

Warszawa, dnia 7 maja 2025 r.

Poz. 72

ZARZĄDZENIE Nr 11/MON
MINISTRA OBRONY NARODOWEJ
z dnia 6 maja 2025 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. z 2024 r. poz. 632 i 1222) zarządza się, co następuje:

Rozdział 1
Postanowienia ogólne

§ 1. 1. Zarządzenie określa:

- 1) organizację i funkcjonowanie kancelarii kryptograficznych oraz organów nadzorujących ich pracę;
- 2) sprawowanie nadzoru nad organami bezpieczeństwa systemów łączności;
- 3) bezpieczeństwo zasobów kryptograficznych;
- 4) dobór i stosownie środków bezpieczeństwa fizycznego;
- 5) organizację przewozu przesyłek kryptograficznych na terenie Rzeczypospolitej Polskiej;
- 6) sposób rejestrowania, kompletowania i niszczenia zasobów kryptograficznych;
- 7) organizację pracy kancelarii kryptograficznych, ich ochronę oraz obieg zasobów kryptograficznych podczas ćwiczeń oraz realizacji zadań poza Miejscem Stałej Dyslokacji jednostki organizacyjnej;
- 8) wzory urzędzeń ewidencyjnych.

2. Przepisów zarządzenia nie stosuje się do zasobów kryptograficznych wykorzystywanych przez podmioty uprawnione do realizacji czynności operacyjno-rozpoznawczych w trakcie ich wykonywania.

§ 2. Użyte w zarządzeniu określenia i skróty oznaczają:

- 1) akta kryptograficzne – odpowiednio opracowane i zabezpieczone zbiory akt dotyczące zasobów kryptograficznych, pogrupowanych zgodnie z wykazem akt, oznaczone właściwą kategorią archiwalną i symbolem klasyfikacyjnym, zawierające:
 - a) publikację i wydawnictwa kryptograficzne,

- b) dokumentację techniczną systemów kryptograficznych i produktów kryptograficznych,
 - c) dokumentację lub pisma dotyczące tematyki kryptograficznej, ewidencji, przechowywania, wykorzystania i niszczenia zasobów kryptograficznych,
 - d) formularze i inne urządzenia ewidencyjne przeznaczone do ewidencji zasobów kryptograficznych;
- 2) archiwizacja – ogół czynności związanych z klasyfikowaniem, kwalifikowaniem, kompletowaniem i przekazywaniem archiwalnych zasobów kryptograficznych do archiwum Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, ich ewidencjonowaniem oraz przechowywaniem w archiwum Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni;
 - 3) archiwum – Archiwum Wyodrębnione Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni – komórkę organizacyjną Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni powołaną do gromadzenia, ewidencjonowania, przechowywania i udostępniania archiwalnych zasobów kryptograficznych wytworzonych i zarejestrowanych w Dowództwie Komponentu Wojsk Obrony Cyberprzestrzeni lub w kancelariach kryptograficznych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz do nadzoru archiwalnego nad tymi zasobami;
 - 4) CCI (ang. „Controlled COMSEC Item/Controlled Cryptographic Item”) – międzynarodowe i stosowane w Organizacji Traktatu Północnoatlantyckiego oznaczenie produktów kryptograficznych lub elementów systemu łączności, które nie posiadają nadanej klauzuli tajności, jednakże z uwagi na wbudowane mechanizmy kryptograficzne lub przeznaczenie podlegają szczególnej ochronie i rozliczalności;
 - 5) CKK MON – Centralną Kancelarię Kryptograficzną Ministerstwa Obrony Narodowej – kancelarię kryptograficzną umiejscowioną w Dowództwie Komponentu Wojsk Obrony Cyberprzestrzeni, będącą nadrzędną kancelarią kryptograficzną dla jednostek organizacyjnych podległych Ministrowi Obrony Narodowej;
 - 6) CUK – Certyfikat Upoważnienia Kryptograficznego – dokument potwierdzający spełnienie wymagań uprawniających do dostępu do materiałów kryptograficznych w określonym zakresie;
 - 7) DKWOC – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni;
 - 8) dokument kryptograficzny – klucz kryptograficzny posiadający cechy identyfikacyjne w postaci nazwy, klauzuli tajności, numeru egzemplarza, numeru serii oraz innych danych pomocniczych, który podlega ewidencji w kancelarii kryptograficznej;
 - 9) dokument kryptograficzny bieżącej edycji – dokument kryptograficzny wykorzystywany w danym momencie do czasu zakończenia terminu jego obowiązywania;
 - 10) dokument kryptograficzny przyszłej edycji – dokument kryptograficzny przeznaczony do przyszłego zabezpieczenia informacji;
 - 11) dokumentacja „KRYPTO” – pisma, zalecenia, wytyczne, instrukcje, publikacje, dokumentacja techniczna, które dotyczą eksploatacji oraz zarządzania materiałami kryptograficznymi;
 - 12) Dowódca KWOC – Dowódcę Komponentu Wojsk Obrony Cyberprzestrzeni;
 - 13) EOZK – elektroniczny obieg zasobów kryptograficznych – ogół przedsięwzięć związanych z rejestrowaniem, przyjmowaniem, przechowywaniem, udostępnianiem, dystrybucją, przygotowaniem do archiwizacji i niszczeniem zasobów kryptograficznych prowadzony w formie elektronicznej;
 - 14) GKK SKW – Główną Kancelarię Kryptograficzną Służby Kontrwywiadu Wojskowego – kancelarię kryptograficzną umiejscowioną w Służbie Kontrwywiadu Wojskowego będącą Główną Kancelarią Kryptograficzną dla Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz jednostek organizacyjnych;
 - 15) Główny użytkownik rozwiązania informatycznego – kierownika jednostki organizacyjnej, w której jest eksploatowane rozwiązanie informatyczne podlegające dopuszczeniu;
 - 16) incydent kryptograficzny – zdarzenie związane z naruszeniem bezpieczeństwa zasobów kryptograficznych;

- 17) inspekcja kryptograficzna – kontrolę funkcjonowania Organu Bezpieczeństwa Systemów Łączności w jednostce organizacyjnej;
- 18) jrw – 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;
- 19) JO – jednostkę organizacyjną – Ministerstwo Obrony Narodowej, jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną;
- 20) kanał kryptograficzny – sposób przesyłania lub przekazywania zasobów kryptograficznych pomiędzy kancelariami kryptograficznymi;
- 21) KK – kancelarię kryptograficzną – etatową komórkę organizacyjną lub wewnętrzną komórkę organizacyjną funkcjonującą w jednostce organizacyjnej, odpowiedzialną za obieg zasobów kryptograficznych, która może realizować zadania związane z ochroną kryptograficzną, takie jak: szyfrowanie i deszyfrowanie informacji niejawnych z wykorzystaniem produktów kryptograficznych;
- 22) kancelaria współpracująca – kancelarię kryptograficzną podległą innej kancelarii kryptograficznej lub będącą kancelarią zaopatrującą/zaopatrywaną zgodnie z obowiązującym systemem zaopatrywania w zasoby kryptograficzne;
- 23) KWP – kartę wzorów podpisów – formularz opisujący umiejscowienie KK w strukturze dowodzenia i systemie dystrybucji, zawierający jej aktualne dane teleadresowe oraz dane osobowe i wzory podpisów personelu tej kancelarii i Oficera Bezpieczeństwa Systemów Łączności;
- 24) KJO – kierownika 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 pełniącą obowiązki kierownika jednostki organizacyjnej;
- 25) kierownik KK – kierownika kancelarii kryptograficznej (w relacjach międzynarodowych – Crypto Custodian) – żołnierza zawodowego, funkcjonariusza lub pracownika KK zajmującego etatowe stanowisko kierownika KK i kierującego jej pracą, podlegającego merytorycznie Oficerowi Bezpieczeństwa Systemów Łączności;
- 26) KOGD – Krajowy Organ Generacji i Dystrybucji – w relacjach międzynarodowych – National Distribution Authority (NDA) – Organ Bezpieczeństwa Systemów Łączności Służby Kontrwywiadu Wojskowego sprawujący nadzór nad bezpieczeństwem zasobów kryptograficznych w jednostkach organizacyjnych oraz nad wymianą zasobów kryptograficznych z podmiotami realizującymi zadania na rzecz resortu obrony narodowej;
- 27) „KRYPTO” – oznaczenie specjalne stosowane do oznaczenia produktów kryptograficznych oraz dokumentacji „KRYPTO”, mające na celu wskazanie, że dostęp do nich posiadają tylko osoby upoważnione;
- 28) klucz kryptograficzny – każdy ciąg danych wytwarzany w produkcie kryptograficznym lub urządzeniu służącym do jego generacji, wykorzystywany do kryptograficznego zabezpieczenia informacji przed jej ujawnieniem lub modyfikacją oraz w realizacji procesu potwierdzenia autentyczności tej informacji przy pomocy produktu kryptograficznego;
- 29) materiał kryptograficzny:
 - a) dokument kryptograficzny,
 - b) produkt kryptograficzny,
 - c) dokumentacja „KRYPTO”;
- 30) MKK – Mobilną Kancelarię Kryptograficzną;
- 31) MSD – Miejsce Stałej Dyslokacji;
- 32) nadrzędna JO – nadrzędną w strukturze dowodzenia jednostkę organizacyjną;
- 33) nadrzędny OBSŁ – Organ Bezpieczeństwa Systemów Łączności występujący w nadrzędnej jednostce organizacyjnej;

- 34) narzędzie kryptograficzne – narzędzie niebędące urządzeniem kryptograficznym, posiadające zaimplementowany co najmniej jeden mechanizm kryptograficzny przeznaczony do zapewnienia bezpieczeństwa przetwarzanym informacjom niejawnym, dla którego wydany został przez uprawniony podmiot stosowny certyfikat lub inny dokument dopuszczający do ochrony informacji niejawnych (np. oprogramowanie);
- 35) NATO (ang. North Atlantic Treaty Organization) – Organizację Traktatu Północnoatlantyckiego;
- 36) obieg zasobów kryptograficznych – ogół przedsięwzięć związanych z rejestrowaniem, przyjmowaniem, przechowywaniem, udostępnianiem, dystrybucją (w tym przewozem), przygotowaniem do archiwizacji i niszczeniem zasobów kryptograficznych;
- 37) Oficer BSŁ – Oficera Bezpieczeństwa Systemów Łączności – uprawnioną osobę do sprawowania nadzoru nad bezpieczeństwem zasobów kryptograficznych w jednostce organizacyjnej;
- 38) OBSŁ – Organ Bezpieczeństwa Systemów Łączności – wyspecjalizowaną komórkę organizacyjną lub zespół osób odpowiedzialnych za zapewnienie organizacyjnych i technicznych wymagań kryptograficznej ochrony informacji niejawnych w systemach łączności występujący w jednostce organizacyjnej;
- 39) organizator systemu łączności – kierownika jednostki organizacyjnej organizującej system łączności lub upoważnionego przez niego kierownika komórki organizacyjnej;
- 40) pełnomocnik ochrony – pełnomocnika do spraw ochrony informacji niejawnych, o którym mowa w art. 14 ust. 2 i 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
- 41) personel KK – personel kancelarii kryptograficznej – żołnierza zawodowego lub funkcjonariusza pełniącego służbę w KK lub pracownika zatrudnionego w KK;
- 42) personel ochrony – osoby przeszkolone, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z ochroną fizyczną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad telewizyjnym systemem nadzoru, a także reagowanie na alarmy lub sygnały awaryjne;
- 43) PKK – Polową Kancelarię Kryptograficzną;
- 44) PKKs – Polową Kancelarię Kryptograficzną na samochodzie;
- 45) pomocnicze urządzenie ewidencyjne – urządzenie ewidencyjne stosowane w KK, które może zostać zniszczone po 12 miesiącach od daty zakończenia prowadzenia tego urządzenia ewidencyjnego;
- 46) pomocniczy sprzęt kryptograficzny – sprzęt nieujęty w definicji urządzenia kryptograficznego oraz narzędzia kryptograficznego, który wymaga specjalnej obsługi lub kontroli przez uprawniony personel w celu ochrony specjalnych układów zabezpieczających;
- 47) pracownik KK – pracownika resortu obrony narodowej zajmującego stanowisko referent/starszy referent/samodzielny referent/specjalista/starszy specjalista w KK;
- 48) przesyłka kryptograficzna – zaewidencjonowane zasoby kryptograficzne w postaci zabezpieczonych, zaadresowanych i odpowiednio oznaczonych paczek lub listów;
- 49) produkt kryptograficzny:
 - a) urządzenie kryptograficzne,
 - b) narzędzie kryptograficzne,
 - c) pomocniczy sprzęt kryptograficzny;
- 50) ron – resort obrony narodowej;
- 51) rozwiązanie informatyczne – rozwiązanie informatyczne, o którym mowa w art. 2 pkt 19 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
- 52) SF 153 (PL) – formularz wykorzystywany do przygotowywania raportów z działalności KK w zakresie przekazywania, niszczenia, inwentaryzacji, posiadania, przekazania odrębnego i kontroli materiałów kryptograficznych;
- 53) SKW – Służbę Kontrwywiadu Wojskowego;

- 54) system kryptograficzny – system składający się z powiązanych ze sobą elementów, które wykorzystując mechanizmy kryptograficzne, zapewniają zabezpieczenie informacji przed jej ujawnieniem lub modyfikacją oraz realizują proces potwierdzenia autentyczności tej informacji;
- 55) system łączności – organizacyjno-techniczny zespół sił i środków łączności, obejmujący systemy teleinformatyczne, systemy łączności radiowej, system pocztowy, system identyfikacji bojowej obiektów, systemy elektronicznej nawigacji, taktyczny system transmisji danych oraz rozwiązania informatyczne;
- 56) Szef KOGD – upoważnionego przez Szefa SKW do kierowania KOGD Dyrektora lub Zastępcę Dyrektora Zarządu VI SKW;
- 57) urządzenie ewidencyjne – księgę, dziennik, wykaz, spis, rejestr, formularz lub kartotekę o ustalonych wzorach, prowadzone w formie pisemnej lub elektronicznej, służące do rejestrowania zasobów kryptograficznych oraz umożliwiające kontrolę ich stanu i obiegu;
- 58) urządzenie kryptograficzne – urządzenie posiadające zaimplementowany co najmniej jeden mechanizm kryptograficzny przeznaczony do zapewnienia bezpieczeństwa przetwarzanym informacjom niejawnym, dla którego wydany został przez uprawniony podmiot stosowny certyfikat lub inny dokument dopuszczający do ochrony informacji niejawnych;
- 59) ustawa – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
- 60) użytkownik – osobę wykonującą czynności służbowe, których realizacja wymaga dostępu do zasobów kryptograficznych;
- 61) WSK RP – Wojskową Służbę Kurierską Rzeczypospolitej Polskiej – wojskową służbę kurierską, której zadania określają odrębne przepisy wydane przez Ministra Obrony Narodowej;
- 62) zasada wiedzy niezbędnej – udostępnianie określonej informacji wyłącznie osobom, którym jest to niezbędne do realizacji czynności służbowych;
- 63) zastępca kierownika KK (w relacjach międzynarodowych – Alternate Crypto Custodian) – żołnierza zawodowego, funkcjonariusza lub pracownika KK zajmującego etatowe stanowisko zastępcy kierownika tej kancelarii;
- 64) zasób kryptograficzny – zbiór obejmujący materiały kryptograficzne oraz inne materiały zaewidencjonowane w kancelarii kryptograficznej;
- 65) zarządzanie materiałami kryptograficznymi – całokształt przedsięwzięć związany z ochroną (bezpieczeństwem) materiałów kryptograficznych, od złożenia zapotrzebowania na dokumenty kryptograficzne, generację, wytwarzanie, ewidencję, dystrybuowanie, eksploatację, aż do ich fizycznego zniszczenia.

