Warszawa, dnia 29 grudnia 2020 r.

Poz. 210

ZARZĄDZENIE Nr 24/MON
MINISTRA OBRONY NARODOWEJ

z dnia 28 grudnia 2020 r.

zmieniające zarządzenie 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. z 2019 r. poz. 742) zarządza się, co następuje:

§ 1. W zarządzeniu Nr 46/MON Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. Urz. Min. Obr. Nar. poz. 401) wprowadza się następujące zmiany:

1) w § 2:
   a) wprowadzenie do wyliczenia otrzymuje brzmienie:
      „Użyte w zarządzeniu określenia i skróty oznaczają:”,
   b) pkt 1 otrzymuje brzmienie:
      „1) akta sprawy – zbiór dokumentów zawierających informacje potrzebne przy rozpatrywaniu sprawy oraz odzwierciedlających przebieg jej załatwienia i rozstrzygania, zaklasyfikowanych zgodnie z jednolitym rzeczowym wykazem akt, umieszczony w teczkach akt oznaczonych właściwą kategorią archiwalną i symbolem klasyfikacyjnym;”,
   c) uchyla się pkt 3,
   d) pkt 4 i 5 otrzymują brzmienie:

„4) archiwizacja – ogół czynności związanych z klasyfikowaniem, kwalifikowaniem, kompletowaniem i przekazywaniem materiałów archiwalnych do archiwum Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, ich ewidencjonowaniem oraz przechowywaniem w archiwum Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni;

5) archiwum – komórkę organizacyjną Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni powołaną w celu gromadzenia i przechowywania materiałów archiwalnych oraz dokumentacji niearchiwalnej, wytworzonej i zgromadzonej w toku działalności Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni i jednostek organizacyjnych podporządkowanych Dyrektorowi Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz kryptograficznych materiałów archiwalnych i kryptograficznej dokumentacji niearchiwalnej wytworzonej i zgromadzonej w Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;”,

e) pkt 13 otrzymuje brzmienie:

„13) inspekcja kryptograficzna – kontrolę stanu ochrony materiałów kryptograficznych, funkcjonowania kancelarii kryptograficznej oraz OBSŁiI w danej jednostce organizacyjnej, realizowaną przez nadrzędny OBSŁiI;”,

f) po pkt 14 dodaje się pkt 14a w brzmieniu:

„14a) jrwa – jednolity rzeczowy wykaz akt – sposób klasyfikowania i kwalifikowania dokumentacji, który określa klasy, według których grupuje się jednolicie w systemie dziesiętnym dokumentację powstającą i gromadzoną w jednostce organizacyjnej, niezależnie od struktury organizacyjnej i podziału kompetencji wewnątrz jednostki organizacyjnej;”,

g) uchyla się pkt 18,

h) pkt 19 i 20 otrzymują brzmienie:

„19) KOGD – Krajowy Organ Generacji i Dystrybucji – Organ Bezpieczeństwa Systemów Łączności i Informatyki, sprawujący nadzór nad bezpieczeństwem materiałów kryptograficznych w jednostkach organizacyjnych oraz nad wymianą materiałów kryptograficznych z podmiotami realizującymi zadania na rzecz resortu obrony narodowej, do którego zadań należy:

a) współpraca z The Military Committee Distribution and Accounting Agency (DACAN) i The Military Committee European Distribution and Accounting Agency (EUDAC),

b) dystrybucja krajowych i międzynarodowych materiałów kryptograficznych,

c) nadzór nad generowaniem, wytwarzaniem dokumentów kryptograficznych służących do zabezpieczenia krajowych potrzeb w zakresie ochrony systemów teleinformatycznych przetwarzających niejawne informacje krajowe i międzynarodowe,

d) określanie sposobu organizacji i funkcjonowania kancelarii kryptograficznych,

e) udzielanie zgody na powoływanie i odwoływanie kancelarii kryptograficznych,

f) udzielanie zgody na generowanie i wytwarzanie dokumentów kryptograficznych poza KOGD,

g) nadzór nad szkoleniem specjalistycznym personelu BSŁiI;

20) kurier – żołnierza, funkcjonariusza lub pracownika wyznaczonego ze składu OBSŁiI lub wykonawcę;”,

i) w pkt 21:

– lit. b otrzymuje brzmienie:

„b) element systemu kryptograficznego, a w szczególności urządzenie kryptograficzne, moduł, blok, podzespół, pomocnicze urządzenie kryptograficzne,”,

– w lit. g średnik zastępuje się przecinkiem i dodaje się lit. h w brzmieniu:

„h) teczki akt kryptograficznych;”,

j) pkt 23 i 24 otrzymują brzmienie:

„23) NCBC – Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni;

24) Oficer BSŁiI – Oficera Bezpieczeństwa Systemów Łączności i Informatyki, który ukończył kurs specjalistyczny uprawniający do sprawowania nadzoru nad bezpieczeństwem materiałów kryptograficznych, o którym mowa w zaleceniach SKW w sprawie powoływania i odwoływania kancelarii kryptograficznej;”,

k) pkt 28 otrzymuje brzmienie:

„28) pomocnicze urządzenie ewidencyjne – urządzenie ewidencyjne stosowane w kancelarii kryptograficznej, które może zostać poddane brakowaniu po 12 miesiącach od daty zakończenia prowadzenia tego urządzenia ewidencyjnego;”,

l) po pkt 31 dodaje się pkt 31a w brzmieniu:

„31a) pracownik kancelarii kryptograficznej – żołnierza, funkcjonariusza lub pracownika pełniącego służbę albo zatrudnionego w kancelarii kryptograficznej, podlegającego bezpośrednio kierownikowi kancelarii kryptograficznej;”,

m) pkt 35 otrzymuje brzmienie:

„35) raport posiadania – wypełniony formularz SF 153 PL określający stan ewidencyjny posiadanych materiałów kryptograficznych będących na ewidencji w kancelarii kryptograficznej, sporządzany na okoliczność przekazania obowiązków kierownika kancelarii kryptograficznej lub wykazania materiałów kryptograficznych, którymi zaopatrywana kancelaria kryptograficzna nie jest obciążona w kancelarii zaopatrującej;”,

n) uchyla się pkt 36,

o) uchyla się pkt 39,

p) pkt 41 otrzymuje brzmienie:

„41) Szef KOGD (w relacjach międzynarodowych – National Distribution Authority) – upoważniony przez Szefa SKW do kierowania KOGD dyrektor lub zastępca dyrektora Zarządu VI SKW;”,

q) pkt 45 i 46 otrzymują brzmienie:

„45) urządzenie kryptograficzne – urządzenie posiadające zaimplementowany co najmniej jeden mechanizm kryptograficzny, przeznaczony do zapewnienia bezpieczeństwa informacjom niejawnym, w tym w szczególności urządzenie, dla którego wydany został certyfikat ochrony kryptograficznej lub które zostało dopuszczone do eksploatacji w trybie art. 50 ust. 7 ustawy;

46) WSK RP – Wojskową Służbę Kurierską Rzeczypospolitej Polskiej, której zadania określają odrębne przepisy wydane przez Ministra Obrony Narodowej;”,

r) pkt 48 otrzymuje brzmienie:

„48) zalecenia SKW – zalecenia SKW w sprawie powoływania i odwoływania kancelarii kryptograficznej;”;

2) w § 3:

a) ust. 1 i 2 otrzymują brzmienie:

„1. W jednostkach organizacyjnych, które planują wykorzystywać materiały kryptograficzne kierownik jednostki organizacyjnej powołuje kancelarię kryptograficzną. W przypadku, gdy powołanie kancelarii kryptograficznej jest niezasadne ze względu na zbyt małą ilość wykorzystywanych materiałów kryptograficznych lub ze względów organizacyjnych, kierownik jednostki organizacyjnej podpisuje z kierownikiem jednostki organizacyjnej posiadającej kancelarię kryptograficzną porozumienie w sprawie zaopatrywania w materiały kryptograficzne.

2. Sposób oraz tryb powoływania i odwoływania kancelarii kryptograficznej określają zalecenia SKW.”,

b) po ust. 5 dodaje się ust. 5a w brzmieniu:

„5a. Warunek, o którym mowa w ust. 5, nie ma zastosowania do urządzeń ewidencyjnych, o których mowa w § 14 ust. 1 pkt 1 lit. a oraz pkt 2 lit. b, które mogą być prowadzone wspólnie dla krajowych i międzynarodowych materiałów kryptograficznych.”,

c) ust. 6 i 7 otrzymują brzmienie:

„6. Za zgodą Szefa KOGD i na podstawie porozumienia, o którym mowa w ust. 1, jednostka organizacyjna posiadająca kancelarię kryptograficzną może zaopatrywać w materiały kryptograficzne inne jednostki organizacyjne nieposiadające kancelarii kryptograficznej. W jednostce organizacyjnej nieposiadającej kancelarii kryptograficznej dopuszcza się przechowywanie materiałów kryptograficznych w kancelarii tajnej w formie depozytu, gdzie sposób przechowywania powinien być opisany szczegółowo w „Procedurach zaopatrywania w materiały kryptograficzne… (podać nazwę jednostki organizacyjnej) przez kancelarię kryptograficzną nr… (podać nazwę jednostki organizacyjnej)”, zwanych dalej „Procedurami”.

