



DZIENNIK URZĘDOWY MINISTRA OBRONY NARODOWEJ

Warszawa, dnia 30 grudnia 2013 r.

Poz. 401

Służba Kontrwywiadu Wojskowego

ZARZĄDZENIE Nr 46 /MON MINISTRA OBRONY NARODOWEJ

z dnia 24 grudnia 2013 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) bezpieczeństwo materiałów kryptograficznych;
 - 4) organizację, funkcjonowanie i zabezpieczenie kancelarii kryptograficznych na okrętach i pomocniczych jednostkach pływających Marynarki Wojennej;
 - 5) organizację pracy kancelarii kryptograficznych, ich ochronę oraz obieg materiałów kryptograficznych podczas ćwiczeń, wojny, a także w czasie realizacji zadań poza granicami kraju;
 - 6) zasady rejestrowania, kompletowania i niszczenia materiałów kryptograficznych;
 - 7) sprawowanie nadzoru nad kancelariami kryptograficznymi;
 - 8) 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 akt dotyczące materiałów kryptograficznych, o których mowa w pkt. 21 lit. d-g, pogrupowanych zgodnie z układem

- dokumentacji określonym w zarządzeniu wydanym na podstawie ustawy o narodowym zasobie archiwalnym i archiwach, oznaczone właściwą kategorią archiwalną i symbolem klasyfikacyjnym;
- 3) archiwista – żołnierza, funkcjonariusza lub pracownika zatrudnionego w kancelarii kryptograficznej, podlegającego bezpośrednio kierownikowi kancelarii kryptograficznej;
 - 4) archiwizacja – ogół czynności związanych z klasyfikowaniem, kwalifikowaniem, kompletowaniem i przekazywaniem materiałów archiwalnych do archiwum oraz ich ewidencjonowanie i przechowywanie w tym archiwum;
 - 5) archiwum – wyodrębnione archiwum jednostki organizacyjnej, w rozumieniu przepisów zarządzenia Ministra Obrony Narodowej wydanego na podstawie ustawy o narodowym zasobie archiwalnym i archiwach;
 - 6) CUK – certyfikat upoważnienia kryptograficznego, dokument potwierdzający spełnienie wymagań uprawniających do dostępu do materiałów kryptograficznych w określonym zakresie;
 - 7) dokument kryptograficzny – każdy ciąg danych utrwalony na dowolnym nośniku, a w szczególności w banku danych kryptograficznych, na papierze, nośniku optycznym lub magnetycznym, posiadający cechy identyfikacyjne w postaci nazwy, klauzuli tajności, numeru egzemplarza, numeru serii oraz innych danych pomocniczych, który wykorzystywany jest do kryptograficznego zabezpieczenia informacji przed jej ujawnieniem lub modyfikacją oraz w realizacji procesu potwierdzenia autentyczności tej informacji przez produkt kryptograficzny;
 - 8) dokument kryptograficzny bieżącej edycji – dokument kryptograficzny wykorzystywany w danym momencie do czasu zakończenia terminu jego obowiązywania;
 - 9) dokument kryptograficzny przyszłej edycji – dokument kryptograficzny przeznaczony do przyszłego zabezpieczenia informacji;
 - 10) elektroniczny obieg dokumentów – proces rejestrowania, przechowywania, obiegu i udostępniania dokumentów realizowany przy wykorzystaniu specjalistycznego systemu teleinformatycznego;
 - 11) ewidencja – służące do rejestrowania materiałów kryptograficznych księgi, dzienniki, formularze, wykazy, spisy, rejestry lub kartoteki oraz elektroniczne bazy danych ustalonych wzorach i formach;
 - 12) GKK – Główną Kancelarię Kryptograficzną – kancelarię kryptograficzną umiejscowioną w SKW będącą Główną Kancelarią Kryptograficzną dla jednostek organizacyjnych resortu obrony narodowej, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i innych jednostek organizacyjnych nadzorowanych przez Ministra Obrony Narodowej;
 - 13) inspekcja kryptograficzna – kontrolę stanu ochrony materiałów kryptograficznych oraz funkcjonowania kancelarii (stacji) kryptograficznej, realizowaną przez OBSŁil, wykonywaną w ramach nadzoru nad ochroną informacji niejawnych;
 - 14) jednostka organizacyjna – Ministerstwo Obrony Narodowej, jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną;
 - 15) kancelaria kryptograficzna – etatową komórkę organizacyjną funkcjonującą w jednostce organizacyjnej, odpowiedzialną 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 narzędzi i certyfikowanych urządzeń kryptograficznych;
 - 16) kierownik jednostki organizacyjnej – dowódcę, szefa, dyrektora, komendanta, prezesa lub inną osobę stojącą na czele jednostki organizacyjnej, która kieruje całokształtem działalności tej jednostki, w tym również osobę czasowo pełniącą jego obowiązki;
 - 17) kierownik kancelarii kryptograficznej (w relacjach międzynarodowych – Crypto Custodian) – wyznaczonego żołnierza, funkcjonariusza lub pracownika zajmującego etatowe stanowisko kierownika kancelarii kryptograficznej i kierującego jej pracą, podlegającego merytorycznie Oficerowi Bezpieczeństwa Systemów Łączności i Informatyki;
 - 18) klasa systemu lub urządzenia alarmowego – kategorię jakości według Normy Obronnej NO-04-A004 "Obiekty Wojskowe. Systemy Alarmowe. Wymagania dotyczące urządzeń";

- 19) 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 krajowych i międzynarodowych materiałów kryptograficznych;
 - b) generację, wytwarzanie dokumentów kryptograficznych służących do zabezpieczenia krajowych potrzeb w zakresie ochrony systemów teleinformatycznych przetwarzających niejawne informacje krajowe i międzynarodowe,
 - c) nadzór nad zarządzaniem materiałami kryptograficznymi,
 - d) określanie sposobu organizacji i funkcjonowania kancelarii kryptograficznych,
 - e) powoływanie i odwoływanie kancelarii kryptograficznych,
 - f) udzielanie zgody na generację i wytwarzanie dokumentów kryptograficznych poza KOGD,
 - g) nadzór nad szkoleniem specjalistycznym personelu BSŁil,
 - h) nadzór nad prawidłowością funkcjonowania OBSŁil oraz przestrzegania przez nich przepisów i procedur;
- 20) kurier – żołnierz, funkcjonariusza lub pracownika wyznaczonego ze składu OBSŁil posiadającego kurs "Personelu kancelarii kryptograficznej" lub kurs "Kurierów materiałów kryptograficznych";
- 21) materiał kryptograficzny:
 - a) dokument kryptograficzny,
 - b) element systemu kryptograficznego, a w szczególności moduł, blok, podzespół, pomocnicze urządzenie kryptograficzne,
 - c) produkt kryptograficzny lub jego część,
 - d) publikację i wydawnictwo kryptograficzne,
 - e) dokumentację techniczną systemów i produktów kryptograficznych,
 - f) dokumentację, pismo dotyczące tematyki kryptograficznej, ewidencji, przechowywania, wykorzystania i niszczenia materiałów kryptograficznych,
 - g) formularz i inne urządzenie ewidencyjne przeznaczone do ewidencji materiałów kryptograficznych;
- 22) nadrzędna jednostka organizacyjna – nadrzędną w strukturze dowodzenia jednostkę organizacyjną;
- 23) NCK – Narodowe Centrum Kryptologii;
- 24) Oficer BSŁil – Oficera Bezpieczeństwa Systemów Łączności i Informatyki – funkcję sprawowaną w celu nadzoru nad bezpieczeństwem materiałów kryptograficznych;
- 25) OBSŁil – Organ Bezpieczeństwa Systemów Łączności i Informatyki, wyspecjalizowaną jednostkę organizacyjną, wewnętrzną komórkę jednostki organizacyjnej lub osobę odpowiedzialną za zapewnienie organizacyjnych, technicznych i programowych wymagań kryptograficznej ochrony informacji niejawnych oraz sprawowanie nadzoru nad funkcjonowaniem systemów kryptograficznych i teleinformatycznych, w których przetwarzane są materiały kryptograficzne; jak również za sprawowanie nadzoru nad zarządzaniem tymi materiałami;
- 26) pełnomocnik ochrony – pełnomocnika 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);
- 27) personel BSŁil – żołnierzy, funkcjonariuszy lub pracowników jednostki organizacyjnej, wchodzących w skład i wykonujących zadania na rzecz OBSŁil;
- 28) pomocnicze urządzenie ewidencyjne – urządzenie ewidencyjne nie podlegające zdaniu do archiwum, stosowane w zależności od potrzeb wynikających z funkcjonowania kancelarii kryptograficznej;
- 29) pomocniczy sprzęt kryptograficzny – sprzęt kryptograficzny będący elementem instalacji kryptograficznej, ale nie ujęty w definicji urządzenia kryptograficznego, który może wymagać specjalnej obsługi lub kontroli w celu ochrony specjalnych układów zabezpieczających;
- 30) potwierdzenie odbioru – fizyczne przekazywanie przez kierownika kancelarii kryptograficznej materiałów kryptograficznych, po złożeniu podpisu przez upoważnionego do odbioru wykonawcę z danej jednostki organizacyjnej;

- 31) pracownik – osobę pozostającą w stosunku pracy z jednostką organizacyjną;
- 32) produkt kryptograficzny – urządzenie lub narzędzie zawierające co najmniej jeden mechanizm kryptograficzny wykorzystywany w celu zapewnienia wymaganego poziomu bezpieczeństwa przetwarzanych informacji;
- 33) przesyłka – materiały w postaci odpowiednio zabezpieczonych, zaadresowanych i oznaczonych paczek lub listów;
- 34) przesyłka kryptograficzna – materiały kryptograficzne w postaci zabezpieczonych, zaadresowanych i odpowiednio oznaczonych paczek lub listów;
- 35) raport posiadania – wypełniony formularz AF 21 PL określający stan ewidencyjny posiadanych materiałów kryptograficznych będących na ewidencji kancelarii kryptograficznej;
- 36) RCZBSiUT – Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych;
- 37) rejestr wzorów podpisów – formularz, którego wzór określa **załącznik nr 1**, opisujący umiejscowienie kancelarii kryptograficznej w strukturze dowodzenia i systemie dystrybucji, zawierający jej dane teleadresowe oraz dane osobowe, wzory podpisów personelu tej kancelarii i Oficera BSŁil;
- 38) SKW – Służbę Kontrwywiadu Wojskowego;
- 39) stacja kryptograficzna – komórkę organizacyjną funkcjonującą w jednostce organizacyjnej realizującą zadania związane z ochroną kryptograficzną (szyfrowanie, deszyfrowanie) informacji niejawnych z wykorzystaniem urządzeń i narzędzi kryptograficznych;
- 40) 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 BSŁil;
- 41) Szef KOGD (w relacjach międzynarodowych – National Distribution Authority) - Szefa Krajowego Organu Generacji i Dystrybucji, to jest Dyrektora Biura Łączności i Informatyki SKW kierującego KOGD z upoważnienia i w imieniu Szefa Służby Kontrwywiadu Wojskowego;
- 42) trwałe urządzenie ewidencyjne – urządzenie ewidencyjne podlegające archiwizacji;
- 43) ustawa – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
- 44) urządzenie ewidencyjne – księgę, dziennik, wykaz, spis, rejestr, formularz lub kartotekę o ustalonych rubrykach, prowadzone w formie pisemnej lub elektronicznej, służące do rejestrowania materiałów kryptograficznych oraz umożliwiające kontrolę ich stanu i obiegu;
- 45) urządzenie kryptograficzne – certyfikowane urządzenie wykorzystywane do zabezpieczenia informacji przekazywanej w dowolnej sieci telekomunikacyjnej, przed jej ujawnieniem, modyfikacją oraz realizacji procesu potwierdzenia autentyczności tej informacji;
- 46) WSK RP – Wojskową Służbę Kurierską Rzeczypospolitej Polskiej, to jest żołnierzy, funkcjonariuszy lub pracowników SKW oraz Centrum Wsparcia Teleinformatycznego Sił Zbrojnych, zwanego dalej „CWT SZ”;
- 47) wykonawca – żołnierza, funkcjonariusza lub pracownika zajmującego określone stanowisko służbowe, wykonującego zadania zgodnie z zakresem obowiązków, posiadającego stosowne poświadczenia bezpieczeństwa i przeszkolenie w zakresie ochrony informacji niejawnych oraz CUK;
- 48) wytyczne SKW – Wytyczne SKW w sprawie powoływania i odwoływania kancelarii kryptograficznych;
- 49) zarządzanie materiałem kryptograficznym – całokształt przedsięwzięć związany z ochroną (bezpieczeństwem) materiałów kryptograficznych, od złożenia zapotrzebowania na dokumenty kryptograficzne, generację, wytwarzanie, ewidencję, dystrybuowanie, aż do ich fizycznego zniszczenia;
- 50) zasada wiedzy niezbędnej – udostępnianie określonej informacji wyłącznie osobom, którym jest to niezbędne do realizacji czynności służbowych;

- 51) zastępca kierownika kancelarii kryptograficznej (w relacjach międzynarodowych – Alternate Crypto Custodian) – wyznaczonego żołnierza, funkcjonariusza lub pracownika zajmującego etatowe stanowisko zastępcy kierownika tej kancelarii.