Rozdział 2

Organizacja i funkcjonowanie kancelarii kryptograficznych oraz organów nadzorujących ich pracę

§ 3. 1. W JO, które planują wykorzystywać zasoby kryptograficzne, KJO w rozkazie lub decyzji powołuje OBSŁ.

2. W skład OBSŁ wchodzi:

- 1) Oficer BSŁ;
- 2) Zastępca (Zastępcy) Oficera BSŁ – według potrzeb;
- 3) etatowy personel KK (co najmniej dwie osoby).

3. KJO zapewnia właściwą strukturę organizacyjną OBSŁ uwzględniając ich zdolność do zabezpieczenia JO w zasoby kryptograficzne w czasie pokoju, kryzysu i wojny, a także użycia lub pobytu jej poza granicami państwa.

4. Tryb i sposób powoływania i odwoływania KK określa w zaleceniach SKW, z upoważnienia Szefa SKW, Szef KOGD.

5. Nadzór nad właściwym funkcjonowaniem OBSŁ JO prowadzony jest przez OBSŁ nadrzędnej JO, a w przypadku OBSŁ:

- 1) Dowództwa Generalnego Rodzajów Sił Zbrojnych, Dowództwa Operacyjnego Rodzajów Sił Zbrojnych, Dowództwa Garnizonu Warszawa, Dowództwa Wojsk Obrony Terytorialnej, Komendy Głównej Żandarmerii Wojskowej lub Inspektoratu Wsparcia Sił Zbrojnych – przez OBSŁ DKWOC;
- 2) DKWOC lub Służby Wywiadu Wojskowego – przez KOGD.

6. Do zadań KOGD należy:

- 1) współpraca z The Military Committee Distribution and Accounting Agency (DACAN) i The Military Committee European Distribution and Accounting Agency (EUDAC);
- 2) pełnienie roli NDA w relacjach międzynarodowych;
- 3) sprawowanie nadzoru nad bezpieczeństwem zasobów kryptograficznych w JO;
- 4) sprawowanie nadzoru nad wymianą zasobów kryptograficznych z podmiotami realizującymi zadania w ron;
- 5) dystrybucja krajowych i międzynarodowych zasobów kryptograficznych;
- 6) nadzór nad generowaniem, wytwarzaniem dokumentów kryptograficznych służących do zabezpieczenia krajowych potrzeb w zakresie ochrony systemów łączności przetwarzających niejawne informacje krajowe i międzynarodowe;
- 7) określanie sposobu zarządzania materiałami kryptograficznymi;
- 8) określanie trybu i sposobu powoływania i odwoływania KK;
- 9) udzielanie zgody na powołanie, zawieszanie, wznowienie funkcjonowania i odwołanie KK;
- 10) udzielanie zgody na generowanie i wytwarzanie dokumentów kryptograficznych poza KOGD, służących do zabezpieczenia potrzeb w zakresie ochrony systemów łączności przetwarzających niejawne informacje krajowe i międzynarodowe;
- 11) nadzór nad szkoleniem specjalistycznym OBSŁ.

7. Do zadań DKWOC należy:

- 1) nadzorowanie i koordynowanie działalności OBSŁ w JO podległych Ministrowi Obrony Narodowej;
- 2) planowanie, organizowanie, prognozowanie rozwoju i eksploatacji oraz nadzór nad funkcjonowaniem ochrony kryptograficznej w systemach łączności ron;
- 3) planowanie, organizowanie, kwalifikowanie oraz sprawowanie nadzoru nad szkoleniami specjalistycznymi OBSŁ;
- 4) prowadzenie ewidencji dokonywanych kontroli lub inspekcji kryptograficznych nadzorowanych OBSŁ;
- 5) opracowywanie i przysyłanie do Szefa KOGD do dnia 30 kwietnia każdego roku sprawozdań za rok ubiegły o stanie ochrony informacji niejawnych w KK JO, z wyszczególnieniem:
 - a) KK objętych kontrolą albo inspekcją kryptograficzną,
 - b) formy nadzoru (inspekcja kryptograficzna, kontrola),
 - c) OBSŁ przeprowadzających inspekcje kryptograficzne albo kontrole,
 - d) stwierdzonych naruszeń ochrony informacji niejawnych w zakresie ochrony zasobów kryptograficznych oraz zastosowanych środków zaradczych;
- 6) generowanie i wytwarzanie dokumentów kryptograficznych służących do zabezpieczenia systemów łączności organizowanych w ron i innych za zgodą Szefa KOGD;
- 7) składanie do KOGD zbiorczych zapotrzebowań na materiały kryptograficzne (w szczególności dokumenty kryptograficzne) pochodzące z wymiany międzynarodowej,

służące do zabezpieczenia funkcjonowania systemów łączności wykorzystywanych w nadzorowanych OBSŁ;

- 8) opiniowanie wniosków organizacyjno-etatowych w zakresie dotyczącym formowania i zmian w strukturach OBSŁ;
- 9) prowadzenie inspekcji kryptograficznych w nadzorowanych OBSŁ;
- 10) nadzorowanie wykorzystywania zasobów kryptograficznych przez OBSŁ w JO podległych Ministrowi Obrony Narodowej;
- 11) przeprowadzanie raz w roku odprawy rozliczeniowo-szkoleniowej dla bezpośrednio nadzorowanych OBSŁ;
- 12) opracowywanie i uzgadnianie z KOGD wytycznych do wykorzystywania produktów kryptograficznych w systemach łączności organizowanych w ron oraz rozwiązań wspomagających funkcjonowanie OBSŁ;
- 13) określanie i uzgadnianie z KOGD systemu zaopatrywania w zasoby kryptograficzne nadzorowanych OBSŁ.

8. Do zadań OBSŁ wszystkich szczebli organizacyjnych, z zastrzeżeniem ust. 6 i 7 należy:

- 1) nadzorowanie i koordynowanie działalności podporządkowanych OBSŁ;
- 2) planowanie i prowadzenie inspekcji kryptograficznych w nadzorowanych OBSŁ;
- 3) prowadzenie ewidencji dokonywanych kontroli lub inspekcji kryptograficznych OBSŁ;
- 4) organizowanie ochrony kryptograficznej w planowanych do uruchomienia oraz eksploatowanych systemach łączności;
- 5) analiza otrzymywanych z podległych OBSŁ zapotrzebowań na zasoby kryptograficzne oraz opracowywanie zapotrzebowań zbiorczych na zasoby kryptograficzne na potrzeby własne, a także OBSŁ podległych;
- 6) nadzorowanie wykorzystywania zasobów kryptograficznych przez podporządkowane OBSŁ;
- 7) opracowywanie i przysyłanie do OBSŁ nadrzędnej JO sprawozdań z funkcjonowania OBSŁ za ubiegły rok;
- 8) określenie terminu przesłania sprawozdania, o którym mowa w pkt 7, dla bezpośrednio podporządkowanych OBSŁ;
- 9) przeprowadzenie raz w roku odprawy rozliczeniowo-szkoleniowej dla bezpośrednio nadzorowanych OBSŁ.

9. W przypadku, gdy:

- 1) w nadrzędnej JO nie funkcjonuje OBSŁ dopuszcza się sprawowanie nadzoru nad zasobami kryptograficznymi z podległych JO przez OBSŁ wskazany przez kierownika nadrzędnej JO;
- 2) w podległej JO nie funkcjonuje OBSŁ dopuszcza się sprawowanie nadzoru nad zasobami kryptograficznymi tej JO przez OBSŁ nadrzędnej JO.

10. Sprawozdanie, o którym mowa w ust. 8 pkt 7, OBSŁ bezpośrednio nadzorowane przez DKWOC przysyłają do DKWOC do dnia 31 marca każdego roku.

11. Zapotrzebowania na zasoby kryptograficzne składa się kanałem kryptograficznym do DKWOC za pośrednictwem właściwego KJO, w której funkcjonuje nadrzędny OBSŁ.

12. W przypadku rozległych systemów łączności zapotrzebowanie zbiorcze na materiały kryptograficzne opracowuje OBSŁ organizatora systemu łączności lub główny użytkownik rozwiązań informatycznego i przysyła kanałem kryptograficznym do DKWOC za pośrednictwem właściwego KJO, w której funkcjonuje nadrzędny OBSŁ.

13. Szczegółowe procedury składania zapotrzebowań, o których mowa w ust. 11, określa Szef KOGD w zaleceniach SKW dotyczących zarządzania materiałami kryptograficznymi.

§ 4. 1. Nadzór nad bezpieczeństwem zasobów kryptograficznych w JO sprawuje osoba wyznaczona rozkazem (decyzją) przez KJO do pełnienia funkcji Oficera BSŁ.

2. W zależności od potrzeb, KJO może wyznaczyć Zastępcę (Zastępców) Oficera BSŁ.

3. Do pełnienia funkcji Oficera BSŁ i Zastępcy Oficera BSŁ wyznacza się osobę, która posiada poświadczenia bezpieczeństwa odpowiednie do klauzuli tajności KK oraz zasobów kryptograficznych planowanych do przetwarzania w JO, aktualne zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych oraz szkolenie specjalistyczne określone w zaleceniach SKW w sprawie sposobu oraz trybu powoływania i odwoływania kancelarii kryptograficznej.

4. W czasie nieobecności Oficera BSŁ, jego obowiązki pełni Zastępca Oficera BSŁ. W przypadku krótkotrwałej, nie dłuższej niż 30 dni, nieobecności Oficera BSŁ i jego Zastępcy, obowiązki Oficera BSŁ pełni kierownik KK.

5. Do zadań i obowiązków Oficera BSŁ należy:

- 1) nadzór nad bezpieczeństwem zasobów kryptograficznych, w tym za sprawdzanie wszystkich miejsc w JO, w których są przechowywane i wykorzystywane te zasoby;
- 2) uzgadnianie bezpośrednio z KJO wszelkich zagadnień związanych z ochroną zasobów kryptograficznych oraz funkcjonowaniem OBSŁ;
- 3) przekazywanie KJO propozycji rozwiązań w sprawach związanych z bezpieczeństwem zasobów kryptograficznych oraz ochroną kryptograficzną systemów łączności JO oraz jednostek jej podległych;
- 4) realizowanie zadań postawionych przez Oficera BSŁ z OBSŁ szczebla nadrzędnego w zakresie ochrony kryptograficznej;
- 5) współpraca z pełnomocnikiem ochrony oraz komórką organizacyjną odpowiedzialną za ochronę obiektów wojskowych w zakresie zastosowanych środków ochrony fizycznej i technicznej przeznaczonych do ochrony zasobów kryptograficznych, w tym prowadzenie sprawdzeń poziomu bezpieczeństwa;
- 6) informowanie nadrzędnego OBSŁ o potrzebach w zakresie zabezpieczenia w zasoby kryptograficzne JO;
- 7) nadzorowanie przekazywania zasobów kryptograficznych poza JO, w tym udzielanie instruktażu osobom realizującym przewóz;
- 8) opracowanie instrukcji pracy KK, zgodnie z załącznikiem nr 1 do zarządzenia;
- 9) opracowanie instrukcji postępowania z zasobami kryptograficznymi w sytuacjach zagrożenia, której zawartość określa Szef KOGD w zaleceniach SKW dotyczących zarządzania materiałami kryptograficznymi;
- 10) opracowanie instrukcji konwojowania zasobów kryptograficznych, zgodnie z załącznikiem nr 2 do zarządzenia;
- 11) wnioskowanie do KJO o kierowanie osób z OBSŁ oraz osób spoza tego organu (posiadających kwalifikacje techniczne związane z informatyką, elektroniką bądź kierunkami pokrewnymi), które mogłyby w przyszłości objąć stanowiska w OBSŁ, na organizowane specjalistyczne kursy i szkolenia;
- 12) dokumentowanie przeprowadzonych instruktaży i szkoleń z zakresu bezpieczeństwa materiałów kryptograficznych;
- 13) wnioskowanie do KJO o wydanie lub anulowanie CUK;
- 14) przeprowadzenie szkolenia co najmniej raz w roku, z zakresu ochrony materiałów kryptograficznych dla osób posiadających CUK;
- 15) prowadzenie ewidencji wydanych CUK oraz monitorowanie ich statusu;
- 16) niezwłoczne meldowanie KJO oraz Oficerowi BSŁ szczebla nadrzędnego o stwierdzonych incydentach kryptograficznych mających wpływ na bezpieczeństwo zasobów kryptograficznych;
- 17) nadzorowanie wykorzystywania, obsługiwanie oraz ochrony produktów kryptograficznych;
- 18) planowanie i organizowanie inspekcji kryptograficznych w bezpośrednio nadzorowanych OBSŁ – nie rzadziej niż co trzy lata;

- 19) monitorowanie terminu ważności certyfikatów wystawionych dla poszczególnych produktów kryptograficznych;
- 20) udział w planowaniu i organizowaniu kontroli materiałów niejawnych w KK, prowadzonej w ramach kontroli okresowej ewidencji, materiałów i obiegu dokumentów;
- 21) opracowywanie zapotrzebowań na zasoby kryptograficzne;
- 22) dokonywanie, nie rzadziej niż raz na kwartał, analizy rejestru zdarzeń systemu sygnalizacji włamań i napadu dla pomieszczeń KK oraz sprawdzeń działania personelu ochrony;
- 23) zarządzanie materiałami kryptograficznymi wykorzystywanymi na potrzeby ochrony informacji w systemach łączności eksploatowanych w JO oraz w JO podległych, w tym planowanie wykorzystywania tych materiałów.

§ 5. 1. Obsługę KK stanowi wyznaczony rozkazem (decyzją) KJO etatowy personel tej kancelarii, w tym:

- 1) kierownik KK;
- 2) zastępca (zastępcy) kierownika KK;
- 3) dodatkowo w zależności od potrzeb:
 - a) pracownik KK,
 - b) szyfrant/starszy szyfrant,
 - c) kurier kryptografii/starszy kurier kryptografii,
 - d) kurier-kierowca,
 - e) kierowca-kurier.

2. Na stanowiska etatowego personelu KK wyznacza się żołnierza zawodowego, funkcjonariusza lub pracownika KK, który posiada poświadczenia bezpieczeństwa odpowiednie do klauzuli tajności KK, oraz zasobów kryptograficznych planowanych do przetwarzania w JO, aktualne zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych oraz szkolenie/szkolenia specjalistyczne określone w zaleceniach SKW w sprawie sposobu oraz trybu powoływania i odwoływania kancelarii kryptograficznej.

