów o stanie posiadanych materiałów kryptograficznych;
13) niszczenie materiałów kryptograficznych zgodnie z obowiązującymi w tym zakresie przepisami i zaleceniami;
14) aktualizacja wykazu zaopatrywanych kancelarii kryptograficznych w jednostkach organizacyjnych na podstawie „Zaświadczeń o funkcjonowaniu kancelarii kryptograficznych" oraz pism odwołujących kancelarie kryptograficzną;
15) zmiana kodów i rotacja kluczy zabezpieczających funkcjonowanie kancelarii kryptograficznych;
16) obsługa urządzeń i narzędzi kryptograficznych;
17) wykonywanie poleceń zleconych przez Oficera BSŁiI związanych z tematyką kryptograficzną.

2. Do obowiązków zastępcy kierownika kancelarii kryptograficznej należy wykonywanie zadań, o których mowa w ust. 1 pkt 2-17, a podczas nieobecności kierownika kancelarii kierowanie pracą kancelarii.

3. Do obowiązków archiwisty, kuriera należy wykonywanie zadań, o których mowa w ust. 1 pkt 2-17.

4. Obowiązki szyfranta określają odrębne przepisy.

5. Szczegółowe obowiązki personelu kancelarii kryptograficznej określa Oficer BSŁiI.

§ 6.1. Przekazanie obowiązków na stanowisku kierownika kancelarii kryptograficznej odbywa się komisyjnie.

2. Komisję, o której mowa w ust. 1 powołuje kierownik jednostki organizacyjnej, w skład której wchodzą:
1) co najmniej jeden przedstawiciel OBSŁiI;
2) co najmniej jeden przedstawiciel organu nadrzędnego;
3) osoba zdająca i przyjmująca obowiązki kierownika kancelarii kryptograficznej.

3. Wniosek o wyznaczenie przedstawiciela organu nadrzędnego do składu komisji, o której mowa w ust. 2 wraz z raportem posiadania, przesyła się na 45 dni przed planowanym terminem zmiany kierownika kancelarii kryptograficznej.

4. Wynikiem pracy komisji jest protokół z przekazania obowiązków oraz raport posiadania materiałów kryptograficznych.

5. Protokół przekazania obowiązków zawiera:
1) nazwy i numery urządzeń ewidencyjnych, na podstawie których dokonano sprawdzenia stanu faktycznego materiałów kryptograficznych pozostających na ewidencji kancelarii kryptograficznej oraz pozycje zapisów w tych urządzeniach;
2) numer ewidencyjny raportu posiadania materiałów kryptograficznych;
3) informacje dotyczące porównania stanu faktycznego materiałów kryptograficznych ze stanem ewidencyjnym;
4) uwagi osoby przyjmującej obowiązki dotyczące ujawnionych nieprawidłowości w zakresie ewidencjonowania i obiegu materiałów kryptograficznych.

6. Protokół przekazania obowiązków wykonuje się w dwóch jednobrzmiących egzemplarzach.

7. Zatwierdzone przez kierownika jednostki organizacyjnej egzemplarze protokołu przechowuje się w kancelarii kryptograficznej:
1) zaopatrującej;
2) własnej.

8. Po przyjęciu obowiązków kierownik kancelarii kryptograficznej przesyła drogą służbową do Szefa KOGD nowy rejestr wzorów podpisów.

9. Na czas nieobecności kierownika kancelarii kryptograficznej i jego zastępcy poniżej 60 dni (urlop, choroba, wyjazd służbowy itp.), obowiązki kierownika pełni etatowa osoba z personelu kancelarii kryptograficznej, posiadająca stosowne poświadczenie bezpieczeństwa oraz zaświadczenie ukończenia kursu personelu kancelarii kryptograficznych, wyznaczona rozkazem dziennym lub decyzją kierownika jednostki organizacyjnej.

10. W przypadku braku etatowego personelu kancelarii kryptograficznej, kierownik tej kancelarii:
1) przekazuje protokolarnie wyłącznie urządzenia ewidencyjne osobie posiadającej stosowne poświadczenie bezpieczeństwa oraz zaświadczenie ukończenia kursu personelu kancelarii kryptograficznych, wyznaczonej rozkazem dziennym lub decyzją kierownika jednostki organizacyjnej;
2) zamyka i oznakowuje szafy oraz urządzenia do przechowywania informacji niejawnych z pozostałymi materiałami kryptograficznymi i oznakowuje swoją pieczęcią okrągłą numerową do teczki pracy lub w inny sposób jednoznacznie identyfikujący kierownika kancelarii.

11. Na czas nieobecności kierownika kancelarii kryptograficznej i jego zastępcy powyżej 60 dni lub w przypadkach innych niż określone w ust. 9, (m.in. śmierć, choroba uniemożliwiająca wykonywanie obowiązków służbowych) przekazanie obowiązków

kierownika kancelarii kryptograficznej realizuje komisja na zasadach określonych w ust. 3-8.

12. Przewodniczący komisji, o której mowa w ust. 11, do czasu przekazania obowiązków oznakowuje urządzenia do przechowywania informacji niejawnych, szafy, sejfy i skrzynie z nieprzekazanymi materiałami kryptograficznymi swoją numerową pieczęcią do teczki pracy lub w inny sposób jednoznacznie identyfikujący przewodniczącego komisji.

13. Protokół przekazania obowiązków podpisują przewodniczący oraz członkowie komisji, o której mowa w ust. 11, a zatwierdza kierownik jednostki organizacyjnej.

§ 7.1. W jednostkach organizacyjnych, w których wykorzystuje się lub planuje się wykorzystywać materiały kryptograficzne, utrzymuje się utworzone, lub tworzy się OBSŁiI nadzorujące pracę kancelarii kryptograficznej i stacji kryptograficznej.

2. OBSŁiI nadzorowane są przez OBSŁiI zgodnie z hierarchią zaopatrywania kancelarii kryptograficznych.

3. KOGD w ramach wykonywanych czynności specjalistycznych nadzoruje RCZBSiUT oraz inne OBSŁiI.

4. RCZBSiUT sprawuje nadzór nad OBSŁiI w dowództwach rodzajów Sił Zbrojnych Rzeczypospolitej Polskiej, Centrum Wsparcia Teleinformatycznego SZ RP, Dowództwie Garnizonu Warszawa, Dowództwie Operacyjnym Sił Zbrojnych, Inspektoracie Wsparcia Sił Zbrojnych, Dowództwie Wojsk Specjalnych i równorzędnych jednostkach organizacyjnych;

5. RCZBSiUT jest odpowiedzialny za:

1) koordynowanie działalności OBSŁiI w jednostkach organizacyjnych, o których mowa w ust. 4;
2) planowanie, organizowanie, prognozowanie rozwoju, eksploatacji i nadzoru nad funkcjonowaniem, systemów ochrony kryptograficznej stosowanych w systemach teleinformatycznych resortu obrony narodowej oraz podczas misji pokojowych i ćwiczeń, a także Wojennego Systemu Dowodzenia;
3) uzgadnianie z KOGD rozwiązań dotyczących prognozowania rozwoju, eksploatacji i nadzoru nad funkcjonowaniem, systemów ochrony kryptograficznej stosowanych w systemach teleinformatycznych resortu obrony narodowej;
4) planowanie, organizowanie oraz sprawowanie nadzoru nad szkoleniami specjalistycznymi personelu BSŁiI;
5) prowadzenie ewidencji dokonywanych kontroli lub inspekcji kryptograficznych nadzorowanych OBSŁiI;
6) opracowywanie i przesyłanie do KOGD do dnia 30 kwietnia każdego roku raportów:
   a) o stanie posiadanych materiałów kryptograficznych w kancelariach kryptograficznych zaopatrywanych bezpośrednio przez kancelarię kryptograficzną RCZBSiUT,
   b) o stanie ochrony informacji niejawnych w podległych kancelariach kryptograficznych za ubiegły rok z wyszczególnieniem:
   — kancelarii kryptograficznych objętych nadzorem,
   — stacji kryptograficznych objętych nadzorem,
   — formy nadzoru (kontrola, inspekcja itp.),
   — organów bezpieczeństwa systemów łączności i informatyki przeprowadzających inspekcje,
   — stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych;
7) prowadzenie ewidencji i realizowanie dystrybucji materiałów kryptograficznych przeznaczonych do użytkowania w jednostkach i komórkach organizacyjnych Sił Zbrojnych RP;
8) prowadzenie inspekcji kryptograficznych w jednostkach i komórkach organizacyjnych Sił Zbrojnych RP;
9) przedstawianie do KOGD zbiorczych zapotrzebowań na materiały kryptograficzne narodowe i sojusznicze dla potrzeb OBSŁiI jednostek i komórek organizacyjnych Sił Zbrojnych RP;
10) nadzorowanie wykorzystywania materiałów kryptograficznych przez OBSŁiI;
11) przeprowadzenie raz w roku odprawy rozliczeniowo-szkoleniowej dla Oficerów BSŁiI z OBSŁiI bezpośrednio nadzorowanych;
12) opracowywanie procedur obsługi urządzeń ochrony kryptograficznej i pomocniczego sprzętu kryptograficznego;
13) przeprowadzenie raz w roku odprawy rozliczeniowo-szkoleniowej dla kierowników kancelarii kryptograficznych bezpośrednio zaopatrywanych.

6. OBSŁiI jednostek organizacyjnych, o których mowa w ust. 4, są odpowiedzialne za:

1) koordynowanie działalności nadzorowanych OBSŁiI;
2) prowadzenie ewidencji dokonywanych kontroli lub/i inspekcji kryptograficznych nadzorowanych OBSŁiI;
3) opracowywanie i przesyłanie do RCZBSiUT do 15 marca każdego roku raportów:
   a) o stanie posiadanych materiałów kryptograficznych w kancelariach kryptograficznych zaopatrywanych bezpośrednio przez własną kancelarię kryptograficzną,
   b) o stanie ochrony informacji niejawnych w podległych kancelariach kryptograficznych za ubiegły rok z wyszczególnieniem:

— kancelarii kryptograficznych objętych nadzorem,
— stacji kryptograficznych objętych nadzorem,
— formy nadzoru (kontrola, inspekcja itp.),
— organów bezpieczeństwa systemów łączności i informatyki przeprowadzających inspekcje,
— stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych;
4) prowadzenie ewidencji i realizacja dystrybucji materiałów kryptograficznych przeznaczonych do użytkowania w zaopatrywanych jednostkach i komórkach organizacyjnych;
5) planowanie, organizowanie, prognozowanie rozwoju, eksploatacji i nadzoru nad funkcjonowaniem systemów ochrony kryptograficznej stosowanych w systemach teleinformatycznych podległych jednostek organizacyjnych;
6) uzgadnianie z RCZBSiUT rozwiązań, o których mowa w pkt 5.
7) prowadzenie inspekcji kryptograficznych w jednostkach organizacyjnych zaopatrywanych w materiały kryptograficzne;
8) przedstawianie do RCZBSiUT zbiorczych zapotrzebowań na narodowe i sojusznicze materiały kryptograficzne dla potrzeb OBSŁiI podległych jednostek organizacyjnych;
9) nadzorowanie wykorzystywania materiałów kryptograficznych przez podległe OBSŁiI;
10) przeprowadzenie raz w roku odprawy rozliczeniowo-szkoleniowej dla Oficerów BSłiI z OBSŁiI bezpośrednio nadzorowanych.

7. OBSŁiI szczebli organizacyjnych nadzorowanych przez organy, o których mowa w ust. 6, odpowiedzialne są za:
1) przedstawianie do nadrzędnych OBSŁiI zapotrzebowań na materiały kryptograficzne;
2) opracowywanie i przesyłanie do kancelarii do dnia 15 lutego każdego roku raportów:
a) o stanie posiadanych materiałów kryptograficznych w kancelariach kryptograficznych zaopatrywanych bezpośrednio przez własną kancelarię,
b) o stanie ochrony informacji niejawnych w podległych kancelariach kryptograficznych za ubiegły rok z wyszczególnieniem:
— kancelarii kryptograficznych objętych nadzorem,
— stacji kryptograficznych objętych nadzorem,
— formy nadzoru (kontrola, inspekcja itp.),
— organów bezpieczeństwa systemów łączności i informatyki przeprowadzających inspekcje,
— stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych;
3) właściwe wykorzystywanie oraz rozliczanie narodowych i sojuszniczych materiałów kryptograficznych;
4) prowadzenie ewidencji oraz realizacja dystrybucji materiałów kryptograficznych;
5) przeprowadzanie inspekcji kryptograficznych w jednostkach organizacyjnych zaopatrywanych w materiały kryptograficzne;
6) realizowanie dodatkowych zadań dotyczących bezpieczeństwa teleinformatycznego oraz zarządzania materiałami kryptograficznymi, postawionych przez OBSŁiI wyższego szczebla organizacyjnego.

8. Kierownik jednostki organizacyjnej w celu nadzoru nad bezpieczeństwem materiałów kryptograficznych powołuje Oficera BSŁiI.

9. Funkcja, o której mowa w ust. 8, sprawowana jest przez:
1) osobę wyznaczoną w RCZBSiUT przez Komendanta RCZBSiUT;
2) szefa (oddziału, wydziału, sekcji, grupy) w komórkach bezpieczeństwa systemów łączności i informatyki;
3) kierownika komórki odpowiedzialnej za organizację łączności w jednostce organizacyjnej w Siłach Zbrojnych RP, w której nie występuje etatowa komórka BSŁiI;
4) kierownika komórki organizacyjnej, w której planowane jest powołanie kancelarii kryptograficznej w jednostce organizacyjnej.

10. Oficer BSŁiI jest odpowiedzialny za zapewnienie bezpieczeństwa materiałom kryptograficznym w tym za sprawdzanie wszystkich miejsc w jednostce organizacyjnej, w których są przechowywane i wykorzystywane te materiały.

11. Do zadań i obowiązków Oficera BSŁiI należy:
1) uzgadnianie bezpośrednio z kierownikiem jednostki organizacyjnej wszelkich zagadnień związanych z ochroną materiałów kryptograficznych oraz funkcjonowaniem OBSŁiI;
2) przedstawianie kierownikowi jednostki organizacyjnej propozycji właściwych rozwiązań w sprawach związanych z bezpieczeństwem materiałów kryptograficznych oraz zabezpieczeniem kryptograficznym systemów teleinformatycznych jednostki organizacyjnej;
3) realizowanie zadań postawionych przez Oficera BSŁiI z OBSŁiI szczebla wyższego (zgodnie z hierarchią systemu OBSŁiI) w zakresie specjalistycznym dotyczącym przechowywania, przesyłania oraz stosowania i wykorzystywania materiałów kryptograficznych;
4) współpraca z pionem ochrony w zakresie zastosowanych środków ochrony fizycznych

i technicznych przeznaczonych do ochrony materiałów kryptograficznych;
5) informowanie nadrzędnego OBSŁiI (zgodnie z hierarchią systemu OBSŁiI) o potrzebach w zakresie zabezpieczenia w materiały kryptograficzne jednostki organizacyjnej;
6) wskazywanie osób odpowiedzialnych za zabezpieczanie dokumentami kryptograficznymi urządzeń kryptograficznych;
7) nadzorowanie przekazywania materiałów kryptograficznych poza jednostkę organizacyjną;
8) sprawdzanie systemów teleinformatycznych, w których przetwarzane są informacje dotyczące tematyki kryptograficznej;
9) opracowanie instrukcji pracy kancelarii kryptograficznej i stacji kryptograficznej (o ile taka istnieje w jednostce organizacyjnej);
10) opracowanie zakresu obowiązków dla personelu BSŁiI oraz nadzorowanie przestrzegania tych obowiązków przez ten personel;
11) opracowanie planów ewakuacji, niszczenia materiałów kryptograficznych na wypadek zagrożenia oraz zapewnienie niezbędnych środków i sprzętu do wdrażania tych planów;
12) wnioskowanie do kierownika jednostki organizacyjnej o kierowanie osób z OBSŁiI oraz osób spoza tego organu (posiadających kwalifikacje techniczne związane z informatyką, elektroniką bądź kierunkami pokrewnymi), które mogłyby w przyszłości objąć stanowiska w OBSŁiI, na organizowane specjalistyczne kursy i szkolenia;
13) dokumentowanie przeprowadzonych instruktaży i szkoleń dotyczących tematyki kryptograficznej;
14) wnioskowanie do kierownika jednostki organizacyjnej o przyznanie CUK;
15) udzielanie osobom, które uzyskały CUK, instruktaży w chwili rozpoczęcia pełnienia obowiązków służbowych związanych z dostępem do materiałów kryptograficznych;
16) przeprowadzenie szkolenia co najmniej raz w roku z zakresu ochrony materiałów kryptograficznych wszystkim osobom posiadającym wystawiony CUK;
17) wnioskowanie do kierownika jednostki organizacyjnej o anulowanie CUK;
18) prowadzenie ewidencji wydanych CUK oraz monitorowanie ich statusu;
19) utrzymywanie i podnoszenie poziomu bezpieczeństwa fizycznego pomieszczeń kancelarii kryptograficznych oraz stacji kryptograficznych, łącznie z prowadzeniem sprawdzeń poziomu bezpieczeństwa w określonych odstępach czasowych;
20) meldowanie kierownikowi jednostki organizacyjnej oraz Oficerowi BSŁiI szczebla nadrzędnego o stwierdzonych incydentach mających wpływ na bezpieczeństwo materiałów kryptograficznych;
21) niezwłoczne składanie pisemnych meldunków bezpośrednio do KOGD o wszelkich stwierdzonych incydentach mających wpływ na bezpieczeństwo materiałów kryptograficznych (zagubienie, czasowa utrata kontroli nad materiałem kryptograficznym, itp.);
22) nadzorowanie poprawności prowadzenia wymaganej dokumentacji w kancelarii kryptograficznej, stacji kryptograficznej;
23) nadzorowanie wykorzystywania, obsługiwania oraz ochrony urządzeń i innych elementów systemów kryptograficznych w stacjach kryptograficznych;
24) okresowe sprawdzanie stosowania przez personel BSŁiI procedur uzbrajania urządzeń kryptograficznych dokumentami kryptograficznymi oraz obsługi przez ten personel urządzeń i narzędzi ochrony kryptograficznej eksploatowanych w jednostce organizacyjnej;
25) planowanie i organizowanie inspekcji kryptograficznych OBSŁiI:
   a) nie rzadziej niż co rok — we własnej jednostce organizacyjnej,
   b) nie rzadziej niż co dwa lata — jednostek organizacyjnych zaopatrywanych w materiały kryptograficzne o jeden szczebel organizacyjny w dół;
26) doraźne sprawdzanie wypełniania zadań oraz znajomości obowiązków przez personel BSŁiI jednostek organizacyjnych zaopatrywanych o jeden szczebel organizacyjny w dół nie rzadziej niż co dwa lata;
27) kontrolowanie terminu upływu ważności certyfikatów wystawionych dla poszczególnych urządzeń oraz certyfikatów/świadectw akredytacji bezpieczeństwa systemu teleinformatycznego dla systemów przetwarzających informacje niejawne dotyczące tematyki kryptograficznej, a w przypadku ich wygaśnięcia wnioskowanie do kierownika jednostki organizacyjnej o zamknięcie tych systemów.

12. Dla systemów teleinformatycznych przetwarzających materiały kryptograficzne inspektora bezpieczeństwa teleinformatycznego wyznacza się spośród pracowników pionu ochrony, a administratora systemu teleinformatycznego można wyznaczyć spośród personelu BSŁiI.

13. System teleinformatyczny, o którym mowa w ust. 12, może być kontrolowany przez inspektora bezpieczeństwa teleinformatycznego tylko w obecności administratora tego systemu. Inspektorowi bezpieczeństwa teleinformatycznego nie wystawia się CUK.