7. W przypadku, o którym mowa w ust. 6, kierownik jednostki organizacyjnej nieposiadającej kancelarii kryptograficznej:

1) wyznacza personel BSŁiI, w tym Oficera BSŁiI i jego zastępcę. Funkcję Oficera BSŁiI i zastępcy Oficera BSŁiI pełni osoba, która ukończyła kurs specjalistyczny uprawniający do sprawowania nadzoru nad bezpieczeństwem materiałów kryptograficznych, o którym mowa w zaleceniach SKW;
2) opracowuje Procedury w czterech egzemplarzach zgodnie z wytycznymi określonymi w załączniku nr 2, we współdziałaniu z kierownikiem jednostki organizacyjnej, który ma obsługiwać tę jednostkę;
3) zatwierdza Procedury oraz przesyła je do kierownika jednostki organizacyjnej posiadającej kancelarię kryptograficzną, celem ich zatwierdzenia;
4) zatwierdzone przez kierownika jednostki organizacyjnej posiadającej kancelarię kryptograficzną Procedury przesyła za pośrednictwem Dyrektora NCBC do Szefa KOGD.”,

d) po ust. 7 dodaje się ust. 7a i 7b w brzmieniu:

„7a. Otrzymane Procedury Dyrektor NCBC uzgadnia i przesyła do akceptacji przez Szefa KOGD.

7b. Po otrzymaniu uzgodnionych i zaakceptowanych Procedur jednostka organizacyjna zaopatrująca, przekazuje egzemplarz nr 3, jednostce organizacyjnej zaopatrywanej oraz rozpoczyna proces zaopatrywania w materiały kryptograficzne.”,

e) po ust. 8 dodaje się ust. 8a w brzmieniu:

„8a. Jeżeli KOGD polecił powołanie kancelarii kryptograficznej, warunkiem wydania kolejnej zgody przez KOGD, o której mowa w ust. 6, jest wskazanie przyczyn niepowołania kancelarii kryptograficznej oraz przedłożenie harmonogramu jej powołania.”;

3) w § 4 w ust. 1 pkt 3 otrzymuje brzmienie:

„3) w zależności od potrzeb szyfrant (szyfranci), pracownik (pracownicy) kancelarii kryptograficznej, kurier (kurierzy).”;

4) w § 5:

a) w ust. 1 pkt 11 otrzymuje brzmienie:

„11) kompletowanie materiałów kryptograficznych oraz przygotowywanie akt spraw do archiwizacji;”,

b) ust. 3 otrzymuje brzmienie:

„3. Do obowiązków pracownika kancelarii kryptograficznej należy wykonywanie zadań, o których mowa w ust. 1 pkt 2-17.”,

c) w ust. 4 pkt 3 otrzymuje brzmienie:

„3) udział w czynnościach związanych z organizacją i przygotowaniem konwoju.”;

5) w § 6:

a) ust. 10 otrzymuje brzmienie:

„10. Dopuszcza się przesyłanie kopii rejestru wzorów podpisów drogą elektroniczną z wykorzystaniem systemu teleinformatycznego posiadającego akredytację bezpieczeństwa teleinformatycznego.”,

b) po ust. 13 dodaje się ust. 13a w brzmieniu:

„13a. Dla OBSŁiI nadzorowanych przez NCBC, zgodę, o której mowa w ust. 13, wydaje Dyrektor NCBC, o czym informuje pisemnie Szefa KOGD.”;

6) w § 7:

a) ust. 1 otrzymuje brzmienie:

„1. W jednostkach organizacyjnych, w których wykorzystuje się lub planuje się wykorzystywać materiały kryptograficzne tworzy się OBSŁiI, którego zadaniem jest nadzorowanie pracy kancelarii kryptograficznej.”,

b) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. W przypadku, gdy w nadrzędnej jednostce organizacyjnej nie funkcjonuje OBSŁiI dopuszcza się sprawowanie nadzoru nad OBSŁiI z podległych jednostek organizacyjnych przez OBSŁiI wskazany przez kierownika nadrzędnej jednostki organizacyjnej.”,

c) ust. 4-6 otrzymują brzmienie:

„4. Terytorialny system zaopatrywania, o którym mowa w ust. 3, określa Dyrektor NCBC w uzgodnieniu z Szefem KOGD.

5. KOGD w ramach wykonywanych czynności nadzoruje NCBC oraz OBSŁiI.

6. Do zadań NCBC należy:

1) nadzorowanie i koordynowanie działalności OBSŁiI w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej;
2) planowanie, organizowanie, prognozowanie rozwoju i eksploatacji oraz nadzór nad funkcjonowaniem systemów ochrony kryptograficznej stosowanych w systemach teleinformatycznych resortu obrony narodowej oraz podczas misji pokojowych i ćwiczeń, a także Wojennego Systemu Dowodzenia;
3) ocena zasadności powołania kancelarii kryptograficznej w jednostce organizacyjnej podległej Ministrowi Obrony Narodowej, opracowywana na wniosek kierownika jednostki organizacyjnej na etapie planowania powołania kancelarii kryptograficznej;
4) planowanie, organizowanie oraz sprawowanie nadzoru nad szkoleniami specjalistycznymi personelu BSŁiI;
5) prowadzenie ewidencji dokonywanych kontroli lub inspekcji kryptograficznych nadzorowanych OBSŁiI;
6) opracowywanie i przesyłanie do KOGD do dnia 30 kwietnia każdego roku sprawozdań za rok ubiegły o stanie ochrony informacji niejawnych w kancelariach kryptograficznych jednostek organizacyjnych, z wyszczególnieniem:
   a) kancelarii kryptograficznych objętych nadzorem,
   b) formy nadzoru (inspekcja, kontrola),
   c) organów bezpieczeństwa systemów łączności i informatyki przeprowadzających inspekcje lub kontrole,
   d) stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych;
7) generowanie i wytwarzanie dokumentów kryptograficznych, służących do zabezpieczenia krajowych potrzeb w zakresie ochrony systemów teleinformatycznych przetwarzających niejawne informacje krajowe i międzynarodowe;
8) prowadzenie inspekcji kryptograficznych w nadzorowanych OBSŁiI;
9) składanie do KOGD zbiorczych zapotrzebowań na materiały kryptograficzne (w szczególności dokumenty kryptograficzne) pochodzące z wymiany

międzynarodowej, służące do zabezpieczenia funkcjonowania systemów kryptograficznych wykorzystywanych w nadzorowanych OBSŁiI;

10) nadzorowanie wykorzystywania materiałów kryptograficznych przez OBSŁiI;

11) przeprowadzanie raz w roku odprawy rozliczeniowo-szkoleniowej dla:

a) Oficerów BSŁiI z bezpośrednio nadzorowanych OBSŁiI,

b) kierowników podległych kancelarii kryptograficznych oraz bezpośrednio zaopatrywanych;

12) opracowywanie procedur obsługi urządzeń kryptograficznych, pomocniczego sprzętu kryptograficznego oraz postępowania z dokumentami kryptograficznymi;

13) przesyłanie do KOGD raz na kwartał raportów zniszczeń, które są opracowywane przez podległe OBSŁiI.”,

d) w ust. 7:

– pkt 3 otrzymuje brzmienie:

„3) opracowywanie i przesyłanie do OBSŁiI nadrzędnej jednostki organizacyjnej sprawozdań o stanie ochrony informacji niejawnych w podległych OBSŁiI za ubiegły rok, z wyszczególnieniem:

a) kancelarii kryptograficznych objętych nadzorem,

b) formy nadzoru (inspekcja, kontrola),

c) organów BSŁiI przeprowadzających inspekcje i kontrole,

d) stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony materiałów kryptograficznych oraz zastosowanych środków zaradczych;”,

– pkt 7 otrzymuje brzmienie:

„7) analizę otrzymywanych z podległych OBSŁiI zapotrzebowań na materiały kryptograficzne oraz opracowywanie zapotrzebowań zbiorczych na materiały kryptograficzne, służące do zabezpieczenia potrzeb własnych oraz podległych OBSŁiI;”,

e) ust. 8-10 otrzymują brzmienie:

„8. Sprawozdanie, o którym mowa w ust. 7 pkt 3, OBSŁiI bezpośrednio podległe oraz bezpośrednio nadzorowane przez NCBC przesyłają do NCBC do dnia 15 marca każdego roku.

9. OBSŁiI składają zapotrzebowania na materiały kryptograficzne drogą służbową do nadrzędnego OBSŁiI, za pośrednictwem kancelarii kryptograficznych. W przypadku rozległych systemów teleinformatycznych (funkcjonujących w więcej niż jednej jednostce organizacyjnej) zapotrzebowanie zbiorcze na materiały kryptograficzne dla

systemu teleinformatycznego opracowuje OBSŁiI organizatora systemu teleinformatycznego i przedstawia je drogą służbową do NCBC. Wzory zapotrzebowań zostały określone w zaleceniach SKW w zakresie zarządzania materiałami kryptograficznymi ZBT 601.