Rozdział 2

Organizacja, funkcjonowanie kancelarii kryptograficznej oraz organy nadzorujące jej pracę

§ 3.

1. W jednostkach organizacyjnych, które planują wykorzystywać materiały kryptograficzne kierownik jednostki organizacyjnej powołuje kancelarię kryptograficzną lub podpisuje stosowne porozumienie z kierownikiem jednostki organizacyjnej posiadającej kancelarię kryptograficzną.
2. Sposób oraz tryb powoływania i odwoływania kancelarii kryptograficznych określają wytyczne SKW.
3. Porozumienie, o którym mowa w ust. 1, określa sposób zaopatrywania w materiały kryptograficzne.
4. Obrót materiałami kryptograficznymi odbywa się wyłącznie pomiędzy jednostkami organizacyjnymi posiadającymi kancelarie kryptograficznie lub odpowiednie porozumienie, określone w ust. 1.
5. Kancelaria kryptograficzna może przyjmować, rejestrować, przechowywać i wysyłać materiały kryptograficzne krajowe i międzynarodowe oraz inne dokumenty związane z tematyką kryptograficzną, pod warunkiem, że będą one fizycznie od siebie oddzielone i rejestrowane w odrębnych urządzeniach ewidencyjnych.
6. Kancelaria kryptograficzna jednostki organizacyjnej może za zgodą Szefa KOGD i na podstawie porozumienia, określonego w ust. 1, zaopatrywać w materiały kryptograficzne inne jednostki organizacyjne nie posiadające kancelarii kryptograficznej.
7. W przypadku, o którym mowa w ust. 6, kierownik jednostki organizacyjnej nie posiadającej kancelarii kryptograficznej powinien:
 - 1) wyznaczyć personel BSŁil, w tym Oficera BSŁil i jego zastępcę;
 - 2) opracować w trzech egzemplarzach, według wzoru określonego w **załączniku nr 2**, 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)”, zwane dalej „Procedurami”;
 - 3) przesłać uzgodnione przez obu kierowników jednostek organizacyjnych Procedury poprzez RCZBSiUT do Szefa KOGD celem ich akceptacji;
 - 4) po otrzymaniu zaakceptowanych przez Szefa KOGD Procedur przesłać egzemplarz nr 3 do jednostki organizacyjnej zaopatrującej w materiały kryptograficzne.
8. Zgoda, o której mowa w ust. 6, jest wydawana na czas określony.
9. W przypadku uzasadnionym względami organizacyjnymi, w jednostce organizacyjnej można powołać więcej niż jedną kancelarię kryptograficzną.
10. Szef KOGD może zalecić powołanie kancelarii kryptograficznej.

§ 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 (archiwisci), 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 kancelarii kryptograficznej;
 - 2) przyjmowanie, rejestrowanie, przechowywanie oraz przekazywanie materiałów kryptograficznych otrzymywanych, wysyłanych oraz wytwarzanych na potrzeby wewnętrzne jednostki organizacyjnej oraz jednostek zaopatrywanych;
 - 3) współdziałanie w planowaniu i prowadzeniu inspekcji kryptograficznych w nadzorowanych 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 oraz prowadzenie wykazów osób upoważnionych do dostępu do materiałów kryptograficznych, którego wzór określa **załącznik nr 3**;
 - 8) posiadanie aktualnych edycji publikacji kryptograficznych i poprawne wprowadzanie do nich zmian;
 - 9) meldowanie Oficerowi BSŁil 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 zaopatrującej oraz nadrzędnej kancelarii kryptograficznej 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 BSŁil 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 kryptograficznej kierowanie jej pracą.
3. Do obowiązków archiwisty należy wykonywanie zadań, o których mowa w ust. 1 pkt. 2÷17.
4. Do obowiązków kuriera należy:
 - 1) wykonywanie zadań, o których mowa w ust. 1 pkt. 2 - 17;
 - 2) przewożenie materiałów kryptograficznych;
 - 3) przygotowanie i organizacja konwoju.

5. Obowiązki szyfranta określają odrębne przepisy.
6. Szczegółowe obowiązki personelu kancelarii kryptograficznej określa Oficer BSŁil.

§ 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 wchodzi:
 - 1) co najmniej jeden przedstawiciel OBSŁil;
 - 2) co najmniej jeden przedstawiciel OBSŁil nadrzędnej jednostki organizacyjnej;
 - 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, przesyła się na 30 dni przed planowanym terminem zmiany kierownika kancelarii kryptograficznej.
4. Wniosek o przesłanie raportu posiadania materiałów kryptograficznych przesyła się do zaopatrującej kancelarii kryptograficznej na 30 dni przed planowanym terminem zmiany kierownika kancelarii kryptograficznej.
5. Wynikiem pracy komisji jest protokół z przekazania obowiązków oraz raport posiadania materiałów kryptograficznych.
6. Protokół przekazania obowiązków zawiera:
 - 1) podstawę przekazania obowiązków;
 - 2) 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;
 - 3) numer ewidencyjny raportu posiadania materiałów kryptograficznych;
 - 4) porównanie stanu faktycznego materiałów kryptograficznych ze stanem ewidencyjnym;
 - 5) uwagi osoby przyjmującej obowiązki dotyczące ujawnionych nieprawidłowości w zakresie ewidencjonowania i obiegu materiałów kryptograficznych.
7. Protokół przekazania obowiązków wykonuje się w dwóch jednobrzmiących egzemplarzach.
8. Zatwierdzone przez kierownika jednostki organizacyjnej egzemplarze protokołu przechowuje się w kancelarii kryptograficznej:
 - 1) nadrzędnej jednostki organizacyjnej;
 - 2) własnej.
9. Po przyjęciu obowiązków kierownik kancelarii kryptograficznej przesyła aktualny rejestr wzorów podpisów.
10. Dopuszcza się przesyłanie kopii rejestru wzorów podpisów drogą elektroniczną poprzez system teleinformatyczny zabezpieczony kryptograficznie (m.in. MIL-WAN).
11. Na czas nieobecności kierownika kancelarii kryptograficznej i jego zastępcy poniżej 60 dni, obowiązki kierownika pełni etatowa osoba z personelu kancelarii kryptograficznej, posiadająca odpowiednie poświadczenia bezpieczeństwa, zaświadczenie ukończenia kursu personelu kancelarii kryptograficznych, wyznaczona rozkazem dziennym lub decyzją kierownika jednostki organizacyjnej.
12. W przypadku, gdy w kancelarii kryptograficznej pozostaje wyłącznie jedna osoba ze składu etatowego personelu, kierownik jednostki organizacyjnej, może wyznaczyć do składu tej kancelarii osobę spełniającą wymagania, o których mowa w ust. 11.
13. W szczególnie uzasadnionych przypadkach, za zgodą Szefa KOGD, do składu kancelarii można wyznaczyć Oficera BSŁil.
14. W przypadku, gdy nie ma możliwości wyznaczenia dodatkowej osoby, o której mowa w ust. 12 lub 13, do składu personelu kancelarii, kancelaria podlega zawieszeniu.
15. Na czas nieobecności kierownika kancelarii kryptograficznej i jego zastępcy powyżej 60 dni przekazanie obowiązków kierownika kancelarii kryptograficznej realizuje komisja na zasadach określonych w ust. 3 - 10.

16. Przewodniczący komisji, o której mowa w ust. 15, 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.
17. Protokół przekazania obowiązków podpisują przewodniczący oraz członkowie komisji, o której mowa w ust. 15, a zatwierdza kierownik jednostki organizacyjnej.

§ 7.

1. W jednostkach organizacyjnych, w których wykorzystuje się lub planuje się wykorzystywać materiały kryptograficzne tworzy się OBSŁil nadzorujące pracę kancelarii (stacji) kryptograficznej.
2. OBSŁil nadzorowane są przez OBSŁil nadrzędnej jednostki organizacyjnej.
3. Zaopatrywanie w materiały kryptograficzne odbywa się zgodnie z terytorialnym systemem zaopatrywania kancelarii kryptograficznych.
4. Terytorialny system zaopatrywania, o którym mowa w ust. 3 określa Komendant RCZBSiUT w uzgodnieniu z Szefem KOGD, a zatwierdza Dyrektor Narodowego Centrum Kryptologii.
5. KOGD w ramach wykonywanych czynności specjalistycznych nadzoruje RCZBSiUT oraz inne OBSŁil.
6. RCZBSiUT jest odpowiedzialne za:
 - 1) koordynowanie działalności OBSŁil;
 - 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) planowanie, organizowanie oraz sprawowanie nadzoru nad szkoleniami specjalistycznymi personelu BSŁil;
 - 4) prowadzenie ewidencji dokonywanych kontroli lub inspekcji kryptograficznych nadzorowanych OBSŁil;
 - 5) opracowywanie i przesyłanie do KOGD do dnia 30 kwietnia każdego roku sprawozdań o stanie ochrony informacji niejawnych w zaopatrywanych kancelariach kryptograficznych za ubiegły rok z wyszczególnieniem:
 - a) kancelarii kryptograficznych objętych nadzorem,
 - b) stacji kryptograficznych objętych nadzorem,
 - c) formy nadzoru (kontrola, inspekcja itp.),
 - d) organów bezpieczeństwa systemów łączności i informatyki przeprowadzających inspekcje,
 - e) stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych.
 - 6) przesyłanie do KOGD bezzwłocznie na bieżąco zmian stanu posiadania urządzeń kryptograficznych w resorcie obrony narodowej;
 - 7) prowadzenie inspekcji kryptograficznych w jednostkach organizacyjnych;
 - 8) przedstawianie do KOGD zbiorczych zapotrzebowań na materiały kryptograficzne krajowe i międzynarodowe dla potrzeb OBSŁil jednostek i komórek organizacyjnych Sił Zbrojnych RP;
 - 9) nadzorowanie wykorzystywania materiałów kryptograficznych przez OBSŁil;
 - 10) przeprowadzenie, raz w roku odprawy rozliczeniowo-szkoleniowej dla Oficerów BSŁil z OBSŁil bezpośrednio nadzorowanych;
 - 11) opracowywanie procedur obsługi urządzeń ochrony kryptograficznej, pomocniczego sprzętu kryptograficznego oraz postępowania z dokumentami kryptograficznymi;
 - 12) przeprowadzenie raz w roku odprawy rozliczeniowo-szkoleniowej dla kierowników kancelarii kryptograficznych bezpośrednio zaopatrywanych;