Rozdział 3

Środki bezpieczeństwa fizycznego

§ 8.1. Kancelarie kryptograficzne cechuje wysoki poziom zagrożenia związany z utratą informacji niejawnych. Lokalizuje się je w pomieszczeniu lub pomieszczeniach spełniających następujące warunki bezpieczeństwa:

1) usytuowanych, z zastrzeżeniem ust. 2 i 3, w budynku o konstrukcji murowanej, betonowej lub innej o podobnych właściwościach (parametrach) konstrukcyjnych, z wejściem ze strefy ochronnej:
   a) dla pomieszczeń, których ściany stanowią granicę strefy ochronnej, jeżeli materiały kryptograficzne nie są przechowywane w urządzeniach, o których mowa w ust. 9 pkt 1, ściany zewnętrzne powinny:
   — być wykonane z materiałów niepalnych, spełniających wymagania klasy odporności pożarowej,
   — spełniać wymagania nośności granicznej odpowiadającej, co najmniej konstrukcji ściany murowanej, wykonanej z cegły pełnej klasy 15 o grubości 32 cm lub betonu zbrojonego o grubości 20 cm,
   b) dla pomieszczeń, których ściany stanowią granicę strefy ochronnej, jeżeli materiały kryptograficzne są przechowywane w urządzeniach, o których mowa w ust. 9 pkt 1, ściany zewnętrzne powinny:
   — być wykonane z materiałów niepalnych, spełniających wymagania w zakresie klasy odporności pożarowej,
   — spełniać wymagania nośności granicznej odpowiadającej, co najmniej konstrukcji ściany murowanej, wykonanej z cegły pełnej klasy 15 o grubości 25 cm lub betonu zbrojonego o grubości 15 cm,
   c) dla pomieszczeń, których ściany nie stanowią granicy strefy ochronnej, jeżeli materiały kryptograficzne nie są przechowywane w urządzeniach, o których mowa w ust. 9 pkt 1, ściany zewnętrzne powinny:
   — być wykonane z materiałów niepalnych, spełniających wymagania w zakresie klasy odporności pożarowej,
   — spełniać wymagania nośności granicznej odpowiadającej, co najmniej konstrukcji ściany murowanej, wykonanej z cegły pełnej klasy 15 o grubości 25 cm lub betonu zbrojonego o grubości 15 cm,
   d) dla pomieszczeń, których ściany nie stanowią granicy strefy ochronnej, jeżeli materiały kryptograficzne są przechowywane w urządzeniach, o których mowa w ust. 9 pkt 1, ściany zewnętrzne powinny:
   — być wykonane z materiałów niepalnych, spełniających wymagania klasy odporności pożarowej,
   — spełniać wymagania nośności granicznej odpowiadającej, co najmniej konstrukcji ściany murowanej, wykonanej z cegły pełnej klasy 15 o grubości 18 cm lub betonu zbrojonego o grubości 10 cm;
2) w przypadku braku możliwości spełnienia warunków grubości ścian, o których mowa w ust. 1, należy zastosować inne dodatkowe zabezpieczenia, które zapewnią czas odporności na włamanie większy niż czas niezbędny do przybycia służb ochrony jednostki organizacyjnej, m.in. czujki sejsmiczne montowane na tych ścianach, stałą obserwację systemem telewizji przemysłowej ścian zewnętrznych i innych narażonych na sforsowanie, wzmocnienie ścian przez ułożenie certyfikowanych metalowych (stalowych) paneli kancelaryjnych;
3) wyposażonych w drzwi wejściowe metalowe spełniające wymagania klasy odporności nie niższej niż RC 4 określone w Polskiej Normie PN-EN 1627, blokowane na 4 krawędziach, zabezpieczone przed wyłamaniem od strony zawiasów, posiadające element samozatrzaskowy uniemożliwiający pozostawienie pomieszczenia otwartego, samozamykacz oraz dodatkowo wyposażone w zamek mechaniczny szyfrowy, co najmniej klasy B według Polskiej Normy PN-EN 1300 co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem (atakiem) radiologicznym (promieniowanie z radioaktywnego źródła nieprzekraczającego równowartości 10 curie, co — 60 z odległości 760 mm przez 20 godzin). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Drzwi powinny być wyposażone w dwa komplety kluczy niezbędnych do ustawiania szyfru. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, co najmniej klasy B według Polskiej Normy PN-EN 1300, pod warunkiem że zamek spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wy-

korzystane do otwarcia zamka przez okres 20 roboczogodzin;

4) wyposażonych w okna zabezpieczone w sposób uniemożliwiający wgląd do pomieszczeń z zewnątrz z zainstalowaniem w otworach okiennych, z zastrzeżeniem pkt 5, kraty wykonanej w ramie z płaskownika stalowego o przekroju nie mniejszym niż 45 x 6 mm, z prętów stalowych o średnicy co najmniej 18 mm, usytuowanych pionowo z prześwitem pomiędzy nimi nie większym niż 150 mm, wzmocnionej płaskownikami stalowymi o przekroju nie mniejszym niż 45 x 6 mm, usytuowanymi w poziomie, w odstępach nie większych niż 500 mm, z tym że jeżeli ze względów architektoniczno-budowlanych nie ma możliwości zainstalowania kraty, dopuszcza się zamontowanie certyfikowanego (kwalifikowanego) okna antywłamaniowego spełniającego wymagania klasy odporności nie niższej niż RC 3 określone w Polskiej Normie PN-EN 1627;
5) otwory okienne, których dolna krawędź znajduje się na wysokości powyżej 5 m od poziomu otaczającego terenu, a górna krawędź więcej niż 3 m od poziomu dachu, wyposaża się w jedno z następujących zabezpieczeń:
   a) siatkę z drutu stalowego o grubości drutu nie mniejszej niż 2 mm, o oczkach nie większych niż 20 x 20 mm lub powierzchni oczka nie większej niż 4 cm^2,
   b) zabezpieczenie przed otwarciem od wewnątrz, wraz z folią antywłamaniową lub certyfikowane (kwalifikowane) okno antywłamaniowe spełniające wymagania klasy odporności nie niższej niż RC 2 N określone w Polskiej Normie PN — EN 1627 z szybą o podwyższonej odporności na włamanie — co najmniej klasy P-3A według PN-EN-356;
6) otwory wentylacyjne o powierzchni powyżej 500 cm^2, siatką o oczkach nie większych niż 10 x 10 mm lub urządzeniami alarmowymi;
7) wyposażonych w kontrolę dostępu, z tym że:
   a) instalowane systemy kontroli dostępu powinny spełniać wymagania techniczne i organizacyjne określone w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe,
   b) w przypadku braku systemu kontroli dostępu prowadzona jest książka wejścia/wyjścia. Dane z ewidencji są przechowywane co najmniej z okresu ostatnich 3 miesięcy;
8) wyposażonych w system alarmowy, z tym że:
   a) powinien on sygnalizować nieuprawnione otwarcie drzwi wejściowych i okien, ruch w pomieszczeniach oraz próby napadu,
   b) powinien spełniać wymagania techniczne i organizacyjne określone w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe;
9) wyposażonych w system sygnalizacji pożaru.

2. Kraty, o których mowa w ust. 1 pkt 4, mogą być rozsuwane lub otwierane pod warunkiem ich zabezpieczenia co najmniej jedną kłódką klasy 5 według PN-EN-12320:2002.

3. Zabrania się lokalizowania kancelarii kryptograficznych na poddaszach.

4. Organizując kancelarię kryptograficzną należy mieć na uwadze wydzielenie pomieszczeń z przeznaczeniem do:
1) pracy personelu kancelarii (stacji) kryptograficznej;
2) przyjmowania interesantów oraz zapoznawania się z materiałami kryptograficznymi;
3) naprawy lub serwisowania urządzeń ochrony kryptograficznej w przypadku kancelarii kryptograficznych organizowanych w jednostkach serwisujących.

5. W zależności od potrzeb organizując kancelarię kryptograficzną wydziela się dodatkowe pomieszczenia z przeznaczeniem na:
1) magazynowanie materiałów kryptograficznych;
2) eksploatację systemów teleinformatycznych;
3) pomieszczenie socjalne dla personelu kancelarii kryptograficznej.

6. Pomieszczenie magazynowe, o którym mowa w ust. 5 pkt 1, wyposaża się w drzwi wejściowe, o których mowa w ust. 1 pkt 3.

7. Część kancelarii kryptograficznej przeznaczoną do przechowywania materiałów kryptograficznych oraz wykonywania pracy przez personel kancelarii, odgradza się barierką albo ścianą działową z okienkiem od części przeznaczonej do wydawania i udostępniania materiałów kryptograficznych.

8. W kancelariach kryptograficznych, w których są przechowywane materiały niejawne oznaczone klauzulą „Ściśle tajne", instaluje się telewizyjny system nadzoru drzwi wejściowych z zewnątrz, z rejestracją zdarzeń oraz elektroniczne systemy kontroli dostępu. Wymagania ogólne dotyczące funkcjonowania elektronicznego systemu kontroli dostępu zawarte są w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe.

9. Kancelarię kryptograficzną wyposaża się w:
1) urządzenia do przechowywania informacji niejawnych, z zastrzeżeniem ust. 1 pkt 1 lit. a i c, odpowiednio do potrzeb w:
   a) szafy stalowe klasy C — do przechowywania materiałów kryptograficznych oznaczonych klauzulą „Ściśle tajne", a także „Tajne", „Poufne" i „Zastrzeżone",
   b) szafy stalowe klasy B — do przechowywania materiałów kryptograficznych oznaczonych

klauzulą „Tajne", a także „Poufne" i „Zastrzeżone",
c) szafy stalowe klasy A — do przechowywania materiałów kryptograficznych oznaczonych klauzulą „Poufne", a także „Zastrzeżone";
2) regały, szafy meblowe lub meble przeznaczone do przechowywania teczek akt lub wydawnictw;
3) sprzęt kwaterunkowo-biurowy;
4) pojemniki lub worki służące do przechowywania materiałów kryptograficznych przeznaczonych do zniszczenia oraz do ewakuacji materiałów;
5) urządzenia klasy V według normy DIN 32757 do niszczenia materiałów kryptograficznych w formie papierowej.

10. Klasyfikację i wymagania techniczne urządzeń, o których mowa w ust. 9 pkt 1, określa załącznik Nr 3.

11. Na drzwiach urządzeń, o których mowa w ust. 9 pkt 1 oraz pomieszczeń kancelarii kryptograficznej, o których mowa w ust. 1 pkt 3 oraz w ust. 6, nakleja się karty informacyjne, których wzór określa załącznik Nr 4.

12. Kancelarie kryptograficzne, w zależności od potrzeb, wyposaża się w niejawne systemy teleinformatyczne.

13. Eksploatacja jawnych systemów teleinformatycznych, z wyjątkiem stacjonarnych aparatów telefonicznych, a w szczególności urządzeń faksowych i systemów podłączonych do sieci INTERNET wymaga zgody Szefa KOGD.

14. Środki bezpieczeństwa fizycznego dla pomieszczeń kancelarii kryptograficznych wyposażonych w systemy teleinformatyczne, o których mowa w ust. 13, regulują odrębne przepisy.

15. W szczególnie uzasadnionych przypadkach, uniemożliwiających spełnienie któregokolwiek z warunków, o których mowa w ust. 1-2 i 6-9, zgodę na zastosowanie alternatywnych środków bezpieczeństwa udziela Szef KOGD.

16. Pomieszczenia kancelarii kryptograficznej obejmuje się bezpośrednią ochroną fizyczną w postaci posterunku wystawionego przy budynku lub okresowym patrolowaniem terenu wokół budynku nie rzadziej niż raz na dzień i dwa razy w nocy. Czas reakcji wartowników/pracowników ochrony w przypadku wystąpienia sytuacji alarmowych i dotarcia do miejsca zdarzenia nie może być dłuższy niż 10 minut.

§ 9.1. W kancelariach kryptograficznych zlokalizowanych w pomieszczeniach, o których mowa w § 8 ust. 1 pkt 1 lit. a i c materiały kryptograficzne, fizycznie od siebie oddzielone (narodowe oraz pochodzące z wymiany międzynarodowej), z zastrzeżeniem ust. 2 i 3, mogą być przechowywane w pomieszczeniach, o których mowa w § 8:
1) ust. 4, w zamykanych regałach, meblach, szafach meblowych, pojemnikach lub pokrowcach uniemożliwiających ich podgląd;
2) ust. 5, na regałach lub szafach meblowych, w pojemnikach lub pokrowcach.

2. Dokumenty kryptograficzne przyszłych edycji pochodzące z wymiany międzynarodowej należy przechowywać w urządzeniach, o których mowa w § 8 ust. 9 pkt 1.

3. Dokumenty kryptograficzne bieżącej edycji niewykorzystywane do pracy urządzeń i narzędzi kryptograficznych eksploatowanych w kancelariach kryptograficznych oraz dokumenty kryptograficzne niezabezpieczone przed podglądem w sposób określony w wydanych przez SKW „Zaleceniach w zakresie postępowania z bezpiecznymi kopertami", należy przechowywać w urządzeniach, o których mowa w § 8 ust. 9 pkt 1.

4. W kancelariach kryptograficznych zlokalizowanych w pomieszczeniach, o których mowa w § 8 ust. 1 pkt 1 lit. b i d materiały kryptograficzne należy przechowywać w urządzeniach, o których mowa w § 8 ust. 9 pkt 1, odrębnych dla materiałów narodowych i pochodzących z wymiany międzynarodowej oraz dokumentów kryptograficznych bieżącej i przyszłych edycji, z zastrzeżeniem ust. 5.

5. Materiały, o których mowa w ust. 4, mogą być przechowywane w jednym urządzeniu, pod warunkiem, że jej konstrukcja pozwala na ich fizyczne rozdzielenie i zamknięcie w odrębnych skrytkach.

6. W przypadkach, o których mowa w ust. 5, klasa urządzenia musi uwzględniać klauzulę tajności najwyżej sklasyfikowanego materiału przechowywanego w tym urządzeniu.

7. Nieeksploatowane urządzenia kryptograficzne z wprowadzonymi dokumentami kryptograficznymi należy deponować w pomieszczeniach, o których mowa w ust. 1 i 4, stosownie do maksymalnej klauzuli urządzenia kryptograficznego i wprowadzonego dokumentu kryptograficznego.

8. W pomieszczeniach służbowych wykonawców nie spełniających standardów bezpieczeństwa, określonych w § 8 ust. 1, 8 i 9, materiały kryptograficzne, o których mowa w § 2 pkt 20:
1) lit. a, d-h należy przechowywać wyłącznie w urządzeniach, o których mowa w § 8 ust. 9 pkt 1 za pisemną zgodą kierownika jednostki organizacyjnej;

2) lit. b i c należy przechowywać zgodnie z procedurami ochrony tych materiałów zatwierdzonymi przez kierownika jednostki organizacyjnej i zaakceptowanymi przez Szefa KOGD.

9. Zabrania się przechowywania materiałów kryptograficznych w pomieszczeniach zlokalizowanych poza strefami ochronnymi z zastrzeżeniem § 29 ust. 1.

10. W szczególnie uzasadnionych przypadkach przechowywanie materiałów kryptograficznych poza strefami ochronnymi może odbywać się za zgodą Szefa KOGD.

§ 10.1. Po zakończeniu pracy, personel kancelarii kryptograficznej zamyka i zabezpiecza urządzenia do przechowywania informacji niejawnych oraz pomieszczenia służbowe kancelarii.

2. Zasady zdawania, przechowywania i wydawania kluczy użytku bieżącego do pomieszczeń służbowych i urządzeń do przechowywania informacji niejawnych, o których mowa w ust. 1, określa plan ochrony informacji niejawnych jednostki organizacyjnej oraz instrukcja pracy kancelarii kryptograficznej, stanowiąca załącznik Nr 5.

3. Klucze zapasowe do pomieszczeń kancelarii kryptograficznej, pomieszczeń magazynowych i urządzeń do przechowywania informacji niejawnych należy przechowywać w zabezpieczonych, oddzielnych pojemnikach lub kopertach w kancelarii tajnej w szafach stalowych co najmniej klasy B, w sposób zapewniający fizyczne ich oddzielenie od kodów, o których mowa w ust. 5 i 7.

4. Oznaczone klucze, o których mowa w ust. 2 i 3, nie oznacza się klauzulą tajności, ale podlegają szczególnej ochronie, między innymi poprzez sprawdzenie podczas otwierania i zamykania urządzenia do przechowywania informacji niejawnych, o których mowa w ust. 3, czy znajdują się w nienaruszonych pojemnikach lub kopertach.

5. Kody dostępu do pomieszczeń kancelarii kryptograficznej, pomieszczeń magazynowych, urządzeń do przechowywania informacji niejawnych, określone w załączniku Nr 6, należy przechowywać w pomieszczeniu kancelarii tajnej lub innej kancelarii danej jednostki organizacyjnej, w szafach stalowych co najmniej klasy B.

6. Kody, o których mowa w ust. 5, oznacza się klauzulą tajności i umieszcza w zabezpieczonych i oznaczonych kopertach, których sposób oznaczania określa załącznik Nr 6.

7. Kody systemu alarmowego do pomieszczeń kancelarii kryptograficznej należy przechowywać w pomieszczeniu kancelarii tajnej lub innej kancelarii danej jednostki organizacyjnej, w szafach stalowych co najmniej klasy B, w sposób zapewniający fizyczne ich oddzielenie od kodów, o których mowa w ust. 5.

8. Kody, o których mowa w ust. 7, posiadają klauzulę tajności i umieszcza się je w zabezpieczonych i oznaczonych kopertach.

9. Zabrania się zapisywania przez użytkowników kodów dostępu w inny sposób niż określony w ust. 8, wynoszenia ich oraz kluczy, o których mowa w ust. 2 i 3, poza teren jednostki organizacyjnej.

10. Kody dostępu, o których mowa w ust. 5, zmienia się:
1) w nowo instalowanych urządzeniach do przechowywania informacji niejawnych i drzwiach z zamkami szyfrowymi;
2) po każdej naprawie lub konserwacji zamka;
3) po przekazaniu obowiązków przez osobę pełniącą służbę albo zatrudnioną w kancelarii kryptograficznej;
4) w przypadku ujawnienia lub podejrzenia ujawnienia kodu osobie nieupoważnionej;
5) w odstępach czasowych nie przekraczających 6 miesięcy od ostatniej zmiany kodu.

11. Kody, o których mowa w ust. 7, zmienia się w przypadku ujawnienia lub podejrzenia ujawnienia kodu osobie nieupoważnionej oraz w przypadku przekazania obowiązków przez osobę pełniącą obowiązki na stanowisku w kancelarii kryptograficznej.

12. W razie utraty, domniemania ujawnienia kluczy, zagubienia kluczy, o których mowa w ust. 2 i 3, należy wymienić zamki, a o fakcie ich utraty lub zagubienia poinformować pisemnie kierownika jednostki organizacyjnej.