10. Nadzór nad bezpieczeństwem materiałów kryptograficznych w jednostce organizacyjnej sprawuje powołany przez kierownika jednostki organizacyjnej Oficer BSŁiI.”,

f) po ust. 10 dodaje się ust. 10a w brzmieniu:

„10a. W czasie nieobecności Oficera BSŁiI, jego obowiązki pełni powołany przez kierownika jednostki organizacyjnej zastępca Oficera BSŁiI. W przypadku nieobecności Oficera BSŁiI i jego zastępcy, obowiązki Oficera BSŁiI pełni kierownik kancelarii kryptograficznej.”,

g) w ust. 11 pkt 1 otrzymuje brzmienie:

„1) osobę wyznaczoną w NCBC przez dyrektora NCBC;”,

h) w ust. 13:

– pkt 2 otrzymuje brzmienie:

„2) przekazywanie kierownikowi jednostki organizacyjnej propozycji rozwiązań w sprawach związanych z bezpieczeństwem materiałów kryptograficznych oraz zabezpieczeniem kryptograficznym systemów teleinformatycznych jednostki organizacyjnej oraz jednostek jej podległych;”,

– pkt 9 otrzymuje brzmienie:

„9) opracowanie instrukcji pracy kancelarii kryptograficznej;”,

– pkt 17 otrzymuje brzmienie:

„17) ścisła współpraca z pełnomocnikiem ochrony kierownika jednostki organizacyjnej w zakresie utrzymywania i podnoszenia poziomu bezpieczeństwa fizycznego pomieszczeń kancelarii kryptograficznych, w tym prowadzenie sprawdzeń poziomu bezpieczeństwa;”,

– pkt 19 i 20 otrzymują brzmienie:

„19) nadzorowanie prowadzenia wymaganej dokumentacji w kancelarii kryptograficznej;

20) nadzorowanie wykorzystywania, obsługiwania oraz ochrony urządzeń i innych elementów systemów kryptograficznych;”,

– w pkt 24 kropkę zastępuje się średnikiem i dodaje się pkt 25 w brzmieniu:

„25) opracowywanie w porozumieniu z administratorem systemu, w którym wykorzystywany jest system kryptograficzny, zapotrzebowania na materiały kryptograficzne.”;

7) w § 8:

a) w ust. 1:

– w pkt 7 lit. a otrzymuje brzmienie:

„a) instalowane systemy kontroli dostępu powinny spełniać wymagania eksploatacyjno-techniczne dla XIX grupy SpW - systemy i urządzenia specjalistyczne do ochrony obiektów, określone przez gestora,”,

– w pkt 8 lit. b otrzymuje brzmienie:

„b) powinien spełniać wymagania eksploatacyjno-techniczne dla XIX grupy SpW - systemy i urządzenia specjalistyczne do ochrony obiektów, określone przez gestora. Dopuszcza się dalsze stosowanie zainstalowanych systemów alarmowych zgodnie z normą PN-EN 50131-1 systemy alarmowe;”,

b) w ust. 4 pkt 1 i 2 otrzymują brzmienie:

„1) pracy personelu kancelarii kryptograficznej;

2) przyjmowania interesantów oraz zapoznawania się z materiałami kryptograficznymi co odnotowuje się w rejestrze interesantów, którego wzór określa załącznik nr 35;”,

c) ust. 8 otrzymuje brzmienie:

„8. W kancelariach kryptograficznych, w których są przechowywane materiały niejawne oznaczone klauzulę tajności „ŚCIŚLE TAJNE”, należy zainstalować telewizyjny system nadzoru drzwi wejściowych z zewnątrz, z rejestracją zdarzeń oraz elektroniczne systemy kontroli dostępu. Wymagania ogólne dotyczące funkcjonowania elektronicznego systemu kontroli dostępu zawarte są w wymaganiach eksploatacyjno-technicznych dla XIX grupy SpW - systemy i urządzenia specjalistyczne do ochrony obiektów, określone przez gestora.”,

d) w ust. 9 pkt 5 otrzymuje brzmienie:

„5) urządzenia klasy P7 według normy DIN 66399 do niszczenia materiałów kryptograficznych w formie papierowej.”,

e) ust. 12 i 13 otrzymują brzmienie:

„12. W kancelariach kryptograficznych, mogą być eksploatowane systemy teleinformatyczne przetwarzające informacje niejawne.

13. Eksploatacja jawnych urządzeń faksowych i systemów podłączonych do sieci INTERNET wymaga zgody Szefa KOGD.”,

f) uchyla się ust. 15;

8) w § 9 ust. 3 otrzymuje brzmienie:

„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 zaleceniach SKW w zakresie zarządzania materiałami kryptograficznymi ZBT 601, należy przechowywać w urządzeniach, o których mowa w § 8 ust. 9 pkt 1.”;

9) w § 10:

a) ust. 6-8 otrzymują brzmienie:

„6. Kody, o których mowa w ust. 5, podlegają ochronie przewidzianej dla materiałów niejawnych klauzuli tajności odpowiadającej najwyżej sklasyfikowanej informacji przechowywanej w pomieszczeniu lub urządzeniu. Kody ewidencjonuje się i umieszcza w zabezpieczonych i oznaczonych kopertach. Sposób oznaczania kodów określa załącznik nr 7.

7. Kody administratora systemu alarmowego wspomagającego ochronę fizyczną pomieszczeń kancelarii kryptograficznej należy przechowywać w pomieszczeniu kancelarii tajnej lub innej kancelarii 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 najwyżej sklasyfikowanej informacji, przechowywanej w pomieszczeniu lub urządzeniu. Kody ewidencjonuje się i umieszcza w zabezpieczonych i oznaczonych kopertach.”,

b) ust. 11 otrzymuje brzmienie:

„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 administratora systemu alarmowego. Kody użytkowników systemu alarmowego wykorzystywane w ramach funkcjonowania kancelarii kryptograficznej zmienia się w przypadku ujawnienia lub podejrzenia ujawnienia kodu osobie nieupoważnionej.”;

10) w § 12:

a) ust. 3 i 4 otrzymują brzmienie:

„3. CUK wystawiany jest przez Oficera BSŁiI w egzemplarzu pojedynczym. Kierownik jednostki organizacyjnej lub upoważniona przez niego osoba zatwierdza fakt wydania CUK w rubryce „PODPIS OSOBY WYDAJĄCEJ UPOWAŻNIENIE” formularza 104 PL, stanowiącego załącznik nr 8.

4. W Ministerstwie Obrony Narodowej, w skład którego wchodzi Sztab Generalny WP, CUK jest zatwierdzany przez Dyrektora NCBC lub osobę przez niego upoważnioną.”,

b) ust. 16 otrzymuje brzmienie:

„16. W przypadkach, o których mowa w ust. 15, pobranie CUK dokumentuje się w rozdziale IV książki ewidencji, o której mowa w ust. 19.”,

c) po ust. 18 dodaje się ust. 18a w brzmieniu:

„18a. Dopuszcza się wydawanie grupowego CUK dla wykonawców z różnych jednostek organizacyjnych, delegowanych do wspólnego wykonania określonych zadań.”,

d) ust. 28 otrzymuje brzmienie:

„28. W przypadku zagubienia CUK, dokument anuluje się rozkazem lub decyzją kierownika jednostki organizacyjnej, który nadał uprawnienie. Oficer OBSŁiI odnotowuje ten fakt w książce ewidencji, o której mowa w ust. 19.”;

11) w § 13:

a) ust. 4 otrzymuje brzmienie:

„4. Instalowane systemy i urządzenia alarmowe powinny spełniać warunki, o których mowa w § 8 ust. 1 pkt 8 lit. b.”,

b) ust. 9 otrzymuje brzmienie:

„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 okrętów i pomocniczych jednostek pływających, materiały kryptograficzne należy przekazać do kancelarii kryptograficznej zaopatrującej w te materiały, w terminie 72 godzin od wejścia do portu.”;

12) w § 14 w ust. 1:

a) w pkt 1 lit. b otrzymuje brzmienie:

„b) dziennik ewidencji, którego wzór określa załącznik nr 36,”,

b) w pkt 2:

– lit. a otrzymuje brzmienie:

„a) pomocnicza książka ewidencji pieczęci, której wzór określa załącznik nr 15,”,

– lit. h i lit. i otrzymują brzmienie:

„h) formularz AF 147 PL przeznaczony do ewidencji kart formularzy SF 153 PL, którego wzór określa załącznik nr 23,

i) raport materiału kryptograficznego (formularz SF 153 PL), wykorzystywany do przygotowywania raportów z działalności kancelarii kryptograficznej w zakresie przekazywania, niszczenia, inwentaryzacji, posiadania, przekazania odręcznego i kontroli, którego wzór określa załącznik nr 24,",

– w lit. j kropkę zastępuje się przecinkiem i dodaje się lit. k w brzmieniu:

„k) formularz SF 153 PL numeruje się z zachowaniem kolejności. Numerację prowadzi się od dnia 1 stycznia do dnia 31 grudnia danego roku kalendarzowego. Po numerze wpisuje się dodatkowo rok według wzoru: 00023-19-PL. Formularz oznaczony jest klauzulą tajności zgodnie z zasadami określonymi w załączniku nr 24. Podczas sporządzania raportów niejawnych nie nadaje się numerów z DEWMK.";

13) w § 16:

a) w ust. 3 w pkt 1 lit. b otrzymuje brzmienie:

„b) w celu ewidencji krajowych i sojuszniczych urządzeń ewidencyjnych oraz teczek z materiałami kryptograficznymi, o których mowa w ust. 2;",

b) ust. 5 otrzymuje brzmienie:

„5. W Rejestrze dokumentacji nie rejestruje się urządzeń ewidencyjnych i teczek z materiałami kryptograficznymi zaewidencjonowanych w latach poprzednich, jeżeli te nadal są prowadzone.";

14) w § 17:

a) ust. 1-7 otrzymują brzmienie:

„§ 17. 1. 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 rejestruje się w dzienniku ewidencji, z podziałem na materiały kryptograficzne jawne i niejawne.

2. Dopuszcza się prowadzenie dziennika ewidencji w formie elektronicznej. Przepisy ust. 3-6 i ust. 8 pkt 2, ust. 9-13 i ust. 18-23 w części dotyczącej pieczęci stosuje się odpowiednio.

3. Dopuszcza się rejestrowanie w jednym dzienniku ewidencji materiałów kryptograficznych otrzymywanych i wysyłanych, o których mowa w § 2 pkt 21 lit. f, z zastrzeżeniem ust. 4.

4. Dla materiałów kryptograficznych otrzymywanych i wysyłanych, o których mowa w § 2 pkt 21 lit. f, można prowadzić w formie elektronicznej oddzielnie dzienniki ewidencji.

5. W dziennikach ewidencji numerację materiałów kryptograficznych, o których mowa w § 2 pkt 21 lit. f, rozpoczyna się w każdym roku kalendarzowym od liczby 1. Dziennik ewidencji prowadzi się do całkowitego wykorzystania wszystkich stron.