- 13) przesyłanie raz na kwartał raportów zniszczeń do KOGD.
7. OBSŁil wszystkich szczebli organizacyjnych, z zastrzeżeniem ust. 6 są odpowiedzialne za:
 - 1) koordynowanie działalności podporządkowanych OBSŁil;
 - 2) prowadzenie ewidencji dokonywanych kontroli lub/i inspekcji kryptograficznych OBSŁil;
 - 3) opracowywanie i przesyłanie do OBSŁil nadrzędnej jednostki organizacyjnej sprawozdań o stanie ochrony informacji niejawnych w podległych OBSŁil za ubiegły rok z wyszczególnieniem:
 - a) kancelarii kryptograficznych objętych nadzorem,
 - b) stacji kryptograficznych objętych nadzorem,
 - c) formy nadzoru (kontrola, inspekcja itp.),
 - d) organów bezpieczeństwa systemów łączności i informatyki przeprowadzających inspekcje,
 - e) stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych;
 - 4) określenie terminu przesłania sprawozdania, o którym mowa w pkt. 3 dla bezpośrednio podporządkowanych organów BSŁil;
 - 5) planowanie, organizowanie, systemów ochrony kryptograficznej stosowanych w systemach teleinformatycznych podległych jednostek organizacyjnych oraz eksploatację i nadzór nad ich funkcjonowaniem;
 - 6) prowadzenie inspekcji kryptograficznych w nadzorowanych jednostkach organizacyjnych;
 - 7) przedstawianie drogą służbową do RCZBSiUT zbiorczych zapotrzebowań na krajowe i międzynarodowe materiały kryptograficzne dla potrzeb OBSŁil nadzorowanych jednostek organizacyjnych;
 - 8) nadzorowanie wykorzystywania materiałów kryptograficznych przez podległe OBSŁil;
 - 9) przeprowadzenie raz w roku odprawy rozliczeniowo-szkoleniowej dla Oficerów BSłil z OBSŁil bezpośrednio nadzorowanych;
 - 10) raz na kwartał przesyłanie raportów zniszczeń do kancelarii zaopatrującej.
8. Sprawozdanie, o którym mowa w ust. 7 pkt. 3, Dowództwo Generalne Rodzajów Sił Zbrojnych, zwane dalej „DG RSZ”, Dowództwo Operacyjne Rodzajów Sił Zbrojnych, zwane dalej „DO RSZ”, Dowództwo Garnizonu Warszawa, zwane dalej „DGW”, Komenda Główna Żandarmerii Wojskowej, zwana dalej „KG ŻW” przesyłają do RCZBSiUT do 15 marca każdego roku.
9. OBSŁil składają zapotrzebowania na materiały kryptograficzne do OBSŁil nadrzędnej jednostki organizacyjnej, za pośrednictwem kancelarii kryptograficznych.
10. Kierownik jednostki organizacyjnej w celu nadzoru nad bezpieczeństwem materiałów kryptograficznych powołuje Oficera BSłil.
11. Funkcja, o której mowa w ust. 10, sprawowana jest przez:
 - 1) osobę wyznaczoną w NCK i RCZBSiUT przez kierownika tej jednostki organizacyjnej;
 - 2) szefa (oddziału, wydziału, sekcji, grupy) w komórkach bezpieczeństwa systemów łączności i informatyki;
 - 3) kierownika komórki odpowiedzialnej za organizację łączności w jednostce organizacyjnej, w której nie występuje etatowa komórka BSłil;
 - 4) kierownika komórki organizacyjnej, w której planowane jest powołanie kancelarii kryptograficznej w jednostce organizacyjnej;
12. Oficer BSłil jest odpowiedzialny za zapewnienie bezpieczeństwa materiałom kryptograficznym w tym za sprawdzanie wszystkich miejsc w jednostce organizacyjnej, w których są przechowywane i wykorzystywane te materiały.
13. Do zadań i obowiązków Oficera BSłil należy:

- 1) uzgadnianie bezpośrednio z kierownikiem jednostki organizacyjnej wszelkich zagadnień związanych z ochroną materiałów kryptograficznych oraz funkcjonowaniem OBSŁil;
- 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 BSŁil z OBSŁil szczebla nadrzędnego w zakresie specjalistycznym dotyczącym przechowywania, przesyłania oraz stosowania i wykorzystywania materiałów kryptograficznych;
- 4) współpraca z pionem ochrony oraz komórką odpowiedzialną za ochronę obiektów wojskowych w zakresie zastosowanych środków ochrony fizycznej i technicznej przeznaczonych do ochrony materiałów kryptograficznych;
- 5) informowanie nadrzędnego OBSŁil o potrzebach w zakresie zabezpieczenia w materiały kryptograficzne jednostki organizacyjnej;
- 6) wskazywanie osób odpowiedzialnych za wymianę w urządzeniach kryptograficznych materiałów 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 BSŁil oraz nadzór nad ich przestrzeganiem;
- 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 OBSŁil oraz osób spoza tego organu (posiadających kwalifikacje techniczne związane z informatyką, elektroniką bądź kierunkami pokrewnymi), które mogłyby w przyszłości objąć stanowiska w OBSŁil, na organizowane specjalistyczne kursy i szkolenia;
- 13) dokumentowanie przeprowadzonych instruktaży i szkoleń dotyczących tematyki kryptograficznej;
- 14) wnioskowanie do kierownika jednostki organizacyjnej o przyznanie lub anulowanie CUK;
- 15) przeprowadzenie szkolenia co najmniej raz w roku z zakresu ochrony materiałów kryptograficznych wszystkim osobom posiadającym wystawiony CUK;
- 16) prowadzenie ewidencji wydanych CUK oraz monitorowanie ich statusu;
- 17) utrzymywanie i podnoszenie poziomu bezpieczeństwa fizycznego pomieszczeń kancelarii (stacji) kryptograficznych, łącznie z prowadzeniem sprawdzeń poziomu bezpieczeństwa w określonych odstępach czasowych;
- 18) niezwłoczne meldowanie kierownikowi jednostki organizacyjnej oraz Oficerowi BSŁil szczebla nadrzędnego o stwierdzonych incydentach mających wpływ na bezpieczeństwo materiałów kryptograficznych;
- 19) nadzorowanie poprawności prowadzenia wymaganej dokumentacji w kancelarii (stacji) kryptograficznej;
- 20) nadzorowanie wykorzystywania, obsługi oraz ochrony urządzeń i innych elementów systemów kryptograficznych w stacjach kryptograficznych;
- 21) okresowe sprawdzanie stosowania przez personel BSŁil procedur uzbrajania urządzeń kryptograficznych dokumentami kryptograficznymi oraz obsługi przez ten personel urządzeń i narzędzi ochrony kryptograficznej eksploatowanych w jednostce organizacyjnej;
- 22) planowanie i organizowanie inspekcji kryptograficznych OBSŁil bezpośrednio nadzorowanych jednostek organizacyjnych - nie rzadziej niż co trzy lata;

- 23) kontrolowanie terminu upływu ważności certyfikatów wystawionych dla poszczególnych urzędów 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;
 - 24) udział w planowaniu i organizowaniu kontroli materiałów niejawnych w kancelarii kryptograficznej, prowadzonej w ramach kontroli okresowej ewidencji, materiałów i obiegu dokumentów.
14. Dla systemów teleinformatycznych przetwarzających materiały kryptograficzne inspektora bezpieczeństwa teleinformatycznego wyznacza się spośród pracowników pionu ochrony, a administratora systemu teleinformatycznego można wyznaczyć spośród personelu BSŁil.
 15. System teleinformatyczny, o którym mowa w ust. 14, może być kontrolowany przez inspektora bezpieczeństwa teleinformatycznego tylko w obecności administratora tego systemu. Inspektorowi bezpieczeństwa teleinformatycznego oraz administratorowi nie wystawia się CUK.
 16. Administrator systemu, o którym mowa w ust. 14, wykonuje zadania związane z administrowaniem systemu bez dostępu do materiałów kryptograficznych.

Rozdział 3

Środki bezpieczeństwa fizycznego

§ 8.

1. Kancelarie kryptograficzne, z uwagi na wysoki poziom zagrożenia związany z utratą informacji niejawnych, lokalizuje się 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 pkt. 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-EN1627, blokowane na 4 krawędziach, zabezpieczone przed wyłamaniem od strony zawiasów, posiadające element samozatrzaszkowy 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 (atakami) radiologicznym (promieniowaniem 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 wykorzystane 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 cm²,
 - 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 cm², 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.
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 tajności "ŚCIŚLE TAJNE", zaleca się zainstalowanie telewizyjnego systemu 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 tajności „ŚCIŚLE TAJNE”, a także „TAJNE”, „POUFNE” i „ZASTRZEŻONE” oraz międzynarodowych odpowiedników tych klauzul tajności,
 - b) szafy stalowe klasy B – do przechowywania materiałów kryptograficznych oznaczonych klauzulą tajności „TAJNE”, a także „POUFNE” i „ZASTRZEŻONE” oraz międzynarodowych odpowiedników tych klauzul tajności,
 - c) szafy stalowe klasy A – do przechowywania materiałów kryptograficznych oznaczonych klauzulą tajności „POUFNE”, a także „ZASTRZEŻONE” oraz międzynarodowych odpowiedników tych klauzul tajności;
 - 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 4.**
 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 ust. 6, nakleja się karty informacyjne, których wzór określa **załącznik nr 5.**
 12. Kancelarie kryptograficzne w zależności od potrzeb, wyposaża się w niejawne systemy teleinformatyczne.
 13. Eksploatacja jawnych systemów teleinformatycznych, z zastrzeżeniem ust. 14, a w szczególności urządzeń faksowych i systemów podłączonych do sieci INTERNET wymaga zgody Szefa KOGD.
 14. Zgoda, o której mowa w ust. 13, nie jest wymagana dla stacjonarnych aparatów telefonicznych.
 15. Środki bezpieczeństwa fizycznego dla pomieszczeń kancelarii kryptograficznych wyposażonych w systemy teleinformatyczne, o których mowa w ust. 13, regulują odrębne przepisy.
 16. 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.
 17. Pomieszczenia kancelarii kryptograficznej obejmuje się bezpośrednią ochroną fizyczną w postaci posterunku wystawionego przy budynku lub okresowym patrołowaniem 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 15 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 (krajowe 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 krajowych i międzynarodowych 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 jego konstrukcja pozwala na ich fizyczne rozdzielanie i zamknięcie w odrębnych skrytkach.
6. W przypadkach, o których mowa w ust. 5, klasa urządzenia musi uwzględniać klauzulę tajności najwyższej 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 tajności urządzenia kryptograficznego i wprowadzonego dokumentu kryptograficznego.
8. W pomieszczeniach służbowych nie spełniających standardów bezpieczeństwa, określonych w § 8 ust. 1, 8 i 9, materiały kryptograficzne, o których mowa w § 2 pkt. 21:
 - 1) lit. a, d+g 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 § 31 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 kryptograficznej.
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, której zawartość stanowi **załącznik nr 6**.
3. Klucze zapasowe do pomieszczeń kancelarii kryptograficznej, pomieszczeń magazynowych i urządzeń do przechowywania informacji niejawnych należy przechowywać w zabezpieczonych, oddzielnych pojemnikach lub kopertach, rejestrowanych w RWD 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. Klucze, o których mowa w ust. 2 i 3, nie oznaczają 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 7**, 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, podlegają ochronie przewidzianej dla materiałów niejawnych o klauzuli tajności odpowiadającej najwyższej sklasyfikowanej informacji przechowywanej w pomieszczeniu/urządzeniu, umieszcza się je w zabezpieczonych i oznaczonych kopertach, których sposób oznaczania określa **załącznik nr 7**.
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, podlegają ochronie przewidzianej dla materiałów niejawnych o klauzuli tajności odpowiadającej najwyższej sklasyfikowanej informacji przechowywanej w pomieszczeniu/urządzeniu, 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

Bezpieczeństwo materiałów kryptograficznych

§ 11.

1. Zgodę na dostęp do materiałów kryptograficznych w danej jednostce organizacyjnej wydaje kierownik jednostki organizacyjnej na wniosek Oficera BSŁil.
2. Zgodę oraz zakres dostępu do materiałów kryptograficznych podaje się w rozkazie lub decyzji kierownika jednostki organizacyjnej i zakres ten wpisuje się do CUK.
3. Za zapewnienie bezpieczeństwa materiałom kryptograficznym, w tym za kontrolę wszystkich miejsc w jednostce organizacyjnej, w których są przechowywane i wykorzystywane materiały kryptograficzne, odpowiada Oficer BSŁil danej jednostki organizacyjnej oraz pełnomocnik ochrony w stosunku do zabezpieczeń fizycznych tych miejsc.
4. W szczególnie uzasadnionych przypadkach za zgodą i na warunkach określonych przez Szefa KOGD, kierownik jednostki organizacyjnej może eksploatować produkty kryptograficzne bez wyznaczania Oficera BSŁil i personelu.
5. W sytuacji określonej w ust. 4 za nadzór nad użytkowaniem oraz bezpieczeństwem produktów kryptograficznych odpowiada Oficer BSŁil jednostki organizacyjnej udostępniającej ten produkt, na zasadach określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego.
6. Dostęp do krajowych materiałów kryptograficznych mogą mieć osoby posiadające:
 - 1) odpowiednie do klauzuli tajności materiałów kryptograficznych poświadczenie bezpieczeństwa lub upoważnienie, o którym mowa w art. 21 pkt. 4 ustawy, uprawniające do dostępu do krajowych materiałów kryptograficznych;
 - 2) aktualne zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych;
 - 3) przeszkolenie zgodne z zakresem dopuszczenia określonym w CUK;
 - 4) Certyfikat Upoważnienia Kryptograficznego (CUK).
7. Dostęp do międzynarodowych materiałów kryptograficznych mogą mieć osoby posiadające:
 - 1) odpowiedni do klauzuli tajności materiałów kryptograficznych certyfikat/poświadczenie NATO (lub odpowiednio UE) lub upoważnienie, o którym mowa w art. 21 pkt. 4 ustawy;
 - 2) aktualne zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych NATO (lub odpowiednio UE);
 - 3) przeszkolenie zgodne z zakresem dopuszczenia określonym w CUK;
 - 4) Certyfikat Upoważnienia Kryptograficznego (CUK).
8. Dostęp do wszelkich materiałów kryptograficznych odbywa się zgodnie z zasadą wiedzy niezbędnej.