Rozdział 4

Zasady organizacji, funkcjonowania i zabezpieczenia kancelarii kryptograficznych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów kryptograficznych na okrętach i pomocniczych jednostkach pływających Marynarki Wojennej

§ 11.1. Kancelarie kryptograficzne na okręcie i pomocniczej jednostce pływającej organizuje się w pomieszczeniach spełniających następujące warunki bezpieczeństwa:
1) zlokalizowanych pod pokładem głównym okrętu lub wyjątkowo w nadbudówce;
2) oddzielonych od innych pomieszczeń trwałymi ścianami (szotami) bez otworów

konstrukcyjnych, z konstrukcją ścian (szotów) uniemożliwiającą przedostanie się do wewnątrz przy użyciu narzędzi ręcznych;

3) nie posiadających okien (iluminatorów), a gdy jest to niemożliwe, okna (iluminatory) powinny być zabezpieczone systemem alarmowym, wykonane ze szkła o zwiększonej odporności na włamanie (klasy od P5 do P8) i zabezpieczone w sposób uniemożliwiający wgląd z zewnątrz;

4) wyposażonych w drzwi wejściowe (włazy) wykonane ze stali, zabezpieczone przed włamaniem od strony zawiasów i ryglowane na trzech pozostałych płaszczyznach, zamykane na zamki odpowiadające wymaganiom określonym w § 8 ust. 1 pkt 3.

2. Pomieszczenia kancelarii kryptograficznych chroni się ogólnookrętową instalacją przeciwpożarową.

3. W kancelarii kryptograficznej instaluje się systemy sygnalizujące próby siłowego otwarcia drzwi wejściowych (włazu), ruch w pomieszczeniach oraz system sygnalizacji napadu.

4. Instalowane systemy i urządzenia alarmowe powinny spełniać warunki, o których mowa w § 8 ust. 9.

5. Kancelarię kryptograficzną wyposaża się w szafę klasy C, wyposażoną w zamykane skrytki umożliwiające odrębne przechowywanie materiałów kryptograficznych o różnych klauzulach tajności oraz urządzenia, o których mowa w § 8 ust. 6 i ust. 9 pkt 5.

6. Podczas postoju w porcie macierzystym, materiały kryptograficzne przekazuje się do kancelarii zabezpieczającej w materiały kryptograficzne, z zastrzeżeniem ust. 8.

7. Podczas postoju w porcie nie będącym portem macierzystym, materiały kryptograficzne z zastrzeżeniem ust. 8 przechowuje się urządzeniach do przechowywania informacji niejawnych, o których mowa w § 8 ust. 9 pkt 1.

8. Podczas postoju w porcie nie demontuje się urządzeń kryptograficznych z systemów łączności.

9. Na okrętach i pomocniczych jednostkach pływających, na których nie ma możliwości zorganizowania kancelarii kryptograficznej, materiały kryptograficzne przechowuje się w kabinie radio lub kabinie dowódcy okrętu w urządzeniach do przechowywania informacji niejawnych, o których mowa w § 8 ust. 9 pkt 1. Po powrocie do macierzystego portu okrętu i pomocniczych jednostek pływających materiały kryptograficzne należy przekazać do kancelarii kryptograficznej zaopatrującej w te materiały.

10. Na okrętach i pomocniczych jednostkach pływających, na których nie ma możliwości zorganizowania kancelarii kryptograficznej materiały kryptograficzne w formie papierowej można niszczyć w urządzeniach, o których mowa w § 8 ust. 9 pkt 5.

11. W szczególnie uzasadnionych przypadkach, uniemożliwiających spełnienie któregokolwiek z warunków dotyczących systemu zabezpieczeń kancelarii kryptograficznej na okrętach i pomocniczych jednostkach pływających Marynarki Wojennej, zgody na zastosowanie alternatywnych środków bezpieczeństwa udziela Szef KOGD.

Rozdział 5

Zasady rejestrowania, kompletowania i niszczenia materiałów kryptograficznych

§ 12.1. Kancelaria kryptograficzna przyjmuje, rejestruje, przechowuje, przekazuje i dystrybuuje materiały kryptograficzne oraz prowadzi następujące urządzenia:

1) trwałe urządzenia ewidencyjne:
   a) rejestr teczek materiałów kryptograficznych, dzienników i książek ewidencyjnych, zwany dalej „Rejestrem dokumentacji" oznaczany jako RTMK, którego wzór określa załącznik Nr 7,
   b) dziennik korespondencji, którego wzór określa załącznik Nr 8,
   c) dziennik ewidencji szyfrogramów, którego wzór określa załącznik Nr 9;
2) pomocnicze urządzenia ewidencyjne:
   a) pomocnicza książka ewidencji pieczęci, której wzór określa załącznik Nr 10,
   b) kartoteka wydanych materiałów kryptograficznych, w skład której wchodzą:
   — rejestr wydanych materiałów kryptograficznych, zwany dalej „RWMK", którego wzór określa załącznik Nr 11,
   — skorowidz rejestrów wydanych materiałów kryptograficznych, zwany dalej „Skorowidzem RWMK", którego wzór określa załącznik Nr 12,
   c) książka doręczeń przesyłek miejscowych, zwana dalej „Książką doręczeń", której wzór określa załącznik Nr 13,
   d) karta zapoznania się z materiałem kryptograficznym oznaczonym klauzulą „Ściśle tajne"/"Tajne", zwana dalej „Kartą zapoznania się z materiałem kryptograficznym", której wzór określa załącznik Nr 14,
   e) karty ewidencyjne dokumentów kryptograficznych (formularz AF 54 A PL), którego wzór określa załącznik Nr 15,
   f) karty ewidencyjne urządzeń ochrony kryptograficznej (formularz AF 54 B PL), którego wzór określa załącznik Nr 16,

g) karty ewidencyjne publikacji, wydawnictw, dokumentacji technicznej i standaryzacyjnej oraz materiałów filmowych dotyczących tematyki kryptograficznej (formularz AF 54 C PL), którego wzór określa załącznik Nr 17,
h) formularz AF 147 PL ewidencjonujący karty formularzy AF 21 PL, którego wzór określa załącznik Nr 18,
i) karta raportów dotyczących środków i materiałów kryptograficznych (formularz AF 21 PL) wykorzystywana do przygotowywania raportów z działalności kancelarii kryptograficznej w zakresie przekazywania, niszczenia, inwentaryzacji, posiadania, wypożyczenia odręcznego i kontroli, której wzór określa załącznik Nr 19,
j) formularz wykazów przesyłek (AF 69 PL), którego wzór określa załącznik Nr 20 w przypadku przekazywania materiałów z kancelarii kryptograficznej do kancelarii kryptograficznej poprzez personel kancelarii lub poprzez Wojskową Służbę Kurierską (Formularza AF 69 PL nie stosuje się w przypadku przekazywania pism poprzez Wojskowy Węzeł Pocztowy lub innych przewoźników, w tej sytuacji stosuje się wykaz przesyłek nadanych).

2. W przypadku funkcjonowania w jednostce organizacyjnej elektronicznego obiegu materiałów kryptograficznych dopuszcza się prowadzenie w kancelarii kryptograficznej komputerowych baz materiałów kryptograficznych oraz urządzeń ewidencyjnych w formie elektronicznej.

3. Dopuszcza się zarządzanie materiałami kryptograficznymi w kancelariach kryptograficznych poprzez zastosowanie elektronicznego systemu zarządzania materiałami kryptograficznymi.

4. W przypadkach uzasadnionych organizacją ochrony informacji kryptograficznych, kancelaria kryptograficzna może prowadzić także inne urządzenia ewidencyjne niż wymienione w ust. 1.

5. Strony urządzeń ewidencyjnych, o których mowa w § 12 ust. 1 pkt 1 lit. b i c, pkt 2 lit. b tiret drugi oraz teczki akt w formie broszur numeruje się i oznacza w sposób określony w rozporządzeniu Prezesa Rady Ministrów wydanym na podstawie art. 6 ust. 9 ustawy. Na ostatniej stronie urządzenia zamieszcza się adnotację o sumarycznej ilości stron poświadczoną podpisem kierownika kancelarii kryptograficznej, datą sporządzenia adnotacji i odciskiem pieczęci „Do pakietów".

§ 13.1. Wzory pieczęci stosowanych w kancelarii kryptograficznej określa załącznik Nr 21.

2. W urządzeniach ewidencyjnych, o których mowa w § 12 ust. 1 pkt 1 lit. a-c zaznacza się początek i koniec roku kalendarzowego, a po zakończeniu roku sporządza się adnotację informującą o pozycji zapisu, na której zakończono ewidencję, potwierdzoną podpisem kierownika kancelarii kryptograficznej i pieczęcią „Do pakietów" oraz wpisuje datę sporządzenia adnotacji.

3. Zapisów w urządzeniach ewidencyjnych dokonuje się czarnym lub niebieskim tuszem (atramentem).

4. Odciski pieczęci nanosi się tuszem w kolorze czerwonym, czarnym lub niebieskim.

5. Zmiany zapisów w urządzeniach ewidencyjnych nanosi się kolorem czerwonym poprzez skreślenie pierwotnego zapisu i umieszczenie obok nowego uwierzytelnionego czytelnym podpisem dokonującego zmiany i wpisaniem daty wprowadzenia zmiany. Zabrania się wycierania, zamazywania i zaklejania zapisów w urządzeniach ewidencyjnych.

6. Adnotacje o zmianie lub zniesieniu jego klauzuli tajności nanosi się kolorem czerwonym, poprzez skreślenie pierwotnego zapisu i wpisanie nowego w stosownej rubryce urządzenia ewidencyjnego (np. „Zniesiono klauzulę tajności" itp.), uwierzytelnionego czytelnym podpisem dokonującego zmiany. Dodatkowo wpisuje się podstawę wprowadzenia zmiany (np. „pismo Nr ... z dnia ...").

7. Zapisy w elektronicznych urządzeniach ewidencyjnych są nieusuwalne; zapis błędny lub omyłkowy wymaga sprostowania przez wykonanie nowego zapisu.

8. W przypadku funkcjonowania w jednostce organizacyjnej elektronicznego obiegu materiałów kryptograficznych, adnotacje o zmianie lub zniesieniu jego klauzuli tajności, rejestruje się w formie elektronicznej.

§ 14.1. Rejestr dokumentacji jest nadrzędnym urządzeniem ewidencyjnym w stosunku do innych urządzeń ewidencyjnych prowadzonych przez kancelarię kryptograficzną.

2. Rejestr dokumentacji zalicza się do trwałych urządzeń ewidencyjnych szczególnego rodzaju, nadrzędnym w stosunku do trwałych i pomocniczych urządzeń ewidencyjnych kancelarii kryptograficznej w danej jednostce organizacyjnej — jest, prowadzony wyłącznie przez kancelarię kryptograficzną jednostki jako księga, przeznaczony do ewidencjonowania:
1) trwałych oraz pomocniczych urządzeń ewidencyjnych prowadzonych przez kancelarię kryptograficzną, jeżeli te ostatnie podlegają zdaniu do archiwum lub pozostają w danej jednostce organizacyjnej;

2) teczek z materiałami kryptograficznymi (każdy tom teczek ewidencjonuje się pod oddzielną pozycją w Rejestrze dokumentacji).

3. Rejestr dokumentacji:

1) zakłada się:
   a) w powołanej kancelarii kryptograficznej jednostki organizacyjnej opatrując go adnotacją o ilości kart, poświadczoną pieczęcią urzędową (pieczęć okrągłą o średnicy 36 mm) z pełną nazwą jednostki organizacyjnej i podpisem jej kierownika lub osoby przez niego upoważnionej,
   b) wspólnie dla urządzeń ewidencyjnych materiałów kryptograficznych;
2) nie podlega żadnej ewidencji;
3) po rozliczeniu wszystkich materiałów kryptograficznych ujętych na jego ewidencji podlega zdaniu do archiwum po rozformowaniu jednostki.

4. Ewidencję urządzeń ewidencyjnych i teczek w Rejestrze dokumentacji prowadzi kierownik kancelarii kryptograficznej w cyklu rocznym, rozpoczynając każdego roku kalendarzowego numerowanie od liczby „1".

5. W „Rejestrze dokumentacji" nie umieszcza się urządzeń ewidencyjnych zaewidencjonowanych w wykazach z lat poprzednich, jeżeli urządzenia te nadal są prowadzone.

§ 15.1. W Dzienniku korespondencji rejestruje się materiały kryptograficzne, o których mowa w § 2 pkt 20 lit. f, otrzymywane i wysyłane (wchodzące i wychodzące) z podziałem na materiały kryptograficzne jawne i niejawne oraz materiały kryptograficzne wytworzone na potrzeby wewnętrzne jednostki organizacyjnej.

2. Dopuszcza się prowadzenie Dziennika korespondencji w formie elektronicznej. Przepisy ust. 3-23, z wyłączeniem ust. 7, ust. 8 pkt 1 i 3, ust. 14, ust. 15-17, w części dotyczącej pieczęci, stosuje się odpowiednio.

3. Dopuszcza się rejestrowanie w jednym Dzienniku korespondencji materiałów kryptograficznych, o których mowa w § 2 pkt 20 lit. f, otrzymywanych i wysyłanych, z zastrzeżeniem ust. 4.

4. Dzienniki korespondencji w formie elektronicznej można prowadzić oddzielnie dla materiałów kryptograficznych, o których mowa w § 2 pkt. 20 lit. f, otrzymywanych i wysyłanych.

5. W Dziennikach korespondencji numerację materiałów kryptograficznych, o których mowa w § 2 pkt 20 lit. f, rozpoczyna się w każdym roku kalendarzowym od liczby 1. Dziennik korespondencji prowadzi się do całkowitego wykorzystania wszystkich stron;

6. W oddzielnych Dziennikach korespondencji rejestruje się materiały kryptograficzne, o których mowa w § 2 pkt 20 lit. f, uzyskane od innych państw oraz organizacji międzynarodowych w ramach realizacji umów międzynarodowych.

7. Po wykorzystaniu wszystkich stron Dziennika korespondencji, zakłada się następny tom i zachowuje ciągłość dotychczasowej numeracji.

8. Zarejestrowanie korespondencji otrzymanej polega na:

1) opatrzeniu pierwszej strony materiału kryptograficznego, o którym mowa w § 2 pkt 20 lit. f, pieczęcią wpływu oraz odciśnięciu pieczęci formularzowej na załącznikach, z zastrzeżeniem, iż pieczęci formularzowej nie używa się do załączników w formie dokumentów personalnych, wydawnictw kryptograficznych, materiałów kryptograficznych, o których mowa w § 2 pkt 20 lit. a-e i g oraz innych materiałów kryptograficznych przesyłanych do akceptacji (uzgodnienia, opiniowania) lub podpisu;
2) wpisaniu w kolejnej pozycji Dziennika korespondencji:
   a) właściwego symbolu klauzuli tajności materiału kryptograficznego,
   b) numeru porządkowego, który wraz z prefiksem w postaci symbolu, o którym mowa w lit. a, stanowi numer ewidencyjny materiału kryptograficznego,
   c) danych ewidencyjnych materiału kryptograficznego, nadanych przez nadawcę (numer wychodzący i data zarejestrowania),
   d) informacji o ilości stron materiału kryptograficznego wraz z załącznikami,
   e) informacji o ilości załączników, ich stron lub nazwy i liczby informatycznych nośników danych, jeżeli załączniki stanowią informatyczne nośniki danych,
   f) w rubryce „Uwagi", informacji o klauzuli tajności pisma przewodniego, jeżeli jest ona niższa niż klauzula najwyżej sklasyfikowanego załącznika;
3) wpisaniu na dokumencie, w odpowiednich polach odcisku pieczęci, daty zarejestrowania materiału kryptograficznego, zgodnie z zapisem w „Dzienniku korespondencji" oraz danych wymienionych w pkt 2 lit. a-b oraz d i e.

9. Korespondencję opatrzoną adnotacją „Do rąk własnych" rejestruje się bez otwierania wewnętrznego opakowania przesyłki, poprzez:

1) wpisanie w odpowiednich rubrykach Dziennika korespondencji zapisów umieszczonych na opakowaniu wewnętrznym przesyłki oraz daty wpływu materiału kryptograficznego;

2) zamieszczenie w rubryce „Uwagi" Dziennika korespondencji adnotacji „Do rąk własnych";
3) odciśnięcie na opakowaniu pieczęci wpływu i wpisaniu numeru ewidencyjnego według Dziennika korespondencji oraz daty wpływu przesyłki.

10. Jeżeli przesyłka opatrzona adnotacją „Do rąk własnych" zawiera kilka materiałów kryptograficznych, o których mowa w § 2 pkt 20 lit. f, to każdy z nich rejestruje się pod odrębną pozycją Dziennika korespondencji, a na opakowaniu wewnętrznym przesyłki umieszcza odciski pieczęci wpływu, w ilości odpowiadającej liczbie materiałów kryptograficznych, z wpisanymi numerami ewidencyjnymi poszczególnych materiałów.

11. Przesyłkę opatrzoną adnotacją „Do rąk własnych" przekazuje się bezpośrednio adresatowi, a w razie jego nieobecności osobie przez niego upoważnionej.

12. Przesyłkę, o której mowa w ust. 10, można zwrócić do kancelarii kryptograficznej w stanie otwartym lub zamkniętym.

13. W przypadku, gdy przesyłka zostanie zwrócona do kancelarii kryptograficznej w otwartym opakowaniu, podlega zarejestrowaniu na zasadach określonych w ust. 8, z tym, że zachowuje się numer ewidencyjny wpisany na opakowaniu i uzupełnia niezapisane rubryki Dziennika korespondencji.

14. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki opatrzonej adnotacją „Do rąk własnych" w kancelarii kryptograficznej w stanie zamkniętym, zapieczętowuje ją swoją pieczęcią okrągłą numerową do teczek pracy albo inną pieczęcią imienną, a kierownik kancelarii kryptograficznej dokonuje, przy udziale adresata, czynności, o których mowa w ust. 12. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten podlega odnotowaniu w rubryce „Uwagi" Dziennika korespondencji.

15. Przy przyjmowaniu przesyłek do kancelarii kryptograficznej:
1) sprawdza się:
   a) prawidłowość adresu,
   b) całość pieczęci i opakowania,
   c) zgodność odcisków pieczęci z nazwą nadawcy,
   d) zgodność numerów na opakowaniu przesyłki z numerami wyszczególnionymi odpowiednio w Wykazie przesyłek wydanych, Książce doręczeń;
2) w przypadku zauważenia nieprawidłowości lub podejrzeń co do zawartości przesyłki, kierownik kancelarii kryptograficznej odmawia jej przyjęcia powiadamiając o tym Oficera BSŁiI;
3) w przypadku stwierdzenia uszkodzenia odcisku pieczęci lub opakowania, kierownik kancelarii kryptograficznej sporządza wraz z przewoźnikiem protokół uszkodzenia, według wzoru określonego w rozporządzeniu Prezesa Rady Ministrów wydanym na podstawie art. 47 ust. 5 ustawy.

16. Po otwarciu przesyłki pracownik kancelarii kryptograficznej sprawdza czy:
1) zawartość przesyłki odpowiada wyszczególnionym na kopercie wewnętrznej numerom ewidencyjnym;
2) liczba stron, załączników i stron załączników jest zgodna z liczbą oznaczoną na poszczególnych materiałach kryptograficznych.

17. Stwierdzone nieprawidłowości dokumentuje się w protokole otwarcia przesyłki, którego jeden egzemplarz dołącza się do materiału kryptograficznego, a drugi przesyła się do nadawcy. Fakt sporządzenia protokołu otwarcia przesyłki podlega odnotowaniu w rubryce „Uwagi" Dziennika korespondencji.

18. Zarejestrowanie korespondencji wysyłanej odbywa się na zasadach, określonych w ust. 8, z tym, że zamiast pieczęci wpływu używa się pieczęci nagłówkowej, a w odpowiednich rubrykach Dziennika korespondencji wpisuje się nazwę adresata, ilość stron materiału kryptograficznego wraz z załącznikami, ilość załączników oraz stron załączników pozostających w aktach lub nazwę i liczbę informatycznych nośników danych, jeżeli załączniki stanowią informatyczne nośniki danych, numer ewidencyjny według Dziennika ewidencji wykonanych materiałów kryptograficznych lub innego urządzenia ewidencyjnego oraz wykonawcę.