6. W oddzielnych dziennikach ewidencji 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 ewidencji, zakłada się następny tom i zachowuje ciągłość dotychczasowej numeracji.”,

b) w ust. 8:

– pkt 1 otrzymuje brzmienie:

„1) opatrzeniu pierwszej strony materiału kryptograficznego, o którym mowa w § 2 pkt 21 lit. f, pieczęcią wpływu oraz odciśnięciu pieczęci formularzowej na załącznikach, z zastrzeżeniem, iż pieczęci formularzowej nie używa się do załączników w formie dokumentów personalnych, wydawnictw kryptograficznych, materiałów kryptograficznych, o których mowa w § 2 pkt 21 lit. a-e i lit. g oraz innych materiałów kryptograficznych przesyłanych do akceptacji, uzgodnienia, opiniowania lub podpisu;”,

– w pkt 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„wpisaniu w kolejnej pozycji dziennika ewidencji:”,

– pkt 3 otrzymuje brzmienie:

„3) wpisaniu na dokumencie, w odpowiednich polach odcisku pieczęci, daty zarejestrowania materiału kryptograficznego, zgodnie z zapisem w dzienniku ewidencji oraz danych wymienionych w pkt 2 lit. a i lit. b oraz lit. d i lit. e.”,

c) ust. 9 i 10 otrzymują brzmienie:

„9. Korespondencję opatrzoną adnotacją „do rąk własnych” rejestruje się bez otwierania wewnętrznego opakowania przesyłki, przez:

1) wpisanie w odpowiednich rubrykach dziennika ewidencji zapisów umieszczonych na opakowaniu wewnętrznym przesyłki oraz daty wpływu materiału kryptograficznego;
2) zamieszczenie w rubryce „Uwagi” dziennika ewidencji adnotacji „do rąk własnych”;
3) odciśnięcie na opakowaniu pieczęci wpływu i wpisaniu numeru ewidencyjnego według dziennika ewidencji 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 ewidencji, a na opakowaniu wewnętrznym przesyłki umieszcza się odciski pieczęci wpływu, w ilości odpowiadającej liczbie materiałów

kryptograficznych, z wpisanymi numerami ewidencyjnymi poszczególnych materiałów.”,

d) ust. 13 i 14 otrzymują brzmienie:

„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 się niezapisane rubryki dziennika ewidencji.

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

e) w ust. 15 w pkt 1 lit. d otrzymuje brzmienie:

„d) zgodność numerów na opakowaniu przesyłki z numerami wyszczególnionymi odpowiednio w wykazie przesyłek wydanych lub książce doręczeń;”,

f) ust. 17-24 otrzymują brzmienie:

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

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 ewidencji wpisuje się nazwę adresata, ilość stron materiału kryptograficznego wraz z załącznikami, ilość załączników oraz stron załączników pozostających w aktach sprawy lub nazwę i liczbę informatycznych nośników danych, jeżeli załączniki stanowią informatyczne nośniki danych, numer ewidencyjny według dziennika ewidencji wykonanych materiałów kryptograficznych lub innego urządzenia ewidencyjnego oraz wykonawcę.

19. W rubryce „Uwagi” dziennika ewidencji wpisuje się datę przekazania materiału kryptograficznego, o którym mowa w § 2 pkt 21 lit. f, numer oraz pozycję zapisu w książce doręczeń albo numer i pozycję zapisu w „Wykazie przesyłek nadanych”, za którym materiał kryptograficzny przekazano adresatowi lub przewoźnikowi.

20. Jeżeli w kancelarii kryptograficznej nie pozostawia się żadnego egzemplarza wysyłanego materiału kryptograficznego, o którym mowa w § 2 pkt 21 lit. f, w rubrykach dziennika ewidencji przeznaczonego do zapisywania informacji o ilości stron materiału kryptograficznego, ilości załączników oraz stron załączników, wpisuje się poziome kreski, natomiast w rubryce „Uwagi" zamieszcza się adnotację o treści „tylko adresat".

21. Przed zarejestrowaniem w dzienniku ewidencji przekazanego do wysłania materiału kryptograficznego, o którym mowa w § 2 pkt 21 lit. f, kierownik kancelarii kryptograficznej lub inna osoba z personelu kancelarii sprawdza czy materiał kryptograficzny:

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

22. W razie niespełnienia któregokolwiek z warunków, o których mowa w ust. 21, kierownik kancelarii kryptograficznej zwraca materiał kryptograficzny do wykonawcy w celu 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 ewidencji 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 ewidencji zamieszcza się adnotację zawierającą jedną z informacji określających:

1) nazwę i numer urządzenia ewidencyjnego oraz numery pozycji, pod którymi zarejestrowano odłączone załączniki;
2) numer wychodzący według dziennika ewidencji, 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 osoby z personelu kancelarii) 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 choćby jednego załącznika.”;

15) uchyla się § 18;

16) w § 19:

a) w ust. 3:

– pkt 1 otrzymuje brzmienie:

„1) pod odrębną pozycją tytuł każdego z otrzymanych materiałów kryptograficznych;”,

– pkt 3 otrzymuje brzmienie:

„3) numer i datę faktury, asygnaty lub formularza SF 153 PL, za którymi przysłano materiały kryptograficzne.”,

b) ust. 4 otrzymuje brzmienie:

„4. Na okładce i stronie tytułowej każdego egzemplarza rejestrowanego materiału kryptograficznego, o którym mowa w § 2 pkt 21 lit. d i e, oraz niezszytych z nim załącznikach odciska się pieczęć biblioteczną zawierającą nazwę kancelarii kryptograficznej lub pieczęć „Do pakietów” oraz wpisuje się numer ewidencyjny z karty AF 54 C PL np. S-4/15, gdzie S-4 oznacza nr segregatora, w którym prowadzone są karty AF 54 C PL, a liczba 15 sekcję, w której ujęto w ewidencji materiał kryptograficzny, o którym mowa w § 2 pkt 21 lit. d i lit. e.”;

17) w § 20 ust. 10 otrzymuje brzmienie:

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

18) w § 23 ust. 1 otrzymuje brzmienie:

„1. Kartę zapoznania się z materiałem kryptograficznym, z zastrzeżeniem ust. 2, zakłada się i dołącza do materiału kryptograficznego pochodzenia krajowego, o którym mowa w § 2 pkt 21 lit. d-f oraz lit. h, o klauzuli tajności „TAJNE” lub „ŚCIŚLE TAJNE”, z chwilą zarejestrowania go po raz pierwszy w urządzeniach ewidencyjnych.”;

19) w § 24:

a) po ust. 2 dodaje się ust. 2a i 2b w brzmieniu:

„2a. Dopuszcza się prowadzenie jednego DEWMK dla różnych technik wytwarzania dokumentów, kilku wykonawców lub systemów teleinformatycznych. W przypadku prowadzenia jednego DEWMK dla różnych technik wytwarzania dokumentów lub kilku systemów teleinformatycznych, w kolumnie „Uwagi” dziennika ewidencji umieszcza się dodatkowe adnotacje (np. „wykonano techniką odręczną”).

2b. Jawne pismo przewodnie, za którym przesłane są załączniki niejawne oznacza się bez jego rejestrowania w DEWMK, z zachowaniem zasad określonych w rozporządzeniu wydanym na podstawie art. 6 ust. 9 ustawy. Ewidencja pisma przewodniego następuje z chwilą ujęcia go w urządzeniu ewidencyjnym kancelarii kryptograficznej.”,

b) w ust. 3:

– pkt 6 otrzymuje brzmienie:

„6) numeru brudnopisu i numeru stron, jeżeli takie były wykorzystywane, numeru ewidencyjnego materiału kryptograficznego i liczby stron w przypadku wykonania jego kopii, dodatkowo numerów ewidencyjnych informatycznych nośników danych, które były wykorzystywane w systemie w przypadku wykonywania dokumentu techniką komputerową;”,

– pkt 8 otrzymuje brzmienie:

„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 organizacyjnej stanowią prefiks sygnatury literowo-cyfrowej, o której mowa w rozporządzeniu wydanym na podstawie art. 6 ust. 9 ustawy (przykładowo Z VI SKW-PF-123/11). Do prefiksu dołącza się numer ewidencyjny dziennika DEWMK, w którym materiał kryptograficzny został zaewidencjonowany (przykładowo DEWMK RTMK 18/10). Sygnatura literowo-cyfrowa umieszczona na wykonanym dokumencie przykładowo ma postać: Z VI SKW-Pf-123/11-DEWMK RTMK 18/10.”,

c) ust. 7 otrzymuje brzmienie:

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

20) uchyla się § 25;

21) w § 26:

a) ust. 2 otrzymuje brzmienie:

„2. Materiały kryptograficzne, o których mowa w ust. 1, wydawane są za pokwitowaniem w dzienniku ewidencji lub za pokwitowaniem odręcznym, wykonanym na formularzu SF 153 PL lub za pokwitowaniem odręcznym na RWMK.”,

b) ust. 11 otrzymuje brzmienie:

„11. Szyfrogramy wychodzące, przekazywane są bezpośrednio przez nadawcę do obsługi produktu kryptograficznego, a szyfrogramy wchodzące, przekazywane są przez obsługę produktu kryptograficznego bezpośrednio adresatowi. Szyfrogramy, po nadaniu lub wykorzystaniu, przekazywane są do kancelarii tajnej, zaś szyfrogramy stanowiące materiał kryptograficzny, na podstawie decyzji kierownika jednostki organizacyjnej przekazywane są do kancelarii kryptograficznej, która ewidencjonuje je w dzienniku korespondencji.”,

c) dodaje się ust. 12 w brzmieniu:

„12. Przyjęcie szyfrogramu w kancelarii kryptograficznej potwierdza się w kolumnie 14 dziennika ewidencji szyfrogramów, poprzez wpisanie numeru ewidencyjnego, pod którym zarejestrowano szyfrogram, przystawienie pieczęci „Do pakietów” oraz złożenie podpisu kierownika kancelarii kryptograficznej bądź zastępcy kierownika lub osoby z personelu kancelarii. W kolumnie 15 zamieszcza się napis „Szyfrogram”.”;

22) w § 27:

a) w ust. 1 pkt 1 otrzymuje brzmienie:

„1) skompletowaniu w teczki akt, jeżeli stanowią materiały archiwalne lub posiadają wartość praktyczną dla jednostki organizacyjnej – teczki skompletowanych akt spina się przy pomocy klipsów 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 materiały kryptograficzne, o których mowa w § 2 pkt 21 lit. d-f, można wydać z kancelarii kryptograficznej na RWMK użytkownika. Materiały kryptograficzne podlegają zwrotowi do kancelarii kryptograficznej bezpośrednio po ich realizacji;”,

b) ust. 2 otrzymuje brzmienie:

„2. Materiały kryptograficzne, o których mowa w § 2 pkt 21 lit. d-f i lit. h oraz w § 14 ust. 1 pkt 1, przechowuje się w kancelarii kryptograficznej z zachowaniem terminów przechowywania określonych w jrwa jednostki organizacyjnej, a po upływie tych terminów występuje się o zgodę na ich brakowanie zgodnie z przepisami wydanymi na podstawie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164) lub przekazuje się je do archiwum.”,

c) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Do materiałów kryptograficznych GKK, które są archiwizowane w SKW, ust. 2 nie stosuje się.”,

d) ust. 3 otrzymuje brzmienie:

„3. Formularze ewidencyjne SF 153 PL przechowuje się przez okres 5 lat, nie wliczając roku bieżącego.”,

e) ust. 5 i 6 otrzymują brzmienie:

„5. Formularze ewidencyjne AF 54 A PL, AF 54 B PL, AF 54 C PL, AF 69 PL, AF 147 PL oraz SF 153 PL nie podlegają archiwizacji.

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

23) § 28 otrzymuje brzmienie:

„§ 28. 1. Materiały kryptograficzne nie będące materiałami archiwalnymi, nie posiadające wartości praktycznej dla jednostki organizacyjnej podlegają zniszczeniu.

2. W przypadku prowadzenia w jednostce organizacyjnej ewidencji materiałów kryptograficznych w wersji elektronicznej, przechowywanej w komputerowych bazach danych, ewidencja nie podlega 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 i lit. g, o klauzuli tajności „TAJNE” i „ŚCIŚLE TAJNE”, które nie zostały włączone do teczek akt kryptograficznych – co najmniej trzyosobowa komisja, powoływana okresowo przez kierownika jednostki organizacyjnej;

2) w odniesieniu do jawnych materiałów kryptograficznych, o których mowa w § 2 pkt 21 lit. f i lit. g, oraz materiałów kryptograficznych zawierających informacje niejawne o klauzuli tajności „ZASTRZEŻONE” oraz „POUFNE” – osoba z personelu kancelarii kryptograficznej wraz z wykonawcą. Zniszczenie materiałów dokumentuje się w rubryce „Uwagi” urządzenia ewidencyjnego adnotacją o treści: „Zniszczono dnia…”, potwierdzoną wpisaniem daty i podpisami zawierającymi imię i nazwisko osób niszczących materiały kryptograficzne;

3) w odniesieniu do materiałów kryptograficznych, o których mowa w § 2 pkt 21 lit. a – kierownik kancelarii kryptograficznej wraz z inną osobą, posiadającą stosowne poświadczenia bezpieczeństwa oraz CUK, występującą w roli świadka, którzy potwierdzają zniszczenie na formularzu SF 153 PL;

4) w odniesieniu do materiałów kryptograficznych, o których mowa w § 2 pkt 21 lit. b i lit. c – powołana na podstawie odrębnych przepisów komisja złożona z przedstawicieli Sił Zbrojnych RP, której przewodniczy przedstawiciel NCBC.

4. Z komisyjnego zniszczenia materiałów kryptograficznych, sporządza się protokół zniszczenia, którego wzór określa załącznik nr 29. Protokół ten podlega archiwizacji.

5. Protokół zniszczenia lub formularz SF 153 PL (AF 21 PL) stanowi dla kierownika kancelarii kryptograficznej podstawę do zdjęcia z ewidencji wyszczególnionych w nich materiałów kryptograficznych, poprzez naniesienie we właściwej rubryce lub rubryce „Uwagi" urządzenia ewidencyjnego adnotacji o dokonanym zniszczeniu.";

24) w § 30 ust. 1 otrzymuje brzmienie:

„1. W przypadku likwidacji (rozformowania) jednostki organizacyjnej postępuje się zgodnie z przepisami wydanymi na podstawie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.";

25) § 36 otrzymuje brzmienie:

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

2. Dystrybucja materiałów kryptograficznych dla pododdziałów sojuszniczych (koalicyjnych) realizujących zadania na terenie Rzeczypospolitej Polskiej odbywa się na podstawie przepisów zawartych w dokumencie „Instructions for the Control safeguarding of NATO Cryptomaterial SDIP 293", zwanym dalej „SDIP–293", obowiązującej edycji oraz zaleceń SKW w sprawie zarządzania materiałami kryptograficznymi ZBT 601.

3. Zgodę na realizację dystrybucji, o której mowa w ust. 2, wydaje Szef KOGD.

4. Zasady postępowania z materiałami kryptograficznymi pochodzącymi z wymiany międzynarodowej określają zalecenia SKW w sprawie zarządzania materiałami kryptograficznymi ZBT 601.";

26) w § 37:

a) ust. 1 otrzymuje brzmienie:

„1. Nadzór nad ochroną materiałów kryptograficznych w organach BSŁiI i kancelariach kryptograficznych realizowany jest przez nadrzędne jednostki organizacyjne w formie inspekcji kryptograficznych.",

b) ust. 3-5 otrzymują brzmienie:

„3. Nadzór, o którym mowa w ust. 1 i 2:

1) nad komórkami organizacyjnymi Ministerstwa Obrony Narodowej oraz jednostkami organizacyjnymi podległymi Ministrowi Obrony Narodowej sprawuje NCBC;

2) nad NCBC oraz nad jednostkami organizacyjnymi nadzorowanymi przez Ministra Obrony Narodowej sprawuje KOGD.

4. Inspekcje kryptograficzne w danej jednostce organizacyjnej przeprowadza się cyklicznie, nie rzadziej niż co 3 lata. W ramach inspekcji kryptograficznej sprawdza się również stan ochrony materiałów kryptograficznych w jednostce organizacyjnej zaopatrywanej na podstawie porozumienia, o którym mowa w § 3 ust. 1.

5. Inspekcja kryptograficzna ma na celu sprawdzenie:

1) bezpieczeństwa kryptograficznego;
2) prowadzenia ewidencji materiałów kryptograficznych;
3) bezpieczeństwa systemów teleinformatycznych przetwarzających dane związane z materiałami kryptograficznymi.”;

27) w § 38:

a) ust. 1 otrzymuje brzmienie:

„1. Inspekcję kryptograficzną zarządza kierownik jednostki organizacyjnej, właściwy dla OBSŁiI przeprowadzającego inspekcję, a realizuje co najmniej dwuosobowa komisja złożona z personelu OBSŁiI.”,

b) ust. 5 otrzymuje brzmienie:

„5. Poszczególne egzemplarze protokołu inspekcji kryptograficznej wraz z kartą inspekcji kryptograficznej przekazywane są do:

1) kancelarii kryptograficznej, w której inspekcja została przeprowadzona;
2) nadrzędnej jednostki organizacyjnej – nie dotyczy OBSŁiI bezpośrednio nadzorowanych przez NCBC lub podległych pod NCBC;
3) NCBC;
4) KOGD.”,

c) po ust. 5 dodaje się ust. 5a w brzmieniu:

„5a. Informację o sposobie usunięcia stwierdzonych nieprawidłowości lub realizacji zaleceń z przeprowadzonej inspekcji kryptograficznej, kierownik kontrolowanej jednostki organizacyjnej przesyła jednostkom organizacyjnym, którym został wysłany protokół z inspekcji.”;

28) w § 40 ust. 2-4 otrzymują brzmienie:

„2. Transport, o którym mowa w ust. 1, odbywa się na podstawie zatwierdzonej przez kierownika jednostki organizacyjnej Instrukcji Konwojowania Materiałów Kryptograficznych, opracowanej na podstawie załącznika nr 34.

3. Na organizację konwoju materiałów kryptograficznych składają się następujące przedsięwzięcia:

1) określenie przedmiotu konwojowania;
2) ustalenie, czy posiadane środki transportu do przewozu mienia wojskowego są

sprawne oraz mają stosowne wyposażenie;

3) określenie czasu wyjazdu i terminu powrotu konwoju;
4) ustalenie składu osobowego konwoju, rodzaju uzbrojenia i wyposażenia konwoju oraz podanie punktu do rozkazu lub decyzji kierownika jednostki organizacyjnej o wyznaczeniu konwoju;
5) przygotowanie planu konwoju i nakazu konwojowania;
6) udzielenie instruktażu członkom konwoju, podczas którego powinno się:
   a) określić zadania konwoju, podając:
      – charakter konwojowanego mienia wojskowego,
      – zadania dowódcy konwoju, konwojentów i innych osób wchodzących w skład konwoju,
      – środki transportu i czas trwania konwoju,
      – trasę konwoju i miejsca zagrożenia,
      – sposób utrzymywania łączności i informowania o nadzwyczajnych wydarzeniach,
   b) szczególnie zwrócić uwagę na:
      – sposób postępowania dowódcy konwoju, konwojentów i innych osób wchodzących w skład konwoju (w szczególności podczas: napadu, katastrofy, uszkodzenia środka transportowego),
      – zasady zachowania tajemnicy odnośnie rodzaju konwoju, jego zabezpieczenia, trasy przejazdu, czasu trwania, organizacji łączności,
      – zasady użycia broni palnej i środków przymusu bezpośredniego,
   c) sprawdzić poziom znajomości zasad wykonywania czynności konwojowych;
7) rozliczenie konwoju po jego zakończeniu.