9. Zasada wiedzy niezbędnej, o której mowa w ust. 8 dotyczy wszystkich osób mających dostęp do materiałów kryptograficznych, bez względu na zajmowane stanowisko służbowe.
10. Personel kancelarii kryptograficznej dokonując ewidencji materiału kryptograficznego zapoznaje się z materiałem kryptograficznym jedynie w taki sposób, który umożliwia jego ewidencję.
11. Zabrania się udostępniania materiału kryptograficznego osobom nieupoważnionym.
12. Zabrania się ujawniania informacji dotyczącej tematyki kryptograficznej uzyskanej podczas wykonywania obowiązków służbowych osobom i instytucjom, które nie są uprawnione do zapoznawania się z takimi informacjami.
13. Zakaz, o którym mowa w ust. 12, obowiązuje również osoby, które przestały pełnić obowiązki służbowe związane z ochroną kryptograficzną lub nie posiadają już dostępu do materiałów kryptograficznych.

§ 12.

1. Materiały kryptograficzne udostępnia się stosownie do zakresu określonego w CUK.
2. Wzór formularza CUK określa **załącznik nr 8**.
3. CUK wystawiany jest w egzemplarzu pojedynczym przez Oficera BSłil za zgodą kierownika jednostki organizacyjnej.
4. Na szczepku:
 - 1) Ministerstwa Obrony Narodowej i Sztabu Generalnego WP, CUK wydaje RCZBSiUT według odrębnych przepisów;
 - 2) NCK, DG RSZ, DO RSZ, DGW, KG ŻW, CUK wystawia Oficer BSłil za zgodą kierownika jednostki organizacyjnej lub osoby przez niego upoważnionej.
5. CUK wystawiany jest osobom, spełniającym wymagania określone w § 11 ust. 6 pkt. 1-3 lub ust. 7 pkt. 1-3, które wykonują obowiązki służbowe związane z dostępem do materiałów kryptograficznych.
6. W szczególnie uzasadnionych przypadkach, kierownik jednostki organizacyjnej może wyrazić zgodę na wystawienie CUK osobie spoza jednostki organizacyjnej, która ma wykonywać obowiązki służbowe związane z dostępem do materiałów kryptograficznych w danej jednostce organizacyjnej, z zastrzeżeniem ust. 7.
7. W przypadkach, o których mowa w ust. 6, po spełnieniu wymagań określonych w § 11 ust. 6 pkt. 1-3 lub ust. 7 pkt. 1-3 kierownik jednostki organizacyjnej może wyrazić zgodę na wystawienie CUK dla osób spoza resortu obrony narodowej po uzyskaniu zgody Szefa KOGD.
8. Oficer BSłil określa w CUK w sposób precyzyjny zakres dostępu do materiałów kryptograficznych.
9. Wystawiony CUK zachowuje ważność we wszystkich jednostkach i komórkach organizacyjnych resortu obrony narodowej.
10. Wystawienie CUK poprzedzone jest instruktażem w zakresie ochrony materiałów kryptograficznych udzielanym przez Oficera BSłil.
11. Tematykę instruktażu, o którym mowa w ust. 10 przedstawia **załącznik nr 9**.
12. Oficer BSłil prowadzi coroczne szkolenie dla osób posiadających CUK.
13. Kierownika jednostki organizacyjnej z zagadnieniami określonymi w **załączniku nr 9** zapoznaje Oficer BSłil danej jednostki organizacyjnej, co potwierdza w dokumentacji, o której mowa ust. 19.
14. CUK przechowywany jest w kancelarii kryptograficznej jednostki organizacyjnej, w której osoby upoważnione mają dostęp do materiałów kryptograficznych.
15. CUK na czas wykonywania czynności służbowych związanych z dostępem do materiałów kryptograficznych w innej jednostce organizacyjnej wydaje się z kancelarii za pokwitowaniem na podstawie rozkazu kierownika jednostki organizacyjnej. CUK podlega zwrotowi po ustaniu przyczyny jego wydania.
16. W przypadkach, o których mowa w ust. 15, pobranie CUK odnotowuje się w RWMK pobierającego ten CUK.

17. Słuchaczom kursów specjalistycznych, których program szkolenia narzuca konieczność zapoznawania z materiałami kryptograficznymi, kierownik jednostki organizacyjnej prowadzącej szkolenie zamiast wystawiania indywidualnego CUK może wystawić Grupowy Certyfikat Upoważnienia Kryptograficznego, którego wzór określa **załącznik nr 10**.
18. Grupowy CUK jest ważny tylko w okresie trwania szkolenia.
19. Oficer BSŁil prowadzi „Książkę ewidencji Certyfikatów Upoważnienia Kryptograficznego i szkoleń”, której wzór określa **załącznik nr 11**.
20. Książkę, o której mowa w ust. 19, ewidencjonuje się w kancelarii kryptograficznej w trwałym urządzeniu ewidencyjnym i przechowuje przez okres 20 lat od daty zakończenia i po tym okresie niszczy protokolarnie zgodnie z przepisami.
21. CUK nie wystawia się:
 - 1) etatowym kierownikom jednostek organizacyjnych i ich zastępcom, w których strukturach występują etatowe OBSŁil;
 - 2) szefowi Sztabu Generalnego WP i jego zastępcom;
 - 3) audytorom SKW prowadzącym audyt bezpieczeństwa systemów teleinformatycznych, w których zastosowano produkty kryptograficzne;
 - 4) osobom realizującym zadania w zakresie serwisowania urządzeń kryptograficznych oraz systemów teleinformatycznych przetwarzających materiały kryptograficzne bez dostępu do tych materiałów;
 - 5) użytkownikom produktów kryptograficznych, którzy nie posiadają dostępu do zaimplementowanych w nich mechanizmów i dokumentów kryptograficznych;
 - 6) kontrolerom Najwyższej Izby Kontroli, Agencji Bezpieczeństwa Wewnętrznego i SKW wykonującym czynności kontrolne wynikające z odrębnych przepisów;
 - 7) pełnomocnikowi ochrony oraz podległym mu pracownikom w trakcie przeprowadzania kontroli przechowywania i zabezpieczeń fizycznych kancelarii kryptograficznej.
22. W uzasadnionych przypadkach wiarygodność danych osobowych określonych w CUK należy potwierdzić innym dokumentem stwierdzającym tożsamość danej osoby.
23. Przy zmianie zakresu dostępu do materiału kryptograficznego lub w przypadku utraty ważności innych zapisów w „części I” formularza CUK, CUK jest anulowany i procedurę wydania CUK przeprowadza się ponownie.
24. Kierownik jednostki organizacyjnej, na wniosek właściwego Oficera BSŁil, anuluje CUK w przypadku:
 - 1) czasowego (na okres przekraczający 60 dni) oddelegowania osoby, której wystawiono CUK, do wykonywania innych czynności służbowych nie związanych z ochroną kryptograficzną;
 - 2) nieobecności spowodowanej długotrwałą chorobą lub urlopem przekraczającym okres 60 dni;
 - 3) zaprzestania działania czynników leżących u podstaw wydania CUK;
 - 4) ubycia lub przeniesienia na inne stanowisko służbowe żołnierza lub rozwiązania stosunku pracy z pracownikiem;
 - 5) upływu terminu obowiązywania dokumentu stanowiącego podstawę jego wydania;
 - 6) utraty ważności danych z „części I” formularza CUK.
25. Anulowanie CUK poprzedza się instruktażem udzielanym przez Oficera BSŁil, o tematyce określonej w pkt. 1-3 **załącznika nr 9**.
26. Informację o odsunięciu osoby od dostępu do materiałów kryptograficznych należy podać w rozkazie lub decyzji kierownika jednostki organizacyjnej.
27. Anulowany CUK przechowuje się w kancelarii kryptograficznej przez okres 3 lat a następnie niszczy za dwoma podpisami złożonymi w książce ewidencji, o której mowa w ust. 19.
28. W przypadku zagubienia CUK, dokument anuluje się rozkazem lub decyzją kierownika jednostki organizacyjnej, który uprawnienie nadał, odnotowuje ten fakt w książce ewidencji, o której mowa w ust. 19, i powiadamia nadrzędny organ BSŁil.

Rozdział 5

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

§ 13.

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 wykonane ze szkła hartowanego, zabezpieczone systemem alarmowym 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 ogólnokrętową 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 kryptograficznej 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 w 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, zgodę na zastosowanie alternatywnych środków bezpieczeństwa udziela Szef KOGD.

Rozdział 6

Zasady rejestrowania, kompletowania i niszczenia materiałów kryptograficznych

§ 14.

1. Kancelaria kryptograficzna przyjmuje, rejestruje, przechowuje, przekazuje i dystrybuje 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 12**;
 - b) dziennik korespondencji, którego wzór określa **załącznik nr 13**;
 - c) dziennik ewidencji szyfrogramów, którego wzór określa **załącznik nr 14**;
 - 2) pomocnicze urządzenia ewidencyjne:
 - a) książka ewidencji pieczęci, której wzór określa **załącznik nr 15**;
 - b) kartoteka wydanych materiałów kryptograficznych, w skład której wchodzi:
 - rejestr wydanych materiałów kryptograficznych, zwany dalej "RWMK", którego wzór określa **załącznik nr 16**;
 - skorowidz rejestrów wydanych materiałów kryptograficznych, zwany dalej "Skorowidzem RWMK", którego wzór określa **załącznik nr 17**;
 - c) książka doręczeń przesyłek miejscowych, zwana dalej "Książką doręczeń", której wzór określa **załącznik nr 18**;
 - d) karta zapoznania się z materiałem kryptograficznym oznaczonym klauzulą tajności "ŚCIŚLE TAJNE"/"TAJNE", zwana dalej "Kartą zapoznania się z materiałem kryptograficznym", której wzór określa **załącznik nr 19**;
 - e) karty ewidencyjne dokumentów kryptograficznych (formularz AF 54 A PL), po wypełnieniu winny otrzymać klauzulę stosowną do klauzuli dokumentów kryptograficznych ujętych na ich ewidencji, jednak nie wyższą niż POUFNE. Wzór karty określa **załącznik nr 20**;
 - f) karty ewidencyjne urządzeń ochrony kryptograficznej (formularz AF 54 B PL), po wypełnieniu winny być oznaczane jako JAWNE. Wzór karty określa **załącznik nr 21**;
 - g) karty ewidencyjne publikacji, wydawnictw, dokumentacji technicznej i standaryzacyjnej oraz materiałów filmowych dotyczących tematyki kryptograficznej (formularz AF 54 C PL), po wypełnieniu winny być oznaczane jako JAWNE. Wzór karty określa **załącznik nr 22**;
 - h) formularz AF 147 PL przeznaczony do ewidencji kart formularzy AF 21 PL, którego wzór określa **załącznik nr 23**;
 - 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 24**;
 - j) formularz wykazów przesyłek (AF 69 PL), którego wzór określa **załącznik nr 25** w przypadku przekazywania materiałów z kancelarii kryptograficznej do kancelarii kryptograficznej poprzez personel kancelarii lub poprzez Wojskową Służbę Kurierską RP (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 uzasadnionych przypadkach kancelaria kryptograficzna może prowadzić także inne urządzenia ewidencyjne niż wymienione w ust. 1.

5. Strony urzędzeń ewidencyjnych, o których mowa w 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 urzędzenia zamieszcza się adnotację o sumarycznej ilości stron poświadczoną podpisem kierownika kancelarii kryptograficznej, datą sporządzenia adnotacji i odciskiem pieczęci „Do pakietów”.

§ 15.

1. Wzory pieczęci stosowanych w kancelarii kryptograficznej określa **załącznik nr 26**.
2. W urzędzeniach ewidencyjnych, o których mowa w §14 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 urzędzeniach ewidencyjnych dokonuje się czarnym lub niebieskim tuszem (atramentem).
4. Odciski pieczęci nanosi się tuszem w kolorze czerwonym, czarnym lub niebieskim.
5. Zmiany zapisów w urzędzeniach 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 urzędzeniach ewidencyjnych.
6. Adnotacje o zmianie lub zniesieniu jego klauzuli tajności nanosi się kolorem czerwonym, poprzez skreślenie pierwotnego zapisu i wpisanie nowego w stosownej rubryce urzędzenia 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 urzędzeniach 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.

§ 16.