3. Personelowi KK nie powierza się dodatkowych zadań nie związanych z funkcjonowaniem KK.

4. Do obowiązków kierownika KK należy:

- 1) kierowanie funkcjonowaniem KK oraz pracą personelu KK;
- 2) przyjmowanie, rejestrowanie, przechowywanie, przekazywanie zasobów kryptograficznych otrzymywanych, wysyłanych oraz wytwarzanych na potrzeby wewnętrzne JO oraz jednostek zaopatrywanych;
- 3) współudział w planowaniu i prowadzeniu inspekcji kryptograficznych w nadzorowanych OBSŁ;
- 4) prowadzenie aktualnej ewidencji zasobów kryptograficznych;
- 5) sporządzanie KWP, której wzór stanowi załącznik nr 3 do zarządzenia i udostępniania go w dedykowanym systemie informatycznym lub przesyłanie do kancelarii współpracujących oraz do DKWOC (CKK MON) i KOGD (GKK SKW);
- 6) dokonywanie sprawdzeń zasobów kryptograficznych;
- 7) sprawdzanie poświadczeń bezpieczeństwa i CUK użytkowników korzystających z materiałów kryptograficznych;
- 8) wprowadzanie otrzymywanych zmian do posiadanych publikacji kryptograficznych;
- 9) meldowanie Oficerowi BSŁ o każdym stwierdzonym naruszeniu bezpieczeństwa fizycznego i kryptograficznego oraz o możliwym lub rzeczywistym zagrożeniu bezpieczeństwa zasobów kryptograficznych;
- 10) udostępnianie i wydawanie materiałów kryptograficznych osobom, o których mowa w pkt 7;

- 11) udzielanie instruktażu dla użytkowników pobierających zasoby kryptograficzne za pokwitowaniem odręcznym;
- 12) kompletowanie zasobów kryptograficznych oraz przygotowywanie akt kryptograficznych do archiwizacji;
- 13) przesyłanie do zaopatrującej KK raportów o stanie posiadanych materiałów kryptograficznych, w przypadku braku EOZK;
- 14) niszczenie zasobów kryptograficznych zgodnie z obowiązującymi w tym zakresie przepisami oraz zaleceniami SKW;
- 15) zmiana kodów i rotacja kluczy zabezpieczających pomieszczenia KK;
- 16) obsługa produktów kryptograficznych;
- 17) realizacja zadań zleconych przez Oficera BSŁ związanych z tematyką kryptograficzną.

5. Do obowiązków zastępcy kierownika KK należy wykonywanie zadań, o których mowa w ust. 4 pkt 2-17, a podczas nieobecności kierownika KK kierowaniem funkcjonowania KK oraz pracą personelu KK.

6. Do obowiązków szyfranta/starszego szyfranta należy:

- 1) obsługa produktów kryptograficznych;
- 2) w przypadku, gdy etatowo wchodzi w skład KK, wykonywanie zadań, o których mowa w ust. 4 pkt 2-17.

7. Do obowiązków pracownika KK należy wykonywanie zadań, o których mowa w ust. 4 pkt 2-17.

8. Do obowiązków kuriera kryptografii/starszego kuriera kryptografii, kuriera-kierowcy oraz kierowcy-kuriera należy:

- 1) przewóz przesyłek kryptograficznych;
- 2) udział w czynnościach związanych z organizacją i przygotowaniem transportu przesyłek kryptograficznych;
- 3) w przypadku, gdy etatowo wchodzi w skład KK, wykonywanie zadań, o których mowa w ust. 4 pkt 2-17.

9. Szczegółowy zakres obowiązków personelu KK określa Oficer BSŁ.

§ 6. 1. Przekazanie obowiązków na stanowisku kierownika KK odbywa się komisyjnie.

2. Komisję powołuje KJO.

3. W skład Komisji wchodzi:

- 1) co najmniej jeden przedstawiciel OBSŁ, pełniący rolę przewodniczącego Komisji;
- 2) co najmniej jeden przedstawiciel nadrzędnej KK;
- 3) osoba zdająca obowiązki kierownika KK;
- 4) osoba przyjmująca obowiązki kierownika KK.

4. Wniosek o wyznaczenie przedstawiciela nadrzędnej KK do składu Komisji, o której mowa w ust. 3, przesyła się co najmniej na 14 dni przed planowanym terminem zmiany przekazania obowiązków kierownika KK.

5. Wynikiem pracy Komisji, o której mowa w ust. 3, jest raport inwentaryzacji zasobów kryptograficznych oraz protokół z przekazania obowiązków kierownika KK, który zawiera:

- 1) podstawę przekazania obowiązków;
- 2) nazwy i numery urządzeń ewidencyjnych, na podstawie których dokonano sprawdzenia stanu faktycznego zasobów kryptograficznych pozostających na ewidencji KK oraz pozycje zapisów w tych urządzeniach;
- 3) numer ewidencyjny raportu inwentaryzacji zasobów kryptograficznych;
- 4) porównanie stanu faktycznego zasobów zaewidencjonowanych w KK ze stanem ewidencyjnym;

5) ewentualne uwagi osoby przyjmującej obowiązki kierownika KK dotyczące ujawnionych nieprawidłowości w zakresie obiegu zasobów kryptograficznych.

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

7. Protokół przekazania obowiązków podpisują członkowie Komisji, o której mowa w ust. 3, a zatwierdza KJO.

8. Zatwierdzone przez KJO egzemplarze protokołu przechowuje się w nadrzędnej i własnej KK.

9. Po przyjęciu obowiązków, kierownik KK sporządza KWP i udostępnia ją w dedykowanym systemie informatycznym lub w przypadku braku dostępu do wyżej wymienionego systemu, przesyła do kancelarii współpracujących oraz do DKWOC (CKK MON) i KOGD (GKK SKW).

§ 7. 1. Na czas nieobecności kierownika KK i jego zastępcy poniżej 60 dni, obowiązki kierownika pełni osoba z personelu KK, wyznaczona w rozkazie lub decyzji KJO.

2. W przypadku, gdy:

- 1) w KK pozostaje wyłącznie jedna osoba ze składu etatowego personelu KK, KJO może zwrócić się z wnioskiem do Szefa KOGD o wyrażenie zgody na czasowe włączenie do składu tej kancelarii osoby niebędącej w OBSŁ, która spełnia wymagania, o których mowa w § 5 ust. 2;
- 2) istnieje uzasadniona potrzeba włączenia dodatkowej osoby do składu KK, KJO może zwrócić się z wnioskiem do Szefa KOGD o wyrażenie zgody na czasowe włączenie do składu tej kancelarii osoby niebędącej w OBSŁ, która spełnia wymagania, o których mowa w § 5 ust. 2.

3. W szczególnie uzasadnionych przypadkach, za zgodą Szefa KOGD, do składu kancelarii można wyznaczyć Oficera BSŁ lub Zastępcę Oficera BSŁ spełniającego wymagania, o których mowa w § 5 ust. 2.

4. Dla OBSŁ nadzorowanych przez DKWOC zgodę, o której mowa w ust. 3, wydaje Dowódca KWOC, o czym również informuje pisemnie Szefa KOGD.

5. Na czas nieobecności kierownika KK powyżej 60 dni przekazanie obowiązków kierownika KK realizuje Komisja w sposób określony w § 6.

6. Przewodniczący Komisji, o której mowa w § 6 ust. 3, do czasu przekazania obowiązków oznakowuje urządzenia do przechowywania informacji niejawnych, szafy, sejfy i skrzynie z nieprzekazanymi zasobami kryptograficznymi swoją numerową pieczęcią do teczki pracy lub w inny sposób jednoznacznie wskazujący dane, pozwalające na identyfikację przewodniczącego komisji.

§ 8. 1. W JO, w których powołanie KK jest niezasadne ze względu na zbyt małą ilość wykorzystywanych materiałów kryptograficznych lub ze względów organizacyjnych, wykorzystywanie materiałów kryptograficznych realizowane jest na podstawie Procedur zaopatrywania w materiały kryptograficzne, zwanych dalej „Procedurami zaopatrywania”, stanowiącymi porozumienie z KJO posiadającej KK, zwanego dalej „KJO zaopatrującym”. Procedury zaopatrywania podlegają uzgodnieniu z Dowódcą KWOC oraz akceptacji Szefa KOGD.

2. W przypadku, o którym mowa w ust. 1, KJO nieposiadającej KK zwanym dalej „KJO zaopatrywanym”:

- 1) powołuje w rozkazie (decyzji) OBSŁ, w skład którego wchodzi Oficer BSŁ i Zastępca Oficera BSŁ;
- 2) opracowuje Procedury zaopatrywania zgodnie z wytycznymi zawartymi w załączniku nr 4 do zarządzenia;
- 3) podpisane Procedury zaopatrywania przesyła do KJO zaopatrującego.

3. Procedury zaopatrywania podpisane przez KJO zaopatrującego przesyłane są kanałem kryptograficznym z wykorzystaniem EOZK do Dowódcy KWOC.

4. Otrzymane Procedury zaopatrywania Dowódca KWOC uzgadnia i przesyła do Szefa KOGD.

5. Szef KOGD informuje pisemnie Dowódcę KWOC o akceptacji Procedur zaopatrywania.

6. Dowódca KWOC informuje pisemnie KJO zaopatrującego o akceptacji Procedur zaopatrywania.

7. W przypadku stwierdzonych uwag przez DKWOC lub KOGD, Procedury zaopatrywania odsyłane są do nadawcy celem ich ponownego opracowania.

8. KJO zaopatrujący informuje KJO zaopatrywanego o możliwości zaopatrywania w materiały kryptograficzne.

9. W szczególnie uzasadnionych przypadkach za zgodą i na warunkach określonych przez Szefa KOGD, KJO może eksploatować materiały kryptograficzne bez powoływania OBSŁ.

10. W przypadku, o którym mowa w ust. 9, za nadzór nad użytkowaniem oraz bezpieczeństwem materiałów kryptograficznych odpowiada Oficer BSŁ JO udostępniającej ten materiał na zasadach określonych w dokumentacji bezpieczeństwa systemu łączności.

Rozdział 3

Bezpieczeństwo materiałów kryptograficznych

§ 9. 1. Zgodę na dostęp do materiałów kryptograficznych w danej JO wydaje KJO, zgodnie z zasadą wiedzy niezbędnej.

2. Dokumentem potwierdzającym zgodę KJO na dostęp do materiałów kryptograficznych jest CUK.

3. Wzór CUK określa formularz 104 PL stanowiący załącznik nr 5 do zarządzenia.

4. Zgodę, o której mowa w ust. 1, stwierdza się w rozkazie lub decyzji KJO.

5. W celu wydania CUK, Oficer BSŁ:

1) określa klauzulę tajności oraz zakres dostępu do materiałów kryptograficznych wynikający z realizowanych czynności wymagających użycia tych materiałów przez osobę, której zostanie wydany CUK;

2) przeprowadza instruktaż w zakresie bezpieczeństwa materiałów kryptograficznych, zgodnie z tematyką określoną w załączniku nr 6 do zarządzenia.

6. Oficerowi BSŁ instruktażu, o którym mowa w ust. 5 pkt 2, udziela:

1) w JO w której powołano KK – Oficer BSŁ szczebla nadrzędnego;

2) w JO zaopatrywanej w materiały kryptograficzne na podstawie Procedur zaopatrywania – Oficer BSŁ JO zaopatrującej.

7. CUK sporządzany jest w egzemplarzu pojedynczym i przechowywany przez Oficera BSŁ.

8. Cyfrowe odwzorowanie CUK Oficer BSŁ zamieszcza w dedykowanym systemie informatycznym. Cyfrowe odwzorowanie CUK dostępne jest dla personelu właściwej KK.

9. Na potrzeby wykonywania czynności służbowych poza JO związanych z dostępem do materiałów kryptograficznych, CUK wydaje się użytkownikowi lub udostępnia się jego cyfrowe odwzorowanie OBSŁ innej JO w dedykowanym systemie informatycznym.

10. Fakt pobrania CUK ewidencjonuje się w „Książce ewidencji wydanych CUK”, której wzór określa załącznik nr 7 do zarządzenia.

11. Zabrania się udostępniania materiałów kryptograficznych 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. Sytuacja, o której mowa w ust. 12, obowiązuje również osoby, które przestały pełnić obowiązki służbowe związane z ochroną kryptograficzną lub nie posiadają już dostępu do materiałów kryptograficznych.

14. CUK wystawiany jest osobom posiadającym:

- 1) odpowiednie do klauzuli tajności aktualne poświadczenie bezpieczeństwa lub certyfikat NATO (UE) wydany przez Agencję Bezpieczeństwa Wewnętrznego albo upoważnienie, o którym mowa w art. 21 ust. 4 pkt 1 ustawy;
- 2) aktualne zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych.

15. W szczególnie uzasadnionych przypadkach, KJO może wydać zgodę na dostęp do materiałów kryptograficznych osobie spoza JO, która ma wykonywać obowiązki służbowe w danej JO.

16. W przypadkach, o których mowa w ust. 15, po spełnieniu wymagań określonych w ust. 14, KJO może wydać zgodę na dostęp do materiałów kryptograficznych osobie spoza JO po uzyskaniu zgody Szefa KOGD.

17. Wystawiony CUK zachowuje ważność we wszystkich JO.

18. Oficer BSŁ prowadzi co najmniej raz w roku szkolenie dla osób posiadających CUK.

19. Oficer BSŁ zapoznaje KJO z zagadnieniami, określonymi w załączniku nr 6 do zarządzenia.

20. Słuchaczom kursów specjalistycznych, których program szkolenia narzuca konieczność zapoznawania się z materiałami kryptograficznymi KJO prowadzącej szkolenie zamiast wydania indywidualnego CUK może wydać grupowy CUK, którego wzór określa załącznik nr 8 do zarządzenia.

21. Grupowy CUK jest ważny tylko w okresie trwania szkolenia.

22. Dopuszcza się wydawanie grupowego CUK dla użytkowników z różnych JO, delegowanych do wspólnego wykonania określonych zadań.

23. Oficer BSŁ prowadzi w dedykowanym systemie informatycznym ewidencję:

- 1) CUK – ewidencja zawiera dane osób posiadających CUK oraz zakres, do którego uprawnieni mają dostęp;
- 2) szkoleń – ewidencja zawiera terminy odbytych szkoleń przez użytkowników, etatowego KJO i jego zastępców.

24. CUK nie wydaje się:

- 1) KJO i ich etatowym zastępcom w JO, w których powołano OBSŁ;
- 2) Szefowi Sztabu Generalnego Wojska Polskiego oraz jego zastępcom;
- 3) przedstawicielom SKW prowadzącym audyt bezpieczeństwa systemów łączności, w których zastosowano produkty kryptograficzne;
- 4) osobom realizującym zadania w zakresie wdrażania i serwisowania produktów kryptograficznych, niewymagające dostępu do dokumentów kryptograficznych;
- 5) użytkownikom produktów kryptograficznych oraz urządzeń oznaczonych symbolem CCI, 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 wykonującym czynności wynikające z ustawy;
- 8) inspektorom bezpieczeństwa teleinformatycznego.