4. Oficer BSŁiI lub osoba przez niego upoważniona udziela instruktażu oraz dokonuje rozliczenia konwoju. ”;

29) uchyla się § 43;
30) załączniki nr 2 i 3 do zarządzenia otrzymują brzmienie określone odpowiednio w załącznikach nr 1 i 2 do niniejszego zarządzenia;
31) załącznik nr 7 do zarządzenia otrzymuje brzmienie określone w załączniku nr 3 do niniejszego zarządzenia;
32) załącznik nr 8 do zarządzenia otrzymuje brzmienie określone w załączniku nr 4 do niniejszego zarządzenia;
33) załącznik nr 12 do zarządzenia otrzymuje brzmienie określone w załączniku nr 5 do niniejszego zarządzenia;

34) uchyla się załącznik nr 13;

35) załącznik nr 15 do zarządzenia otrzymuje brzmienie określone w załączniku nr 6 do niniejszego zarządzenia;

36) załączniki nr 21–23 do zarządzenia otrzymują brzmienie określone odpowiednio w załącznikach nr 7-9 do niniejszego zarządzenia;

37) załącznik nr 24 do zarządzenia otrzymuje brzmienie określone w załączniku nr 10 do niniejszego zarządzenia;

38) uchyla się załącznik nr 28;

39) załącznik nr 29 do zarządzenia otrzymuje brzmienie określone w załączniku nr 11 do niniejszego zarządzenia;

40) załącznik nr 31 do zarządzenia otrzymuje brzmienie określone w załączniku nr 12 do niniejszego zarządzenia;

41) załączniki nr 33 i 34 do zarządzenia otrzymują brzmienie określone odpowiednio w załącznikach nr 13 i 14 do niniejszego zarządzenia;

42) dodaje się załączniki nr 35 i 36 w brzmieniu określonym odpowiednio w załącznikach nr 15 i 16 do niniejszego zarządzenia.

§ 2. Urządzenia ewidencyjne wykorzystywane przed dniem wejścia w życie niniejszego zarządzenia mogą być wykorzystywane do czasu wyczerpania posiadanych zapasów, jednak nie dłużej niż do dnia 31 grudnia 2022 r.

§ 3. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Obrony Narodowej: z up. *W. Skurkiewicz*

Załączniki do zarządzenia Nr 24/MON
Ministra Obrony Narodowej
z dnia 28 grudnia 2020 r. (poz. 210)

Załącznik nr 1

Wytyczne do sporządzania procedur 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 jednostki organizacyjnej zaopatrywanej względem jednostki organizacyjnej zaopatrującej: … (podległa/ nadrzędna/ równorzędna/ niezależna służbowo),
   d) przyczyna/powód zaopatrywania w materiały kryptograficzne: … (uzasadnienie),
   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 jednostki organizacyjnej 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);
9) wykaz osób funkcyjnych wraz z kierownikiem i zastępcą kierownika jednostki organizacyjnej zaopatrywanej upoważnionych do pobierania materiałów kryptograficznych – tabela;
10) wykaz urządzeń ewidencyjnych i dokumentacji dodatkowo prowadzonych przez jednostkę zaopatrującą – tabela.

Procedury należy opracować w 4 egzemplarzach:

Egz. nr 1 – KOGD.

Egz. nr 2 – NCBC.

Egz. nr 3 – jednostka organizacyjna zaopatrywana.

Egz. nr 4 – jednostka organizacyjna zaopatrująca.

Uwaga:

Procedury podlegają uzgodnieniu przez Dyrektora NCBC oraz wymagają akceptacji przez Szefa KOGD.

Załącznik nr 2

Wykaz osób upoważnionych do dostępu do materiałów kryptograficznych

WZÓR

Klauzula tajności

Egzemplarz pojedynczy

WYKAZ

OSÓB .....

(NAZWA JEDNOSTKI ORGANIZACYJNEJ)

UPOWAŻNIONYCH DO DOSTĘPU DO MATERIAŁÓW KRYPTOGRAFICZNYCH

Lp.	Stopień wojskowy	Imię i nazwisko	Nazwa jednostki organizacyjnej	Zakres i numer poświadczenia bezpieczeństwa	Termin ważności poświadczenia bezpieczeństwa do klauzuli tajności:				Nr CUK	Uwagi
					Ściśle tajne/ Cosmic Top Secret	Tajne/ Secret	Poufne/ Confidential	Zastrzeżone/ Restricted		
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.

Załącznik nr 3

Formularz z kodami dostępu, kodami systemu alarmowego do pomieszczeń kancelarii 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*……..
NR FABRYCZNY SZAFY *……..

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)

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*……..
NR FABRYCZNY SZAFY *……..

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 najwyżej sklasyfikowanej informacji przechowywanej w pomieszczeniu/urządzeniu

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 NIEPRZEŹROCZYSTEJ KOPERCIE

INSTYTUCJA:	**ODDZIAŁ:**	**WYDZIAŁ:**
NR FABRYCZNY POJEMNIKA/SEJFU:	**NR POMIESZCZENIA:**	**DATA OSTATNIEJ ZMIANY KOMBINACJI:**

KOD SYSTEMU ALARMOWEGO:**

KOMBINACJA/*****

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

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

(miejsce zagięcia kartki)

[redacted]

Podlega ochronie przewidzianej dla materiałów niejawnych o klauzuli tajności *……..

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

Załącznik nr 4

WZÓR

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[1], DO KTÓREGO UPRAWNIONY MA DOSTĘP**	
6. OŚWIADCZENIE SKŁADANE W MOMENCIE PRZYZNANIA CERTYFIKATU: Ja, _____ niniejszym oświadczam, że zostałem przeszkolony w zakresie bezpieczeństwa kryptograficznego przez _____. Rozumiem, że ochrona niejawnych informacji kryptograficznych ma najwyższe znaczenie oraz że utrata lub ujawnienie informacji kryptograficznych może spowodować nieusuwalną szkodę dla bezpieczeństwa narodowego i/lub NATO*. Zostałem przeszkolony w zakresie przepisów bezpieczeństwa dotyczących ujawniania informacji odnoszących się do kryptograficznych systemów narodowych i/lub NATO*. Znam instrukcje kryptograficzne narodowe i/lub NATO*, odnoszące się do ochrony niejawnych informacji kryptograficznych, do których zostałem upoważniony.		
7. PODPIS: **DATA:**	**8. PODPIS OSOBY WYDAJĄCEJ UPOWAŻNIENIE:** **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: **DATA:**	**11. PODPIS OSOBY ANULUJĄCEJ UPOWAŻNIENIE:** **DATA:**	

[1]Należy szczegółowo określić wykaz materiałów kryptograficznych, do których nadaje się dostęp np. materiały kryptograficzne dotyczące PCŁU lub IFF itp.

* niepotrzebne skreślić

Formularz 104 P

Załącznik nr 5

WZÓR

Rejestr teczek materiałów kryptograficznych, dzienników i książek ewidencyjnych

Strona lewa

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

Strona prawa

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

Załącznik nr 6

WZÓR

Pomocnicza książka ewidencji pieczęci

w …….
(nr lub nazwa jednostki organizacyjnej)

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/decyzji unieważniającego zagubioną (utraconą) pieczęć
1.	2.	3.	4.	5.	6.	7.	8.

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

Załącznik nr 7

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

WZÓR

KRYPTO

KARTA EWIDENCYJNA ŚRODKÓW I MATERIAŁÓW KRYPTOGRAFICZNYCH - SPRZĘT

NAZWA SKRÓCONA:	KLAUZULA TAJNOŚCI	PEŁNA NAZWA:	

DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER SF 153 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER SF 153 PL	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI

Sekcja…. /Strona….

FORMULARZ AF 54 B PL

KRYPTO								
DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER SF 153 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER SF 153 PL	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI
Sekcja…. /Strona….								

FORMULARZ AF 54 B PL

Załącznik nr 8

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

WZÓR

KRYPTO

KARTA EWIDENCYJNA ŚRODKÓW I MATERIAŁÓW KRYPTOGRAFICZNYCH - PUBLIKACJE

NAZWA SKRÓCONA:			KLAUZULA TAJNOŚCI	PEŁNA NAZWA:				
DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER SF 153 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER SF 153 PL	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI

Sekcja…. /Strona….

FORMULARZ AF 54 C PL

KRYPTO								
DANE WCHODZĄCE				**ROZDYSPONOWANIE**				
NUMER LUB ILOŚĆ	ODEBRANE OD	NUMER SF 153 PL	DATA ODBIORU	PRZESŁANO DO/ ZNISZCZONO	NUMER SF 153 PL	DATA WYSŁANIA / ZNISZCZENIA	AKTUALNY STAN	UWAGI
Sekcja…. /Strona….								