1. Rejestr dokumentacji jest nadrzędnym urzędzeniem ewidencyjnym w stosunku do innych urzędzeń ewidencyjnych prowadzonych przez kancelarię kryptograficzną.
2. Rejestr dokumentacji zalicza się do trwałych urzędzeń ewidencyjnych szczególnego rodzaju, nadrzędnym w stosunku do trwałych i pomocniczych urzędzeń ewidencyjnych kancelarii kryptograficznej w danej jednostce organizacyjnej jest prowadzony wyłącznie przez kancelarię kryptograficzną jednostki jako księga, przeznaczony do ewidencjonowania:
 - 1) trwałych oraz pomocniczych urzędzeń 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 urzędzeń 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 urzędów 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 urzędów ewidencyjnych zaewidencjonowanych w wykazach z lat poprzednich, jeżeli urządzenia te nadal są prowadzone.

§ 17.

1. W Dzienniku korespondencji rejestruje się materiały kryptograficzne, o których mowa w § 2 pkt. 21 lit. f, otrzymywane i wysyłane (wchodzące i wychodzące) oraz materiały kryptograficzne wytworzone na potrzeby wewnętrzne jednostki organizacyjnej z podziałem na materiały kryptograficzne jawne i niejawne.
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. 21 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. 21 lit. f, otrzymywanych i wysyłanych.
5. W Dziennikach korespondencji numerację materiałów kryptograficznych, o których mowa w § 2 pkt. 21 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. 21 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. 21 lit. f, pieczęcią wpływu oraz odcisnięciu 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. 21 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 tajności najwyższej 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) odcisnięcie 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. 21 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, opieczętowuje 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 BSłil;
 - 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 urzędnienia ewidencyjnego oraz wykonawcę.

19. W rubryce "Uwagi" Dziennika korespondencji wpisuje się datę przekazania materiału kryptograficznego, o którym mowa w § 2 pkt. 21 lit. f, numer oraz pozycję zapisu w Księżce 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. 21 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. 21 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. 21 lit. f, sporządzone w jednostce organizacyjnej na potrzeby własne ewidencjonuje się w Dzienniku korespondencji jak korespondencję otrzymaną, z wyjątkiem danych, o których mowa w 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 urzędnienia 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.

§ 18.

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.

§ 19.

1. W Kartach AF 54 C PL rejestruje się materiały kryptograficzne, o których mowa w § 2 pkt. 21 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 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 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. 21 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 w miejscu określonym na karcie.
5. Każdą poszczególną pozycję, tytuł, ewidencjonuje się oddzielnie na odrębnej karcie AF 54 C PL.

§ 20.

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 kryptograficzną wykonawcom:
 - 1) dokumentów kryptograficznych zarejestrowanych w innych urządzeniach ewidencyjnych, jeżeli:
 - a) rubryka urzędu 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) 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 urzędnika, 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 wrywania stron, wpisuje się numer ewidencyjny, o którym mowa w ust. 5, łamany przez numer karty (np. RWMK 10/Pf-8/1, 2, 3 ...). Fakt wrywania 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 urzędnika ewidencyjnego.
9. W przypadku przerejestrowania materiału kryptograficznego do RWMK innego wykonawcy lub zaewidencjonowania w innym urzędzie 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 komisijnemu 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.

§ 21.

1. Wykazów przesyłek nadanych oraz formularzy AF 69 PL nie ewidencjonuje się w żadnym urzędzie ewidencyjnym. Wykazom nadaje się kolejne numery, zaczynając numerowanie w każdym roku kalendarzowym od liczby "1".
2. W przypadku przekazania materiałów kryptograficznych poprzez kancelarie kryptograficzne 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.

§ 22.

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 komisijnemu zniszczeniu.

§ 23.

1. Kartę zapoznania się z materiałem kryptograficznym zakłada się i dołącza do materiału kryptograficznego pochodzenia krajowego, o którym mowa w § 2 pkt. 21 lit. d-f o klauzuli tajności „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.

§ 24.

1. Wykonawcy wytwarzający materiały kryptograficzne, o których mowa w § 2 pkt. 21 lit. d-f prowadzą Dziennik ewidencji wykonanych materiałów kryptograficznych, zwany dalej „DEWMK”, którego wzór określa **załącznik nr 27**.

2. DEWMK służy do rejestrowania materiałów kryptograficznych, o których mowa w ust. 1, wytworzonych w jednostce organizacyjnej, w szczególności techniką komputerową, maszynopisaną, 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 wydanego na podstawie art. 6 ust. 9 ustawy 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 tajności „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 tajności „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 komisijnemu 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.

§ 25.

1. Biblioteka przyjmuje, rejestruje, przechowuje, udostępnia i przekazuje materiały kryptograficzne, o których mowa w § 2 pkt. 21 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 kryptograficzną 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 kryptograficznej) oraz każdorazowo po zwrocie przez użytkownika, a ponadto podlega corocznemu sprawdzeniu.

6. W szczególnie uzasadnionych przypadkach ewidencję biblioteki można wspomóc przez stosowanie pomocniczych kart dopuszczenia do materiału kryptograficznego, których wzór określa **załącznik nr 28**.

§ 26.

1. Kancelaria kryptograficzna przekazuje materiały kryptograficzne wyłącznie wykonawcom posiadającym CUK, z zastrzeżeniem wykonawców wymienionych w § 12 ust. 21 oraz stosowne poświadczenie bezpieczeństwa lub odpowiedni certyfikat NATO (UE).
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, o których mowa w ust. 1, których pomieszczenia służbowe nie spełniają warunków dotyczących przechowywania i zabezpieczenia materiałów kryptograficznych, 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. Wszelkie materiały kryptograficzne mogą być przekazywane pomiędzy wykonawcami jedynie za pośrednictwem kancelarii kryptograficznej.
10. Materiały kryptograficzne ostatecznie załatwionych spraw powinny być niezwłocznie przekazane do kancelarii kryptograficznej.
11. 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).

§ 27.

1. Materiały kryptograficzne, o których mowa w § 2 pkt. 21 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 w § 2 pkt. 21 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 5 lat, nie wliczając roku bieżącego.
 4. Formularze AF 54 A, B, C PL nie podlegają ewidencji i przechowuje się je przez okres 5 lat od ich 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. Zgody, o której 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.

§ 28.

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. 21 lit. f, o klauzuli tajności „TAJNE” i „ŚCIŚLE TAJNE” co najmniej trzysobowa komisja, powoływana okresowo przez kierownika jednostki organizacyjnej;
 - 2) w odniesieniu do materiałów kryptograficznych, o których mowa w § 2 pkt. 21 lit. f, oznaczonych jako „jawne” oraz zawierających informacje niejawne o klauzuli tajności „ZASTRZEŻONE” oraz „POUFNE”, odbywa się w obecności osoby z personelu kancelarii kryptograficznej lub

wykonawcy, a fakt zniszczenia dokumentuje się w rubryce "Uwagi" urzędnika 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. 21 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 komisijnego zniszczenia materiałów kryptograficznych, o których mowa w ust. 3 pkt. 1, sporządza się protokół zniszczenia, którego wzór określa **załącznik nr 29**.
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 we właściwej rubryce lub rubryce „Uwagi” urzędnika ewidencyjnego adnotacji o dokonanych fakcie.

§ 29.

1. Materiał kryptograficzny w formie papierowej uważa się za ostatecznie zniszczony, jeżeli został pocięty w urzędzie, o którym mowa w § 8 ust. 9 pkt. 5 lub zmielony na miął 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 opłombowanych przez personel kancelarii kryptograficznej workach lub pojemnikach, w kancelarii kryptograficznej, lub innym pomieszczeniu jednostki organizacyjnej zabezpieczonym jak kancelaria kryptograficzna.
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.

§ 30.

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 7

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

§ 31.

1. Na czas ćwiczeń 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.

§ 32.

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.

§ 33.

Kancelarię kryptograficzną, o której mowa w § 31 ust. 1, organizuje się w osobnych kontenerach, pomieszczeniach na Stanowisku Dowodzenia, przy spełnieniu poniższych warunków:

- 1) wokół kancelarii kryptograficznej wydziela się strefę ochronną (jeśli możliwe – ogrodzoną) z jednym wejściem;
- 2) przy kancelarii kryptograficznej wystawia się całodobowy posterunek wartowniczy;
- 3) na czas nieobecności personelu materiał kryptograficzny należy przechowywać w zamkniętych szafach meblowych lub skrzyniach metalowych (nie dotyczy pracujących urzędów kryptograficznych).

§ 34.

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

§ 35.

Mobilne/polowe 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 8

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

§ 36.

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 9

Sprawowanie nadzoru nad kancelariami kryptograficznymi

§ 37.

1. Nadzór nad ochroną materiałów kryptograficznych w kancelariach kryptograficznych, realizowany jest przez nadrzędne jednostki organizacyjne w formie inspekcji kryptograficznych, z zastrzeżeniem ust. 3.
2. Nadzór nad powoływaniem kancelarii kryptograficznych realizowany jest przez nadrzędne jednostki organizacyjne, z zastrzeżeniem ust. 3.

3. Nadzór, o którym mowa w ust. 1 i 2:
 - 1) dla DG RSZ, DO RSZ, DGW, KG ŻW sprawuje RCZBSiUT;
 - 2) dla NCK, RCZBSiUT oraz przedsiębiorstw państwowych, dla których Minister Obrony Narodowej jest organem założycielskim, jednostką organizacyjną lub związek organizacyjny, wchodzące w skład Sił Zbrojnych sprawuje KOGD.
4. Inspekcje kryptograficzne kancelarii kryptograficznej przeprowadza się cyklicznie, nie rzadziej niż co 3 lata.
5. Inspekcja kryptograficzna ma na celu sprawdzenie:
 - 3) bezpieczeństwa kryptograficznego;
 - 4) prowadzenia ewidencji materiałów kryptograficznych;
 - 5) bezpieczeństwa systemów teleinformatycznych przetwarzających dane związane z materiałami kryptograficznymi.

§ 38.

1. Inspekcję kryptograficzną kancelarii kryptograficznej zarządza kierownik nadrzędnej jednostki organizacyjnej, a realizuje komisja złożona z upoważnionych członków OBSŁil, której przewodniczącym jest Oficer BSŁil.
2. Inspekcję kryptograficzną, o której mowa w ust. 1 przeprowadza się wykorzystując m.in. dokumenty określone w ust. 7.
3. Protokół z inspekcji kryptograficznej tworzy się w zależności od potrzeb w trzech lub czterech jednobrzmiących egzemplarzach.
4. Protokół, o którym mowa wyżej, przewodniczący komisji przedstawia do podpisu kierownikowi jednostki organizacyjnej, w której przeprowadzono inspekcję kryptograficzną wraz z załączoną kartą inspekcji.
5. Poszczególne egzemplarze protokołu inspekcji kryptograficznej wraz z kartą inspekcji kryptograficznej przekazuje się do:
 - 1) kancelarii kryptograficznej, w której inspekcja była przeprowadzana;
 - 2) nadrzędnej jednostki organizacyjnej – nie dotyczy inspekcji prowadzonych w OBSŁil DG RSZ, DO RSZ, DGW,-KG ŻW;
 - 3) KOGD;
 - 4) RCZBSiUT.
6. Prowadząc inspekcję kryptograficzną w jednostce organizacyjnej posiadającej więcej niż jedną kancelarię kryptograficzną dla każdej kancelarii sporządza się odrębny protokół z inspekcji kryptograficznej.
7. Wzór:
 - 1) upoważnienia do przeprowadzenia inspekcji kryptograficznej, określa **załącznik nr 30**;
 - 2) planu przeprowadzenia inspekcji kryptograficznej, określa **załącznik nr 31**;
 - 3) protokołu z inspekcji kryptograficznej, określa **załącznik nr 32**;
 - 4) karty inspekcji kryptograficznej, **określa załącznik nr 33**.

§ 39.

W przypadku stwierdzenia rażących uchybień w postępowaniu z materiałami kryptograficznymi należy przerwać inspekcję kryptograficzną i zabezpieczyć materiał dowodowy oraz w trybie pilnym powiadomić Szefa KOGD.

Rozdział 10

Transport materiałów kryptograficznych

§ 40.

1. Za organizację transportu materiałów kryptograficznych odpowiada kierownik jednostki organizacyjnej organizującej transport.
2. Transport, o którym mowa w ust. 1, odbywa się na podstawie zatwierdzonych przez kierownika jednostki organizacyjnej Procedur Transportowania Materiałów Kryptograficznych, opracowanych na podstawie **załącznika nr 34**.
3. Na organizację konwoju materiałów kryptograficznych składa się przygotowanie rozkazu (zarządzenia) wyjazdu kurierskiego, planu konwoju oraz udzielenia instruktażu osobom wyznaczonym do udziału w konwoju.
4. Instruktażu, o którym mowa w ust. 3, udziela Oficer BSŁil lub osoba przez niego upoważniona.

Rozdział 11

Przepisy przejściowe i końcowe

§ 41.