25. W uzasadnionych przypadkach wiarygodność danych osobowych określonych w CUK należy potwierdzić innym dokumentem stwierdzającym tożsamość danej osoby.

26. Przy zmianie zakresu dostępu lub w przypadku utraty ważności innych zapisów w „części I” CUK, CUK jest anulowany i procedurę wydania CUK przeprowadza się ponownie.

27. CUK anuluje się 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, funkcjonariusza lub rozwiązania stosunku pracy z pracownikiem;
- 5) zmiany danych osobowych;
- 6) upływu terminu obowiązywania lub cofnięcia dokumentu stanowiącego podstawę jego wydania.

28. Anulowanie CUK wiąże się z cofnięciem zgody, o której mowa w ust. 1. Fakt ten stwierdza się w rozkazie lub decyzji KJO i poprzedza się instruktażem udzielanym przez Oficera BSŁ, o tematyce określonej w pkt 1-3 załącznika nr 6 do zarządzenia.

29. W przypadku:

- 1) konieczności anulowania CUK z powodu nieobecności przekraczającej okres 60 dni oraz braku możliwości przeprowadzenia instruktażu, Oficer BSŁ wpisuje w poz. 10 formularza CUK powód nieudzielenia instruktażu;
- 2) komisyjnego rozliczenia użytkownika z JO, przewodniczący komisji powołanej do jego rozliczenia potwierdza ten fakt własnoręcznym podpisem w poz. 10 formularza CUK.

30. Anulowany CUK przechowuje się w KK przez okres 2 lat a następnie Oficer BSŁ niszczy formularz poświadczając ten fakt w dedykowanym systemie informatycznym. W przypadku rozformowania JO formularze anulowanych CUK niepodlegających zniszczeniu przekazywane są do następcy prawnego rozformowanej JO i niszczone po upływie 2 lat od daty jego anulowania.

31. W przypadku niezamierzonego zniszczenia lub zagubienia CUK, Oficer BSŁ informuje pisemnie KJO o zaistniałym fakcie.

32. CUK, o którym mowa w ust. 31, anuluje się w rozkazie (decyzji) KJO.

§ 10. 1. Materiały kryptograficzne, od wstępnego projektu, badań, wytworzenia, wdrożenia do produkcji, a także w trakcie eksploatacji, aż do chwili ich fizycznego zniszczenia, podlegają ewidencji w KK oraz kontroli i nadzorowi przez OBSŁ.

2. Niejawne materiały kryptograficzne oznacza się zgodnie z obowiązującymi przepisami w sprawie oznaczania materiałów niejawnych i zapewnia się im ochronę na poziomie odpowiednim do klauzuli tajności materiału.

3. Urządzenia oznaczone symbolem CCI oraz urządzenia kryptograficzne nieposiadające nadanej klauzuli tajności, stanowią materiał jawny podlegający szczególnej ochronie. Jednakże ze względu na zastosowanie w ich konstrukcjach mechanizmów kryptograficznych, urządzenia te podlegają ewidencji w KK.

4. Urządzeniom oznaczonym symbolem CCI oraz urządzeniom kryptograficznym nieposiadającym nadanej klauzuli tajności w każdej sytuacji zapewnia się ochronę przed ich utratą, kradzieżą, sabotażem, działalnością szpiegowską oraz nieautoryzowanym dostępem.

5. Urządzenia oznaczone symbolem CCI oraz urządzenia kryptograficzne nieposiadające nadanej klauzuli tajności, które nie są wykorzystywane w bieżącej eksploatacji, powinny być przechowywane w KK lub w innym pomieszczeniu zapewniającym ochronę przed utratą, kradzieżą, sabotażem lub działalnością szpiegowską, spełniającym wymagania klimatyczno-temperaturowe, określone dla danego typu sprzętu w instrukcjach eksploatacji i kartach katalogowych.

6. Odpowiedzialność za prawidłowe zorganizowanie zabezpieczenia urządzeń oznaczonych symbolem CCI oraz urządzeń kryptograficznych nieposiadających nadanej klauzuli tajności spoczywa na KJO.

7. Bezpośrednią odpowiedzialność za bezpieczeństwo eksploatowanych urządzeń oznaczonych symbolem CCI oraz urządzeń nieposiadających nadanej klauzuli tajności, w tym ich transport, przechowywanie i w trakcie operacyjnego użycia, ponosi użytkownik.

8. Urządzenia oznaczone symbolem CCI z zaimplementowanymi niejawnymi dokumentami kryptograficznymi należy chronić jak materiał niejawny o najwyższej klauzuli tajności wprowadzonych dokumentów kryptograficznych jeżeli doktryna bezpieczeństwa wydana przez The Military Committee Communications and Information Systems Security and Evaluation Agency (SECAN) dotycząca wykorzystania produktu kryptograficznego nie stanowi inaczej.

9. Dostęp do urządzeń oznaczonych symbolem CCI oraz urządzeń kryptograficznych bez zaimplementowanych niejawnych dokumentów kryptograficznych, nie wymaga posiadania przez użytkownika poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych.

10. Dostęp do urządzeń oznaczonych symbolem CCI z zaimplementowanymi niejawnymi dokumentami kryptograficznymi, wymaga posiadania przez użytkownika odpowiedniego do klauzuli tajności dokumentów poświadczenia bezpieczeństwa.

Rozdział 4

Sposób określania poziomu zagrożeń

§ 11. 1. Dokumentację, o której mowa w art. 43 ust. 4 ustawy, określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą w JO opracowuje się na podstawie:

- 1) załącznika nr 1 do rozporządzenia wydanego na podstawie art. 47 ust. 1 pkt 1 i 3-6 ustawy;
- 2) informacji otrzymanych od SKW, Żandarmerii Wojskowej, Policji lub osób funkcjonujących odpowiedzialnych za ochronę obiektów wojskowych, dotyczących ewentualnych zagrożeń związanych z działalnością obcych służb specjalnych, sabotażu, zamachu terrorystycznego lub innej działalności przestępczej;
- 3) wyników działalności kontrolnej i ocen stanu zabezpieczenia informacji niejawnych i przeglądów stanu ochrony fizycznej informacji niejawnych.

2. W przypadku wzrostu poziomu zagrożeń, w celu zmniejszenia ryzyka do akceptowalnego poziomu, wzmacnia się system bezpieczeństwa, w tym w szczególności poprzez zastosowanie rozwiązań organizacyjnych, dostępnych środków ochrony, stałej ochrony fizycznej do czasu powrotu do stanu pierwotnego bądź wyeliminowania czynnika powodującego wzrost zagrożenia.

Rozdział 5

Dobór i stosowanie środków bezpieczeństwa fizycznego

§ 12. 1. KK, w których przechowuje się i wykorzystuje zasoby kryptograficzne, z uwagi na wysoki poziom zagrożenia związany z utratą informacji niejawnych, lokalizuje się w pomieszczeniach z zastosowanymi środkami bezpieczeństwa fizycznego.

2. W zależności od poziomu zagrożeń, w KK stosuje się adekwatne do poziomu zagrożeń środki bezpieczeństwa fizycznego dobrane według załącznika nr 9 do zarządzenia.

3. Pomieszczenia KK powinny w szczególności spełniać wymagania określone w części III załącznika nr 9 do zarządzenia:

- 1) konstrukcja pomieszczenia – uzyskuje co najmniej 2 pkt w kategorii K2;

2) drzwi do pomieszczenia – co najmniej Typ 3 kategoria K3, wyposażone w dwa zamki, w tym jeden zamek szyfrowy określony w Typ 4 kategoria K3;

3) okna pomieszczenia – Typ 4 kategoria K4.

4. Pomieszczenia KK, powinny posiadać:

1) kanały wentylacyjne i techniczne zabezpieczone w sposób uniemożliwiający przedostanie się do pomieszczenia z zewnątrz;

2) system alarmowy zbudowany z certyfikowanych urządzeń, spełniający wymagania eksploatacyjno-techniczne dla XIX grupy SpW – Systemy i urządzenia specjalistyczne do ochrony obiektów. Dopuszcza się dalsze stosowanie zainstalowanych systemów alarmowych wykonanych zgodnie z Polską Normą PN-EN 50131-1 Systemy alarmowe.

5. Do przechowywania zasobów kryptograficznych wykorzystuje się niżej wymienione urządzenia:

1) szafy stalowe klasy C – do przechowywania zasobów kryptograficznych zawierających informacje niejawne oznaczonych klauzulą „ściśle tajne”, a także „tajne”, „poufne” i „zastrzeżone”;

2) szafy stalowe klasy B – do przechowywania zasobów kryptograficznych zawierających informacje niejawne oznaczonych klauzulą „tajne”, a także „poufne” i „zastrzeżone”;

3) szafy stalowe klasy A – do przechowywania zasobów kryptograficznych zawierających informacje niejawne oznaczonych klauzulą „poufne”, a także „zastrzeżone”.

6. Sposób przechowywania zasobów kryptograficznych o klauzuli „zastrzeżone” w urządzeniach innych niż wymienione w ust. 5 określa się w instrukcji, o której mowa w art. 43 ust. 5 ustawy.

7. Klasyfikację i wymagania techniczne urządzeń, o których mowa w ust. 5, określa załącznik nr 10 do zarządzenia.

8. KK wyposaża się dodatkowo w:

1) urządzenia do niszczenia papierowych zasobów kryptograficznych, których wymiary ścinka nie przekraczają wartości 1 mm x 5 mm;

2) narzędzia dewastacyjne do niszczenia fizycznego zasobów kryptograficznych;

3) pojemniki lub worki służące do przechowywania zasobów kryptograficznych przeznaczonych do zniszczenia oraz do ewakuacji;

4) przycisk medyczny służący do powiadamiania personelu ochrony o zagrożeniu życia;

5) regały, szafy meblowe lub meble przeznaczone do przechowywania teczek akt kryptograficznych;

6) sprzęt kwaterunkowo-biurowy.

9. Do czasu wyposażenia KK w urządzenie do niszczenia papierowych zasobów kryptograficznych, o którym mowa w ust. 8 pkt 1, zezwala się na wykorzystywanie urządzeń do niszczenia:

1) krajowych papierowych materiałów niejawnych w zależności od klauzuli, zgodnie z zarządzeniem Nr 58/MON Ministra Obrony Narodowej z dnia 11 grudnia 2017 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych (Dz. Urz. Min. Obr. Nar. poz. 226 oraz z 2019 r. poz. 137);

2) papierowych materiałów niejawnych NATO, zgodnie z Directive on the Security of NATO Classified Information AC/35-D/2002-REV 5;

3) papierowych materiałów niejawnych UE, zgodnie z IA Security Guidelines on the Management of EU crypto material and COMSEC items IASG 2-03.

10. Organizując KK należy wydzielić pomieszczenia z przeznaczeniem do:

1) pracy personelu KK;

2) przyjmowania interesantów.

11. W zależności od potrzeb organizując KK wydziela się dodatkowe pomieszczenia z przeznaczeniem na:

- 1) magazynowanie zasobów kryptograficznych;
- 2) eksploatację systemów łączności;
- 3) pomieszczenie socjalne dla personelu KK.

12. W szczególnie uzasadnionych przypadkach, uniemożliwiających spełnienie warunków, o których mowa w ust. 2-4 oraz ust. 8, po przedstawieniu alternatywnych rozwiązań w zakresie zabezpieczeń fizycznych i technicznych oraz uzyskaniu pozytywnej opinii Dowódcy KWOC, zgodę na zastosowanie alternatywnych środków bezpieczeństwa udziela Szef KOGD.

§ 13. 1. Dopuszcza się lokalizowanie stacjonarnych KK w MKK, PKK i PKKs, zwanych dalej „kontenerami”.

2. Kontenery, w których mają być przechowywane materiały kryptograficzne, powinny spełniać wymagania konstrukcyjne oraz wymagania zabezpieczenia fizycznego i technicznego, określone w załączniku nr 11 do zarządzenia, z uwzględnieniem konieczności uzyskania pozytywnej opinii wydanej przez SKW potwierdzającej spełnienie wymagań w zakresie zabezpieczenia fizycznego i technicznego.

3. Wszelkie odstępstwa w zakresie zabezpieczeń fizycznych i technicznych kontenerów, wymagają zgody Szefa KOGD.

§ 14. 1. Dokumenty kryptograficzne bieżącej i przyszłej edycji należy przechowywać w urządzeniach do przechowywania informacji niejawnych, o których mowa w § 12 ust. 5.

2. Krajowe i międzynarodowe zasoby kryptograficzne mogą być przechowywane w jednym urządzeniu do przechowywania informacji niejawnych pod warunkiem, że jego konstrukcja pozwala na ich fizyczne rozdzielenie i zamknięcie w odrębnych skrytkach.

3. W przypadku, o którym mowa w ust. 2, klasa urządzenia musi uwzględniać klauzulę tajności najwyższej sklasyfikowanego zasobu kryptograficznego przechowywanego w tym urządzeniu.

4. Nieeksploatowane produkty kryptograficzne z wprowadzonymi dokumentami kryptograficznymi należy deponować w pomieszczeniach zabezpieczonych stosownie do maksymalnej klauzuli tajności produktu kryptograficznego i wprowadzonego dokumentu kryptograficznego.

5. W KK, mogą być eksploatowane systemy łączności przetwarzające informacje niejawne.

6. Eksploatacja jawnych urządzeń faksowych i systemów podłączonych do sieci INTERNET wymaga zgody Szefa KOGD.

7. Zgoda, o której mowa w ust. 6, nie jest wymagana dla stacjonarnych aparatów telefonicznych.

§ 15. 1. Wszystkie pomieszczenia, w których przetwarzane są zasoby kryptograficzne o klauzuli „poufne” lub wyższej powinny posiadać zabezpieczenie okien uniemożliwiające wgląd z zewnątrz.

2. Zasoby kryptograficzne oznaczone klauzulą „poufne”, „tajne” i „ściśle tajne”, w innych niż KK pomieszczeniach służbowych, niespełniających kryteriów punktacji określonych w załączniku nr 9 do zarządzenia, należy przechowywać w urządzeniach do przechowywania materiałów niejawnych oraz należy spełnić jeden z następujących warunków:

- 1) pomieszczenie jest wyposażone w system alarmowy określony w Typ 3 kategoria K9;
- 2) pomieszczenie jest chronione całodobowo przez personel ochrony posiadający odpowiednie poświadczenie bezpieczeństwa dostosowane do klauzuli chronionych zasobów;
- 3) strefa jest chroniona całodobowo przez personel ochrony w formie posterunku lub patroli zorganizowanych, w sposób wynikający z określonego poziomu zagrożeń, zgodnie z zasadami określonymi w kategorii K10 w części III załącznika nr 9 do zarządzenia.

3. W przypadku produktów kryptograficznych zabezpieczających pracę funkcjonujących systemów łączności wymogu przechowywania ich w urządzeniach do przechowywania materiałów niejawnych nie stosuje się.

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

5. W przypadku platform bojowych niebędących w dyżurach bojowych, dopuszcza się pozostawienie produktów kryptograficznych na platformach, pod warunkiem zapewnienia im stałej ochrony na stanowiskach parkowania (przechowywania).