19. W rubryce „Uwagi" Dziennika korespondencji wpisuje się datę przekazania materiału kryptograficznego, o którym mowa w § 2 pkt 20 lit. f, numer oraz pozycję zapisu w Książce doręczeń albo numer i pozycję zapisu w „Wykazie przesyłek nadanych", za którym materiał kryptograficzny przekazano adresatowi lub przewoźnikowi.

20. Jeżeli w kancelarii kryptograficznej nie pozostawia się żadnego egzemplarza wysyłanego materiału kryptograficznego, o którym mowa w § 2 pkt 20 lit. f, w rubrykach Dziennika korespondencji przeznaczonego do zapisywania informacji o ilości stron materiału kryptograficznego, ilości załączników oraz stron załączników, wpisuje się poziome kreski, natomiast w rubryce „Uwagi" zamieszcza adnotację o treści „tylko adresat".

21. Przed zarejestrowaniem w Dzienniku korespondencji materiału kryptograficznego, o którym mowa w § 2 pkt 20 lit. f, przekazanego do wysłania,

kierownik kancelarii kryptograficznej lub inna osoba z personelu kancelarii sprawdza czy materiał kryptograficzny:

1) został właściwie wykonany i oznaczony;
2) wytworzono w ilości egzemplarzy podanej w rozdzielniku;
3) zawiera dane określające faktyczną ilość stron, załączników i stron załączników przesyłanych do adresata oraz pozostawianych w aktach;
4) został podpisany przez osobę uprawnioną (upoważnioną) do podpisywania materiałów kryptograficznych.

22. W razie niespełnienia któregokolwiek z warunków, o których mowa w ust. 21, kierownik kancelarii kryptograficznej zwraca materiał kryptograficzny wykonawcy do poprawienia lub uzupełnienia.

23. Materiały kryptograficzne, o których mowa w § 2 pkt 20 lit. f, sporządzone w jednostce organizacyjnej na potrzeby własne ewidencjonuje się w Dzienniku korespondencji jak korespondencję otrzymaną, z wyjątkiem danych, o których mowa w § 15 ust. 8 pkt 2 lit. c.

24. W przypadku odłączenia od pisma przewodniego jednego lub więcej załączników, w rubryce „Uwagi" Dziennika korespondencji zamieszcza się adnotację zawierającą jedną z informacji:

1) nazwę i numer urządzenia ewidencyjnego oraz numery pozycji, pod którymi zarejestrowano odłączone załączniki;
2) numer wychodzący według Dziennika korespondencji, za którym załączniki odesłano do innej jednostki organizacyjnej;
3) numer i pozycję protokołu zniszczenia, albo adnotację o zniszczeniu potwierdzoną czytelnymi podpisami kierownika kancelarii kryptograficznej (zastępcy kierownika lub kancelisty) i wykonawcy; w zależności od klauzuli tajności zniszczonego załącznika;
4) zapis „Załączniki rozpisano na piśmie" w przypadku gdy liczba załączników uniemożliwia dokonanie zapisu w rubryce „Uwagi". Tego rodzaju pismo nie podlega zniszczeniu do czasu istnienia choć jednego załącznika.

§ 16.1. W przypadku funkcjonowania w jednostce organizacyjnej elektronicznego obiegu dokumentów, w kancelarii kryptograficznej prowadzi się komputerowe bazy materiałów kryptograficznych. Dopuszcza się prowadzenie komputerowych baz dokumentów oddzielnie dla poszczególnych klauzul tajności i dla materiałów kryptograficznych obejmujących rok kalendarzowy.

2. W komputerowych bazach dokumentów rejestruje się informacje w zakresie tożsamym z zakresem informacyjnym Dziennika korespondencji, z zastrzeżeniem ust. 3 i 4.

3. W przypadku wykorzystywania systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych, dodatkowo dopuszcza się rejestrowanie materiałów kryptograficznych w formie elektronicznej.

4. W elektronicznym obiegu materiałów kryptograficznych dekretacja wpisywana na piśmie przewodnim zostaje zastąpiona równoważną dekretacją elektroniczną, opatrzoną danymi jednoznacznie identyfikującymi osobę dokonującą dekretacji, a także znacznikiem daty i czasu; dekretacje elektroniczne rejestruje się w komputerowych bazach dokumentów.

§ 17.1. W Kartach ewidencyjnych publikacji (AF 54 C PL) rejestruje się materiały kryptograficzne, o których mowa w § 2 pkt 20 lit. d i e, wytwarzane na potrzeby jednostki organizacyjnej lub otrzymane.

2. W przypadku funkcjonowania w jednostce organizacyjnej elektronicznego obiegu dokumentów, dopuszcza się prowadzenie Kart ewidencyjnych publikacji (AF 54 C PL) w formie elektronicznej zamiast papierowej. Przepisy ust. 3, w części dotyczącej pieczęci, stosuje się odpowiednio.

3. Materiały kryptograficzne, o których mowa w ust. 1, rejestruje się wpisując w Kartach ewidencyjnych publikacji (AF 54 C PL):

1) pod odrębną pozycją tytuł każdego z otrzymanych materiałów kryptograficznych, według kolejności ich wpływu;
2) ilość i numery egzemplarzy każdego tytułu materiału kryptograficznego;
3) numer i datę faktury, asygnaty lub formularza AF 21 PL, za którymi materiały kryptograficzne przysłano.

4. Na okładce i stronie tytułowej każdego egzemplarza rejestrowanego materiału kryptograficznego, o którym mowa w § 2 pkt 20 lit. d i e oraz nie zszytych z nim załącznikach odciska się pieczęć biblioteczną zawierającą nazwę kancelarii kryptograficznej lub pieczęć „Do pakietów" oraz wpisuje numer ewidencyjny z karty AF 54 C PL.

5. Każdą poszczególną pozycję, tytuł, ewidencjonuje się oddzielnie na odrębnej karcie AF 54 C PL.

§ 18.1. W RWMK rejestruje się:

1) materiały kryptograficzne służące do utrwalania informacji kryptograficznych:
   a) zeszyty pracy, notatniki, arkusze papieru przeznaczone do wykonywania dokumentów, brudnopisów lub odręcznego wykonywania czystopisów, sprawozdań,

bloki szyfrogramów i telegramów związanych z tematyką kryptograficzną,
b) informatyczne nośniki danych;
2) załączniki odłączone od pism przewodnich, nie podlegające ewidencji w innych urządzeniach.

2. RWMK służy także do dokumentowania faktu pobrania i zwrotu wydawanych przez kancelarię kryptograficznej wykonawcom:
1) dokumentów kryptograficznych zarejestrowanych w innych urządzeniach ewidencyjnych, jeżeli:
a) rubryka urządzenia ewidencyjnego, przeznaczona do pokwitowania materiału kryptograficznego, została całkowicie wykorzystana,
b) rodzaj materiału kryptograficznego albo dekretacja sporządzona na nim wskazują, że będzie on udostępniany większej liczbie osób;
2) wydawnictw, dokumentacji technicznej i standaryzacyjnej i innych dokumentów związanych z tematyką kryptograficzną zarejestrowanych w urządzeniach ewidencyjnych, które nie mają rubryk przeznaczonych do kwitowania pobieranych i zwracanych materiałów kryptograficznych.

3. RWMK rejestruje się w Skorowidzu RWMK:
1) imiennie dla wykonawców;
2) według numerów ewidencyjnych lub sygnatur, jeżeli są prowadzone dla poszczególnych dokumentów albo wydawnictw.

4. Numerem ewidencyjnym RWMK jest numer porządkowy, pod którym został on zarejestrowany w Skorowidzu RWMK.

5. Numer ewidencyjny materiału kryptograficznego zarejestrowanego w RWMK składa się z nazwy urządzenia, numeru, o którym mowa w ust. 4, łamanego przez liczbę porządkową pozycji, pod którą wpisano do RWMK materiał kryptograficzny, poprzedzoną symbolem jego klauzuli tajności (np. RWMK 10/Pf-8).

6. W przypadkach, o których mowa w ust. 2, zapisy rozpoczyna się od wpisania w kolumnie 4 RWMK numeru ewidencyjnego materiału kryptograficznego lub sygnatury wydawnictwa, bez wpisywania w kolumnie 2 numeru porządkowego.

7. Na grzbietach oraz kartach bloków telegramów, szyfrogramów i innych materiałów zbroszurowanych zarejestrowanych w RWMK, przeznaczonych do wyrywania stron, wpisuje się numer ewidencyjny, o którym mowa w ust. 5, łamany przez numer karty (np. RWMK 10/Pf-8/1, 2, 3 ...). Fakt wyrwania karty kierownik kancelarii kryptograficznej lub inna osoba dokonująca tej czynności potwierdza na grzbiecie materiału kryptograficznego podpisem oraz odciskiem pieczęci.

8. Materiały kryptograficzne zarejestrowane w RWMK, po zwróceniu ich do kancelarii kryptograficznej, podlegają zniszczeniu lub przerejestrowaniu do RWMK innego wykonawcy albo innego urządzenia ewidencyjnego.

9. W przypadku przerejestrowania materiału kryptograficznego do RWMK innego wykonawcy lub zaewidencjonowania w innym urządzeniu ewidencyjnym, w dotychczasowej ewidencji dokonuje się adnotacji o przerejestrowaniu materiału kryptograficznego z wyszczególnieniem nowego numeru ewidencyjnego.

10. RWMK przeznaczony do rejestrowania dokumentacji służby dyżurnej stacji kryptograficznej zakłada się w dwóch egzemplarzach, z których jeden przechowuje się w kancelarii kryptograficznej, a drugi stanowiący podstawę do przekazywania przez służbę materiałów kryptograficznych, w pomieszczeniu tej służby.

11. Po wykorzystaniu wszystkich pozycji w RWMK, dołącza się nową kartę zachowując poprzednio nadany numer i ciągłość numeracji.

12. Rozliczony RWMK wykonawcy, który ubył z jednostki organizacyjnej, po sprawdzeniu przez komisję powołaną do przeprowadzenia inspekcji kryptograficznej wykonywanej w ramach kontroli rocznej stanu ochrony informacji niejawnych podlega komisyjnemu zniszczeniu, nie wcześniej jednak niż po upływie roku od daty jego rozliczenia. Do momentu zniszczenia rozliczony „RWMK" przechowuje się w kancelarii kryptograficznej. Zniszczone RWMK są wyszczególniane w załączniku do protokołu z inspekcji kryptograficznych.

§ 19.1. Wykazów przesyłek nadanych oraz formularzy AF 69 PL nie ewidencjonuje się w żadnym urządzeniu ewidencyjnym. Wykazom nadaje się kolejne numery, zaczynając numerowanie w każdym roku kalendarzowym od liczby „1".

2. W przypadku przekazania materiałów kryptograficznych poprzez kancelarie kryptograficznej z wykorzystaniem „Wykazu Przesyłek Nadanych" przewoźnik potwierdza przyjęcie przesyłek do przekazania na dwóch egzemplarzach wykazu, o którym mowa w ust. 1, zapisem liczbowym i słownym o ilości przyjętych przesyłek oraz uwierzytelnia podpisem i odciskiem pieczęci „Do pakietów" lub innej pieczęci służbowej przeznaczonej do pokwitowania nadania lub odbioru przesyłki, przy czym jeden egzemplarz wykazu pozostaje w kancelarii nadawcy, a drugi jest przeznaczony dla przewoźnika.

3. W przypadku przekazywania materiału kryptograficznego poprzez personel kancelarii

kryptograficznej lub Wojskową Służbę Kurierską z zastosowaniem formularza AF 69 PL przewoźnik potwierdza przyjęcie przesyłek do przekazania na tzw. „kopii roboczej", która zostaje zniszczona po dostarczeniu wykazu podpisanego przez właściwego adresata. Na formularzach nie stosuje się pieczęci „Do Pakietów". Potwierdzeniem jest czytelny podpis wraz z podanym stopniem i nazwiskiem odbiorcy oraz datą i godziną przekazania.

4. W przypadku przekazywania materiałów kryptograficznych o klauzuli tajności „TAJNE", „ŚCIŚLE TAJNE", dodatkowy trzeci egzemplarz Wykazu przesyłek nadanych, przesyła się wraz z przesyłką, w wewnętrznej kopercie, adresatowi, który potwierdza na nim odbiór przesyłki i odsyła do nadawcy.

5. Kierownik kancelarii kryptograficznej wpisuje w rubryce „Uwagi" w Wykazie przesyłek nadanych, numery ewidencyjne pod jakimi poszczególne przesyłki zostały zarejestrowane w Dzienniku korespondencji.

6. Kancelaria kryptograficzna przechowuje wykazy, o których, mowa w ust. 1 i 2, w specjalnie przeznaczonych do tego celu segregatorach. Wykazy o których mowa w ust. 1 i 2, podlegają zniszczeniu po okresie dwóch lat od zakończenia ewidencji w roku bieżącym.

7. Szczegółowe zasady stosowania Wykazu przesyłek nadanych określa rozporządzenie Prezesa Rady Ministrów wydane na podstawie art. 47 ust. 5 ustawy.

§ 20.1. W Książce doręczeń rejestruje się fakt doręczenia materiałów kryptograficznych do kancelarii kryptograficznej adresata, stacjonującego w tej samej miejscowości, bezpośrednio przez personel kancelarii nadawcy.

2. Kierownik kancelarii kryptograficznej adresata potwierdza odbiór materiałów kryptograficznych podpisem w odpowiedniej rubryce Książki doręczeń, uwierzytelnionym odciskiem pieczęci „Do pakietów".

3. Książkę doręczeń prowadzi się do całkowitego wykorzystania, zaczynając numerowanie w każdym roku kalendarzowym od liczby „1".

4. Książkę doręczeń ewidencjonuje się w RWMK kierownika kancelarii kryptograficznej.

5. Książka doręczeń, po okresie dwóch lat od zakończenia ewidencji w roku bieżącym podlega komisyjnemu zniszczeniu.

§ 21.1. Kartę zapoznania się z materiałem kryptograficznym zakłada się i dołącza do materiału kryptograficznego pochodzenia narodowego, o którym mowa w § 2 pkt 20 lit. d-f o klauzuli „Tajne", „Ściśle Tajne" z chwilą zarejestrowania go po raz pierwszy w urządzeniach ewidencyjnych — z zastrzeżeniem ust. 2.

2. W przypadku funkcjonowania w jednostce organizacyjnej elektronicznego obiegu materiałów kryptograficznych dopuszcza się prowadzenie Kart zapoznania się z materiałem kryptograficznym w formie elektronicznej zamiast papierowej. Przepisy ust. 3-9 stosuje się odpowiednio.

3. W Karcie zapoznania się z materiałem kryptograficznym dokumentuje się każdorazowe udostępnienie wykonawcom materiałów kryptograficznych, o których mowa w ust. 1.

4. Dokumentowanie w formie elektronicznej udostępnienia materiału kryptograficznego polega na potwierdzeniu tej czynności wykonaniem dekretacji elektronicznej przez wykonawcę. Przepis § 16 ust. 4 stosuje się odpowiednio.

5. Fakt zapoznania się z materiałem kryptograficznym, o którym mowa w ust. 1, rejestruje się w Karcie zapoznania się z materiałem kryptograficznym wystawionej dla całego zbioru.

6. Przepis ust. 5 stosuje się odpowiednio do teczek akt.

7. Kart zapoznania się z materiałem kryptograficznym nie zakłada się dla materiałów kryptograficznych pochodzących z wymiany międzynarodowej.

8. Kartę zapoznania się z materiałem kryptograficznym przesyła się lub archiwizuje wraz z materiałem kryptograficznym, którego dotyczy albo z protokołem jego zniszczenia.

9. W przypadku funkcjonowania w jednostce organizacyjnej elektronicznego obiegu dokumentów i prowadzenia Kart zapoznania się z materiałem kryptograficznym w formie elektronicznej zamiast papierowej, zapewnia się możliwość wydrukowania Kart zapoznania się z materiałem kryptograficznym, a wydruki traktuje się na zasadach równoważnych z dokumentami papierowymi.

§ 22.1. Wykonawcy wytwarzający materiały kryptograficzne, o których mowa w § 2 pkt 20 lit. d-f prowadzą Dziennik ewidencji wykonanych materiałów kryptograficznych, zwany dalej „DEWMK", którego wzór określa załącznik Nr 22.

2. DEWMK służy do rejestrowania materiałów kryptograficznych, o których mowa w ust. 1, wytworzonych w jednostce organizacyjnej, w szczególności

techniką komputerową, maszynopisania, powielania, naświetlania, kreślenia lub odręczną.

3. Zarejestrowanie materiału kryptograficznego w DEWMK polega na wpisaniu pod kolejną pozycją dziennika:

1) symbolu klauzuli tajności;
2) liczby porządkowej;
3) daty oddania brudnopisu do podpisania lub materiału kryptograficznego do powielenia;
4) adresata lub nazwy materiału kryptograficznego;
5) nazwiska osoby sporządzającej materiał kryptograficzny;
6) numeru brudnopisu i nr stron (numeru materiału kryptograficznego i liczby stron w przypadku wykonania kopii);
7) nazwiska osoby wykonującej materiał kryptograficzny (merytorycznego wykonawcy materiału kryptograficznego lub osoby zamawiającej kopie);
8) liczby egzemplarzy i liczby stron w pojedynczym egzemplarzu przy czym oznaczenie klauzuli tajności i liczba porządkowa z DEWMK łamane przez dwie ostatnie cyfry roku kalendarzowego poprzedzone skrótem nazwy jednostki (komórki) organizacyjnej stanowią prefiks sygnatury literowo-cyfrowej, o której mowa w § 3 ust. 1 pkt 1 lit. b rozporządzenia Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 159, poz. 1069) np. BŁI SKW-PF-123/11. Do prefiksu dołącza się numer ewidencyjny dziennika „DEWMK", w którym materiał kryptograficzny został zaewidencjonowany (np. DEWMK RTMK 18/10). Sygnatura literowo-cyfrowa umieszczona na wykonanym dokumencie ma postać: BŁI SKW-Pf-123/11-DEWMK RTMK 18/10.

4. Dodatkowo wytworzony materiał kryptograficzny o klauzuli „Ściśle Tajne", „Tajne" i „Poufne", w szczególności odpis, kopię lub reprodukcję rejestruje się każdorazowo pod odrębną pozycją DEWMK. Wykonanie kopii, odpisu lub reprodukcji materiału kryptograficznego o klauzuli „Ściśle Tajne", „Tajne" i „Poufne wymaga pisemnej zgody kierownika jednostki organizacyjnej dysponującej tym materiałem lub upoważnionej przez niego osoby.

5. DEWMK prowadzi się do całkowitego wykorzystania jego kart, rozpoczynając każdego roku kalendarzowego numerowanie od liczby „1".

6. Wytworzone i ujęte w DEWMK materiały kryptograficzne wykonawca rejestruje w urządzeniach ewidencyjnych kancelarii kryptograficznej, w terminie do 30 dni od daty ich wytworzenia.

7. Zakończony DEWMK, po sprawdzeniu przez komisję powołaną do prowadzenia inspekcji kryptograficznej podlega komisyjnemu zniszczeniu, nie wcześniej jednak niż po upływie 5 lat od daty zakończenia. Do momentu zniszczenia zakończone „DEWMK" przechowuje się w kancelarii kryptograficznej. Zniszczone DEWMK są wyszczególniane w załączniku do protokołu z inspekcji kryptograficznej.