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 BSŁil, 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 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. Do czasu wyposażenia jednostek organizacyjnych w urzędzenia 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.
6. 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 miazgę papierową, spaleniu w piecu lub rozpuszczeniu w kadziach z ługiem w zakładach papierniczych pod nadzorem co najmniej trzyosobowej komisji.
7. Zezwala się na stosowanie urządzeń do przechowywania informacji niejawnych, którym wydano certyfikaty zgodnie z wymaganiami zawartymi w:
 - 1) zarządzeniu Nr 58/MON Ministra Obrony Narodowej z dnia 22 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. Urz. MON z 2011 r. Nr 25 poz. 403);
 - 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 oraz z 2010r. Nr 5, poz. 49);
 - 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 oraz z 2004 r. Nr 3, poz. 15).

§ 42.

Korespondencja dotycząca tematyki kryptograficznej w jednostkach organizacyjnych realizujących wymianę materiałów kryptograficznych na podstawie porozumienia, o którym mowa w § 3 ust. 1 odbywa się poprzez kancelarie tajne.

§ 43.

Dokumenty opracowane na podstawie załączników nr 1, 6, 14, 27, 29, 32, 34 powinny posiadać stosowną klauzulę tajności oraz inne oznaczenia zgodne z rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz. 1692).

§ 44.

Traci moc zarządzenie Nr 58/MON Ministra Obrony Narodowej z dnia 22 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. Urz. MON Nr 25, poz. 403).

§ 45.

Zarządzenie wchodzi w życie z dniem 1 stycznia 2014 r.

Minister Obrony Narodowej: *T. Siemoniak*

REJESTR WZORÓW PODPISÓW	
DANYCH KANCELARII KRYPTOGRAFICZNEJ	
Numer kancelarii	860048/
Z dnia <input type="text"/> - <input type="text"/> - <input type="text"/>	
Kancelaria podlega pod	860048/
Kancelaria odbiera materiał kryptograficzny od	860048/
Adres:	
Adres Kurierski	860048/
Ulica/Budynek/Pokój	
Kod, miasto	
Kraj	
Adres do wiadomości	
Dane telefoniczno-faksowe:	
IVSN	
DSN	
Tel. jawny	
Tel. CA MON	
Tel. utajniony 1	Typ
Tel. utajniony 2	Typ
Fax. utajniony	
Fax. jawny	

WZORY PODPISÓW

Oficer Bezpieczeństwa Systemów Łączności i Informatyki

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Data zmiany			
Nr telefonu			
Podpis			

Kierownik Kancelarii Kryptograficznej / Cryptocustodian

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Data zmiany			
Podpis			

..... (**)

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Podpis			

..... (**)

Nazwisko i imię			
Stopień		Rodz. wojsk	
Certyfikat		Data wyznaczenia	
Podpis			

Potwierdzenie:

m.p.

.....
(Podpis kierownika jednostki organizacyjnej)

** - wpisać kolejno etatowy personel kancelarii kryptograficznej

Procedury zaopatrywania w materiały kryptograficzne ... (podać nazwę jednostki organizacyjnej) przez kancelarię kryptograficzną nr ... (podać nazwę jednostki organizacyjnej);
Procedury powinny zawierać m.in. następujące informacje:

1. Informacje ogólne

- a. Pełna nazwa i adres jednostki organizacyjnej zaopatrywanej;
- b. Pełna nazwa i adres jednostki organizacyjnej zaopatrującej, dane i adres (jeżeli inny) kancelarii zaopatrującej (Zaświadczenie nr .../... o funkcjonowaniu kancelarii kryptograficznej ważne do ..., klauzula tajności przetwarzanych informacji);
- c. Zależność służbowa j.o. zaopatrywanej względem j.o. zaopatrującej: ... (podległa/ nadrzędna/ równorzędna/ niezależna służbowo)
- d. Przyczyna/powód zaopatrywania w materiały kryptograficzne: ... (uzasadnić);
- e. Typ/rodzaj/ klauzule tajności materiałów kryptograficznych będących przedmiotem zaopatrywania;
- f. Prognozowany czas zaopatrywania w materiały kryptograficzne;
- g. Realizacja/ zawieszenie realizacji/ cofnięcie realizacji przedmiotowych procedur;
- h. Sprawowanie nadzoru w jednostce zaopatrywanej.

2. Dostęp do materiałów kryptograficznych

- a. Personel Bezpieczeństwa Systemów Łączności i Informatyki (BSŁiI) w ... (nazwa j.o. zaopatrywanej);
- b. Wydawanie Certyfikatów Upoważnienia Kryptograficznego (CUK).

3. Procedury wykonywania/wydawania materiałów kryptograficznych

- a. Krajowych;
- b. Międzynarodowych.

4. Przechowywanie materiałów kryptograficznych

5. Niszczenie materiałów kryptograficznych

6. Transport materiałów kryptograficznych

7. Postępowanie na wypadek zagrożenia

8. Odpowiedzialność osób funkcyjnych w zakresie prowadzenia urządzeń ewidencyjnych (formularzy)

Wykaz osób funkcyjnych upoważnionych do pobierania materiałów kryptograficznych – tabela

Wykaz urządzeń ewidencyjnych i dokumentacji dodatkowo prowadzonych przez jednostkę zaopatrującą – tabela

Procedury należy opracować w 3 egzemplarzach:

Egz. nr 1 – KOGD;

Egz. nr 2 – jednostka zaopatrywana

Egz. nr 3 – jednostki zaopatrująca

Uwaga:

Procedury podlegają uzgodnieniu przez Komendanta RCZBSiUT oraz akceptacji Szefa KOGD.

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 rygłem 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 (rygłe w średnicy min. 12 mm lub przekroju min. 112 mm², 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 (rygłe w średnicy min. 12 mm lub przekroju min. 112 mm², 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 zaślepiiony 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 rygłem na czterech krawędziach.
4. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygłe w średnicy min. 15 mm lub przekroju min. 175 mm², 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 (rygłe w średnicy min. 15 mm lub przekroju min. 175 mm², 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; rygłe 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 pokrętko 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 zaślepiiony 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 wielopłaszczyznowej 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 rygłem na czterech krawędziach.
4. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygłe w średnicy min. 15 mm lub przekroju min. 175 mm², 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 (rygłe w średnicy min. 15 mm lub przekroju min. 175 mm², 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; rygłe 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 pokrętko 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 (atakami) 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.		
STOPIEN, NAZWISKO i IMIĘ:		NUMER TELEFONU DOMOWEGO:
ADRES DOMOWY:		
STOPIEN, 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 pokrętki przynajmniej 4 razy (4 pełne obroty).

Data	Otwarto przez (inicjały)	Godz.	Zamknięt o przez (inicjały)	Godz.	Sprawdzono przez (inicjały)	Godz.	Data	Otwarto przez (inicjały)	Godz.	Zamknięt o 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. Personel Organu Bezpieczeństwa Systemów Łączności i Informatyki.
4. Obowiązki personelu 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.

**Formularz z kodami dostępu, kodami systemu alarmowego do pomieszczeń kancelarii (stacji)
kryptograficznej, urządzeń do przechowywania materiałów niejawnych**

Oznaczenie koperty

		Podlega ochronie przewidzianej dla materiałów niejawnych
		o klauzuli tajności** Egz. nr
KOD DOSTĘPU*..... KOD SYSTEMU ALARMOWEGO*..... KOD DO POMIESZCZENIA NR*..... SZAFY NR FABRYCZNY *.....		
ADRES:		
.....		
<u>PRAWO POBRANIA POSIADAJĄ:</u>		
1	(stopień wojskowy, imię i nazwisko)	
2	(stopień wojskowy, imię i nazwisko)	
3	(stopień wojskowy, imię i nazwisko)	
4	(stopień wojskowy, imię i nazwisko)	
Podlega ochronie przewidzianej dla materiałów niejawnych o klauzuli tajności **.....		

strona 1
Kody

Podlega ochronie
przewidzianej dla materiałów niejawnych

o klauzuli tajności**
Egz. nr

KOD DO POMIESZCZENIA NR*
SZAFY 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)


(miejsce zagięcia kartki)
.....

Podlega ochronie przewidzianej dla materiałów niejawnych o klauzuli tajności **

* - niepotrzebne skreślić

** - klauzula tajności odpowiada najwyższej sklasyfikowanej informacji przechowywanej w pomieszczeniu/urzędzeniu

strona 2
Kody

KOMBINACJA ZAMKA SZYFROWEGO		Podlega ochronie Przewidzianej dla materiałów niejawnych o klauzuli tajności*..... Egz. nr
FORMULARZ TEN POWINIEN BYĆ ZGIĘTY W POŁOWIE I ODPOWIEDNIO ZAMKNIĘTY W NIEPRZEŻROCZYSTEJ 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	
<p>** 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.</p> <p style="text-align: center;">(miejsce zagięcia kartki)</p> <p>-----</p>		
		
Podlega ochronie przewidzianej dla materiałów niejawnych o klauzuli tajności *.....		

* - klauzula tajności odpowiada najwyższej sklasyfikowanej informacji przechowywanej w pomieszczeniu/urządzeniu

Certyfikat Upoważnienia Kryptograficznego

KRYPTO		
CERTYFIKAT UPOWAŻNIENIA KRYPTOGRAFICZNEGO		
CZĘŚĆ I		
1. IMIĘ I NAZWISKO:	2. STOPIEŃ/ STANOWISKO:	3. NUMER KOLEJNY:
4. NUMER I DATA WAŻNOŚCI a) POŚWIADCZENIA BEZPIECZEŃSTWA: b) CERTYFIKATU BEZPIECZEŃSTWA:	5. KLAUZULA TAJNOŚCI MATERIAŁÓW KRYPTOGRAFICZNYCH ORAZ ZAKRES, DO KTÓREGO UPRAWNIONY MA DOSTĘP	
6. OŚWIADCZENIE SKŁADANE W MOMENCIE PRYZNANIA 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:	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:	11. PODPIS OSOBY ANULUJĄCEJ UPOWAŻNIENIE:	
DATA:	DATA:	

* niepotrzebne skreślić **Formularz 104PL**

Tematyka omawiana podczas instruktażu związanego z wystawieniem CUK

1. Akty prawne i normatywne regulujące problematykę ochrony materiałów niejawnych, w szczególności kryptograficznych;
2. Odpowiedzialność karna i dyscyplinarna;
3. Zasada wiedzy niezbędnej;
4. Rodzaje materiałów kryptograficznych i sposób ich oznaczania;
5. Zasady udostępniania materiałów kryptograficznych;
6. Zasady przechowywania materiałów kryptograficznych;
7. Zasady przekazywania materiałów kryptograficznych;
8. Zasady niszczenia materiałów kryptograficznych;
9. Postępowanie w sytuacjach zagrożenia.

Grupowy CUK

KRYPTO		
GRUPOWY CERTYFIKAT UPOWAŻNIENIA KRYPTOGRAFICZNEGO		
CZĘŚĆ I		
NUMER KOLEJNY:		
KLAUZULA TAJNOSCI MATERIAŁÓW KRYPTOGRAFICZNYCH ORAZ ZAKRES, DO KTÓREGO UPRAWNIENI MAJĄ DOSTĘP:		
OŚWIADCZENIE SKŁADANE W MOMENCIE PRYZNANIA CERTYFIKATU:		
<p>Ja, niżej podpisany 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 krajowego i/lub NATO*. Zostałem przeszkolony w zakresie przepisów bezpieczeństwa dotyczących ujawniania informacji odnoszących się do kryptograficznych systemów krajowych i/lub NATO*. Znam instrukcje kryptograficzne krajowe i/lub NATO*, odnoszące się do ochrony niejawnych informacji kryptograficznych, do których zostałem upoważniony.</p>		
	STOPIEŃ/STANOWISKO, IMIĘ I NAZWISKO:	DATA:
1.	NUMER I DATA WAŻNOŚCI a) POŚWIADCZENIA BEZPIECZEŃSTWA: b) CERTYFIKATU BEZPIECZEŃSTWA:	PODPIS:
	STOPIEŃ/STANOWISKO, IMIĘ I NAZWISKO:	DATA:
2.	NUMER I DATA WAŻNOŚCI a) POŚWIADCZENIA BEZPIECZEŃSTWA: b) CERTYFIKATU BEZPIECZEŃSTWA:	PODPIS:
	STOPIEŃ/STANOWISKO, IMIĘ I NAZWISKO:	DATA:
....	NUMER I DATA WAŻNOŚCI a) POŚWIADCZENIA BEZPIECZEŃSTWA: b) CERTYFIKATU BEZPIECZEŃSTWA:	PODPIS:
PODPIS OSOBY WYDAJĄCEJ CERTYFIKAT:		
DATA:		

CZĘŚĆ II**OŚWIADCZENIE SKŁADANE PRZY ANULOWANIU CERTYFIKATU:**

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

1.	STOPIEŃ/STANOWISKO, IMIĘ I NAZWISKO:	DATA:
		PODPIS:
2.	STOPIEŃ/STANOWISKO, IMIĘ I NAZWISKO:	DATA:
		PODPIS:
...	STOPIEŃ/STANOWISKO, IMIĘ I NAZWISKO:	DATA:
		PODPIS:

PODPIS OSOBY ANULUJĄCEJ UPOWAŻNIENIE:

DATA:

**KSIĄŻKA EWIDENCJI WYDANYCH
CERTYFIKATÓW UPOWAŻNIENIA KRYPTOGRAFICZNEGO I SZKOLEŃ**

Rozpoczęto dnia

Zakończono dnia

SPIS TREŚCI

1. Rozdział I ewidencja wydanych Certyfikatów Upoważnienia Kryptograficznego po 30 str.
2. Rozdział II ewidencja wydanych Grupowych Certyfikatów Upoważnienia Kryptograficznego po 10 str.
3. Rozdział III ewidencja szkoleń prowadzonych dla osób posiadających wystawiony Certyfikat Upoważnienia Kryptograficznego po 20 str.
4. Rozdział IV ewidencja wydawania Certyfikatów Upoważnienia Kryptograficznego na okres wykonywania czynności służbowych poza jednostką organizacyjną po 10 str.