6. Za zapewnienie bezpieczeństwa zasobom kryptograficznym w tym za kontrolę wszystkich miejsc w JO, w których są przechowywane i wykorzystywane te zasoby, odpowiada Officer BSL danej JO oraz pełnomocnik ochrony, jeżeli zasoby kryptograficzne stanowią materiał niejawny, w stosunku do zabezpieczeń fizycznych tych miejsc.

7. Zabrania się przechowywania zasobów kryptograficznych w pomieszczeniach zlokalizowanych poza strefami ochronnymi.

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

§ 16. 1. Po zakończeniu pracy, personel KK zamyka i zabezpiecza urządzenia do przechowywania informacji niejawnych oraz pomieszczenia KK.

2. Plan ochrony informacji niejawnych JO określa zasady zdawania, przechowywania i wydawania:

- 1) kluczy użytku bieżącego do pomieszczeń KK i urządzeń do przechowywania informacji niejawnych;
- 2) kluczy zapasowych do pomieszczeń KK i urządzeń do przechowywania informacji niejawnych;
- 3) kodów zamków szyfrowych do pomieszczeń KK i urządzeń do przechowywania informacji niejawnych;
- 4) kodów administratora systemu alarmowego.

3. Klucze, o których mowa w ust. 2 pkt 2, należy przechowywać, w sposób zapewniający fizyczne ich oddzielenie od kodów, o których mowa w ust. 2 pkt 3 i 4.

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

5. Kody, o których mowa w ust. 2 pkt 3 i 4, 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 12 do zarządzenia.

6. Zabrania się zapisywania przez użytkowników kodów w inny sposób niż określony w ust. 5, wnoszenia ich oraz kluczy, o których mowa w ust. 2 pkt 1 i 2, poza teren JO.

7. Kody, o których mowa w ust. 2 pkt 3, 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 KK;
- 4) w przypadku ujawnienia lub podejrzenia ujawnienia kodu osobie nieupoważnionej;
- 5) w odstępach czasowych nieprzekraczających 6 miesięcy od ostatniej zmiany kodu.

8. Kody do systemu alarmowego 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 KK zmienia się w przypadku ujawnienia lub podejrzenia ujawnienia kodu osobie nieupoważnionej oraz cyklicznie. Częstotliwość zmiany kodów do systemu alarmowego określa plan ochrony informacji niejawnych JO.

9. W razie utraty lub zagubienia kluczy, o których mowa w ust. 2 pkt 1 i 2, należy wymienić zamki, a o fakcie ich utraty lub zagubienia poinformować niezwłocznie pisemnie KJO.

§ 17. 1. KK na okręcie i pomocniczej jednostce pływającej organizuje się w pomieszczeniach spełniających następujące warunki bezpieczeństwa:

- 1) oddzielonych od innych pomieszczeń trwałymi ścianami uniemożliwiającymi przedostanie się do wewnątrz;
- 2) nieposiadających okien (iluminatorów), a gdy jest to niemożliwe, okna (iluminatory) powinny być zabezpieczone w sposób uniemożliwiający wgląd i wejście z zewnątrz;
- 3) wyposażonych w drzwi wejściowe (włazy) wykonane ze stali, zabezpieczone przed włamaniem, zamykane na dwa zamki mechaniczne o skomplikowanym mechanizmie (lub dwa zamki w tym jeden zamek szyfrowy określony w Typ 4 kategoria K3).

2. Pomieszczenia KK powinny być chronione ogólnookrętową (lub zintegrowaną z zainstalowanym systemem alarmowym) instalacją przeciwpożarową.

3. W pomieszczeniach KK instaluje się systemy alarmowe spełniające wymagania określone co najmniej w Typ 1 kategoria K9 w części III załącznika nr 9 do zarządzenia.

4. W przypadku braku możliwości montażu zabezpieczeń, o których mowa w ust. 1-3, pomieszczenia należy objąć szczególnym nadzorem dyżurnej służby (służby wachtowej) na okręcie lub pomocniczych jednostkach pływających.

5. Podczas postoju w porcie, zasoby kryptograficzne przechowuje się w KK okrętu.

6. W przypadku produktów kryptograficznych zabezpieczających pracę funkcjonujących systemów łączności, ust. 5 nie stosuje się.

§ 18. 1. KJO odpowiada za organizację ochrony zasobów kryptograficznych na pokładach statków powietrznych, która ma na celu zapewnienie stałego nadzoru nad nimi.

2. W JO, w której stacjonują statki powietrzne, za ochronę zasobów kryptograficznych znajdujących się na wyposażeniu tych statków powietrznych, odpowiedzialny jest kierownik tej JO, który stosuje środki ochrony fizycznej uniemożliwiające ujawnienie informacji niejawnych odpowiednio do przechowywanych zasobów.

3. Podczas wykonywania lotu za ochronę zasobów kryptograficznych, znajdujących się na pokładzie statku powietrznego, odpowiada jego dowódca.

4. Po wylądowaniu poza MSD na lotnisku wojskowym na terenie kraju, za ochronę zasobów kryptograficznych znajdujących się na pokładzie statku powietrznego, odpowiedzialny jest dowódca bazy, w której wylądował statek powietrzny.

5. W przypadku lądowania poza MSD na terenie kraju na lotniskach cywilnych lub innych miejscach, w szczególności: lądowanie awaryjne, lądowanie w miejscu przygodnym, lądowanie w ramach zadań poszukiwawczo-ratowniczych, za ochronę zasobów kryptograficznych znajdujących się na pokładzie statku powietrznego, odpowiedzialny jest jego dowódca. Ochrona fizyczna statku powietrznego w przypadku lotniska cywilnego jest sprawowana przez służby ochrony lotniska (SOL), zgodnie z miejscowymi procedurami, a jeżeli jest to niewystarczające to przez ŻW.

6. W przypadku lądowania poza MSD poza granicami kraju na terenie państw NATO – ochrona fizyczna sprawowana jest przez miejscowe służby ochronne zgodnie z miejscowymi procedurami, jeżeli jest niewystarczająca – przez organa policji wojskowej.

7. W przypadku lądowania poza MSD poza granicami kraju na terenie państw spoza NATO niebędących teatrem działań wojennych stosuje się procedury postępowania określone w dokumentach normatywnych NATO oraz w ewentualnych porozumieniach w przypadku planowanych lądowań.

8. W przypadkach, o których mowa w ust. 5-7, do czasu stwierdzenia przez dowódcę statku powietrznego, że ochrona zasobów kryptograficznych jest wystarczająca, za zapewnienie właściwej ochrony odpowiada dowódca statku powietrznego.

9. W sytuacji gdy lądowanie statku powietrznego nastąpi na terenie obcego państwa, które nie jest sojusznikiem Rzeczypospolitej Polskiej, za ochronę zasobów kryptograficznych, znajdujących się na pokładzie statku powietrznego odpowiada jego dowódca. W sytuacji krytycznej dowódca statku powietrznego nie opuszcza go do czasu, aż uzna, iż jest on bezpieczny.

Rozdział 6

Sprawowanie nadzoru nad funkcjonowaniem Organu Bezpieczeństwa Systemów Łączności

§ 19. 1. Nadzór nad funkcjonowaniem OBSŁ realizowany jest przez nadrzędne OBSŁ w formie inspekcji kryptograficznych lub innej formie kontroli.

2. Inspekcje kryptograficzne w danej JO przeprowadza się cyklicznie przez nadrzędny OBSŁ, nie rzadziej niż co 3 lata.

3. W celu zapewnienia spójnej realizacji inspekcji kryptograficznych, OBSŁ przesyłają pisemną informację o zaplanowanych inspekcjach na dany rok kalendarzowy do nadrzędnego OBSŁ, nie później niż do końca września roku poprzedzającego dany rok.

4. OBSŁ bezpośrednio nadzorowane przez DKWOC przesyłają pisemną informację o zaplanowanych inspekcjach na przyszły rok kalendarzowy do DKWOC nie później niż do końca października roku poprzedzającego.

5. Inspekcja kryptograficzna ma na celu sprawdzenie:

- 1) organizacji i funkcjonowania OBSŁ;
- 2) zastosowanych środków bezpieczeństwa fizycznego i technicznego w pomieszczeniach KK;
- 3) bezpieczeństwa przechowywanych i eksploatowanych zasobów kryptograficznych;
- 4) prowadzenia obiegu zasobów kryptograficznych w KK;
- 5) bezpieczeństwa materiałów kryptograficznych wytwarzanych i przetwarzanych w systemach łączności.

6. W ramach inspekcji kryptograficznej dopuszcza się sprawdzenie JO, zaopatrywanej w materiały kryptograficzne na podstawie Procedur zaopatrywania.

7. W sytuacji, o której mowa w ust. 6, sporządza się odrębny protokół z inspekcji kryptograficznej.

§ 20. 1. Inspekcję kryptograficzną zarządza KJO, właściwy dla OBSŁ przeprowadzającego inspekcję. Wzór planu przeprowadzenia inspekcji kryptograficznej stanowi załącznik nr 13 do zarządzenia.

2. Inspekcję, o której mowa w ust. 1, realizuje co najmniej dwuosobowa komisja złożona z personelu OBSŁ, posiadająca imienne upoważnienie do przeprowadzenia inspekcji kryptograficznej, którego wzór określa załącznik nr 14 do zarządzenia.

3. Dopuszcza się włączenie do składu komisji, o której mowa w ust. 2, innej osoby niezbędnej do prawidłowego przeprowadzenia inspekcji.

4. Wynikiem prac komisji jest Protokół z inspekcji kryptograficznej, którego wzór określa załącznik nr 15 do zarządzenia.

5. Protokół z inspekcji kryptograficznej tworzy się w egzemplarzu pojedynczym i przedstawia do podpisu KJO, w której przeprowadzono inspekcję kryptograficzną.

6. Protokół, o którym mowa w ust. 4, KJO przesyła kanałem kryptograficznym z wykorzystaniem EOZK do nadrzędnych OBSŁ oraz KOGD.

7. W przypadku stwierdzenia uwag, ujętych w protokole, informację o sposobie ich usunięcia KJO przesyła do nadrzędnych OBSŁ oraz KOGD w terminie do 30 dni, od dnia sporządzenia protokołu.

§ 21. W przypadku stwierdzenia incydentu kryptograficznego związanego z naruszeniem bezpieczeństwa zasobów kryptograficznych należy przerwać inspekcję kryptograficzną i zabezpieczyć materiał dowodowy oraz niezwłocznie powiadomić Szefa KOGD.

Rozdział 7

Przewóz przesylek kryptograficznych na terenie Rzeczypospolitej Polskiej

§ 22. 1. Za organizację przewozu zasobów kryptograficznych odpowiada KJO.

2. Przewóz zasobów kryptograficznych pomiędzy KK realizowany jest w postaci przesylek kryptograficznych i odbywa się kanałem kryptograficznym.

3. Na terytorium Rzeczypospolitej Polskiej przewóz przesylek kryptograficznych realizowany jest przez OBSŁ.

4. Poza terytorium Rzeczypospolitej Polskiej przewóz przesylek kryptograficznych realizowany jest przez WSK RP, na zasadach określonych w odrębnych przepisach.

5. Przewóz przesylek kryptograficznych odbywa się na podstawie:

- 1) rozkazu (decyzji) KJO w sprawie wyznaczenia organizatora i składu konwoju;
- 2) instrukcji konwojowania zasobów kryptograficznych;
- 3) planu przeprowadzenia konwoju, opracowanego przez dowódcę konwoju.

6. Plan przeprowadzenia konwoju podlega ewidencji w KK i przechowywany jest zgodnie z jrwą JO, jednak nie krócej niż 12 m-cy od daty zakończenia konwoju.

7. W przypadku produktów kryptograficznych oraz urządzeń oznaczonych symbolem CCI będących integralną częścią sprzętu wojskowego (np. platformy bojowe, sprzęt łączności), przewóz i ochrona tych produktów i urządzeń realizowane są przez etatowe załogi.

§ 23. 1. Wydane użytkownikowi w rejonie prowadzenia działań bojowych, ćwiczeń lub w stanach nadzwyczajnych zasoby kryptograficzne, wykorzystywane na platformach bojowych przewozi się zgodnie z przyjętą taktyką działania wojsk bez konieczności organizowania konwoju.

2. Taktyka działania wojsk musi uwzględniać całodobową ochronę zasobów kryptograficznych podczas przemieszczania i działań poza MSD.

3. Sytuacja, o której mowa w ust. 1, nie ma zastosowania w przypadku przewozu zasobów kryptograficznych do rejonu prowadzenia ćwiczeń lub z tego rejonu.

Rozdział 8

Zasady obiegu zasobów kryptograficznych

§ 24. 1. KK odpowiada za prawidłowy obieg zasobów kryptograficznych w JO.

2. Prowadzi się wspólną ewidencję krajowych i międzynarodowych zasobów kryptograficznych.

3. Podstawowym narzędziem do ewidencji zasobów kryptograficznych jest EOZK.

4. W przypadku braku EOZK w JO dopuszcza się prowadzenie niżej wymienionych urządzeń ewidencyjnych:

- 1) Rejestru teczek materiałów kryptograficznych, dzienników i ksiąg ewidencyjnych, zwany dalej „RTMK”, którego wzór określa załącznik nr 16 do zarządzenia;
- 2) dziennika ewidencyjnego,

- 3) dziennika ewidencji szyfrogramów, którego wzór określa załącznik nr 17 do zarządzenia;
- 4) kartoteki wydanych zasobów kryptograficznych, w skład której wchodzi:
 - a) skorowidz rejestrów wydanych dokumentów, zwany dalej „Skorowidzem RWD”,
 - b) rejestr wydanych dokumentów, zwany dalej „RWD”;
- 5) książki doręczeń przesyłek miejscowych, zwaną dalej „Książką doręczeń”, której wzór określa załącznik nr 18 do zarządzenia;
- 6) książki depozytu zasobów kryptograficznych, zwaną dalej „Książką depozytu”, której wzór określa załącznik nr 19 do zarządzenia;
- 7) dziennika ewidencji wykonanych dokumentów, zwany dalej „DEWD”;
- 8) karty zapoznania się z materiałem niejawnym oznaczonym klauzulą tajności „ŚCIŚLE TAJNE”/„TAJNE”;
- 9) karty ewidencyjnej dokumentu kryptograficznego (formularz AF 54 A PL), której wzór określa załącznik nr 20 do zarządzenia;
- 10) karty ewidencyjnej produktu kryptograficznego (formularz AF 54 B PL), której wzór określa załącznik nr 21 do zarządzenia;
- 11) karty ewidencyjnej publikacji, wydawnictw kryptograficznych oraz dokumentacji technicznej systemów i produktów kryptograficznych (formularz AF 54 C PL), której wzór określa załącznik nr 22 do zarządzenia;
- 12) formularza AF 147 PL przeznaczony do ewidencji kart formularzy SF 153 (PL), którego wzór określa załącznik nr 23 do zarządzenia;
- 13) formularza SF 153 (PL) – raport materiału kryptograficznego, którego wzór określa załącznik nr 24 do zarządzenia;
- 14) formularza wykazów przesyłek (AF 69 PL), którego wzór określa załącznik nr 25 do zarządzenia;
- 15) rejestru wydanych przedmiotów.