§ 23.1. Biblioteka przyjmuje, rejestruje, przechowuje, udostępnia i przekazuje materiały kryptograficzne o których mowa w § 2 pkt 20 lit. d i e prowadzi, osobno dla poszczególnych tytułów, kartę ewidencyjną pozycji bibliotecznych na formularzach AF 54 C PL.

2. Wydawanie pozycji bibliotecznych, o których mowa w ust. 1, odbywa się na zasadzie pokwitowania odręcznego na formularzu AF 21 PL numerowanym od pozycji 7000 do 7999 lub w przypadku przekroczenia numeru 7999 od pozycji 8000 do 8999.

3. Formularz AF 21 PL, o którym mowa w ust. 2 służy do dokumentowania faktu pobrania i zwrotu wydawanych przez kancelarię kryptograficznej materiałów kryptograficznych, o których mowa w ust. 1.

4. Każdorazowo przed wydaniem oraz po zwrocie wypożyczonego materiału kryptograficznego, kierownik kancelarii kryptograficznej sprawdza ilość stron danej pozycji.

5. Materiał kryptograficzny, o którym mowa w ust. 1, z wyłączeniem materiałów filmowych oraz na informatycznych nośnikach danych podlega sprawdzeniu przez personel kancelarii kryptograficznej co do zgodności ilości stron w momencie rejestracji (przyjęcia na stan kancelarii) oraz każdorazowo po zwrocie przez użytkownika, a ponadto podlega corocznemu sprawdzeniu.

6. Do pomocy ewidencji biblioteki dopuszcza się stosowanie pomocniczych kart dopuszczenia do materiału kryptograficznego, której wzór określa załącznik Nr 23.

§ 24.1. Kancelaria kryptograficzna przekazuje materiały kryptograficzne wyłącznie wykonawcom posiadającym stosowne poświadczenia bezpieczeństwa oraz CUK, którego wzór określa załącznik Nr 24, w przypadku gdy osoba ta pełni obowiązki w pomieszczeniu ujętym w planie ochrony jednostki i przeznaczonym do przechowywania materiałów niejawnych o stosownej klauzuli bezpieczeństwa.

2. Przekazywane materiały kryptograficzne, o których mowa w ust. 1, wydawane są za pokwitowaniem w Dzienniku korespondencji, za pokwitowaniem

odręcznym, wykonanym na formularzu AF 21 PL lub za pokwitowaniem odręcznym na RWMK.

3. Kierownik lub personel kancelarii kryptograficznej udostępnia lub przekazuje materiały kryptograficzne osobom, o których mowa w ust. 1 na podstawie zamieszczonej na dokumencie dekretacji lub polecenia kierownika jednostki organizacyjnej albo osoby przez niego upoważnionej.

4. Urządzenia do przechowywania informacji niejawnych mogą być wykorzystywane wyłącznie przez jednego wykonawcę, chyba że konstrukcja tego urządzenia pozwala na fizyczne oddzielenie posiadanych przez wykonawców materiałów kryptograficznych i zamknięcie ich w odrębnych skrytkach.

5. Wykonawcom, których pomieszczenia służbowe nie spełniają warunków dotyczących przechowywania i zabezpieczenia materiałów kryptograficznych, o których mowa w ust 1, umożliwia się udostępnienie tych materiałów jedynie w pomieszczeniach kancelarii kryptograficznej.

6. Wykonawca, któremu udostępniono materiały kryptograficzne ma obowiązek zachowania środków bezpieczeństwa uniemożliwiających dostęp do tych materiałów osobom nieuprawnionym.

7. Wykonawcy przechowujący w pomieszczeniach służbowych materiały kryptograficzne (m.in. klucze CIK), przed udaniem się na urlop, szkolenie lub w podróż służbową mają obowiązek zdania ich do kancelarii kryptograficznej. Przekazanie materiałów niezbędnych do prowadzenia bieżącej działalności jednostki organizacyjnej osobie zastępującej, następuje poprzez kancelarię kryptograficzną na polecenie kierownika jednostki organizacyjnej.

8. Przesyłki opatrzone adnotacją „Pilne" kancelaria kryptograficzna przekazuje adresatom bezzwłocznie, wpisując w rubryce „Uwagi" urządzenia ewidencyjnego datę i godzinę doręczenia.

9. Przekazywanie materiałów kryptograficznych poza jednostkę organizacyjną, z zastrzeżeniem szyfrogramów, odbywa się wyłącznie poprzez kancelarie kryptograficzne.

10. Wszelkie materiały kryptograficzne mogą być przekazywane pomiędzy wykonawcami jedynie za pośrednictwem kancelarii kryptograficznej.

11. Materiały kryptograficzne ostatecznie załatwionych spraw powinny być niezwłocznie przekazane do kancelarii kryptograficznej.

12. Szyfrogramy wychodzące przekazywane są bezpośrednio przez nadawcę do stacji kryptograficznej (szyfrowej) a szyfrogramy wchodzące przekazywane są przez personel stacji kryptograficznej bezpośrednio adresatowi. Szyfrogramy po nadaniu (wykorzystaniu) przekazywane są do kancelarii tajnej lub kancelarii kryptograficznej zgodnie z decyzją kierownika jednostki organizacyjnej gdzie podlegają ewidencji w Dzienniku korespondencji. Dodatkowo w kolumnie 15 umieszcza się napis „Szyfrogram". Fakt przyjęcia szyfrogramu w kancelarii kryptograficznej potwierdza się w kolumnie 14 Dziennika ewidencji szyfrogramów poprzez wpisanie numeru ewidencyjnego, pod którym zarejestrowano szyfrogram, odciskiem pieczęci „Do pakietów" i podpisem kierownika kancelarii kryptograficznej (zastępcy kierownika lub kancelisty).

§ 25.1. Materiały kryptograficzne, o których mowa w § 2 pkt 20 lit. d-f, otrzymane lub wytworzone w jednostce organizacyjnej podlegają:

1) skompletowaniu w teczki akt, jeżeli stanowią materiały archiwalne lub posiadają wartość praktyczną dla jednostki organizacyjnej, w sposób określony w zarządzeniu, o którym mowa w § 2 pkt 4, (Teczki skompletowanych akt zszywa się (podszywa) po upływie dwóch lat od ostatecznego zakończenia spraw na polecenie kierownika jednostki organizacyjnej lub upoważnionej przez niego osoby. Za datę rozpoczęcia teczki należy przyjąć datę wpływu pierwszego pisma z danej tematyki. W uzasadnionych przypadkach za zgodą kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej materiał kryptograficzny, o którym mowa w ust. 1, można wydać z kancelarii kryptograficznej na RWMK użytkownika. Materiał kryptograficzny podlega zwrotowi do kancelarii kryptograficznej bezpośrednio po jego realizacji.);
2) zwrotowi do nadawcy, jeżeli określił on taki sposób postępowania z przesłanymi materiałami;
3) bieżącemu niszczeniu.

2. Materiały kryptograficzne, o których mowa § 2 pkt 20 lit d-f, przechowuje się w kancelarii kryptograficznej zgodnie z terminami określonymi w wykazie rzeczowym akt, a po upływie tego czasu występuje się do RCZBSiUT o zgodę na ich zniszczenie lub w przypadku ich szczególnej wartości przekazuje się poprzez RCZBSiUT do właściwego archiwum, które obsługuje RCZBSiUT, z zastrzeżeniem materiałów kryptograficznych GKK i kancelarii kryptograficznej bezpośrednio im podległych.

3. Formularze ewidencyjne AF 21 PL przechowuje się przez okres 3 lat, nie wliczając roku bieżącego.

4. Formularze AF 54 A, B, C PL przechowuje się przez okres 3 lat od jego zakończenia i rozliczenia materiału kryptograficznego ujętego na danym formularzu.

5. Formularze AF 21 PL, AF 54 A PL, AF 54 B PL, AF 54 C PL, AF 69 PL oraz AF 147 PL nie podlegają archiwizacji.

6. Kierownik jednostki organizacyjnej w razie konieczności, w szczególnych przypadkach może wyrazić pisemną zgodę na rozszycie teczki akt z podszytą dokumentacją i wyjęcie potrzebnego materiału kryptograficznego.

7. Zapisu, o którym mowa w ust. 6, dokonuje się na ostatniej stronie teczki akt potwierdzając czytelnym podpisem i odciskiem pieczęci urzędowej.

8. Rozszycia teczki dokonuje wyłącznie kierownik kancelarii kryptograficznej.

9. W przypadku wyłączenia na stałe materiału kryptograficznego z teczki kierownik kancelarii kryptograficznej na ostatniej stronie teczki akt dokonuje zapisu: komu materiał przekazano (nr wykazu przesyłek lub liczba porządkowa książki doręczeń, ilości kart i numery stron wyłączonego materiału) potwierdzając datą dokonanych czynności oraz czytelnym podpisem.

10. Materiał kryptograficzny wyłączony na stałe z teczki akt podlega ponownemu ujęciu w bieżącej ewidencji kancelarii kryptograficznej.

11. Teczka akt, o której mowa w ust. 6 podlega ponownemu sprawdzeniu w zakresie ilości stron tej teczki przez najbliższą komisję inspekcji kryptograficznej dokonując odpowiedniej adnotacji w protokole z tej inspekcji.

§ 26.1. Materiały kryptograficzne nie będące materiałami archiwalnymi, nie posiadające wartości praktycznej dla jednostki organizacyjnej lub nieaktualne, które nie zostały wszyte do teczek akt podlegają zniszczeniu, z zastrzeżeniem ust. 2.

2. W przypadku funkcjonowania w jednostce organizacyjnej elektronicznego obiegu dokumentów, dokumenty przechowywane w komputerowych bazach dokumentów nie podlegają niszczeniu.

3. Materiały kryptograficzne, o których mowa w ust. 1, zakwalifikowane do zniszczenia, niszczą odpowiednio:

1) w odniesieniu do materiałów kryptograficznych, o których mowa w § 2 pkt 20 lit. f i h o klauzuli „Tajne" i „Ściśle Tajne" co najmniej trzyosobowa komisja, powoływana okresowo przez kierownika jednostki organizacyjnej.
2) w odniesieniu do materiałów kryptograficznych, o których mowa w § 2 pkt 20 lit. f i h, „jawnych" oraz zawierających informacje niejawne o klauzuli „Zastrzeżone" oraz „Poufne", odbywa się w obecności osoby z personelu kancelarii kryptograficznej lub wykonawcy, a fakt zniszczenia dokumentuje się w rubryce „Uwagi" urządzenia ewidencyjnego adnotacją o treści: „Zniszczono dnia ...", potwierdzoną wpisaniem daty i czytelnymi podpisami osób niszczących materiały kryptograficzne.
3) w odniesieniu do materiałów kryptograficznych, o których mowa w § 2 pkt 20 lit. a-e oraz g kierownik kancelarii kryptograficznej wraz z zastępcą lub inną osobą posiadającą stosowne poświadczenie bezpieczeństwa występującą w roli świadka, potwierdzając zniszczenie na formularzu AF 21 PL na podstawie odrębnych przepisów.

4. Z komisyjnego zniszczenia materiałów kryptograficznych, o których mowa w ust. 3 pkt 1, sporządza się protokół zniszczenia, którego wzór określa załącznik Nr 25.

5. Protokół zniszczenia lub formularz AF 21 PL numerowany od pozycji 5000 do 5999 stanowi dla kierownika kancelarii kryptograficznej podstawę do zdjęcia z ewidencji wyszczególnionych w nim materiałów kryptograficznych, poprzez naniesienie w rubryce „Uwagi" odpowiedniego urządzenia ewidencyjnego adnotacji o dokonanym fakcie.

§ 27.1. Materiał kryptograficzny w formie papierowej uważa się za ostatecznie zniszczony, jeżeli został pocięty w urządzeniu, o którym mowa w § 8 ust. 9 pkt 5 lub zmielony na miał papierowy, lub spalony w piecu lub rozpuszczony w kadziach z ługiem w zakładach papierniczych.

2. Jeżeli w jednostce organizacyjnej, z przyczyn technicznych, ostateczne zniszczenie materiałów kryptograficznych, o których mowa w ust. 1 jest niemożliwe, niszczy się je wstępnie przez kilkakrotne przedarcie, przy czym wstępnego zniszczenia dokonuje odpowiednio kierownik kancelarii kryptograficznej pod nadzorem członków komisji albo wykonawcy.

3. Wstępnie zniszczone materiały kryptograficzne, do chwili ich przekazania do wytypowanej jednostki organizacyjnej lub wyspecjalizowanego zakładu, w celu ostatecznego zniszczenia, przechowuje się w oplombowanych przez personel kancelarii kryptograficznej workach lub pojemnikach, w kancelarii kryptograficznej, lub innym pomieszczeniu jednostki organizacyjnej zabezpieczonym jak kancelaria.

4. Osoby, o których mowa w ust. 1, nadzorujące niszczenie materiałów kryptograficznych zapewniają zachowanie warunków uniemożliwiających wgląd do nich osobom nieupoważnionym.

5. Zabrania się wywożenia częściowo zniszczonych materiałów kryptograficznych oraz kopert

i innych opakowań, w których otrzymano te materiały na wysypiska śmieci.

6. Materiały kryptograficzne, inne niż wskazane w ust. 1, niszczy się na podstawie odrębnych przepisów.

§ 28.1. W razie likwidacji (rozformowania) jednostki organizacyjnej postępuje się według odrębnych przepisów.

2. Personel kancelarii kryptograficznej likwidowanej jednostki organizacyjnej może być przeniesiony na inne stanowiska służbowe z chwilą całkowitego rozliczenia i przekazania materiałów kryptograficznych pozostających na ewidencji jednostki organizacyjnej.

Rozdział 6

Funkcjonowanie i ochrona kancelarii kryptograficznych podczas ćwiczeń, wojny oraz realizacji zadań poza terenem jednostki organizacyjnej

§ 29.1. Na czas ćwiczeń, wojny oraz realizacji zadań poza terenem jednostki organizacyjnej materiały kryptograficzne zabezpieczane są przez polową lub mobilną kancelarię kryptograficzną, którą powołuje się według odrębnych przepisów.

2. W przypadku, gdy ćwiczenia odbywają się na terenie jednostki organizacyjnej, w której powołana jest stacjonarna kancelaria kryptograficzna nie powołuje się oddzielnej kancelarii kryptograficznej. Powołana kancelaria kryptograficzna obsługuje ćwiczenia i zapewnia materiały kryptograficzne niezbędne do przeprowadzania tych ćwiczeń.

§ 30.Kierownik jednostki organizacyjnej zapewnia niezbędne siły i środki do przewozu polowej/mobilnej kancelarii kryptograficznej i jej dokumentacji podczas ćwiczeń oraz na czas prowadzenia działań wojennych.

§ 31.Kancelarię kryptograficzną, o której mowa w § 29 ust. 1, organizuje się w oddzielnych samochodach, budowlach, schronach lub kontenerach, rozmieszczonych w rejonie stanowiska dowodzenia, jak najbliżej Centrum Dowodzenia, przy czym:

1) obszar wokół kancelarii kryptograficznej powinien być ogrodzony i posiadać nie więcej niż jedno strzeżone wejście;
2) kancelaria kryptograficzna powinna mieć zapewnioną całodobową ochronę;
3) na czas nieobecności personelu materiał kryptograficzny powinien być przechowywany w zamykanych szafach meblowych lub skrzyniach metalowych (nie dotyczy pracujących urządzeń kryptograficznych);
4) niewykorzystywane urządzenia kryptograficzne mogą być przechowywane w kancelarii kryptograficznej bez wprowadzonych dokumentów kryptograficznych.

§ 32.Kancelarie kryptograficzne realizujące zadania poza granicami kraju powołuje się według odrębnych przepisów.

§ 33.Kontenery przeznaczone na polowe lub mobilne kancelarie kryptograficzne muszą spełniać wymagania zawarte w odrębnych przepisach oraz posiadać pozytywną opinię wydaną przez SKW potwierdzającą spełnienie wymagań z zakresu zabezpieczenia fizycznego i technicznego tych kontenerów.

Rozdział 7

Zasady rejestrowania, kompletowania i niszczenia materiałów kryptograficznych pochodzących z wymiany międzynarodowej

§ 34. Zasady rejestrowania, kompletowania i niszczenia materiałów kryptograficznych pochodzących z wymiany międzynarodowej regulują odrębne przepisy wynikające z umów i porozumień międzynarodowych, których Polska jest stroną.

Rozdział 8

Sprawowanie nadzoru nad kancelariami kryptograficznymi

§ 35.1. Nadzór nad ochroną materiałów kryptograficznych w kancelarii kryptograficznych realizowany jest przez poszczególne jednostki organizacyjne zgodnie z hierarchią zaopatrywania kancelarii kryptograficznej, o której mowa w § 3 ust. 1 i 2, w formie inspekcji kryptograficznych.

2. Inspekcje kryptograficzne kancelarii kryptograficznej bezpośrednio zaopatrywanych przeprowadza się cyklicznie, nie rzadziej niż co 2 lata.

3. Inspekcja kryptograficzna ma na celu sprawdzenie:

1) bezpieczeństwa kryptograficznego;
2) prowadzenia ewidencji materiałów kryptograficznych;
3) bezpieczeństwa systemów teleinformatycznych przetwarzających informacje dotyczące tematyki kryptograficznej.

§ 36.1. Inspekcję kryptograficzną dla nadzorowanej i zaopatrywanej pośrednio i bezpośrednio

kancelarii kryptograficznej zarządza kierownik jednostki organizacyjnej kancelarii kryptograficznej zaopatrującej, a realizuje komisja złożona z upoważnionych członków OBSŁiI, której przewodniczącym jest Oficer BSŁiI.

2. Protokół z inspekcji kryptograficznej tworzy się w zależności od potrzeb w kilku jednobrzmiących egzemplarzach.

3. Po przeprowadzeniu inspekcji kryptograficznej przewodniczący komisji przedstawia do podpisu kierownikowi jednostki organizacyjnej podlegającej sprawdzeniu protokół z inspekcji kryptograficznej z załączoną kartą inspekcji.

4. Podpisany egzemplarz nr 1 protokołu z inspekcji kryptograficznej wraz z kartą inspekcji kryptograficznej przechowywany jest w kancelarii kryptograficznej, w której inspekcja była przeprowadzana.

5. Egzemplarz nr 2, 3 i 4 protokołu z inspekcji kryptograficznej wraz z kopią karty inspekcji kryptograficznej przesyła się zgodnie z hierarchicznym sposobem zaopatrywania do jednostki organizacyjnej przeprowadzającej tę inspekcję, KOGD oraz w przypadku inspekcji kryptograficznej jednostki organizacyjnej zaopatrywanej w materiały kryptograficzne przez RCZBSiUT do RCZBSiUT.

6. Prowadząc inspekcję kryptograficzną w jednostce organizacyjnej posiadającej więcej niż jedną kancelarię kryptograficzną (m.in. Centrum Wsparcia Teleinformatycznego) dla każdej kancelarii kryptograficznej osobno sporządza się kolejny egzemplarz protokołu z inspekcji kryptograficznej wraz z kopią karty inspekcji kryptograficznej.

7. Wzór:
1) upoważnienia do przeprowadzenia inspekcji kryptograficznej, określa załącznik Nr 26;
2) planu przeprowadzenia inspekcji kryptograficznej, określa załącznik Nr 27;
3) protokołu z inspekcji kryptograficznej, określa załącznik Nr 28;
4) karty inspekcji kryptograficznej, określa załącznik Nr 29.

§ 37.1. W przypadku stwierdzenia rażących uchybień w postępowaniu z materiałami kryptograficznymi należy przerwać inspekcję kryptograficzną i zabezpieczyć materiał dowodowy oraz w trybie pilnym wnioskować o zarządzenie kontroli w trybach określonych w odrębnych przepisach.