ROZDZIAŁ I EWIDENCJA WYDANYCH CERTYFIKATÓW UPOWAŻNIENIA KRYPTOGRAFICZNEGO

Strona lewa:

Lp.	Stopień, imię i nazwisko osoby otrzymującej CUK	Stanowisko służbowe lub funkcja osoby, której wydawano CUK	Numer CUK	Zakres dostępu do materiałów kryptograficznych (klauzula tajności materiałów kryptograficznych oraz zakres do którego uprawniony ma odstęp)
1.	2.	3.	4.	5.

Strona prawa:

Data wystawienia CUK	Data ważności CUK	Numer poświadczenia bezpieczeństwa/Certyfikatu, klauzula tajności oraz data ważności	Wydający CUK		Adnotacje o anulowaniu CUK (nr rozkazu data)	Adnotacje o zniszczeniu (data i 2 podpisy)	Uwagi
			Stopień, imię i nazwisko	Numer rozkazu na podstawie którego wydano CUK			
6.	7.	8.	9.	10.	11.	12.	13.

ROZDZIAŁ II EWIDENCJA WYDANYCH GRUPOWYCH CERTYFIKATÓW UPOWAŻNIENIA KRYPTOGRAFICZNEGO

Strona lewa:

Lp.	Nazwa grupy, której wydano Grupy CUK/ Powód wydania	Numer CUK	Zakres dostępu do materiałów kryptograficznych <i>(klauzula tajności materiałów kryptograficznych oraz zakres do którego uprawniony ma odstęp)</i>	Data		Wydający CUK		Adnotacje o anulowaniu CUK <i>(nr rozkazu data)</i>	Adnotacje o zniszczeniu <i>(data i 2 podpisy)</i>	Uwagi
				wystawienia CUK	ważności CUK	Stopień, imię i nazwisko	Numer rozkazu na podstawie którego wydano CUK			
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.

Strona prawa:

Lp.	Nazwa grupy, której wydano Grupy CUK/ Powód wydania	Numer CUK	Zakres dostępu do materiałów kryptograficznych <i>(klauzula tajności materiałów kryptograficznych oraz zakres do którego uprawniony ma odstęp)</i>	Data		Wydający CUK		Adnotacje o anulowaniu CUK <i>(nr rozkazu data)</i>	Adnotacje o zniszczeniu <i>(data i 2 podpisy)</i>	Uwagi
				wystawienia CUK	ważności CUK	Stopień, imię i nazwisko	Numer rozkazu na podstawie którego wydano CUK			
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.

**ROZDZIAŁ III EWIDENCJA SZKOLEŃ
PROWADZONYCH DLA OSÓB POSIADAJĄCYCH WYSTAWIONY
CERTYFIKAT UPOWAŻNIENIA KRYPTOGRAFICZNEGO**

Strona lewa:

Lp.	Stopień, imię i nazwisko osoby szkolonej	Stopień, imię i nazwisko osoby szkolącej	Data szkolenia	Podpis	
				osoby szkolonej	osoby szkolącej
1.	2.	3.	4.	5.	6.

Strona prawa:

Lp.	Stopień, imię i nazwisko osoby szkolonej	Stopień, imię i nazwisko osoby szkolącej	Data szkolenia	Podpis	
				osoby szkolonej	osoby szkolącej
1.	2.	3.	4.	5.	6.

**ROZDZIAŁ IV EWIDENCJA
POBRAŃ CERTYFIKATÓW UPOWAŻNIENIA KRYPTOGRAFICZNEGO NA
OKRES WYKONYWANIA CZYNNOŚCI SŁUŻBOWYCH POZA JEDNOSTKĄ
ORGANIZACYJNĄ**

Strona lewa:

Lp.	Numer certyfikatu	Stopień, imię i nazwisko posiadacza CUK	Cel wydania	Numer rozkazu stanowiącego podstawę wydania	Data wydania i podpis pobierającego	Data zwrotu i podpis przyjmującego	Uwagi
1.	2.	3.	4.	5.	6.	7.	8.

Strona prawa:

Lp.	Numer certyfikatu	Stopień, imię i nazwisko posiadacza CUK	Cel wydania	Numer rozkazu stanowiącego podstawę wydania	Data wydania i podpis pobierającego	Data zwrotu i podpis przyjmującego	Uwagi
1.	2.	3.	4.	5.	6.	7.	8.

Rejestr teczek materiałów kryptograficznych, dzienników i ksiąg ewidencyjnych

Strona lewa

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

Strona prawa

Komórka odpowiedzialna za prowadzenie teczek, dziennika, książki itp.	Pokwitowanie odbioru teczek, 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.

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.	

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	4.	Nazwa jednostki organizacyjnej, stopień wojskowy, imię i nazwisko	5.		
1.	2.	3.	4.	5.	6.	7.		

Książka ewidencji pieczęci

W
 (nr lub nazwa jednostki wojskowej)

Lp.	Od kogo otrzymano, numer i data pisma	Odbitka pieczęci	Opis 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.

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 znieszeniu lub przerejestrowaniu
1	2	3	4	5	6	7	8	9

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 TAJNOSCI	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 oznaczony jest klauzulą tajności przez nadawcę;
- 2) numery od 3001 do 3999 stosuje się dla raportów ewidencji materiałów kryptograficznych wychodzących. Formularz oznacza się klauzulą tajności POUFNE w odniesieniu do dokumentów niejawnych;
- 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 tajności POUFNE;
- 4) numery od 6001 do 6999 stosuje się dla raportów przyjęcia na posiadanie lub inwentaryzacji materiału kryptograficznego. Formularz oznacza się klauzulą tajności POUFNE dla raportu inwentaryzacji a dla raportu posiadania o klauzulę tajności niżej niż zawarte w raporcie załączniki;
- 5) numery od 7001 do 7999 stosuje się dla raportów ewidencji wypożyczeń materiału kryptograficznego. Formularz oznacza się klauzulą tajności w zależności od klauzuli tajności przesyłanych dokumentów (stosując zasadę – oznaczać o klauzulę tajności niżej niż zawarte w raporcie załączniki), przy czym przesyłając urządzenia, formularz oznacza się jako JAWNE;
- 6) numery od 8001 do 8999 stosuje się dla raportów pomocniczych. Formularz można oznaczyć klauzulą tajności.


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.

Wzory pieczęci

Lp.	Wzór pieczęci	Opis pieczęci	Uwagi
1.	 <p style="text-align: center;"> MINISTERSTWO OBRONY NARODOWEJ * MINISTRY OF NATIONAL DEFENCE ** File No Warsaw - POLAND </p>	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.	<p style="text-align: center;"> MINISTERSTWO OBRONY NARODOWEJ * MINISTRY OF NATIONAL DEFENCE ** File No Received on Enclosure Sheets </p>	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 wkłesa 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.	<u>UNCLASSIFIED</u> nieklasyfikowane	Pieczęć informacyjna – wypukła do tuszu, o długości 40 mm i szerokości 12 mm.	
7.	<u>RESTRICTED</u> ZASTRZEŻONE	Pieczęć informacyjna – wypukła do tuszu, o długości 42 mm i szerokości 12 mm.	
8.	<u>CONFIDENTIAL</u> POUFNE	Pieczęć informacyjna – wypukła do tuszu, o długości 52 mm i szerokości 12 mm.	
9.	<u>SECRET</u> TAJNE	Pieczęć informacyjna – wypukła do tuszu, o długości 33 mm i szerokości 12 mm.	
10.	<u>TOP SECRET</u> ŚCIŚLE TAJNE	Pieczęć informacyjna – wypukła do tuszu, o długości 53 mm i szerokości 12 mm.	
11.	<u>TO BE DELIVERED PERSONALLY</u> do rąk własnych	Pieczęć informacyjna - wypukła do tuszu, o długości 53 mm i szerokości 12 mm.	
12.	<u>URGENT</u> PILNE	Pieczęć informacyjna – wypukła do tuszu, o długości 35 mm i szerokości 12 mm.	

13.	<u>REGISTERED LETTER</u> polecony	Pieczęć informacyjna – wypukła do tuszu, o długości 37 mm i szerokości 12 mm.	
14.	<u>NATO</u>	Pieczęć informacyjna – prostokątna, o długości 44 mm i szerokości 15 mm, wypukła do tuszu.	
15.	<u>UE</u>	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.	
18.	* Nr (data) (miejsce postoiu)	Pieczęć służbowa – prostokątna, o długości 54 mm i szerokości 33 mm, wypukła, do tuszu.	* Nazwa jednostki (komórki) organizacyjnej

19.	<div style="border: 1px solid black; padding: 10px;"> <p>* Nr Wpłynęło (data) Zał. Stron</p> </div>	Pieczęć służbowa wpływu pism – prostokątna, o długości 54 mm i szerokości 27 mm., wypukła, do tuszu.	* Nazwa jednostki (komórki) organizacyjnej.
20.		Pieczęć służbowa do pakietów – o średnicy 30 mm, wypukła do tuszu oraz wklęsła do laku, z nazwą lub numerem jednostki (komórki) organizacyjnej na otoku.	
21.	<p>* (miejsce postoiu)</p>	Pieczęć służbowa – prostokątna, o długości 54 mm i szerokości 33 mm, wypukła do tuszu	* Nazwa jednostki (komórki) organizacyjnej
22.	<u>ZASTRZEŻONE</u>	Pieczęć pomocnicza	
23.	<u>POUFNE</u>	Pieczęć pomocnicza	
24.	<u>TAJNE</u>	Pieczęć pomocnicza	
25.	<u>ŚCIŚLE TAJNE</u>	Pieczęć pomocnicza	
26.	PILNE	Pieczęć pomocnicza	
27.	BARDZO PILNE	Pieczęć pomocnicza	

28.	Do rąk własnych	Pieczęć pomocnicza					
29.	Zniszczono dn. 1. 2. podpisy	Pieczęć pomocnicza					
30.	<u>ZASTRZEŻONE</u> RWMK Nr	Pieczęć pomocnicza					
31.	<u>POUFNE</u> RWMK Nr	Pieczęć pomocnicza					
32.	<u>TAJNE</u> RWMK Nr	Pieczęć pomocnicza					
33.	<u>ŚCIŚLE TAJNE</u> RWMK Nr	Pieczęć pomocnicza					
34.	Niniejszy (a) zawiera (.....) ponumerowanych kart (stron). Dn. " " 20... r. (kierownik kancelarii)	Pieczęć pomocnicza					
35.	<table border="1" style="width: 100%; text-align: center;"> <tr> <td>Zał. Nr ...</td> <td>Wchodz.</td> </tr> <tr> <td>Stron.....</td> <td>Do pismaNr z dn. Wychodz.</td> </tr> </table>	Zał. Nr ...	Wchodz.	Stron.....	Do pismaNr z dn. Wychodz.	Pieczęć pomocnicza	
Zał. Nr ...	Wchodz.						
Stron.....	Do pismaNr z dn. Wychodz.						