5. Wzory dokumentów, o których mowa w:

- 1) ust. 4 pkt 2, 8 i 15, określa rozporządzenie wydane na podstawie art. 47 ust. 1 pkt 2 i 7-11 ustawy;
- 2) ust. 4 pkt 4 i 7, określa zarządzenie Nr 58/MON Ministra Obrony Narodowej z dnia 11 grudnia 2017 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych.

6. W uzasadnionych przypadkach KK może prowadzić także inne urządzenia ewidencyjne niż wymienione w ust. 4.

7. Strony urządzeń ewidencyjnych, o których mowa w ust. 4 pkt 2-4 lit. a i pkt 7 oraz teczki akt kryptograficznych, w formie broszur numeruje się i oznacza w sposób określony w rozporządzeniu wydanym na podstawie art. 6 ust. 9 ustawy. Na ostatniej stronie urządzenia zamieszcza się adnotację o sumarycznej ilości stron poświadczoną podpisem kierownika KK, datą sporządzenia adnotacji i odciskiem pieczęci „Do pakietów”.

8. W urządzeniach ewidencyjnych, o których mowa w ust. 4 pkt 2-4 lit. a i pkt 7, 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 KK i pieczęcią „Do pakietów” oraz wpisuje datę sporządzenia adnotacji.

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

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

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

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

13. Zapisy w EOZK są nieusuwalne, zapis błędny lub omyłkowy wymaga sprostowania przez wykonanie nowego zapisu.

14. W przypadku funkcjonowania w JO EOZK, adnotacje o zmianie lub zniesieniu klauzuli tajności, rejestruje się w formie elektronicznej.

§ 25. 1. RTMK jest nadrzędnym urządzeniem ewidencyjnym w stosunku do innych urządzeń ewidencyjnych prowadzonych przez KK.

2. W RTMK ewidencjonuje się:

- 1) urządzenia ewidencyjne wymienione w § 24 ust. 4 pkt 2-7;
- 2) teczki z dokumentacją „KRYPTO” (każdy tom teczek ewidencjonuje się pod oddzielną pozycją w RTMK).

3. RTMK zakłada się w powołanej KK JO opatrując go adnotacją o ilości kart, poświadczoną pieczęcią urzędową z pełną nazwą JO i podpisem jej kierownika lub osoby przez niego upoważnionej.

4. RTMK nie podlega ewidencji i po rozliczeniu wszystkich zasobów kryptograficznych ujętych na jego ewidencji podlega zdaniu do archiwum po rozformowaniu JO.

5. Ewidencję urządzeń ewidencyjnych i teczek w RTMK prowadzi personel KK w cyklu rocznym, rozpoczynając każdego roku kalendarzowego numerowanie od liczby „1”.

§ 26. 1. Zasoby kryptograficzne, o których mowa w § 2 pkt 1 lit. c, otrzymywane i wysyłane (wchodzące i wychodzące) oraz zasoby kryptograficzne wytworzone na potrzeby wewnętrzne JO rejestruje się w dzienniku ewidencji, z podziałem na zasoby kryptograficzne jawne i niejawne.

2. Dopuszcza się prowadzenie dziennika ewidencji w formie elektronicznej.

3. Dopuszcza się rejestrowanie w jednym dzienniku zasobów kryptograficznych otrzymywanych i wysyłanych, o których mowa w § 2 pkt 1 lit. c, z zastrzeżeniem ust. 4.

4. Dla zasobów kryptograficznych otrzymywanych i wysyłanych, o których mowa w § 2 pkt 1 lit. c, można prowadzić w formie elektronicznej oddzielnie dzienniki ewidencji.

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

6. Po wykorzystaniu wszystkich stron dziennika ewidencji, zakłada się następny tom i zachowuje ciągłość dotychczasowej numeracji.

7. Zarejestrowanie korespondencji otrzymanej polega na:

- 1) opatrzeniu pierwszej strony zasobu kryptograficznego, o którym mowa w § 2 pkt 1 lit. c, pieczęcią wpływu oraz odcisnięciu pieczęci formularzowej na załącznikach, z zastrzeżeniem, iż pieczęci formularzowej nie używa się do załączników w formie dokumentów personalnych, zasobów kryptograficznych, o których mowa w § 2 pkt 1 lit. a i b oraz lit. d, oraz innych zasobów kryptograficznych przesyłanych do akceptacji, uzgodnienia, opiniowania lub podpisu;
- 2) wpisaniu w kolejnej pozycji dziennika ewidencji:
 - a) właściwego symbolu klauzuli tajności zasobu kryptograficznego,
 - b) numeru porządkowego, który wraz z prefiksem w postaci symbolu, o którym mowa w lit. a, stanowi numer ewidencyjny zasobu kryptograficznego, o którym mowa w § 2 pkt 1 lit. c,
 - c) danych ewidencyjnych zasobu kryptograficznego, nadanych przez nadawcę (numer wychodzący i data zarejestrowania),
 - d) informacji o ilości stron zasobu 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 najwyżej sklasyfikowanego załącznika;
- 3) wpisaniu na dokumencie, w odpowiednich polach odcisku pieczęci, daty zarejestrowania zasobu kryptograficznego, zgodnie z zapisem w dzienniku ewidencji oraz danych wymienionych w pkt 2 lit. a i b oraz lit. d i e.

8. 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 zasobu kryptograficznego;
- 2) zamieszczenie w rubryce „Uwagi” dziennika ewidencji adnotacji „do rąk własnych”;
- 3) odcisnięcie na opakowaniu pieczęci wpływu i wpisaniu numeru ewidencyjnego według dziennika ewidencji oraz daty wpływu przesyłki.

9. Jeżeli przesyłka opatrzona adnotacją „do rąk własnych” zawiera kilka zasobów kryptograficznych, o których mowa w § 2 pkt 1 lit. c, 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 zasobów kryptograficznych, z wpisanymi numerami ewidencyjnymi poszczególnych zasobów.

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

11. Przesyłkę, o której mowa w ust. 10, można zwrócić do KK w stanie otwartym lub zamkniętym.

12. W przypadku, gdy przesyłka zostanie zwrócona do KK w otwartym opakowaniu, podlega zarejestrowaniu w sposób określony w ust. 8, z tym, że zachowuje się numer ewidencyjny wpisany na opakowaniu i uzupełnia się niezapisane rubryki dziennika ewidencji.

13. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki opatrzonej adnotacją „do rąk własnych” w KK w stanie zamkniętym, opieczętowuje ją swoją numerową pieczęcią okrągłą do teczek pracy albo inną pieczęcią imienną, a kierownik KK dokonuje, przy udziale adresata, czynności, o których mowa w ust. 10. W takim przypadku przesyłka jest przechowywana w formie zapieczętowanego pakietu, a fakt ten podlega odnotowaniu w rubryce „Uwagi” dziennika ewidencji.

14. Przy przyjmowaniu przesyłek do KK:

- 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 lub książce doręczeń;
- 2) w przypadku zauważenia nieprawidłowości lub podejrzeń co do zawartości przesyłki, kierownik KK odmawia jej przyjęcia powiadamiając o tym Oficera BSŁ;
- 3) w przypadku stwierdzenia uszkodzenia odcisku pieczęci lub opakowania, kierownik KK sporządza wraz z przewoźnikiem protokół w sprawie uszkodzenia przesyłki, według wzoru określonego w rozporządzeniu wydanym na podstawie art. 47 ust. 5 ustawy.

15. Po otwarciu przesyłki pracownik KK 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 zasobach kryptograficznych.

16. Stwierdzone nieprawidłowości dokumentuje się w protokole otwarcia przesyłki, którego jeden egzemplarz dołącza się do zasobu kryptograficznego, a drugi przesyła do

nadawcy. Fakt sporządzenia protokołu otwarcia przesyłki podlega odnotowaniu w rubryce „Uwagi” dziennika ewidencji.

17. Zarejestrowanie korespondencji wysyłanej odbywa się w sposób określony w ust. 7 z tym, że zamiast pieczęci wpływu używa się pieczęci nagłówkowej, a w odpowiednich rubrykach dziennika ewidencji wpisuje się nazwę adresata, ilość stron zasobu 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 DEWD lub innego urzędnika ewidencyjnego oraz wykonawcę.

18. W rubryce „Uwagi” dziennika ewidencji wpisuje się datę przekazania zasobu kryptograficznego, o którym mowa w § 2 pkt 1 lit. c, numer oraz pozycję zapisu w książce doręczeń albo numer i pozycję zapisu w „Wykazie przesyłek nadanych”, za którym zasób kryptograficzny przekazano adresatowi lub przewoźnikowi.

19. Jeżeli w KK nie pozostawia się żadnego egzemplarza wysyłanego zasobu kryptograficznego, o którym mowa w § 2 pkt 1 lit. c, w rubrykach dziennika ewidencji przeznaczonych do zapisywania informacji o ilości stron zasobu kryptograficznego, ilości załączników oraz ilości stron załączników, wpisuje się poziome kreski, natomiast w rubryce „Uwagi” zamieszcza się adnotację o treści „tylko adresat”.

20. Przed zarejestrowaniem w dzienniku ewidencji przekazanego do wysłania zasobu kryptograficznego, o którym mowa w § 2 pkt 1 lit. c, kierownik KK lub inna osoba z personelu KK sprawdza czy zasób 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 KJO lub osobę upoważnioną przez niego.

21. W razie niespełnienia któregokolwiek z warunków, o których mowa w ust. 20, kierownik KK zwraca zasób kryptograficzny do wykonawcy w celu poprawienia lub uzupełnienia.

22. Zasoby kryptograficzne, o których mowa w § 2 pkt 1 lit. c, sporządzone w JO na potrzeby własne, ewidencjonuje się w dzienniku ewidencji jak korespondencję otrzymaną.

23. W przypadku odłączenia od pisma przewodniego jednego lub więcej załączników, w rubryce „Uwagi” dziennika ewidencji zamieszcza się adnotację zawierającą jedną z informacji obejmujących:

- 1) nazwę i numer urzędnika ewidencyjnego oraz numery pozycji, pod którymi zarejestrowano odłączone załączniki;
- 2) numer wychodzący według dziennika ewidencji, za którym załączniki odesłano do innej JO;
- 3) numer i pozycję protokołu zniszczenia albo adnotację o zniszczeniu potwierdzoną czytelnymi podpisami przedstawiciela personelu KK i użytkownika lub innej osoby z OBSŁ, 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.

§ 27. 1. W kartach AF 54 A PL rejestruje się materiały kryptograficzne, o których mowa w § 2 pkt 29 lit. a.

2. Materiały kryptograficzne, o których mowa w § 2 pkt 29 lit. a, rejestruje się wpisując w kartach AF 54 A PL:

- 1) klauzulę i nazwę otrzymanego materiału kryptograficznego;
- 2) edycję, numer seryjny, ilość otrzymanego materiału kryptograficznego;
- 3) numer i datę otrzymanego formularza SF 153 (PL), za którymi przysłano materiały kryptograficzne;
- 4) datę ważności otrzymanego materiału kryptograficznego.

3. W części B karty AF 54 A PL wpisuje się dane dotyczące dystrybucji oraz zniszczenia materiałów kryptograficznych, o których mowa w § 2 pkt 29 lit. a.

4. Nowy otrzymany materiał kryptograficzny, o którym mowa w § 2 pkt 29 lit. a, ewidencjonuje się na odrębnej karcie AF 54 A PL.

§ 28. 1. W kartach AF 54 B PL rejestruje się materiały kryptograficzne o których mowa w § 2 pkt 29 lit. b.

2. Materiały kryptograficzne, o których mowa w § 2 pkt 29 lit. b, rejestruje się wpisując w kartach AF 54 B PL:

- 1) klauzulę, nazwę i numer otrzymanego materiału kryptograficznego;
- 2) numer i datę otrzymanego formularza SF 153 (PL) lub pisma, za którym przysłano materiały kryptograficzne oraz datę odbioru.

3. W celu dystrybucji materiałów kryptograficznych, o których mowa w § 2 pkt 29 lit. b, w kartach AF 54 B PL wpisuje się:

- 1) dokąd przesłano materiał kryptograficzny;
- 2) numer formularza SF 153 (PL) lub pisma, za którym przesłano materiał kryptograficzny;
- 3) aktualny stan posiadanego materiału kryptograficznego.

4. Nowy otrzymany materiał kryptograficzny, o którym mowa w § 2 pkt 29 lit. b, ewidencjonuje się na odrębnej karcie AF 54 B PL.

§ 29. 1. W kartach AF 54 C PL rejestruje się zasoby kryptograficzne, o których mowa w § 2 pkt 1 lit. a i b oraz pkt 29 lit. c, wytwarzane na potrzeby JO lub otrzymane.

2. Materiały kryptograficzne, o których mowa w § 2 pkt 1 lit. a i b oraz pkt 29 lit. c, rejestruje się wpisując w kartach AF 54 C PL:

- 1) klauzulę, nazwę i numer otrzymanego materiału kryptograficznego;
- 2) numer i datę otrzymanego formularza SF 153 (PL) lub pisma, za którym przysłano materiały kryptograficzne oraz datę odbioru.

3. W celu dystrybucji materiałów kryptograficznych, o których mowa w § 2 pkt 1 lit. a i b oraz pkt 29 lit. c, w kartach AF 54 C PL wpisuje się:

- 1) dokąd przesłano materiał kryptograficzny;
- 2) numer formularza SF 153 (PL) lub pisma, za którym przesłano materiał kryptograficzny;
- 3) aktualny stan posiadanego materiału kryptograficznego.

4. Nowy otrzymany materiał kryptograficzny, o którym mowa w § 2 pkt 1 lit. a i b oraz pkt 29 lit. c, ewidencjonuje się na odrębnej karcie AF 54 C PL.

§ 30. 1. W RWD rejestruje się:

- 1) zasoby kryptograficzne służące do utrwalania informacji dotyczącej tematyki kryptograficznej:
 - 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, niepodlegające ewidencji w innych urządzeniach.

2. W RWD dokumentuje się fakt pobrania i zwrotu wydawanych przez KK wykonawcom:

- 1) zasobów kryptograficznych zarejestrowanych w innych urządzeniach ewidencyjnych, jeżeli:
 - a) rubryka urządzenia ewidencyjnego, przeznaczona do pokwitowania zasobu kryptograficznego, została całkowicie wykorzystana,
 - b) rodzaj zasobu kryptograficznego albo dekretna sporządzona na nim wskazują, że będzie on udostępniany większej liczbie osób;

- 2) dokumentacji technicznej i standaryzacyjnej oraz innych dokumentów związanych z tematyką kryptograficzną zarejestrowanych w urządzeniach ewidencyjnych, które nie mają rubryk przeznaczonych do kwitowania pobieranych i zwracanych zasobów kryptograficznych.

3. RWD rejestruje się w Skorowidzu RWD:

- 1) imiennie dla wykonawców;
- 2) według numerów ewidencyjnych lub sygnatur, jeżeli są prowadzone dla poszczególnych dokumentów albo wydawnictw.