FORMULARZ AF 54 C PL

Załącznik nr 9

WZÓR

Formularz AF 147 PL
…………(rok)

KRYPTO

KARTA EWIDENCJI FORMULARZY SF 153 PL				**JEDNOSTKA ORGANIZACYJNA : ……………………….**	**KANCELARIA Nr: 860048/….**	**NUMERACJA: …………**	**ROK:** …………	**STRONA: …. z …**
Nr formularza	**Data**	**Od / Do**	**Numer wykazu przesyłek**	**Typ transakcji:**		**Uwagi**	**Zakończony przez:**	**Data zakończenia:**

Załącznik nr 10

WZÓR

Raport materiału kryptograficznego (formularz SF 153PL)

RAPORT MATERIAŁU KRYPTOGRAFICZNEGO												
1.		PRZEKAZANIE		INWENTARYZACJA		ZNISZCZENIE		PRZEKAZANIE ODRĘCZNE		INNE		
2.	**OD**: **KANCELARIA NR**:						3.DATA WYKONANIA		4. NUMER WYCHODZĄCY			
							5. DATA TRANSAKCJI		6. NUMER WCHODZĄCY			
7.	**OD**: **KANCELARIA NR**:						8.	ALC:				
							1. Rozliczane poprzez numer seryjny 2. Rozliczane ilościowo 4. Wymagane stworzenie posiadania – otrzymano z innego źródła 6. Rozliczane do COR poprzez EKMS 7. Rozliczane lokalnie bez EKMS					
9.	NAZWA SKRÓCONA / EDYCJA				10. ILOŚĆ		11. NUMER			12.ALC	13.UWAGI/TERMIN OBOWIĄZYWANIA/ PRZEZNACZENIE	
							POCZĄTKOWY		KOŃCOWY			
PONIŻEJ BRAK POZYCJI KRYPTOGRAFICZNYCH												
Egz.nr 1-….												
Egz.nr 2-….												
Egz.nr 3-….												
PONIŻEJ BRAK WPISU												
14.	MATERIAŁ ZOSTAŁ: (X-zaznacz właściwe)			ODEBRANY			ZINWENTARYZOWAY			ZNISZCZONY		INNE
15.		UPOWAŻNIONY ODBIORCA (X-zaznacz właściwe)						ŚWIADEK				INNA OSOBA
a. PODPIS				b. STOPIEŃ			a. PODPIS			b. STOPIEŃ		
c. NAZWISKO (drukowane litery)				d. RODZAJ WOJSK			c. NAZWISKO (drukowane litery)			d. RODZAJ WOJSK		
16. DO WIADOMOŚCI:												

FORMULARZ SF 153

Formularz SF 153 PL oznaczony jest klauzulą:

1) Przekazania lub przyjęcia urządzenia kryptograficznego – JAWNE
2) Przekazania lub przyjęcia publikacji – JAWNE
3) Przekazania lub przyjęcia dokumentów kryptograficznych – ZASTRZEŻONE
4) Lokalne posiadanie – POUFNE, jeśli zawiera tylko sprzęt to – ZASTRZEŻONE
5) Zniszczenie – POUFNE
6) Przekazanie odręczne:
    a) urządzenia kryptograficznego – JAWNE;
    b) publikacji – JAWNE;
    c) dokumentów kryptograficznych – ZASTRZEŻONE.

Załącznik nr 11

WZÓR

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

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

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

Załącznik nr 12

Plan przeprowadzenia inspekcji kryptograficznej

WZÓR

Miejscowość, data

„Z A T W I E R D Z A M”

……..……..……..

(kierownik jednostki organizacyjnej zarządzającej inspekcję kryptograficzną)

…….…….

(stopień, imię i nazwisko)

Dnia …..……. 20… r.

P L A N
PRZEPROWADZENIA INSPEKCJI KRYPTOGRAFICZNEJ

I. Temat inspekcji kryptograficznej:

Inspekcja kryptograficzna w ……

II. Cel inspekcji kryptograficznej:

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

III. Zakres inspekcji kryptograficznej:

BEZPIECZEŃSTWO MATERIAŁÓW KRYPTOGRAFICZNYCH

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

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

PROWADZENIE EWIDENCJI MATERIAŁÓW KRYPTOGRAFICZNYCH

1. Sprawdzenie „Rejestru teczek materiałów kryptograficznych, dzienników i książek ewidencyjnych”.
2. Sprawdzenie znajomości i przestrzeganie przez kierownika kancelarii kryptograficznej oraz jego zastępcę umiejętności postępowania z materiałami kryptograficznymi, a także przestrzegania zasad ich ewidencji.
3. Sprawdzenie, czy prowadzona ewidencja odzwierciedla wszystkie posiadane materiały kryptograficzne.
4. Sprawdzenie ewidencji niejawnej korespondencji wchodzącej i wychodzącej (szyfrogramy, faxy) dotyczącej tematyki kryptograficznej oraz sprawdzenie prawidłowości ich obiegu.
5. Sprawdzenie zapisów na korespondencji wchodzącej oraz sposobu ich realizacji.
6. Sprawdzenie sposobu dokonywania sprawdzeń przez personel BSŁiI urządzeń ewidencyjnych oraz materiałów kryptograficznych.
7. Sprawdzenie zgodności realizowanych inspekcji kryptograficznych oraz sprawdzeń z zasadami zapewniającymi ciągłą ochronę i nadzór.
8. Sprawdzenie czy materiały kryptograficzne, które zostały wykorzystane lub przestały obowiązywać są zniszczone zgodnie z obowiązującymi w tym zakresie przepisami.
9. Sprawdzenie prawidłowości wykonania protokołów zniszczonych materiałów kryptograficznych.

10. Sprawdzenie terminowego przesyłania do NCBC potwierdzeń zniszczenia materiałów kryptograficznych.
11. Sprawdzenie publikacji kryptograficznych zawierających wprowadzone zmiany i poprawki oraz czy są one właściwie ewidencjonowane.
12. Sprawdzenie posiadania w kancelarii kryptograficznej dokumentu określającego klasyfikację rzeczową akt kryptograficznych (wypisu z Jednolitego Rzeczowego Wykazu Akt/wykazu/rejestru jednostki organizacyjnej dotyczącej kancelarii kryptograficznej).

BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH

1. Sprawdzenie, czy w jednostce organizacyjnej, w której przeprowadzana jest inspekcja kryptograficzna, są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne dotyczące tematyki kryptograficznej za pomocą systemów teleinformatycznych.
2. Sprawdzenie przestrzegania wymagań w zakresie ochrony informacji niejawnych dotyczących tematyki kryptograficznej, które są przetwarzane, wytwarzane, przechowywane i przesyłane w systemach teleinformatycznych eksploatowanych w kancelarii kryptograficznej oraz u wykonawców.
3. Sprawdzenie, czy system teleinformatyczny, o którym mowa w pkt 1, posiada zatwierdzoną przez Służbę Kontrwywiadu Wojskowego lub Agencję Bezpieczeństwa Wewnętrznego dokumentację bezpieczeństwa lub/i ważny certyfikat bezpieczeństwa teleinformatycznego lub 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 kryptograficznej:

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

V. Skład komisji:

Przewodniczący - ……..
Członkowie: - ……..
- ….....

VI. Sposób przedstawienia wyników inspekcji kryptograficznej:

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

PRZEWODNICZĄCY KOMISJI
…….
(stopień, imię i nazwisko)

Załącznik nr 13

WZÓR

Karta inspekcji kryptograficznej

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

Lp.	Zagadnienie podlegające sprawdzeniu	Wynik i podpis		Uwagi
		Pozytywny	Negatywny	
BEZPIECZEŃSTWO MATERIAŁÓW KRYPTOGRAFICZNYCH				
1.	Sprawdzenie zaświadczenia o funkcjonowaniu kancelarii kryptograficznej lub aktualnego certyfikatu bezpieczeństwa zespołu pomieszczeń kancelarii kryptograficznej.			
2.	Analiza zawartości teczki z protokołami inspekcji kryptograficznych i innych form kontroli.			
3.	Sprawdzenie posiadania przez personel BSŁiI, wykonawców i inne osoby funkcyjne mające 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.			*Wypisać osoby funkcyjne personelu BSŁiI wraz z Oficerem BSŁiI oraz wszystkie za okres objęty inspekcją kryptograficzną daty ważności poświadczeń bezpieczeństwa, certyfikatów NATO / UE, ich klauzule tajności, zaświadczenia o przeszkoleniu*

Lp.	Zagadnienie podlegające sprawdzeniu	Wynik i podpis		Uwagi
		Pozytywny	Negatywny	
4.	Sprawdzenie prawidłowości wyznaczenia na stanowiska personelu BSŁiI oraz poprawności wystawiania kart wzorów podpisów ww. personelu. (sprawdzenie rozkazów personalnych oraz ciągłości zajmowania stanowiska. W przypadku gdy kierownik kancelarii kryptograficznej jest nieobecny więcej niż 60 dni to następuje sprawdzenie przekazania obowiązków dla zastępcy kierownika kancelarii kryptograficznej).			
5.	Sprawdzenie posiadanych kursów specjalistycznych personelu BSŁiI.			
6.	Sprawdzenie prawidłowości wydania oraz aktualności wydanych certyfikatów upoważnienia kryptograficznego. *(Wydanie CUK przez D-cę na wniosek Szefa* OBSŁiI *po wyznaczeniu rozkazem personalnym na stanowisko, instruktaż. Sprawdzenie „Wykazu wydanych CUK" i CUK pod kątem zakresu obowiązków).*			
7.	Sprawdzenie poprawności ewidencji szkoleń w zakresie bezpieczeństwa materiałów kryptograficznych *(plany, konspekty, lista obecności).*			
8.	Sprawdzenie funkcjonowania stref ochronnych, systemu alarmowego oraz kontroli dostępu.			
9.	Sprawdzenie kontroli dostępu do pomieszczeń kryptograficznych, materiałów kryptograficznych oraz pomocniczego sprzętu kryptograficznego.			
10.	Sprawdzenie zabezpieczenia kluczy użytku bieżącego oraz kluczy zapasowych do pomieszczeń i urządzeń do przechowywania informacji niejawnych, w których przechowywane są materiały kryptograficzne.			
11.	Sprawdzenie dokonywania zmian ustawień kodów dostępu (kombinacji) w zamkach szyfrowych oraz sprawdzenie przechowywania kodów dostępu zamków szyfrowych.			
12.	Sprawdzenie certyfikatów drzwi wejściowych do kancelarii kryptograficznej oraz urządzeń do przechowywania informacji niejawnych, w których przechowywane są materiały kryptograficzne.			