36.	<p style="text-align: center;">OTWIERAĆ TYLKO W KANCELARII KRYPTOGRAFICZNEJ</p>	<p>Pieczęć pomocnicza – wypukła, do tuszu, o długości 55 mm i szerokości 25 mm</p>	
37.	<p style="text-align: center;">TO BE OPENED IN CRYPTO ACCOUNTS ONLY</p>	<p>Pieczęć pomocnicza – wypukła, do tuszu, o długości 55 mm i szerokości 25 mm</p>	

Dziennik ewidencji wykonanych materiałów kryptograficznych

(technika odręczna, maszynopisanie, komputerowa, kreślenie, powielanie 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 egzemplarzy	stron egzemplarza	Pokwitowanie odbioru			Adnotacje		Uwagi
		imię i nazwisko	data	podpis	o wystaniu	o zniszczeniu	
8	9	10	11	12	13	14	15

ZEZWALAM
na zniszczenie materiałów kryptograficznych
wyszczególnionych w protokole

Miejscowość, dnia

.....
(stanowisko, stopień wojskowy, imię, nazwisko)

PROTOKÓŁ ZNISZCZENIA MATERIAŁÓW KRYPTOGRAFICZNYCH

Nr ...

Zgodnie z rozkazem dziennym (decyzją) Nr z dnia, komisja w składzie:

- przewodniczący:
(stopień wojskowy, imię i nazwisko; klauzula tajności, numer i data ważności
poświadczenia bezpieczeństwa)

- członkowie:
(stopień wojskowy, imię i nazwisko; klauzula tajności, numer i data ważności
poświadczenia)

.....
(stopień wojskowy, imię i nazwisko; klauzula tajności, 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) wstępnie* w dniu przez
(określenie sposobu zniszczenia materiału)

Pojemnik ze zniszczonymi wstępnie materiałami opieczętowano pieczęcią okrągłą numerową do teczek pracy Nr

Imię, nazwisko, klauzula tajności, numer i data ważności poświadczenia bezpieczeństwa oraz podpis:

- osób, które wstępnie zniszczyły materiały kryptograficzne:
- osób nadzorujących wstępne zniszczenie:

2) ostatecznie* w dniu przez
(określenie sposobu zniszczenia materiału)

Imiona, nazwiska oraz podpisy:

- przewodniczący:
- członkowie:
.....

* niepotrzebne skreślić

Wzór upoważnienia do przeprowadzenia inspekcji kryptograficznej

.....
(nazwa organu zarządzającego inspekcją kryptograficzną)

Miejscowość, data

UPOWAŻNIENIE Nr/....

Na podstawie Zarządzenia Nr .../MON Ministra Obrony Narodowej z dnia ...
20... r. w sprawie szczególnego sposobu organizacji i funkcjonowania 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 inspekcją kryptograficzną)

Ważność upoważnienia przedłuża się do dnia

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

mp.

(pieczęć okrągła organu zarządzającego inspekcją 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 OBSŁil.

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 teczek z protokołami inspekcji kryptograficznych oraz innych form kontroli.
3. Sprawdzenie posiadania przez personel BSŁil, 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 BSŁil oraz poprawności wystawiania kart wzorów podpisów ww. personelu.
5. Sprawdzenie posiadanych kursów specjalistycznych personelu BSŁil.
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 ksiąg 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 niejawnnej 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 BSłil urzędzeń 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 niejawnnych 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 dniach20... 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)

KRYPTO

Protokół z przeprowadzenia inspekcji kryptograficznej

Miejscowość, data
Egz. nr

PROTOKÓŁ

z inspekcji kryptograficznej

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

zarządzonej przez
(osoba uprawniona do zarządzania 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 BSŁil-,
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 OBSŁil poddanego inspekcji kryptograficznej

VI. Ustalenia inspekcji kryptograficznej

(opis ustaleń inspekcji kryptograficznej zgodny z celami i zakresem ujętymi w planie inspekcji kryptograficznej oraz kartą inspekcji kryptograficznej, rozbieżności wykazane w karcie inspekcji)

.....

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.)

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 inspekcją 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 -

..... -

Karta inspekcji 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)		Uwagi
		Poz.	Neg.	
BEZPIECZEŃSTWO MATERIAŁÓW KRYPTOGRAFICZNYCH				
1.	Sprawdzenie zaświadczenia o funkcjonowaniu kancelarii kryptograficznej lub aktualnego certyfikatu bezpieczeństwa zespołu pomieszczeń kancelarii kryptograficznej.			
2.	Analiza zawartości teczek z protokołami inspekcji kryptograficznych i innych form kontroli.			
3.	Sprawdzenie posiadania przez personel BSŁil, wykonawców i inne osoby funkcyjne mające dostęp do materiałów kryptograficznych poświadczeń bezpieczeństwa narodowych oraz ich odpowiedników NATO, UE oraz sprawdzenie dostępu do informacji niejawnych zgodnie z zasadą „wiedzy niezbędnej” w odniesieniu do klauzuli tajności określonej w zaświadczeniu o funkcjonowaniu kancelarii kryptograficznej lub aktualnego certyfikatu bezpieczeństwa zespołu pomieszczeń kancelarii kryptograficznej.			<i>(Wypisać osoby funkcyjne personelu BSŁil wraz z Oficerem BSŁil oraz wszystkie za okres objęty inspekcją kryptograficzną daty ważności poświadczeń bezpieczeństwa, certyfikatów NATO / UE, ich klauzule tajności, zaświadczenia o przeszkoleniu)</i>

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały)		Uwagi
		Poz.	Neg.	
4.	Sprawdzenie prawidłowości wyznaczenia na stanowiska personelu BSŁil oraz poprawności wystawiania kart wzorów podpisów ww. personelu. <i>(Rozkazy personalne, ciągłość zajmowania stanowiska, jak >60 dni nieobecności kier. KK to przekazanie obowiązków)</i>			
5.	Sprawdzenie posiadanych kursów specjalistycznych personelu BSŁil.			
6.	Sprawdzenie prawidłowości wydania oraz aktualności wydanych certyfikatów upoważnienia kryptograficznego. <i>(Wydanie CUK przez D-cę na wniosek Szefa OBSŁil po wyznaczeniu rozkazem personalnym na stanowisko, instruktaż. Sprawdzenie „Wykazu wydanych CUK” i CUKów pod kątem zakresu obowiązków)</i>			
7.	Sprawdzenie poprawności ewidencji szkoleń w zakresie bezpieczeństwa materiałów kryptograficznych. <i>(plany konspekty, lista obecności)</i>			
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.			

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały)		Uwagi
		Poz.	Neg.	
12.	Sprawdzenie certyfikatów drzwi wejściowych do kancelarii kryptograficznej oraz urzędzeń 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 urzędzeń kryptograficznych, a także sprawdzenie przechowywania zapasowych urzędzeń 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”.			

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały)		Uwagi
		Poz.	Neg.	
22.	Sprawdzenie znajomości i przestrzeganie przez kierownika kancelarii kryptograficznej oraz jego zastępcę umiejętności postępowania z materiałami kryptograficznymi, a także przestrzegania zasad ich ewidencji.			
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 BSŁil sprawdzeń urzędzeń 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 zaopatrującej kancelarii 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)		Uwagi
		Poz.	Neg.	
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.			(wymienić nazwy systemów teleinformatycznych)
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. 33 posiada zatwierdzoną przez SKW lub ABW dokumentację bezpieczeństwa lub/i ważny certyfikat/ świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.			(wymienić daty zatwierdzenia dokumentacji bezpieczeństwa, numery certyfikatów lub świadectw w odniesieniu do systemów teleinformatycznych z pkt. 33)
36.	Sprawdzenie, czy kierownik jednostki organizacyjnej wyznaczył: osobę lub zespół osób zwanych administratorem systemu, odpowiedzialnych za funkcjonowanie systemów teleinformatycznych, o których mowa w pkt. 33, a także pracownika pionu ochrony odpowiedzialnego za bieżące sprawdzanie zgodności funkcjonowania tych systemów ze szczególnymi wymaganiami bezpieczeństwa.			
37.	Sprawdzenie czy dokumentacja bezpieczeństwa jest właściwie aktualizowana (czy istnieją aneksy).			(wymienić aneksy i daty)
38.	Sprawdzenie czy sprzęt i oprogramowanie systemu jest zgodne z wykazem w dokumentacji bezpieczeństwa systemu.			(jeżeli jest rozbieżność wykazać co się nie zgadza)
39.	Sprawdzenie czy wszyscy użytkownicy zostali zapoznani z PBE i poświadczyli to własnoręcznym podpisem.			(jeżeli jest rozbieżność wykazać co się nie zgadza)

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały)		Uwagi
		Poz.	Neg.	
40.	Sprawdzenie czy Administrator systemu teleinformatycznego prowadzi archiwizację dzienników zdarzeń tworzonych przez system (gdzie i jak przechowuje ich kopie).			<i>(wykazać gdzie i jak przechowuje ich kopie)</i>
41.	Sprawdzenie czy nośniki danych systemu teleinformatycznego (m.in. dyski twarde) są właściwie oznaczone i zaewidencjonowane.			<i>(podać numery seryjne dysków twardego systemu oraz ich numery ewidencyjne – klauzule tajności)</i>
42.	Sprawdzenie czy Inspektor bezpieczeństwa teleinformatycznego (BTI) dokonywał analizy dzienników zdarzeń zgodnie z opracowanymi procedurami.			<i>(podać systemy w odniesieniu do pkt. 33 oraz daty analizy dzienników zdarzeń)</i>
43.	Sprawdzenie czy Administrator systemu teleinformatycznego zabezpieczył hasłem wejście do BIOS komputera.			
44.	Sprawdzenie czy procedury deponowania haseł Administratora są właściwie realizowane (BIOS, system, terminy zmiany haseł).			<i>(m.in. podać daty zmiany haseł)</i>
45.	Sprawdzenie czy wszystkie osoby wytwarzające dokumenty (wg. DEWMK) znajdują się na liście użytkowników uprawnionych do pracy w systemie.			
46.	Sprawdzenie czy użytkownicy znają swoje uprawnienia i zadania.			
47.	Sprawdzenie listy kont użytkowników systemu i porównanie jej zgodności z wnioskami założenia konta.			<i>(jeżeli jest rozbieżność wykazać co się nie zgadza)</i>
48.	Sprawdzenie czy nadane prawa użytkownikom systemu są zgodne z dokumentacją bezpieczeństwa systemu.			<i>(jeżeli jest rozbieżność wykazać co się nie zgadza)</i>
49.	Sprawdzenie czy procedury przeciwdziałania infekcjom wirusowym są właściwie realizowane.			<i>(jeżeli jest rozbieżność wykazać co się nie zgadza)</i>
50.	Sprawdzenie aktualizacji oprogramowania antywirusowego. Czy aktualizacja jest przeprowadzana zgodnie z zapisami dokumentacji bezpieczeństwa?			<i>(wykazać co jaki czas aktualizowana jest baza wirusów)</i>

LP	Zagadnienie podlegające sprawdzeniu	Wynik (inicjały)		Uwagi
		Poz.	Neg.	
51.	Sprawdzenie czy Administrator systemu teleinformatycznego prowadzi okresowe szkolenia użytkowników z zakresu użytkowania systemu.			
52.	Sprawdzenie czy Inspektor BTI prowadzi okresowe szkolenia użytkowników z zakresu użytkowania systemu.			
53.	Sprawdzenie czy informatyczne nośniki danych (IND) wykorzystywane w systemie są oznaczone i zarejestrowane zgodnie z procedurami zawartymi w dokumentacji bezpieczeństwa.			
54.	Sprawdzenie czy na nośnikach systemu są przechowywane informacje niejawne o klauzuli tajności wyższej niż klauzula tajności systemu.			<i>(jeżeli jest rozbieżność wykazać co się nie zgadza)</i>
55.	Sprawdzenie czy procedury deponowania dysku twardego systemu są realizowane zgodnie z zapisami dokumentacji bezpieczeństwa.			<i>(jeżeli jest rozbieżność wykazać co się nie zgadza)</i>
56.	Sprawdzenie czy Dziennik Ewidencji Wykonanych Materiałów Kryptograficznych jest prowadzony właściwie.			<i>(jeżeli jest rozbieżność wykazać co się nie zgadza)</i>

Procedury transportowania materiałów kryptograficznych

Procedury powinny zawierać m.in. następujące informacje:

Wprowadzenie (wyszczególnienie aktów prawnych dotyczących konwojowania)

Definicje (definicje określeń zawartych w procedurach)

Organizacja konwoju

Zadania osób funkcyjnych

Standardowe procedury postępowania z materiałami kryptograficznymi

Procedury postępowania z materiałami kryptograficznymi w sytuacjach szczególnych

Załączniki:

Wzór Wytocznych Nr _____/.....

z dnia _____ 20.... r. w sprawie organizacji konwoju do przewozu materiałów kryptograficznych

Plan konwoju.