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

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

6. W przypadkach, o których mowa w ust. 2, zapisy rozpoczyna się od wpisania w kolumnie 4 RWD numeru ewidencyjnego zasobu 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 RWD, przeznaczonych do wrywania stron, wpisuje się numer ewidencyjny, o którym mowa w ust. 5, łamany przez numer karty (np. RWD 10/Pf-8/1, 2, 3 ...). Fakt wrywania karty kierownik KK lub inna osoba z personelu KK dokonująca tej czynności potwierdza na grzbiecie zasobu kryptograficznego podpisem, odciskiem pieczęci oraz opatrunkiem datą.

8. Zasoby kryptograficzne zarejestrowane w RWD, po zwróceniu ich do KK, podlegają zniszczeniu lub przerejestrowaniu do RWD innego wykonawcy albo innego urządzenia ewidencyjnego.

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

10. RWD przeznaczony do rejestrowania dokumentacji służby dyżurnej zakłada się w dwóch egzemplarzach, z których jeden przechowuje się w KK, a drugi, stanowiący podstawę do przekazywania przez służbę dyżurną zasobów kryptograficznych, w pomieszczeniu tej służby.

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

12. Rozliczony RWD użytkownika, który ubył z JO, po sprawdzeniu przez komisję powołaną do przeprowadzenia kontroli okresowej w ramach kontroli rocznej stanu ochrony informacji niejawnych podlega komisijnemu zniszczeniu. Do momentu zniszczenia rozliczony RWD przechowuje się w KK. Zniszczone RWD są wyszczególniane w załączniku do protokołu z kontroli okresowej.

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

2. W przypadku przekazania zasobów kryptograficznych poprzez KK 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. Formularz AF 69 PL stosowany jest wyłącznie w przypadku przekazywania zasobów kryptograficznych pomiędzy KK, z wykorzystaniem personelu KK lub kurierów WSK RP.

4. W przypadku przekazywania zasobu kryptograficznego poprzez personel KK lub WSK RP 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.

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

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

7. Sposób stosowania „Wykazu przesyłek nadanych” określa rozporządzenie wydane na podstawie art. 47 ust. 5 ustawy.

§ 32. 1. W Księżce doręczeń rejestruje się fakt doręczenia zasobów kryptograficznych do KK adresata, stacjonującego w tej samej miejscowości, bezpośrednio przez personel KK nadawcy.

2. Kierownik KK adresata potwierdza odbiór zasobów 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 RWD kierownika KK.

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

§ 33. 1. Kartę zapoznania się z zasobem kryptograficznym, z zastrzeżeniem ust. 2, zakłada się i dołącza do zasobu kryptograficznego pochodzenia krajowego, o którym mowa w § 2 pkt 1 lit. a-c oraz klauzuli tajności „TAJNE” lub „SCISLE TAJNE”, z chwilą zarejestrowania go po raz pierwszy w urządzeniach ewidencyjnych.

2. W przypadku funkcjonowania w JO EOZK dopuszcza się prowadzenie Kart zapoznania się z zasobem kryptograficznym w formie elektronicznej. Przepisy ust. 3-9 stosuje się odpowiednio.

3. W Karcie zapoznania się z zasobem kryptograficznym dokumentuje się każdorazowe udostępnienie użytkownikowi zasobów kryptograficznych, o których mowa w ust. 1.

4. Dokumentowanie w formie elektronicznej udostępnienia zasobu kryptograficznego polega na potwierdzeniu tej czynności wykonaniem dekretacji elektronicznej przez użytkownika.

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

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

7. Kart zapoznania się z zasobem kryptograficznym nie zakłada się dla zasobów kryptograficznych pochodzących z wymiany międzynarodowej.

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

9. W przypadku funkcjonowania w JO EOZK i prowadzenia Kart zapoznania się z zasobem kryptograficznym w formie elektronicznej, zapewnia się możliwość wydrukowania Kart zapoznania się z zasobem kryptograficznym, a wydruki traktuje się na zasadach równoważnych z dokumentami papierowymi.

§ 34. 1. Użytkownicy wytwarzający zasoby kryptograficzne, o których mowa w § 2 pkt 1 lit. a-c, prowadzą DEWD.

2. DEWD służy do rejestrowania zasobów kryptograficznych, o których mowa § 2 pkt 1 lit. a-c, wytworzonych w JO, w szczególności techniką komputerową, maszynopisania, powielania, naświetlania, kreślenia lub odręczną.

3. Dopuszcza się prowadzenie jednego DEWD dla różnych technik wytwarzania dokumentów, kilku użytkowników lub systemów łączności. W przypadku prowadzenia jednego

DEWD dla różnych technik wytwarzania dokumentów lub kilku systemów łączności, w kolumnie „Uwagi” dziennika ewidencji umieszcza się dodatkowe adnotacje (np. „wykonano techniką odręczną”).

4. Jawne pismo przewodnie, za którym przesłane są załączniki niejawne oznacza się bez jego rejestrowania w DEWD, w sposób określony w rozporządzeniu wydanym na podstawie art. 6 ust. 9 ustawy. Ewidencja pisma przewodniego następuje z chwilą ujęcia go w urządzeniu ewidencyjnym KK.

5. Zarejestrowanie zasobu kryptograficznego w DEWD polega na wpisaniu pod kolejną pozycją dziennika:

- 1) symbolu klauzuli tajności;
- 2) liczby porządkowej;
- 3) daty wykonania dokumentu;
- 4) nazwy wykonanego dokumentu;
- 5) sposobu lub metody wykonania dokumentu;
- 6) nazwy systemu, w którym wykonano dokument lub nr informatycznego nośnika danych, z którego wykonano wydruk lub nr dokumentu, z którego wykonano kopię;
- 7) nazwiska osoby wykonującej dokument;
- 8) liczby egzemplarzy i liczby stron w pojedynczym egzemplarzu, przy czym oznaczenie klauzuli tajności i liczba porządkowa z DEWD łamane przez dwie ostatnie cyfry roku kalendarzowego poprzedzone skrótem nazwy JO stanowią prefiks sygnatury literowo-cyfrowej, o której mowa w rozporządzeniu wydanym na podstawie art. 6 ust. 9 ustawy (przykładowo Z VI SKW-PF-100/24). Do prefiksu dołącza się numer ewidencyjny dziennika DEWD, w którym zasób kryptograficzny został zaewidencjonowany (przykładowo DEWD RTMK 18/10). Sygnatura literowo-cyfrowa umieszczona na wykonanym dokumencie przykładowo ma postać: Z VI SKW-Pf-100/24-DEWD RTMK 18/10.

6. Dodatkowo wytworzony zasób kryptograficzny o klauzuli tajności „ŚCIŚLE TAJNE”, „TAJNE” i „POUFNE”, w szczególności odpis, kopię lub reprodukcję rejestruje się każdorazowo pod odrębną pozycją DEWD. Wykonanie kopii, odpisu lub reprodukcji zasobu kryptograficznego o klauzuli tajności „ŚCIŚLE TAJNE”, „TAJNE” i „POUFNE” wymaga pisemnej zgody KJO dysponującej tym zasobem lub upoważnionej przez niego osoby.

7. DEWD prowadzi się do całkowitego wykorzystania jego kart, rozpoczynając każdego roku kalendarzowego numerowanie od liczby „1”.

8. Wytworzone i ujęte w DEWD zasoby kryptograficzne użytkowników rejestruje w urządzeniach ewidencyjnych KK, w terminie do 30 dni od daty ich wytworzenia.

9. Zakończony DEWD, po sprawdzeniu przez komisję powołaną do przeprowadzenia kontroli okresowej, podlega komisijnemu zniszczeniu, nie wcześniej jednak niż po upływie 5 lat od daty zakończenia. Do momentu zniszczenia zakończone DEWD przechowuje się w KK. Zniszczone DEWD są wyszczególniane w załączniku do protokołu z kontroli okresowej.

§ 35. 1. KK przekazuje zasoby kryptograficzne wyłącznie użytkownikom posiadającym stosowne poświadczenie bezpieczeństwa lub certyfikat NATO (UE) wydany przez Agencję Bezpieczeństwa Wewnętrznego albo upoważnienie, o którym mowa w art. 21 ust. 4 pkt 1 ustawy oraz CUK, w przypadku przekazywania materiałów kryptograficznych.

2. Zasoby kryptograficzne, o których mowa w ust. 1, wydawane są za pokwitowaniem w dzienniku ewidencji albo za pokwitowaniem odręcznym, wykonanym na formularzu SF 153 (PL) lub na RWD.

3. Dopuszcza się wydawanie zasobów kryptograficznych, o których mowa w ust. 1, z wykorzystaniem pomocniczych urządzeń ewidencyjnych, założonych w tym celu.

4. Kierownik lub personel KK udostępnia lub przekazuje zasoby kryptograficzne osobom, o których mowa w ust. 1, na podstawie zamieszczonej na dokumencie dekretacji lub polecenia KJO albo osoby przez niego upoważnionej.

5. W przypadku funkcjonowania w JO EOZK, udostępnienie lub przekazanie, o którym mowa w ust. 4, odbywa się na podstawie elektronicznej dekretacji KJO albo osoby przez niego upoważnionej.

6. Użytkownikom, o których mowa w ust 1, których pomieszczenia służbowe nie spełniają warunków dotyczących przechowywania i zabezpieczenia zasobów kryptograficznych, umożliwia się udostępnienie tych zasobów jedynie w pomieszczeniach KK, z zastrzeżeniem § 45.

7. Fakt przyjęcia użytkownika w KK oraz zapoznania się przez niego z zasobami kryptograficznymi odnotowuje się w rejestrze interesantów, którego wzór określa załącznik nr 26 do zarządzenia.

8. Użytkownik, któremu udostępniono zasoby kryptograficzne ma obowiązek zachowania środków bezpieczeństwa uniemożliwiających dostęp do tych zasobów osobom nieuprawnionym.

9. Użytkownicy przechowujący w pomieszczeniach służbowych zasoby kryptograficzne, przed udaniem się na urlop, szkolenie lub w podróż służbową mają obowiązek zdania ich do KK. Przekazanie zasobów niezbędnych do prowadzenia bieżącej działalności JO osobie zastępującej, następuje poprzez KK na polecenie KJO.

10. Przesyłki opatrzone adnotacją „Pilne” KK przekazuje adresatom bezzwłocznie, wpisując w rubryce „Uwagi” urządzenia ewidencyjnego datę i godzinę doręczenia.

11. Wszelkie zasoby kryptograficzne mogą być przekazywane pomiędzy uprawnionymi do ich otrzymania użytkownikami jedynie za pośrednictwem KK, z zastrzeżeniem § 45.

12. Zasoby kryptograficzne ostatecznie załatwionych spraw powinny być niezwłocznie przekazane do KK.

13. 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 będące zasobem kryptograficznym, na podstawie decyzji KJO przekazywane są do KK, która ewidencjonuje je w dzienniku korespondencji.

14. Przyjęcie szyfrogramu w KK potwierdza się w kolumnie 14 dziennika ewidencji szyfrogramów, poprzez wpisanie numeru ewidencyjnego, pod którym zarejestrowano szyfrogram, przystawienie pieczęci „Do pakietów” oraz złożenie podpisu przez osobę z personelu KK. W kolumnie 15 zamieszcza się napis „Szyfrogram”.

§ 36. 1. Zasoby kryptograficzne, o których mowa w § 2 pkt 1 lit. a-c, otrzymane lub wytworzone w JO podlegają:

- 1) skompletowaniu w teczki akt, jeżeli stanowią zasoby archiwalne lub posiadają wartość praktyczną dla JO – teczki skompletowanych akt spina się przy pomocy klipsów po upływie dwóch lat od ostatecznego zakończenia spraw na polecenie KJO lub upoważnionej przez niego osoby. Za datę rozpoczęcia teczki przyjmuje się datę wpływu pierwszego pisma z danej tematyki;
- 2) w uzasadnionych przypadkach za zgodą KJO lub osoby przez niego upoważnionej zasoby kryptograficzne, o których mowa w § 2 pkt 1 lit. a-c, można wydać z KK na RWD użytkownika. Zasoby kryptograficzne podlegają zwrotowi do KK bezpośrednio po ich realizacji;
- 3) zwrotowi do nadawcy, jeżeli określił on taki sposób postępowania z przesłanymi zasobami;
- 4) bieżącemu niszczeniu.

2. Zasoby kryptograficzne, o których mowa w § 2 pkt 1 lit. a-c, oraz urządzenia ewidencyjne, o których mowa w § 24 ust. 4 pkt 1-3, przechowuje się w KK z zachowaniem terminów przechowywania określonych w jrw a JO, 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.

3. Do zasobów kryptograficznych GKK SKW, które są archiwizowane w SKW, ust. 2 nie stosuje się.

4. Formularze ewidencyjne SF 153 (PL) przechowuje się przez okres 5 lat, nie wliczając roku bieżącego.

5. Formularze AF 54 A, B, C PL nie podlegają ewidencji i przechowywane są przez okres 5 lat od ich zakończenia i rozliczenia zasobu kryptograficznego ujętego na danym formularzu.

6. 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.

7. KJO w razie konieczności, w szczególnych przypadkach może wyrazić pisemną zgodę na rozszycie teczki akt kryptograficznych i wyjęcie potrzebnego zasobu kryptograficznego.

8. Zgody, o której mowa w ust. 7, dokonuje się na ostatniej stronie teczki akt kryptograficznych potwierdzając czytelnym podpisem i odciskiem pieczęci urzędowej.

9. Rozszycia teczki dokonuje wyłącznie kierownik KK.

10. W przypadku wyłączenia na stałe zasobu kryptograficznego z teczki kierownik KK na ostatniej stronie teczki akt kryptograficznych dokonuje zapisu: komu zasób przekazano (nr wykazu przesyłek lub liczba porządkowa książki doręczeń, ilości kart i numery stron wyłączonego zasobu) potwierdzając datą dokonanie czynności oraz czytelnym podpisem.

11. Zasób kryptograficzny wyłączony na stałe z teczki akt kryptograficznych podlega ponownemu ujęciu w bieżącej ewidencji KK.

12. Teczka akt kryptograficznych, o której mowa w ust. 7, podlega ponownemu sprawdzeniu w zakresie ilości stron tej teczki przez najbliższą komisję inspekcji kryptograficznej, która dokonuje odpowiedniej adnotacji w protokole z tej inspekcji.

§ 37. 1. Zasoby kryptograficzne niebędące zasobami archiwalnymi i nieposiadające wartości praktycznej dla JO podlegają zniszczeniu.

2. W przypadku prowadzenia w JO ewidencji zasobów kryptograficznych w wersji elektronicznej, przechowywanej w komputerowych bazach danych, ewidencja nie podlega niszczeniu.