2. Do dnia 30 kwietnia każdego roku RCZBSiUT przesyła do KOGD raport o stanie ochrony informacji niejawnych w podległych kancelariach kryptograficznych za ubiegły rok z wyszczególnieniem:
1) kancelarii kryptograficznych objętych nadzorem;
2) stacji kryptograficznych objętych nadzorem;
3) formy nadzoru (kontrola, inspekcja itp.);
4) organów bezpieczeństwa systemów łączności i informatyki przeprowadzających inspekcje;
5) stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych.

Rozdział 9

Przepisy przejściowe i końcowe

§ 38.1. Pomieszczenia kancelarii kryptograficznych podlegają inspekcji zastosowanych środków ochrony fizycznej i technicznej.

2. Za przygotowanie pomieszczeń kancelarii kryptograficznej do inspekcji, o której mowa w ust. 1, odpowiada Oficer BSŁiI, a za zastosowanie środków bezpieczeństwa fizycznego dla tych pomieszczeń odpowiada pełnomocnik ochrony.

3. Pełnomocnik ochrony lub podlegli mu pracownicy uprawnieni są do przeprowadzania kontroli w zakresie prowadzenia ewidencji, przechowywania i zabezpieczenia fizycznego wszystkich materiałów niejawnych znajdujących się na ewidencji.

4. Uprawnienia, o których mowa w ust. 3, nie dotyczą zapoznawania się z zasadami funkcjonowania systemów ochrony kryptograficznej, w szczególności z algorytmami kryptograficznymi i materiałami kryptograficznymi.

5. Osobom, o których mowa w ust. 3, nie wystawia się CUK.

6. Zezwala się na prowadzenie dotychczasowych urządzeń ewidencyjnych do czasu ich zakończenia

7. Do czasu wyposażenia jednostek organizacyjnych w urządzenia do niszczenia materiałów kryptograficznych w formie papierowej, spełniających wymagania techniczne, o których mowa w § 8 ust. 9 pkt 5, dopuszcza się wykorzystywanie obecnie eksploatowanych urządzeń, nie dłużej jednak niż do dnia 31 grudnia 2015 r.

8. Ścinki materiałów kryptograficznych zniszczonych w obecnie eksploatowanych urządzeniach do niszczenia dokumentów nie spełniających wymagań, o których mowa w § 8 ust. 9 pkt 5 podlegają zmieleniu na miał papierowy, spaleniu w piecu lub rozpuszczeniu w kadziach z ługiem w zakładach papierniczych pod nadzorem co najmniej trzyosobowej komisji.

9. Zezwala się na stosowanie urządzeń do przechowywania informacji niejawnych, którym wydano certyfikaty zgodnie z wymaganiami zawartymi w:

1) zarządzeniu Nr 12/MON Ministra Obrony Narodowej z dnia 12 marca 2010 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 5, poz. 49 z późn. zm.);
2) zarządzeniu Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 21, poz. 203 z późn. zm.);
3) zarządzeniu Nr 49/MON Ministra Obrony Narodowej z dnia 7 sierpnia 2002 r. w sprawie szczególnych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 15, poz. 149 z późn. zm.).

§ 39. Zarządzenie wchodzi w życie z dniem 1 stycznia 2012 r.[1)]

Załączniki do zarządzenia Nr 58/MON
Ministra Obrony Narodowej
z dnia 22 grudnia 2011 r. (poz. 403)

Załącznik Nr 1

Procedury zaopatrywania w materiały kryptograficzne ... (podać nazwę jednostki organizacyjnej) przez kancelarię kryptograficzną nr ...(podać nazwę jednostki organizacyjnej);

Informacje ogólne
Dostęp do materiałów kryptograficznych — bezpieczeństwo osobowe
Procedury wydawania materiałów kryptograficznych
- Procedury wydawania narodowych materiałów kryptograficznych
  - Dokumenty kryptograficzne
  - Publikacje, dokumentacja techniczna, itp.
  - Urządzenia kryptograficzne
- Procedury wydawania sojuszniczych materiałów kryptograficznych
  - Przechowywanie materiałów kryptograficznych
  - Niszczenie materiałów kryptograficznych

Odpowiedzialność osób funkcyjnych w zakresie prowadzenia urządzeń ewidencyjnych (formularzy)
Arkusz uzgodnień pomiędzy jednostką zaopatrującą i zaopatrywaną
Wykaz osób funkcyjnych upoważnionych do pobierania materiałów kryptograficznych — tabela
Wykaz urządzeń ewidencyjnych i dokumentacji dodatkowo prowadzonych przez jednostkę zaopatrującą — tabela

[1)] Niniejsze zarządzenie było poprzedzone zarządzeniem Nr 12/MON Ministra Obrony Narodowej z dnia 12 marca 2010 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych (Dz. Urz. MON Nr 5, poz. 49 z późn. zm.), które utraciło moc z dniem wejścia w życie niniejszego zarządzenia na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

Załącznik Nr 2

Wykaz osób upoważnionych do dostępu do materiałów kryptograficznych
Klauzula tajności
Egzemplarz pojedynczy

WYKAZ
osób .....
(nazwa jednostki (komórki) organizacyjnej)

upoważnionych do dostępu do materiałów kryptograficznych

Lp.	Stopień wojskowy	Imię i nazwisko	Nazwa jednostki (komórki) organizacyjnej	Zakres i numer poświadczenia bezpieczeństwa	Termin ważności poświadczenia bezpieczeństwa do klauzuli:				Uwagi
					Ściśle tajne	Tajne	Poufne	Zastrzeżone	
1	2	3	4	5	6	7	8	9	10

Klasyfikacja i wymagania techniczne urządzeń do przechowywania materiałów kryptograficznych

I. Szafa stalowa klasy A

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 1 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone ryglem co najmniej na trzech krawędziach.
4. Szafa musi być wyposażona w zamek mechaniczny kluczowy, co najmniej klasy A wg Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem.
5. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm^2, rozstaw rygli max. 450 mm).
6. Szafy dwuskrzydłowe powinny być wyposażone w mechanizm dźwigowy, umieszczony na skrzydle aktywnym, blokujący je na co najmniej 3 krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm^2, rozstaw rygli max. 450 mm); skrzydło aktywne musi blokować skrzydło bierne na całej ich wysokości. W przypadku niezależnego zamykania obu skrzydeł każde z nich powinno być wyposażone w oddzielny mechanizm ryglujący.
7. Podstawa szafy musi posiadać te same rozmiary co wierzch. W szafie może znajdować się zaślepiony otwór umożliwiający jej zakotwienie.
8. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, potwierdzający zgodność wyrobu z wymaganiami klasy A.
9. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:
   1) nazwę wyrobu;
   2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
   3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu;
   4) masę.

II. Szafa stalowa klasy B

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 3 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone ryglem na czterech krawędziach.
4. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygle w średnicy min. 15 mm lub przekroju min. 175 mm^2, rozstaw rygli max. 450 mm); rygiel przyzawiasowy może być stały.
5. Szafy dwuskrzydłowe powinny być wyposażone w mechanizm ryglowy, umieszczony na skrzydle aktywnym, blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygle w średnicy min. 15 mm lub przekroju min. 175 mm^2, rozstaw rygli max. 450 mm); skrzydło aktywne musi blokować skrzydło bierne na całej ich wysokości. W przypadku niezależnego zamykania obu skrzydeł każde z nich powinno być wyposażone w oddzielny mechanizm ryglujący; rygle przyzawiasowe mogą być stałe.
6. Mechanizm ryglowy w drzwiach musi być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglowy, w tym:
   1) zamek mechaniczny kluczowy, co najmniej klasy B wg Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem;
   2) zamek mechaniczny szyfrowy, co najmniej klasy B wg Polskiej Normy PN-EN 1300 co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Z szafą powinny być dostarczone dwa komplety kluczy do zmiany kodu. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, co najmniej klasy B wg Polskiej Normy PN-EN 1300, pod warunkiem że zamek spełnia te same wymagania co zamek mechaniczny szyfrowy

oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.

7. Podstawa szafy musi posiadać te same rozmiary co wierzch. W szafie może znajdować się zaślepiony otwór umożliwiający jej zakotwienie.
8. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, potwierdzający zgodność wyrobu z wymaganiami klasy B.
9. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:
   1) nazwę wyrobu;
   2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
   3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu;
   4) masę.

III. Szafa stalowa klasy C

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane ze stali konstrukcyjnej wyższej jakości, o grubości min. 5 mm, a w przypadku konstrukcji wielopłaszczowej grubość płaszcza zewnętrznego powinna wynosić min. 3 mm. Połączenia korpusu szafy powinny zapewnić dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone ryglem na czterech krawędziach.
4. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygle w średnicy min. 15 mm lub przekroju min. 175 mm^2, rozstaw rygli max. 450 mm); rygiel przyzawiasowy może być stały.
5. Szafy dwuskrzydłowe powinny być wyposażone w mechanizm ryglowy, umieszczony na skrzydle aktywnym, blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygle w średnicy min. 15 mm lub przekroju min. 175 mm^2, rozstaw rygli max. 450 mm); skrzydło aktywne musi blokować skrzydło bierne na całej ich wysokości. W przypadku niezależnego zamykania obu skrzydeł każde z nich powinno być wyposażone w oddzielny mechanizm ryglujący; rygle przyzawiasowe mogą być stałe.
6. Mechanizm ryglowy w drzwiach musi być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglowy, w tym:
   1) zamek mechaniczny kluczowy, co najmniej klasy B wg Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem;
   2) zamek mechaniczny szyfrowy, co najmniej klasy B wg Polskiej Normy PN-EN 1300 co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem (atakiem) radiologicznym (promieniowanie z radioaktywnego źródła nieprzekraczającego równowartości 10 curie, co — 60 z odległości 760 mm przez 20 godzin). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy od ustawiania szyfru.
      Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, co najmniej klasy B wg Polskiej Normy PN-EN 1300, pod warunkiem że zamek spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.
7. Podstawa szafy musi posiadać te same rozmiary co wierzch. W szafie może znajdować się zaślepiony otwór umożliwiający jej zakotwienie.
8. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, potwierdzający zgodność wyrobu z wymaganiami klasy C.
9. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:
   1) nazwę wyrobu;
   2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
   3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu;
   4) masę.

Karty informacyjne

PODSTAWOWE INFORMACJE DOTYCZĄCE POMIESZCZENIA/DRZWI/URZĄDZENIA DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH		
NAZWA JEDNOSTKI ORGANIZACYJNEJ:	ODDZIAŁ:	WYDZIAŁ:
DRZWI/URZĄDZENIE DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH NR:	POKÓJ NR:	DATA OSTATNIEJ ZMIANY KOMBINACJI ZAMKA:
W przypadku znalezienia otwartego pomieszczenia/ drzwi/ urządzenia do przechowywania informacji niejawnych należy niezwłocznie poinformować jedną z niżej wymienionych osób oraz oficera dyżurnego.		
STOPIEŃ, NAZWISKO i IMIĘ:		NUMER TELEFONU DOMOWEGO:
ADRES DOMOWY:		
STOPIEŃ, NAZWISKO i IMIĘ:		NUMER TELEFONU DOMOWEGO:
ADRES DOMOWY:		

FORMULARZ AF79 PL

EWIDENCJA SPRAWDZENIA ZAMKNIĘCIA DRZWI/URZĄDZENIA DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH

Jednostka org.:	**Nr drzwi/ urządzenia do przechowywania informacji niejawnych:**	**Rok:**	
Nr budynku:	**Nr pomieszczenia:**	Miesiąc:	Miesiąc:

Niniejszym oświadczam, że dokonałem otwarcia, zamknięcia lub sprawdzenia zamknięcia drzwi/urządzenia do przechowywania informacji niejawnych w czasie wskazanym w tabeli co stwierdzam swoim podpisem (inicjałami). Podczas zamykania lub też sprawdzania zamknięcia zamka szyfrowego dokonałem przekręcenia jego pokrętła przynajmniej 4 razy (4 pełne obroty).

Data	Otwarto przez (inicjały)	Godz.	Zamknięto przez (inicjały)	Godz.	Sprawdzono przez (inicjały)	Godz.	Data	Otwarto przez (inicjały)	Godz.	Zamknięto przez (inicjały)	Godz.	Sprawdzono przez (inicjały)	Godz.
01/							01/						
02/							02/						
03/							03/						
04/							04/						
05/							05/						
06/							06/						
07/							07/						
08/							08/						
09/							09/						
10/							10/						
11/							11/						
12/							12/						
13/							13/						
14/							14/						
15/							15/						
16/							16/						
17/							17/						
18/							18/						
19/							19/						
20/							20/						
21/							21/						
22/							22/						
23/							23/						
24/							24/						
25/							25/						
26/							26/						
27/							27/						
28/							28/						
29/							29/						
30/							30/						
31/							31/						

Zawartość Instrukcji pracy kancelarii kryptograficznej

Instrukcja pracy kancelarii kryptograficznej powinna zawierać następującą tematykę:

1. Zadania kancelarii kryptograficznej.
2. Opis lokalnego i globalnego środowiska bezpieczeństwa oraz wyposażenia kancelarii kryptograficznej.
3. Członkowie Organu Bezpieczeństwa Systemów Łączności i Informatyki.
4. Obowiązki członków Organu Bezpieczeństwa Systemów Łączności i Informatyki.
5. Harmonogram pracy kancelarii kryptograficznej.
6. Procedura rutynowego niszczenia materiałów kryptograficznych.
7. Sposób zabezpieczania kodów dostępu i kluczy zapasowych.
8. Załączniki:
   1) lista aktów prawnych, wytycznych, zaleceń normujących pracę kancelarii kryptograficznej;
   2) szkic Globalnego Środowiska Bezpieczeństwa;
   3) szkic Lokalnego Środowiska Bezpieczeństwa;
   4) plan pomieszczeń kancelarii kryptograficznej;
   5) lista osób zapoznanych z instrukcją.

Tabela z kodami dostępu, kodami systemu alarmowego do pomieszczeń kancelarii (stacji) kryptograficznej, urządzeń do przechowywania informacji niejawnych

Klauzula tajności
Egz. nr. ....

KOMBINACJA ZAMKA SZYFROWEGO		
FORMULARZ TEN POWINIEN BYĆ ZGIĘTY W POŁOWIE I ODPOWIEDNIO ZAMKNIĘTY W NIEPRZEŹROCZYSTEJ KOPERCIE		
INSTYTUCJA:	**ODDZIAŁ:**	**WYDZIAŁ:**
NR FABRYCZNY POJEMNIKA/SEJFU:	**NR POMIESZCZENIA:**	**DATA OSTATNIEJ ZMIANY KOMBINACJI:**
KOD SYSTEMU ALARMOWEGO:**		

KOMBINACJA*/**			
1. OBRÓT W LEWO	.....	RAZY DO NUMERU	.....
2. OBRÓT W PRAWO	.....	RAZY DO NUMERU	.....
3. OBRÓT W LEWO	.....	RAZY DO NUMERU	.....
4. OBRÓT W PRAWO	.....	RAZY DO NUMERU	.....
5. OBRÓT W LEWO	.....	RAZY DO NUMERU	.....

* JEŚLI KOMBINACJA ZACZYNA SIĘ PRZEKRĘCENIEM POKRĘTŁA ZAMKA SZYFROWEGO W LEWO, ZACZYNAMY OPIS OD POZYCJI 1.
JEŚLI KOMBINACJA ZACZYNA SIĘ PRZEKRĘCANIEM POKRĘTŁA ZAMKA SZYFROWEGO W PRAWO, ZACZYNAMY OPIS OD POZYCJI 2.
** WYPEŁNIAĆ MIĘKKIM OŁÓWKIEM.

(miejsce zagięcia kartki)

KLAUZULA TAJNOŚCI

Sposób opisania koperty z kodami dostępu, kodami systemu alarmowego do pomieszczeń kancelarii (stacji) kryptograficznej, urządzeń do przechowywania informacji niejawnych

Klauzula tajności
Egz. nr. .....

KOD DO …….. NR FABRYCZNY ……..
ADRES: .....
.....

PRAWO POBRANIA POSIADAJĄ:
1 .....
(stopień wojskowy, imię i nazwisko)
2 .....
(stopień wojskowy, imię i nazwisko)
3 .....
(stopień wojskowy, imię i nazwisko)
4 .....
(stopień wojskowy, imię i nazwisko)
5 .....
(stopień wojskowy, imię i nazwisko)

(miejsce zagięcia kartki)
.....

KLAUZULA TAJNOŚCI

Rejestr teczek materiałów kryptograficznych, dzienników i książek ewidencyjnych

Strona lewa

Oznaczenie klauzuli tajności	Numer kolejny zapisu	Adnotacje dot. zniesienia bądź zmiany klauzuli tajności	Nazwa teczki, dziennika, książki itp.	Data rozpoczęcia	Data zakończenia	Liczba stron
1	2	3	4	5	6	7

Strona prawa

Komórka odpowiedzialna za prowadzenie teczki, dziennika, książki itp.	Pokwitowanie odbioru teczki, dziennika, książki itp.			Adnotacje o przekazaniu do archiwum lub zniszczeniu	Uwagi
	imię i nazwisko osoby prowadzącej	data i podpis	potwierdzenie zwrotu - data i podpis		
8	9	10	11	12	13

Załącznik Nr 8

Dziennik korespondencji

Strona lewa

Oznaczenie klauzuli tajności	Numer kolejny zapisu	Adnotacje dot. zniesienia bądź zmiany klauzuli tajności	Numer i data dokumentu otrzymanego	Nazwa instytucji nadawcy (przy odbiorze), adresata (przy wysyłce)	Jakiej sprawy dotyczy	Liczba		
						stron dokumentu wraz z załącznikami	załączników	stron załączników
1	2	3	4	5	6	7	8	9

Strona prawa

Numer według DEWMK	Kto wykonał dokument, komu przekazano lub numer RWMK	Pokwitowanie i data		Symbol (numer) akt, w których przechowuje się dokument	Uwagi
		wykonawcy pobierającego dokument do załatwienia	pracownika kancelarii potwierdzającego zwrot dokumentu		
10	11	12	13	14	15

Załącznik Nr 9

.....
(klauzula tajności)
Egzemplarz pojedynczy

DZIENNIK EWIDENCJI SZYFROGRAMÓW

Data założenia ..... r.
Data zakończenia ..... r.

Lewa strona

Kolejny numer wchodzący lub wychodzący	Nr wych. Nadawcy lub skrót nazwa jednostki organizacyjnej	Data i godzina otrzymania	**NADAWCA**	**ADRESAT**	Krótka treść	Ilość egz.
			Nazwa jednostki organizacyjnej, stopień wojskowy, imię i nazwisko	Nazwa jednostki organizacyjnej, stopień wojskowy, imię i nazwisko		
1	2	3	4	5	6	7

Prawa strona

DANE O DOKUMENTACH KRYPTOGRAFICZNYCH I BRUDNOPISACH			Ilość grup	Numer szyfrotelegramu	Potwierdzenie	Nr teczki i arkusza szyfrogramu	Uwagi
Nazwa i nr dokumentu kryptograficznego (segment/ odcinek/ tablica)	Nr brudn. Ilość segm./ odcinka/ tabl	Zniszczono data i podpisy		Grupa orientacyjna			
8	9	10	11	12	13	14	15

Załącznik Nr 10

Pomocnicza książka ewidencji pieczęci

w ……

(nr lub nazwa jednostki wojskowej)

Lp.	Od kogo otrzymano, numer i data pisma	Odbitka pieczęci	Odpis i nr fabryczny pieczęci metalowej	Data, stopień, imię i nazwisko oraz podpis otrzymującego pieczęć	Data i podpis prowadzącego ewidencję – przyjmującego pieczęć	Numer pisma, data i adresat, któremu wysłano – przekazano pieczęcie	Uwagi Data i numer rozkazu unieważniającego zagubioną (utraconą) pieczęć
1	2	3	4	5	6	7	8

Uwaga:
W rubryce 5 w stosunku do każdej pozycji ujętej w ewidencji należy przewidzieć miejsce na pokwitowanie i datę otrzymania przez użytkownika pieczęci i w rubryce 6 na datę odbioru i podpis prowadzącego ewidencję w przypadku zwrotu pieczęci. Prowadzący ewidencję składa swój podpis w obecności zdającego pieczęć.