Lp.	Zagadnienie podlegające sprawdzeniu	Wynik i podpis		Uwagi
		Pozytywny	Negatywny	
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 kontrola postępowania z pozostałościami powstającymi w trakcie niszczenia.			
19.	Sprawdzenie poprawności oznakowania nośników informacji.			
20.	Sprawdzenie u wykonawców sposobu przechowywania materiałów kryptograficznych.			
PROWADZENIE EWIDENCJI MATERIAŁÓW KRYPTOGRAFICZNYCH				
21.	Sprawdzenie „Rejestru teczek materiałów kryptograficznych, dzienników i książek ewidencyjnych”.			
22.	Sprawdzenie znajomości i przestrzeganie przez kierownika kancelarii kryptograficznej oraz jego zastępcę umiejętności postępowania z materiałami kryptograficznymi, a także przestrzegania zasad ich ewidencji.			

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

Lp.	Zagadnienie podlegające sprawdzeniu	Wynik i podpis		Uwagi
		Pozytywny	Negatywny	
BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH				
33.	Sprawdzenie, czy w jednostce organizacyjnej, w której przeprowadzana jest inspekcja kryptograficzna, przy użyciu systemów teleinformatycznych są wytwarzane, przechowywane, przetwarzane lub przekazywane materiały kryptograficzne.			(wymienić nazwy systemów teleinformaty-cznych)
34.	Sprawdzenie w kancelarii kryptograficznej oraz u wykonawców dokumentów niejawnych przestrzegania wymagań w zakresie ochrony informacji niejawnych dotyczących tematyki kryptograficznej przetwarzanych, wytwarzanych, przechowywanych i przesyłanych w systemach teleinformatycznych eksploatowanych w kancelarii kryptograficznej.			
35.	Sprawdzenie, czy system teleinformatyczny, o którym mowa w pkt 33, posiada zatwierdzoną przez SKW lub ABW dokumentację bezpieczeństwa systemu teleinformatycznego lub/i ważny certyfikat/ świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.			(wymienić daty zatwierdzenia dokumentacji bezpieczeństwa systemu teleinformaty-cznego, numery certyfikatów lub świadectw w odniesieniu do systemów teleinformaty-cznych z pkt 33)
36.	Sprawdzenie, czy kierownik jednostki organizacyjnej wyznaczył administratora systemu teleinformatycznego, odpowiedzialnego 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 teleinformatycznego jest zgodne z wykazem w dokumentacji bezpieczeństwa systemu teleinformatycznego.			*(jeżeli jest rozbieżność wykazać co się nie zgadza)*

Lp.	Zagadnienie podlegające sprawdzeniu	Wynik i podpis		Uwagi
		Pozytywny	Negatywny	
39.	Sprawdzenie czy wszyscy użytkownicy zostali zapoznani z Procedurami Bezpiecznej Eksploatacji (PBE) i poświadczyli to własnoręcznym podpisem.			*(jeżeli jest rozbieżność wykazać co się nie zgadza)*
40.	Sprawdzenie czy administrator systemu teleinformatycznego prowadzi archiwizację dzienników zdarzeń tworzonych przez system (gdzie i jak przechowuje ich kopie).			*(wykazać gdzie i jak przechowuje się ich kopie)*
41.	Sprawdzenie czy nośniki danych systemu teleinformatycznego (m.in. dyski twarde) są właściwie oznaczone i zaewidencjonowane.			*(podać numery seryjne dysków twardych systemu oraz ich numery ewidencyjne, klauzule tajności)*
42.	Sprawdzenie czy Inspektor bezpieczeństwa teleinformatycznego (BTI) dokonywał analizy dzienników zdarzeń zgodnie z opracowanymi procedurami.			*(podać systemy w odniesieniu do pkt 33 oraz daty analizy dzienników zdarzeń)*
43.	Sprawdzenie czy administrator systemu teleinformatycznego zabezpieczył hasłem wejście do BIOS komputera.			
44.	Sprawdzenie czy procedury deponowania haseł administratora systemu teleinformatycznego są właściwie realizowane (BIOS, system, terminy zmiany haseł).			*(m.in. podać daty zmiany haseł)*
45.	Sprawdzenie czy wszystkie osoby wytwarzające dokumenty (wg DEWMK) znajdują się na liście użytkowników uprawnionych do pracy w systemie teleinformatycznym.			
46.	Sprawdzenie czy użytkownicy znają swoje uprawnienia i zadania.			
47.	Sprawdzenie listy kont użytkowników systemu teleinformatycznego i porównanie jej zgodności z wnioskami założenia konta.			*(jeżeli jest rozbieżność wykazać co się nie zgadza)*
48.	Sprawdzenie czy nadane prawa użytkownikom systemu teleinformatycznego są zgodne z dokumentacją bezpieczeństwa systemu teleinformatycznego.			*(jeżeli jest rozbieżność wykazać co się nie zgadza)*

Lp.	Zagadnienie podlegające sprawdzeniu	Wynik i podpis		Uwagi
		Pozytywny	Negatywny	
49.	Sprawdzenie czy procedury przeciwdziałania komputerowym infekcjom wirusowym są właściwie realizowane.			*(jeżeli jest rozbieżność wykazać co się nie zgadza)*
50.	Sprawdzenie aktualizacji oprogramowania antywirusowego oraz czy aktualizacja jest przeprowadzana zgodnie z zapisami dokumentacji bezpieczeństwa systemu teleinformatycznego.			*(wykazać co jaki czas aktualizowana jest baza wirusów)*
51.	Sprawdzenie czy administrator systemu teleinformatycznego prowadzi okresowe szkolenia użytkowników z zakresu użytkowania systemu teleinformatycznego.			
52.	Sprawdzenie czy Inspektor BTI prowadzi okresowe szkolenia użytkowników z zakresu użytkowania systemu teleinformatycznego.			
53.	Sprawdzenie czy informatyczne nośniki danych (IND) wykorzystywane w systemie teleinformatycznym są oznaczone i zarejestrowane zgodnie z procedurami zawartymi w dokumentacji bezpieczeństwa systemu teleinformatycznego.			
54.	Sprawdzenie czy na nośnikach systemu teleinformatycznego są przechowywane informacje niejawne o klauzuli tajności wyższej niż klauzula tajności systemu teleinformatycznego.			*(jeżeli jest rozbieżność proszę ją wykazać)*
55.	Sprawdzenie czy procedury deponowania dysku twardego systemu teleinformatycznego są realizowane zgodnie z zapisami dokumentacji bezpieczeństwa systemu teleinformatycznego.			*(jeżeli jest rozbieżność proszę ją wykazać)*
56.	Sprawdzenie czy Dziennik Ewidencji Wykonanych Materiałów Kryptograficznych jest prowadzony właściwie.			*(jeżeli jest rozbieżność proszę ją wykazać)*

Załącznik nr 14

Instrukcja konwojowania materiałów kryptograficznych

Instrukcja powinna zawierać m.in. następujące informacje:

1. Wprowadzenie (wyszczególnienie aktów prawnych dotyczących konwojowania)
2. Definicje (definicje określeń zawartych w instrukcji)
3. Organizacja konwoju
4. Zadania osób funkcyjnych
5. Standardowe procedury postępowania z materiałami kryptograficznymi
6. Procedury postępowania z materiałami kryptograficznymi w sytuacjach szczególnych
7. Załączniki:
   a) Wytyczne w sprawie organizacji konwoju do przewozu materiałów kryptograficznych,
   b) Plan konwoju.

Załącznik nr 15

WZÓR

REJESTR INTERESANTÓW

Jednostka organizacyjna				**Budynek jednostki organizacyjnej**		**Pomieszczenie jednostki organizacyjnej**			
Data	Stopień	Imię i nazwisko	Nazwa i numer dokumentu tożsamości	Miejsce wizyty	Podpis	Czas wejścia	Czas wyjścia	Upoważnienie wydane przez kierownika jednostki organizacyjnej	
								Imię i nazwisko	Podpis

Załącznik nr 16

WZÓR

DZIENNIK EWIDENCYJNY

strona lewa

Symbol oznaczenia klauzuli tajności	Numer kolejny zapisu	Adnotacje dot. obowiązywania klauzuli tajności lub jej zniesienia albo zmiany	Data rejestracji dokumentu	Nazwa nadawcy/adresata	Numer i data dokumentu otrzymanego	Nazwa dokumentu lub czego dotyczy	Liczba egzemplarzy wytworzonego dokumentu	Liczba		
								stron dokumentu lub innych jednostek miary	załączników	stron wszystkich załączników lub innych jednostek miary
1	2	3	4	5	6	7	8	9	10	11

strona --------/---------

strona prawa

Nr dokumentu z którego wykonano druk, kopię, wyciąg, odpis, tłumaczenie, lub numer nośnika	Imię i nazwisko lub inne dane identyfikujące wykonawcę dokumentu	Data, imię i nazwisko oraz podpis osoby pobierającej dokument	Potwierdzenie zwrotu dokumentu (data i podpis)	Adnotacje		Informacje uzupełniające/ Uwagi (np. symbol klasyfikacyjny wykazu akt)
				o wysłaniu dokumentu lub załącznika (pozycja w książce doręczeń przesyłek miejscowych/pozycja wykazu przesyłek nadanych/załącznik do pisma nr …)	o wybrakowaniu lub przekazaniu do archiwum	
12	13	14	15	16	17	18

strona --------/-------