Załącznik Nr 11

Rejestr wydanych materiałów kryptograficznych

REJESTR WYDANYCH MATERIAŁÓW KRYPTOGRAFICZNYCH Nr ……..

.....	.....	.....
Stopień wojskowy	*Imię i nazwisko lub nazwa materiału kryptograficznego*	*Nazwa jednostki (komórki) organizacyjnej*

Oznaczenie klauzuli tajności	Lp.	Adnotacje dot. zniesienia bądź zmiany klauzuli tajności	Nr ewidencyjny materiału kryptograficznego	Nazwa materiału kryptograficznego lub stopień wojskowy i nazwisko wykonawcy	ilość stron lub nr egz.	Data i pokwitowanie wykonawcy	Data i pokwitowanie kancelarii	Adnotacja o zniszczeniu lub przerejestrowaniu
1	2	3	4	5	6	7	8	9

Załącznik Nr 12

Skorowidz rejestrów wydanych materiałów kryptograficznych

Strona lewa

Lp.	Stopień wojskowy	Imię i nazwisko lub nazwa jednostki (komórki) organizacyjnej	Data założenia

Strona prawa

Data zakończenia	Adnotacje o zniszczeniu	Uwagi

Załącznik Nr 13

Książka doręczeń przesyłek miejscowych

Lp.	Data przyjęcia przesyłki (dzień, miesiąc, godzina)	Numer ewidencyjny dokumentu	Adresat	Potwierdzenie odbioru dokumentu	
				stopień wojskowy, imię i nazwisko	Pieczęć, data i podpis
1	2	3	4	5	6

Załącznik Nr 14

KARTA ZAPOZNANIA SIĘ Z MATERIAŁEM KRYPTOGRAFICZNYM OZNACZONYM KLAUZULĄ „ŚCIŚLE TAJNE”/„TAJNE”[2]

Nr ……

Lp.	UDOSTĘPNIENIE MATERIAŁU KRYPTOGRAFICZNEGO			ZWROT MATERIAŁU KRYPTOGRAFICZNEGO			uwagi
	Imię i nazwisko osoby, której materiał kryptograficzny udostępniono	data	podpis	Imię i nazwisko osoby, której materiał kryptograficzny zwrócono	data	Podpis	

[2] Niepotrzebne skreślić

Karty ewidencyjne dokumentów kryptograficznych (Formularz AF 54 A PL)

KLAUZULA TAJNOŚCI KRYPTO

Strona ze stron

Karta rejestracyjna pozycji materiału kryptograficznego

CZĘŚĆ A Dane wchodzące			KLAUZULA:	Pełna nazwa:				Nazwa skrócona:		Kancelaria
Rejestr / edycja	Numer seryjny		Ilość	Otrzymane od	Numer formularza	Data odbioru	Data ważności	Zniszczenie	Inwentaryzacja	Uwagi
	Początkowy	Końcowy								
CZĘŚĆ B Dane wychodzące										

Rejestr / edycja	Ilość	Numer seryjny		Dyspozycje		Dyspozycje	Dyspozycje		Zniszczenie lokalne		Zniszczenie zbiorcze
		Początek	Koniec	Kancelaria	Dane	Kancelaria	Dane	Kancelaria	Dane		

KLAUZULA TAJNOŚCI KRYPTO

Skrócona nazwa *:*

FORMULARZ AF 54 A PL

KLAUZULA TAJNOŚCI
KRYPTO

Strona ze stron

Rejestr / edycja	Ilość	Numer seryjny		Dyspozycje		Dyspozycje		Dyspozycje		Zniszczenie lokalne	Zniszczenie grupowe
		Początek	Koniec	Kancelaria	Dane	Kancelaria	Dane	Kancelaria	Dane		

KLAUZULA TAJNOŚCI
KRYPTO

Skrócona nazwa :

Karty ewidencyjne urządzeń ochrony kryptograficznej (formularz AF 54 B PL)

KRYPTO

KARTA EWIDENCYJNA ŚRODKÓW I MATERIAŁÓW KRYPTOGRAFICZNYCH - SPRZĘT

NAZWA SKRÓCONA:			KLAUZULA	PEŁNA NAZWA:				
DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER AF 21 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER AF 21 PL	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI

FORMULARZ AF 54 B PL

KRYPTO

DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER AF 21 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER AF 21 PL	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI

FORMULARZ AF 54 B PL

Karty ewidencyjne publikacji, wydawnictw, dokumentacji technicznej i standaryzacyjnej oraz innych materiałów kryptograficznych (formularz AF 54 C PL)

KRYPTO

KARTA EWIDENCYJNA ŚRODKÓW I MATERIAŁÓW KRYPTOGRAFICZNYCH - PUBLIKACJE

NAZWA SKRÓCONA:			KLAUZULA	PEŁNA NAZWA:				
DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER AF 21 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER AF 21 PL)	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI

FORMULARZ AF 54 C PL

KRYPTO

DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER AF 21 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER AF 21 PL	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI

FORMULARZ AF 54 C PL

Formularz AF 147 PL ewidencjonujący Karty formularzy AF 21 PL

……
(ROK)

KRYPTO

KARTA EWIDENCJI FORMULARZY AF 21 PL				**JEDNOSTKA ORGANIZACYJNA : ……**	**KANCELARIA Nr: 860048/….**	**NUMERACJA: ……**	**ROK:** ……	**STRONA: …. Z …**
Nr formularza	**Data**	**Od / Do**	**Numer wykazu przesyłek**	**Typ transakcji:**		**Uwagi**	**Zakończony przez:**	**Data zakończenia:**

……
(ROK)

Karta raportów dotyczących środków i materiałów kryptograficznych (formularz AF 21 PL)

RAPORT		KRYPTO
OD: NR KANCELARII		DO: NR KANCELARII

UŻYTKOWNIK	TYP TRANSAKCJI	NUMER	DATA

	NAZWA MATERIAŁU KRYPTOGRAFICZNEGO	KLAUZULA	ILOŚĆ	POCZ. NR EWIDENCYJNY	KOŃC. NR EWIDENCYJNY	UWAGI

~~~~~~PONIŻEJ BRAK POZYCJI KRYPTOGRAFICZNYCH~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

KOPIA 1 -
KOPIA 2 -
KOPIA 3 -

~~~~~~PONIŻEJ BRAK WPISU~~~~~~

TYP TRANSAKCJI	NADAWCA/POTWIERDZAJĄCY	ODBIORCA/POTWIERDZAJĄCY
1. ZNISZCZENIE/KASOWANIE 2. PRZEKAZANIE 3. POSIADANIE 4. ZNISZCZENIE/KASOWANIE ZBIORCZE 5. INWENTARYZACJA ZBIORCZA 6. INWENTARYZACJA 7. PRZEKAZANIE KRAJOWE 8. INNE	PODPIS: NAZWISKO: STOPIEŃ: RODZ. WOJSK: DATA:	PODPIS: NAZWISKO: STOPIEŃ: RODZ. WOJSK: DATA:

FORMULARZ AF 21 PL

Formularz AF 21 PL prowadzony jest według poniższej numeracji:

1) numery od 1001 do 1999 stosuje się dla raportów ewidencji materiałów kryptograficznych wchodzących. Formularz oznacza się klauzulą „ZASTRZEŻONE”;
2) numery od 3001 do 3999 stosuje się dla raportów ewidencji materiałów kryptograficznych wychodzących. Formularz oznacza się klauzulą „ZASTRZEŻONE”;
3) numery od 5001 do 5999 stosuje się dla raportów ewidencji zniszczenia materiału kryptograficznego (nie dotyczy pism związanych z tematyką kryptograficzną). Formularz oznacza się klauzulą „POUFNE”;
4) numery od 6001 do 6999 stosuje się dla raportów przyjęcia na posiadanie lub inwentaryzacji materiału kryptograficznego. Formularz oznacza się klauzulą „POUFNE”;
5) numery od 7001 do 7999 stosuje się dla raportów ewidencji wypożyczeń materiału kryptograficznego;
6) numery od 8001 do 8999 stosuje się dla raportów pomocniczych.

Numerację prowadzi się od dnia 1 stycznia do dnia 31 grudnia. Po czterocyfrowym numerze wpisujemy dodatkowo rok oraz skrót PL wg wzoru: 1001-11 -PL.

Wykaz przesyłek (formularz AF 69 PL)

POTWIERDZENIE ODBIORU POJEMNIKA/PACZKI/WORKA	**NUMER WYKAZU:**	**LICZBA PACZEK:**
OD:	**DO:**	

Lp.	INICJAŁY	NUMER EWIDENCYJNY	PRIORYTET	OD	DO
////////	*/////////////////*	*////PONIŻEJ////*	*////BRAK////*	*///WPISU///*	*/////////////////*

INSTRUKCJE SPECJALNE: BRAK *KOPIE ZWRÓCIĆ DO NADAWCY / KOPIA DLA ADRESATA*

CZAS I DATA PAKOWANIA:	*CZAS I DATA ODBIORU:*
NAZWISKO/STOPIEŃ/PODPIS OSOBY PAKUJĄCEJ:	*NAZWISKO/STOPIEŃ/PODPIS OSOBY ODBIERAJĄCEJ:*

FORMULARZ AF 69 PL

Załącznik Nr 21

Wzory pieczęci

Materiałów kryptograficznych wymienianych w ramach realizacji porozumień międzynarodowych:

Lp.	Wzór pieczęci	Opis pieczęci	Uwagi
1.	MINISTERSTWO OBRONY NARODOWEJ *…… MINISTRY OF NATIONAL DEFENCE **…… File No …… …… Warsaw - POLAND	Pieczęć nagłówkowa – prostokątna, o długości 54 mm i szerokości 33 mm, wypukła do tuszu.	* Nazwa jednostki (komórki) organizacyjnej – w języku polskim. ** Nazwa jednostki (komórki) organizacyjnej – w języku angielskim.
2.	**MINISTERSTWO OBRONY NARODOWEJ** *…… **MINISTRY OF NATIONAL DEFENCE** **…… **File No** …… **Received on** …… **Enclosure** …… **Sheets** ……	Pieczęć wpływu pism – prostokątna, o długości 54 mm i szerokości 27 mm, wypukła do tuszu.	* Nazwa jednostki (komórki) organizacyjnej – w języku polskim. ** Nazwa jednostki (komórki) organizacyjnej – w języku angielskim.
3.		Pieczęć do pakietów o średnicy 30 mm, wypukła do tuszu oraz wklęsła do laku, z napisami na otoku: “✶MON✶ nazwa jednostki (komórki) organizacyjnej – w języku polskim” lub “✶MOND✶ nazwa jednostki (komórki) organizacyjnej – w języku angielskim”.	

4.	 MINISTERSTWO OBRONY NARODOWEJ *…… MINISTRY OF NATIONAL DEFENCE **……	Pieczęć firmująca – prostokątna o długości 54 mm i szerokości 20 mm, wypukła do tuszu.	* Nazwa jednostki (komórki) organizacyjnej – w języku polskim. ** Nazwa jednostki (komórki) organizacyjnej – w języku angielskim.
5.	MATERIAŁY KRYPTOGRAFICZNE PODLEGAJĄ CODZIENNEMU ZWROTOWI DO KANCELARII * ……	Pieczęć informacyjna – wypukła do tuszu, o długości 75 mm i szerokości 24 mm.	* Skrócona nazwa jednostki (komórki) organizacyjnej.
6.	UNCLASSIFIED nieklasyfikowane	Pieczęć informacyjna – wypukła do tuszu, o długości 40 mm i szerokości 12 mm.	
7.	RESTRICTED zastrzeżone	Pieczęć informacyjna – wypukła do tuszu, o długości 42 mm i szerokości 12 mm.	
8.	CONFIDENTIAL poufne	Pieczęć informacyjna – wypukła do tuszu, o długości 52 mm i szerokości 12 mm.	
9.	SECRET tajne	Pieczęć informacyjna – wypukła do tuszu, o długości 33 mm i szerokości 12 mm.	
10.	TOP SECRET ściśle tajne	Pieczęć informacyjna – wypukła do tuszu, o długości 53 mm i szerokości 12 mm.	
11.	TO BE DELIVERED PERSONALLY do rąk własnych	Pieczęć informacyjna - wypukła do tuszu, o długości 53 mm i szerokości 12 mm.	
12.	URGENT pilne	Pieczęć informacyjna – wypukła do tuszu, o długości 35 mm i szerokości 12 mm.	
13.	REGISTERED LETTER polecony	Pieczęć informacyjna – wypukła do tuszu, o długości 37 mm i szerokości 12 mm.	

14.	N A T O	Pieczęć informacyjna – prostokątna, o długości 44 mm i szerokości 15 mm, wypukła do tuszu.	
15.	U E	Pieczęć informacyjna – prostokątna, o długości 30 mm i szerokości 15 mm, wypukła do tuszu.	
16.	Enclosure No …… to …… of …… Załącznik Nr …… do pisma Nr ……	Pieczęć formularzowa – wypukła, do tuszu, o długości 54 mm i szerokości 22 mm.	
17.	Disposed on …… 1. …… 2. …… Signatures Zniszczono dn. …… 1. …… 2. …… podpisy	Pieczęć formularzowa – wypukła, do tuszu, o długości 54 mm i szerokości 28 mm.	

Załącznik Nr 22

Dziennik ewidencji wykonanych materiałów kryptograficznych

DZIENNIK EWIDENCJI WYKONANYCH MATERIAŁÓW KRYPTOGRAFICZNYCH

(techniką odręczną, maszynopisania, komputerową, kreślenia, powielania lub naświetlania)

KRYPTO

Strona lewa

Oznaczenie klauzuli tajności	L.p.	Data oddania brudnopisu do przepisania lub materiału kryptograficznego do powielenia	Adres albo nazwa materiału kryptograficznego	Nazwisko osoby sporządzającej materiał kryptograficzny	Nr brudnopisu i numery stron (nr materiału kryptograficznego i liczba stron)	Nazwisko osoby wykonującej materiał kryptograficzny
1	2	3	4	5	6	7

Strona prawa

Liczba wykonanych		Pokwitowanie odbioru			Adnotacje		Uwagi
egzemplarzy	stron egzemplarza	imię i nazwisko	data	podpis	o wysłaniu	o zniszczeniu	
8	9	10	11	12	13	14	15

Karta dopuszczenia do materiału kryptograficznego

Nr bibl.: ……

Temat: ……

Tytuł: ……

L.p.	Nazwisko i imię osoby upoważnionej	Kom. org.	Dekretacja z pisma (nr i data)	Imię i nazwisko osoby uprawnionej do dekretacji	Data i podpis osoby uprawnionej do dekretacji

Certyfikat Upoważnienia Kryptograficznego

KRYPTO

CERTYFIKAT UPOWAŻNIENIA KRYPTOGRAFICZNEGO

CZĘŚĆ I

1. IMIĘ I NAZWISKO:	**2. STOPIEŃ/ STANOWISKO:**	**3. NUMER KOLEJNY:**

4. NUMER I DATA WAŻNOŚCI	**5. KLAUZULA MATERIAŁÓW KRYPTOGRAFICZNYCH ORAZ ZAKRES, DO KTÓREGO UPRAWNIONY MA DOSTĘP**
a) POŚWIADCZENIA BEZPIECZEŃSTWA: **b) CERTYFIKATU BEZPIECZEŃSTWA:**	

6. OŚWIADCZENIE SKŁADANE W MOMENCIE PRZYZNANIA CERTYFIKATU:

Ja, _____ niniejszym oświadczam, że zostałem przeszkolony w zakresie bezpieczeństwa kryptograficznego przez _____. Rozumiem, że ochrona niejawnych informacji kryptograficznych ma najwyższe znaczenie oraz że utrata lub ujawnienie informacji kryptograficznych może spowodować nieusuwalną szkodę dla bezpieczeństwa narodowego i/lub NATO*. Zostałem przeszkolony w zakresie przepisów bezpieczeństwa dotyczących ujawniania informacji odnoszących się do kryptograficznych systemów narodowych i/lub NATO*. Znam instrukcje kryptograficzne narodowe i/lub NATO*, odnoszące się do ochrony niejawnych informacji kryptograficznych, do których zostałem upoważniony.

7. PODPIS OSOBY UPOWAŻNIONEJ:	**8. PODPIS OSOBY WYDAJĄCEJ UPOWAŻNIENIE:**
DATA:	**DATA:**

CZĘŚĆ II

9. OŚWIADCZENIE SKŁADANE PRZY ANULOWANIU CERTYFIKATU:

Ja, _____ niniejszym oświadczam, że zostałem poinformowany o anulowaniu mojego certyfikatu. Rozumiem znaczenie dalszej ochrony niejawnych informacji kryptograficznych dla bezpieczeństwa narodowego i/lub NATO*, rozumiem także, że wciąż jestem związany przepisami bezpieczeństwa narodowego i/lub NATO* do nie ujawniania niejawnych informacji kryptograficznych narodowych i/lub NATO*.

10. PODPIS:	**8. PODPIS OSOBY ANULUJĄCEJ UPOWAŻNIENIE:**
DATA:	**DATA:**

* niepotrzebne skreślić

Formularz 104PL

ZEZWALAM
na zniszczenie materiałów kryptograficznych
wyszczególnionych w protokole
.....
(stanowisko, stopień wojskowy, imię, nazwisko)

Miejscowość, dnia
KRYPTO

PROTOKÓŁ ZNISZCZENIA MATERIAŁÓW KRYPTOGRAFICZNYCH

Nr …

Zgodnie z rozkazem dziennym (decyzją) Nr ..... z dnia ....., komisja w składzie:
- przewodniczący: .....
(stopień wojskowy, imię i nazwisko; klauzula, numer i data ważności poświadczenia bezpieczeństwa)
- członkowie: .....
(stopień wojskowy, imię i nazwisko; klauzula, numer i data ważności poświadczenia)
.....
(stopień wojskowy, imię i nazwisko; klauzula, numer i data ważności poświadczenia)

zakwalifikowała niżej wymienione materiały kryptograficzne do zniszczenia:

Lp.	Nazwa materiału kryptograficznego	Nr ewidencyjny	Nr wg DEWMK	Ilość egz.	Nr egz.	Ilość stron (inna jednostka miary)	Uwagi
1	2	3	4	5	6	7	8

- PODPISY: .....
- .....
- .....

Materiały kryptograficzne wymienione w pozycjach ..... zostały zniszczone:
1) <u>wstępnie</u>* w dniu ..... przez .....
(określenie sposobu zniszczenia materiału)
Pojemnik ze zniszczonymi wstępnie materiałami opieczętowano pieczęcią okrągłą numerową do teczek pracy Nr .....
Imię, nazwisko, klauzula, numer i data ważności poświadczenia bezpieczeństwa oraz podpis:
   - osób, które wstępnie zniszczyły materiały kryptograficzne:
   - osób nadzorujących wstępne zniszczenie:
2) <u>ostatecznie</u>* w dniu ..... przez .....
(określenie sposobu zniszczenia materiału)

Imiona, nazwiska oraz podpisy:
- przewodniczący: .....
- członkowie: .....
.....

* niepotrzebne skreślić

Wzór upoważnienia do przeprowadzenia inspekcji kryptograficznej

……. Miejscowość, data
(nazwa organu zarządzającego inspekcję kryptograficzną)

UPOWAŻNIENIE Nr ……../….

Na podstawie Zarządzenia Nr …/MON Ministra Obrony Narodowej z dnia … 2011 r. w sprawie szczególnego sposobu organizacji kancelarii kryptograficznych

upoważniam:

Pana/Panią .....
(stopień, imię i nazwisko osoby przeprowadzającej inspekcję kryptograficzną)
do przeprowadzenia inspekcji kryptograficznej w .....
(nazwa i adres jednostki podlegającej inspekcji)

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

Ważność upoważnienia upływa z dniem ..... 20... r.

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

mp.
(pieczęć okrągła organu zarządzającego inspekcję kryptograficzną)

Ważność upoważnienia przedłuża się do dnia .....

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

mp.
(pieczęć okrągła organu zarządzającego inspekcję kryptograficzną)

Plan inspekcji kryptograficznej

Miejscowość, data

„Z A T W I E R D Z A M”

……..……..……..

(kierownik jednostki (komórki) organizacyjnej zarządzającej inspekcję kryptograficzną)

…….

(stopień, imię i nazwisko)

Dnia ….…… 20… r.

P L A N
PRZEPROWADZENIA INSPEKCJI KRYPTOGRAFICZNEJ

I. Temat inspekcji kryptograficznej:
Inspekcja kryptograficzna w ……

II. Cel inspekcji kryptograficznej:

1. Dokonać oceny funkcjonowania OBSŁiI.
2. ..... .

III. Zakres inspekcji:

BEZPIECZEŃSTWO MATERIAŁÓW KRYPTOGRAFICZNYCH

1. Sprawdzenie posiadania aktualnego certyfikatu bezpieczeństwa zespołu pomieszczeń kancelarii kryptograficznej lub zaświadczenia o funkcjonowaniu kancelarii kryptograficznej.
2. Analiza zawartości teczki z protokołami inspekcji kryptograficznych oraz innych form kontroli.
3. Sprawdzenie posiadania przez personel BSŁiI, wykonawców i inne osoby funkcyjne mające ograniczony dostęp do materiałów kryptograficznych poświadczeń bezpieczeństwa narodowych oraz ich odpowiedników NATO, UE oraz sprawdzenie dostępu do informacji niejawnych zgodnie z zasadą „wiedzy niezbędnej”.
4. Sprawdzenie prawidłowości wyznaczenia na stanowiska personelu BSŁiI oraz poprawności wystawiania kart wzorów podpisów ww. personelu.
5. Sprawdzenie posiadanych kursów specjalistycznych personelu BSŁiI.
6. Sprawdzenie prawidłowości wydania oraz aktualności wydanych certyfikatów upoważnienia kryptograficznego.

7. Sprawdzenie poprawności ewidencji szkoleń w zakresie bezpieczeństwa materiałów kryptograficznych.
8. Sprawdzenie funkcjonowania stref ochronnych, systemu alarmowego oraz kontroli dostępu.
9. Sprawdzenie kontroli dostępu do pomieszczeń kryptograficznych, materiałów kryptograficznych oraz pomocniczego sprzętu kryptograficznego.
10. Sprawdzenie zabezpieczenia kluczy użytku bieżącego oraz kluczy zapasowych do pomieszczeń i urządzeń przechowywania informacji niejawnych, w których przechowywane są materiały kryptograficzne.
11. Sprawdzenie dokonywania zmian ustawień kodów dostępu (kombinacji) w zamkach szyfrowych oraz sprawdzenie przechowywania kodów dostępu zamków szyfrowych.
12. Sprawdzenie certyfikatów drzwi wejściowych do kancelarii kryptograficznej oraz urządzeń do przechowywania informacji niejawnych, w których przechowywane są materiały kryptograficzne.
13. Sprawdzenie przeprowadzenia przez personel kancelarii kryptograficznej prawidłowości zakończenia pracy (kontrola na koniec każdego dnia pracy).
14. Sprawdzenie zabezpieczeń eksploatowanych urządzeń kryptograficznych, a także sprawdzenie przechowywania zapasowych urządzeń ochrony kryptograficznej i pomocniczego sprzętu kryptograficznego.
15. Sprawdzenie posiadania planów kolejności niszczenia i ewakuacji w pomieszczeniach, w których przechowywane są materiały kryptograficzne.
16. Porównanie opracowanych planów działania na wypadek zagrożenia z planami ochrony danej jednostki organizacyjnej.
17. Sprawdzenie stanu środków przeznaczonych do niszczenia oraz ewakuacji materiałów kryptograficznych.
18. Sprawdzenie zasad niszczenia materiałów kryptograficznych, w tym dokumentów kryptograficznych, które przestały obowiązywać lub zostały wykorzystane, oraz sprawdzenie postępowania z pozostałościami powstającymi w trakcie niszczenia.
19. Sprawdzenie poprawności oznakowania nośników informacji.

20. Sprawdzenie u wykonawców sposobu przechowywania materiałów kryptograficznych.

PROWADZENIE EWIDENCJI MATERIAŁÓW KRYPTOGRAFICZNYCH

1. Sprawdzenie „Rejestru teczek materiałów kryptograficznych, dzienników i książek ewidencyjnych”.
2. Sprawdzenie znajomości i przestrzeganie przez kierownika kancelarii kryptograficznej oraz jego zastępcę umiejętności postępowania z materiałami kryptograficznymi,
   a także przestrzegania zasad ich ewidencji.
3. Sprawdzenie, czy prowadzona ewidencja odzwierciedla wszystkie posiadane materiały kryptograficzne.
4. Sprawdzenie ewidencji niejawnej korespondencji wchodzącej i wychodzącej (szyfrogramy, faxy) dotyczącej tematyki kryptograficznej oraz sprawdzenie prawidłowości ich obiegu.
5. Sprawdzenie zapisów na korespondencji wchodzącej oraz sposobu ich realizacji.
6. Sprawdzenie sposobu dokonywania sprawdzeń przez personel BSŁiI urządzeń ewidencyjnych oraz materiałów kryptograficznych.
7. Sprawdzenie zgodności realizowanych inspekcji kryptograficznych oraz sprawdzeń z zasadami zapewniającymi ciągłą ochronę i nadzór.
8. Sprawdzenie czy materiały kryptograficzne, które zostały wykorzystane lub przestały obowiązywać są zniszczone zgodnie z obowiązującymi w tym zakresie przepisami.
9. Sprawdzenie prawidłowości wykonania protokołów zniszczonych materiałów kryptograficznych.
10. Sprawdzenie terminowego przesyłania do RCZBSiUT potwierdzeń zniszczenia materiałów kryptograficznych.
11. Sprawdzenie publikacji kryptograficznych zawierających wprowadzone zmiany i poprawki oraz czy są one właściwie ewidencjonowane.
12. Sprawdzenie posiadania wypisu dotyczącego kancelarii kryptograficznej z „Rzeczowego Wykazu Akt” jednostki organizacyjnej.

BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH

1. Sprawdzenie, czy w jednostce, w której przeprowadzana jest inspekcja kryptograficzna, przy użyciu systemów teleinformatycznych są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne dotyczące tematyki kryptograficznej.
2. Sprawdzenie przestrzegania wymagań w zakresie ochrony informacji niejawnych dotyczących tematyki kryptograficznej przetwarzanych, wytwarzanych, przechowywanych i przesyłanych w systemach teleinformatycznych eksploatowanych w kancelarii kryptograficznej oraz u wykonawców.
3. Sprawdzenie, czy system teleinformatyczny, o którym mowa w pkt 1 posiada zatwierdzoną przez SKW lub ABW dokumentację bezpieczeństwa lub/i ważny certyfikat/ świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.
4. Sprawdzenie, czy kierownik jednostki organizacyjnej wyznaczył: osobę lub zespół osób zwanych administratorem systemu, odpowiedzialnych za funkcjonowanie systemów teleinformatycznych, o których mowa w pkt 1, a także pracownika pionu ochrony odpowiedzialnego za bieżące sprawdzanie zgodności funkcjonowania tych systemów ze szczególnymi wymaganiami bezpieczeństwa.

IV. Termin przeprowadzenia inspekcji:

Inspekcja przeprowadzona zostanie w dniach ……..…..20… r.

V. Skład komisji:

Przewodniczący - ……..

Członkowie: - ……..

VI. Sposób przedstawienia wyników inspekcji:

Na podstawie ustaleń inspekcji w kancelarii sporządzony zostanie protokół z inspekcji przedstawiony kierownikowi jednostki (komórki) organizacyjnej zarządzającej inspekcję (oraz Informacja do ……..…).

PRZEWODNICZĄCY KOMISJI

……

(stopień, imię i nazwisko)

Protokół z przeprowadzenia inspekcji kryptograficznej

Miejscowość, data
Egz. nr ……...

P R O T O K Ó Ł

z inspekcji kryptograficznej

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

zarządzonej przez ……..……..……..……..
(osoba uprawniona do zarządzenia inspekcji kryptograficznej)

I. Inspekcję kryptograficzną przeprowadziła komisja z ……..……..…….
(nazwa jednostki (komórki) organizacyjnej)

w składzie:

- ……. - przewodniczący
- …….
- …….

II. Inspekcję kryptograficzną przeprowadzono w dniach ……..... **r., obejmując nią okres od** ……..
do ……... **r.**

III. Temat inspekcji kryptograficznej:

„Inspekcja kryptograficzna w ……”.

IV. Osoby funkcyjne z Organu Bezpieczeństwa Systemów Łączności i Informatyki:

- Oficer BSŁiI - ....., na stanowisku od .....; poprzednio - ..... od ... do ….;
- Kierownik kancelarii kryptograficznej - ……....., na stanowisku od .....; poprzednio - ..... od ... do ….;
- Zastępca kierownika kancelarii kryptograficznej - ……....., na stanowisku od .....; poprzednio - ..... od ... do ….;
- *(inne osoby odpowiedzialne za badaną problematykę)*

V. Ogólna charakterystyka OBSŁiI poddanego inspekcji kryptograficznej

VI. Ustalenia inspekcji kryptograficznej

(opis ustaleń inspekcji kryptograficznej zgodny z celami i zakresem ujętymi w planie inspekcji kryptograficznej oraz Kartą inspekcji kancelarii kryptograficznej)

……..……..……..……

VII. Podsumowanie:

Ogólna ocena wyników inspekcji kryptograficznej *(w formie pisemnej)* ……..……...…...……...….

VIII. Wnioski i zalecenia:

1. ……

2. ……..…..

(Przedstawić wnioski i zalecenia wynikające z ustaleń inspekcji kryptograficznej, w chronologii wynikającej z opisu ustaleń, w przypadku braku zaleceń należy dokonać wpisu - „Zaleceń nie wydano”.)

Kierownik jednostki organizacyjnej, w której przeprowadzono inspekcję kryptograficzną w ciągu 7 dni od daty przedstawienia niniejszego protokołu zobowiązuje się na usunięcie nieprawidłowości opisanych w niniejszym protokole i w formie pisemnej informuje kierownika jednostki organizacyjnej zarządzającej inspekcję kryptograficzną, o sposobie usunięcia tych nieprawidłowości i podjęciu działań zmierzających do zapobieżenia ich występowania.

KIEROWNIK JEDNOSTKI ORGANIZACYJNEJ	**PRZEWODNICZĄCY INSPEKCJI KRYPTOGRAFICZNEJ**
……	…….
(stopień, imię i nazwisko)	*(stopień, imię i nazwisko)*

Sporządzono w …egzemplarzach:

Egz. Nr 1 - …….
Egz. Nr 2 - …….
Egz. Nr 3 - …….
Egz. Nr 4 - …….

Karta inspekcji kancelarii kryptograficznej

Nazwa jednostki organizacyjnej:	
Okres objęty inspekcją kryptograficzną:	
Nr kancelarii kryptograficznej:	Data:
Kierownik KK:	Dokonujący inspekcji:
Z-ca kierownika KK:	Dokonujący inspekcji:
……..	…….

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały) Poz.	Neg.	Uwagi
BEZPIECZEŃSTWO MATERIAŁÓW KRYPTOGRAFICZNYCH				
1.	Sprawdzenie posiadania aktualnego certyfikatu bezpieczeństwa zespołu pomieszczeń kancelarii kryptograficznej.			
2.	Analiza zawartości teczki z protokołami inspekcji kryptograficznych i innych form kontroli.			
3.	Sprawdzenie posiadania przez personel BSŁiI, wykonawców i inne osoby funkcyjne mające ograniczony dostęp do materiałów kryptograficznych poświadczeń bezpieczeństwa narodowych oraz ich odpowiedników NATO, UE oraz sprawdzenie dostępu do informacji niejawnych zgodnie z zasadą „wiedzy niezbędnej”. *(Ważność poświadczeń bezpieczeństwa, certyfikatów NATO / UE, zaświadczenia o przeszkoleniu)*			
4.	Sprawdzenie prawidłowości wyznaczenia na stanowiska personelu BSŁiI oraz poprawności wystawiania kart wzorów podpisów ww. personelu. *(Rozkazy personalne, ciągłość zajmowania stanowiska, jak >60 dni nieobecności kier. KK to przekazanie obowiązków)*			

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały) Poz.	Neg.	Uwagi
5.	Sprawdzenie posiadanych kursów specjalistycznych personelu BSŁiI.			
6.	Sprawdzenie prawidłowości wydania oraz aktualności wydanych certyfikatów upoważnienia kryptograficznego. *(Wydanie CUK przez D-cę na wniosek Szefa* OBSŁiI *po wyznaczeniu rozkazem personalnym na stanowisko, instruktaż. Sprawdzenie „Wykazu wydanych CUK" i CUKów pod kątem zakresu obowiązków)*			
7.	Sprawdzenie poprawności ewidencji szkoleń w zakresie bezpieczeństwa materiałów kryptograficznych. *(plany konspekty, lista obecności)*			
8.	Sprawdzenie funkcjonowania stref ochronnych, systemu alarmowego oraz kontroli dostępu.			
9.	Sprawdzenie kontroli dostępu do pomieszczeń kryptograficznych, materiałów kryptograficznych oraz pomocniczego sprzętu kryptograficznego.			
10.	Sprawdzenie zabezpieczenia kluczy użytku bieżącego oraz kluczy zapasowych do pomieszczeń i urządzeń do przechowywania informacji niejawnych, w których przechowywane są materiały kryptograficzne.			
11.	Sprawdzenie dokonywania zmian ustawień kodów dostępu (kombinacji) w zamkach szyfrowych oraz sprawdzenie przechowywania kodów dostępu zamków szyfrowych.			
12.	Sprawdzenie certyfikatów drzwi wejściowych do kancelarii kryptograficznej oraz urządzeń do przechowywania informacji niejawnych, w których przechowywane są materiały kryptograficzne.			
13.	Sprawdzenie przeprowadzenia przez personel kancelarii kryptograficznej prawidłowości zakończenia pracy (kontrola na koniec każdego dnia pracy).			

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały) Poz.	Neg.	Uwagi
14.	Sprawdzenie zabezpieczeń eksploatowanych urządzeń kryptograficznych, a także sprawdzenie przechowywania zapasowych urządzeń ochrony kryptograficznej i pomocniczego sprzętu kryptograficznego.			
15.	Sprawdzenie posiadania planów kolejności niszczenia i ewakuacji w pomieszczeniach, w których przechowywane są materiały kryptograficzne.			
16.	Porównanie opracowanych planów działania na wypadek zagrożenia z planami ochrony danej jednostki organizacyjnej.			
17.	Sprawdzenie stanu środków przeznaczonych do niszczenia oraz ewakuacji materiałów kryptograficznych.			
18.	Sprawdzenie zasad niszczenia materiałów kryptograficznych, w tym dokumentów kryptograficznych, które przestały obowiązywać lub zostały wykorzystane, oraz kontrola postępowania z pozostałościami powstającymi w trakcie niszczenia.			
19.	Sprawdzenie poprawności oznakowania nośników informacji.			
20.	Sprawdzenie u wykonawców sposobu przechowywania materiałów kryptograficznych.			
PROWADZENIE EWIDENCJI MATERIAŁÓW KRYPTOGRAFICZNYCH				
21.	Sprawdzenie „Rejestru teczek materiałów kryptograficznych, dzienników i książek ewidencyjnych”.			
22.	Sprawdzenie znajomości i przestrzeganie przez kierownika kancelarii kryptograficznej oraz jego zastępcę umiejętności postępowania z materiałami kryptograficznymi, a także przestrzegania zasad ich ewidencji.			

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały) Poz.	Neg.	Uwagi
23.	Sprawdzenie, czy prowadzona ewidencja odzwierciedla wszystkie posiadane materiały kryptograficzne.			
24.	Sprawdzenie ewidencji niejawnej korespondencji wchodzącej i wychodzącej (szyfrogramy, faxy) dotyczącej tematyki kryptograficznej oraz sprawdzenie prawidłowości ich obiegu.			
25.	Sprawdzenie zapisów na korespondencji wchodzącej oraz sposobu ich realizacji.			
26.	Sprawdzenie sposobu dokonywania przez personel BSŁiI sprawdzeń urządzeń ewidencyjnych oraz bezpieczeństwa materiałów kryptograficznych.			
27.	Sprawdzenie zgodności realizowanych sprawdzeń bezpieczeństwa materiałów kryptograficznych z zasadami zapewniającymi ciągłą ochronę i nadzór.			
28.	Sprawdzenie czy materiały kryptograficzne, które zostały wykorzystane lub przestały obowiązywać są zniszczone zgodnie z obowiązującymi w tym zakresie przepisami.			
29.	Sprawdzanie prawidłowości wykonania protokołów zniszczonych materiałów kryptograficznych.			
30.	Sprawdzenie terminowego przesyłania do RCZBSiUT potwierdzeń zniszczenia materiałów kryptograficznych.			
31.	Sprawdzenie publikacji kryptograficznych zawierających wprowadzone zmiany i poprawki oraz czy są one właściwie ewidencjonowane.			
32.	Sprawdzenie posiadania wypisu dotyczącego kancelarii kryptograficznej z „Rzeczowego Wykazu Akt” jednostki organizacyjnej.			

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały) Poz.	Neg.	Uwagi
BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH				
33.	Sprawdzenie, czy w jednostce, w której przeprowadzania jest inspekcja kryptograficzna, przy użyciu systemów teleinformatycznych są wytwarzane, przechowywane, przetwarzane lub przekazywane materiały kryptograficzne.			
34.	Sprawdzenie przestrzegania wymagań w zakresie ochrony informacji niejawnych dotyczących tematyki kryptograficznej przetwarzanych, wytwarzanych, przechowywanych i przesyłanych w systemach teleinformatycznych eksploatowanych w kancelarii kryptograficznej oraz u wykonawców.			
35.	Sprawdzenie, czy system teleinformatyczny, o którym mowa w pkt. 1 posiada zatwierdzoną przez SKW lub ABW dokumentację bezpieczeństwa lub/i ważny certyfikat/ świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.			
36.	Sprawdzenie, czy kierownik jednostki organizacyjnej wyznaczył: osobę lub zespół osób zwanych administratorem systemu, odpowiedzialnych za funkcjonowanie systemów teleinformatycznych, o których mowa w pkt. 1, a także pracownika pionu ochrony odpowiedzialnego za bieżące sprawdzanie zgodności funkcjonowania tych systemów ze szczególnymi wymaganiami bezpieczeństwa.			