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

- 1) w odniesieniu do zasobów kryptograficznych, o których mowa w § 2 pkt 1 lit. c-d klauzuli tajności „TAJNE” i „ŚCISLE TAJNE”, które nie zostały włączone do teczek akt kryptograficznych – co najmniej trzyosobowa komisja, powoływana okresowo przez KJO;
- 2) w odniesieniu do jawnych zasobów kryptograficznych, o których mowa w § 2 pkt 1 lit. c-d, oraz zasobów kryptograficznych zawierających informacje niejawne o klauzuli tajności „ZASTRZEŻONE” oraz „POUFNE” – osoba z personelu KK wraz z wykonawcą lub inną osobą z OBSŁ. Zniszczenie zasobów dokumentuje się w rubryce „Uwagi” urządzenia ewidencyjnego adnotacją o treści: „Zniszczono dnia...”, potwierdzoną wpisaniem daty i podpisami zawierającymi imię i nazwisko osób niszczących zasoby kryptograficzne;
- 3) w odniesieniu do zasobów kryptograficznych, o których mowa w § 2 pkt 29 lit. a – kierownik KK wraz z inną osobą, posiadającą stosowne poświadczenia bezpieczeństwa lub certyfikat NATO (UE) wydany przez Agencję Bezpieczeństwa Wewnętrznego oraz CUK, występującą w roli świadka, którzy potwierdzają zniszczenie na formularzu SF 153 (PL);
- 4) w odniesieniu do zasobów kryptograficznych, o których mowa w § 2 pkt 29 lit. b, powołana na podstawie odrębnych przepisów komisja złożona z przedstawicieli Sił Zbrojnych Rzeczypospolitej Polskiej, której przewodniczy przedstawiciel DKWOC.

4. Z komisyjnego zniszczenia zasobów kryptograficznych, o których mowa w ust. 1, sporządza się protokół zniszczenia, którego wzór określa załącznik nr 27 do zarządzenia. Protokół ten podlega archiwizacji.

5. Protokół zniszczenia, o którym mowa w ust. 4, lub formularz SF 153 (PL) stanowi dla kierownika KK podstawę do zdjęcia z ewidencji wyszczególnionych w nich zasobów kryptograficznych, poprzez naniesienie we właściwej rubryce lub rubryce „Uwagi” urządzenia ewidencyjnego adnotacji o dokonanym zniszczeniu wraz z datą tej czynności.

§ 38. 1. Zasób kryptograficzny w formie papierowej uważa się za ostatecznie zniszczony, jeżeli został pocięty w urządzeniu, o którym mowa w § 12 ust. 8 pkt 1, lub zmielony na miazgę papierową, lub spalony w piecu lub rozpuszczony w kadziach z ługiem w zakładach papierniczych.

2. Jeżeli w JO, z przyczyn technicznych, ostateczne zniszczenie zasobów kryptograficznych, o których mowa w ust. 1 jest niemożliwe, niszczy się je wstępnie przez

kilkakrotne przedarcie, przy czym wstępnego zniszczenia dokonuje odpowiednio kierownik KK pod nadzorem członków komisji albo wykonawcy lub innej osoby z OBSŁ.

3. Wstępnie zniszczone zasoby kryptograficzne, do chwili ich przekazania do wytypowanej JO lub wyspecjalizowanego zakładu, w celu ostatecznego zniszczenia, przechowuje się w opłombowanych przez personel KK workach lub pojemnikach, w KK, lub innym pomieszczeniu JO zabezpieczonym jak KK.

4. Osoby, o których mowa w ust. 2, nadzorujące niszczenie zasobów kryptograficznych zapewniają zachowanie warunków uniemożliwiających wgląd do nich osobom nieupoważnionym.

5. Zabrania się wywożenia częściowo zniszczonych zasobów kryptograficznych oraz kopert i innych opakowań, w których otrzymano te zasoby na wysypiska śmieci.

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

§ 39. 1. Produkt kryptograficzny, w tym CCI, na skutek działań operacyjnych lub wystąpienia sytuacji zagrożenia może ulec:

- 1) zniszczeniu, m.in. jako element platformy bojowej lub uzbrojenia;
- 2) utracie kontroli jako skutek wystąpienia incydentu kryptograficznego związanego z naruszeniem bezpieczeństwa materiałów kryptograficznych.

2. W przypadku zaistnienia sytuacji, o których mowa w ust. 1, produkt kryptograficzny podlega zdjęciu z ewidencji KK.

3. Zdjęcie produktu kryptograficznego z ewidencji KK następuje na podstawie formularza SF 153 (PL), gdzie w wierszu 1 należy wybrać pole:

- 1) w przypadku zniszczenia – „ZNISZCZENIE”;
- 2) w przypadku utraty kontroli nad produktem kryptograficznym – „INNE” i zamieścić przyczynę np. zagubienie, kradzież.

4. Formularz SF 153 (PL) podpisuje kierownik KK oraz osoba poświadczająca zaistniałą sytuację, o której mowa w ust. 1.

5. W przypadku, przekazania produktu kryptograficznego użytkownikowi jako przekazanie odrębne, użytkownik zwraca swój egzemplarz formularza SF 153 (PL) do KK.

§ 40. 1. W przypadku rozformowania JO postępuje się zgodnie z przepisami wydanymi na podstawie ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

2. Personel KK likwidowanej JO może być przeniesiony na inne stanowiska służbowe z chwilą całkowitego rozliczenia i przekazania zasobów kryptograficznych pozostających na ewidencji JO.

Rozdział 9

Organizacja pracy kancelarii kryptograficznych, ich ochrona oraz obieg zasobów kryptograficznych podczas ćwiczeń oraz realizacji zadań poza MSD JO

§ 41. 1. Poza MSD, w trakcie działań bojowych, ćwiczeń lub w stanach nadzwyczajnych zasoby kryptograficzne wykorzystuje się i chroni zgodnie z przyjętą taktyką działania wojsk.

2. Taktyka działania wojsk musi uwzględniać postępowanie z zasobami kryptograficznymi, w tym podczas przemieszczania i działań poza MSD.

§ 42. 1. Na czas realizacji zadań i ćwiczeń przez JO poza MSD, zasoby kryptograficzne mogą być zabezpieczane przez połowę KK. Tryb oraz sposób powoływania i odwoływania połowej kancelarii kryptograficznej określa w zaleceniach SKW Szef KOGD.

2. W przypadku, gdy ćwiczenia odbywają się w MSD, zasadniczym sposobem zabezpieczenia w zasoby kryptograficzne jest wykorzystanie stacjonarnej KK. Dopuszcza się wykorzystanie połowej KK, w zależności od przyjętego scenariusza ćwiczeń.

§ 43. KJO zapewnia niezbędne siły i środki do przewozu połowej KK i jej dokumentacji podczas ćwiczeń oraz na czas prowadzenia działań wojennych.

§ 44. 1. Polową KK, o której mowa w § 42 ust. 1, organizuje się:

- 1) w kontenerach;
- 2) w pomieszczeniach;
- 3) w namiotach na stanowisku dowodzenia.

2. Polowa KK powinna spełniać warunki ochrony uwzględniające:

- 1) wydzielenie ogrodzonej strefy nadzorowanej;
- 2) konieczność zorganizowania całodobowego strzeżonego wejścia do strefy nadzorowanej, w której zlokalizowana jest polowa KK;
- 3) konieczność wykonywania patroli przez personel ochrony w obrębie strefy nadzorowanej;
- 4) określenie sposobu gospodarowania kluczami do polowej KK i urządzeń do przechowywania informacji niejawnych oraz kodami zamków szyfrowych.

3. Polową KK wyposaża się w:

- 1) urządzenia do przechowywania informacji niejawnych;
- 2) urządzenia do niszczenia papierowych zasobów kryptograficznych, których wymiary ścinka nie przekraczają wartości 1 mm x 5 mm;
- 3) narzędzia dewastacyjne do niszczenia fizycznego zasobów kryptograficznych;
- 4) pojemniki lub worki służące do przechowywania zasobów kryptograficznych przeznaczonych do zniszczenia oraz do ewakuacji.

4. Pozyskiwane w ramach nowych dostaw kontenery kolejnej generacji (PKKs-2), w których mają być przechowywane materiały kryptograficzne, powinny spełniać wymagania konstrukcyjne oraz wymagania w zakresie zabezpieczenia fizycznego i technicznego, określone w załączniku nr 28 do zarządzenia, z uwzględnieniem uzyskania pozytywnej opinii wydanej przez SKW potwierdzającej spełnienie wymagań w zakresie zabezpieczenia fizycznego i technicznego.

5. Wszelkie odstępstwa w zakresie zabezpieczeń fizycznych i technicznych, ochrony oraz wyposażenia polowej KK wymagają zgody Szefa KOGD.

§ 45. 1. W JO, w których powołana jest KK i nie ma możliwości obsługi użytkowników przez personel KK podczas działań operacyjnych oraz ćwiczeń poza MSD, wyznacza się odpowiednią ilość osób zabezpieczających potrzeby użytkowników w zakresie eksploatacji materiałów kryptograficznych.

2. Do obowiązków osób, o których mowa w ust. 1, należy:

- 1) udostępnianie i wydawanie materiałów kryptograficznych użytkownikom posiadającym CUK;
- 2) prowadzenie aktualnej ewidencji materiałów kryptograficznych, pobranych z KK i wydanych użytkownikom, z wykorzystaniem formularzy SF 153 (PL);
- 3) dokonywanie sprawdzeń materiałów kryptograficznych pobranych z KK i wydanych użytkownikom;
- 4) meldowanie Oficerowi BSŁ o każdym stwierdzonym incydencie kryptograficznym mającym wpływ na bezpieczeństwo materiałów kryptograficznych oraz o możliwym lub rzeczywistym zagrożeniu utraty materiałów kryptograficznych;
- 5) udzielanie instruktażu użytkownikom pobierającym materiały kryptograficzne;
- 6) przesyłanie do KK raportów o stanie posiadanych materiałów kryptograficznych;
- 7) niszczenie materiałów pobranych z KK, zgodnie z obowiązującymi w tym zakresie przepisami;
- 8) przewóz przesyłek kryptograficznych;
- 9) obsługa produktów kryptograficznych;
- 10) realizacja zadań zleconych przez Oficera BSŁ związanych z tematyką kryptograficzną.

3. Osoby, o których mowa w ust. 1:

- 1) wyznacza się w rozkazie (decyzji) KJO;
- 2) wyznacza się spośród żołnierzy zawodowych, posiadających poświadczenie bezpieczeństwa odpowiednie do klauzuli tajności eksploatowanych materiałów kryptograficznych lub certyfikat NATO (UE) wydany przez Agencję Bezpieczeństwa Wewnętrznego, aktualne zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych, CUK oraz szkolenia specjalistyczne adekwatne do realizowanych obowiązków, o których mowa w ust. 2.

Rozdział 10

Postanowienia szczególne

§ 46. 1. W razie wystąpienia okoliczności trudnych do przewidzenia, w szczególności w czasie stanów nadzwyczajnych lub wojny, w których typowe sposoby ochrony zasobów kryptograficznych mogą być niemożliwe do wykorzystania lub ich użycie pogorszy bezpieczeństwo informacji, KJO może wyrazić zgodę na odstępstwa od przyjętych rozwiązań, pod warunkiem zapewnienia realizacji celów określonych w ustawie i niniejszym zarządzeniu, po zaakceptowaniu ryzyk związanych z odstępstwami.

2. Zgodę na odstępstwa dokumentuje się w odpowiednim do szczebla dowodzenia/kierowania dokumencie decyzyjnym.

3. W warunkach bojowych, kiedy kontakt z KJO jest niemożliwy lub może spowodować zagrożenie, sposób ochrony zasobów kryptograficznych określa dowódca pododdziału (równorzędny), a w przypadku jego braku, osoba będąca w posiadaniu tych zasobów.

Rozdział 11

Przepisy przejściowe i końcowe

§ 47. 1. Zastosowany przed wejściem w życie niniejszego zarządzenia system środków bezpieczeństwa fizycznego, obejmujący rozwiązania organizacyjne, a także wyposażenie pomieszczeń KK w urządzenia służące do ochrony informacji niejawnych oraz elektroniczne systemy pomocnicze wspomagające ochronę informacji niejawnych, nie ulega modyfikacji, pod warunkiem, że poziom zagrożeń nie wzrośnie.

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 2026 r.

§ 48. Traci moc zarządzenie 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 oraz z 2020 r. poz. 210).

§ 49. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Obrony Narodowej: z up. *P. Bejda*

Zawartość Instrukcji pracy kancelarii kryptograficznej

Instrukcja pracy KK powinna zawierać następującą tematykę:

- 1) zadania KK;
- 2) opis lokalnego i globalnego środowiska bezpieczeństwa oraz wyposażenia KK;
- 3) personel OBSŁ;
- 4) obowiązki personelu OBSŁ;
- 5) harmonogram pracy KK;
- 6) procedura rutynowego niszczenia zasobów kryptograficznych;
- 7) sposób zabezpieczania kodów dostępu i kluczy zapasowych;
- 8) załączniki:
 - a) lista aktów prawnych, wytycznych, zaleceń normujących pracę KK,
 - b) szkic Środowiska Bezpieczeństwa Globalnego,
 - c) szkic Środowiska Bezpieczeństwa Lokalnego,
 - d) plan pomieszczeń KK,
 - e) lista osób zapoznanych z instrukcją.

Uwaga:

Na instrukcji pracy KK nie nanosi się oznaczenia „KRYPTO”.

Instrukcja konwojowania zasobów 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 zasobami kryptograficznymi;
- 6) procedury postępowania z zasobami kryptograficznymi w sytuacjach szczególnych;
- 7) załączniki:

Plan przeprowadzenia konwoju, w którym w szczególności umieszcza się:

- a) podstawę prawną przeprowadzenia konwoju (nr rozkazu lub decyzji osoby zarządzającej oraz ich datę wydania),
- b) rodzaj i ilość konwojowanego zasobu kryptograficznego,
- c) siły i środki oraz czas prowadzenia konwoju,
- d) trasę (zasadniczą i zapasową) prowadzonego konwoju,
- e) szczegółowe zadania dla poszczególnych członków konwoju,
- f) szczegółowe zasady postępowania dla poszczególnych członków konwoju w sytuacji napadu lub innego zagrożenia,
- g) system łączności (środki łączności, abonenci, kryptonimy, i numery telefonów),
- h) zasady współdziałania z wojskowymi organami porządkowymi, w tym z Żandarmerią Wojskową oraz Policją,
- i) zasady stosowania środków przymusu bezpośredniego oraz użycia broni palnej.

Uwaga:

Na instrukcji konwojowania zasobów kryptograficznych nie nanosi się oznaczenia „KRYPTO”.

WZÓR

KARTA WZORÓW PODPISÓW KANCELARII KRYPTOGRAFICZNEJ		
Numer kancelarii	860048/	z dnia - -
Kancelaria podlega pod	860048/	
Kancelaria odbiera zasoby kryptograficzne od	860048/	
Klauzula tajności kancelarii kryptograficznej	PL NATO UE	
Adres:		
Adres Kurierski	860048/	
Ulica/Budynek/Pomieszczenie		
Kod, miasto		
Kraj		
Adres do wiadomości		
Dane telefoniczno-faksowe:		
IVSN		
DSN		
Tel. jawny		
Tel. CA MON		
Tel. niejawnny 1	Typ	
Tel. niejawnny 2	Typ	
Fax. jawny		
Fax. niejawnny		

WZORY PODPISÓW			
Oficer Bezpieczeństwa Systemów Łączności / COMSEC			
Nazwisko i imię			
Stopień		Rodz. wojsk	
Numer i data ważności Poświadczenia Bezpieczeństwa		Data wyznaczenia	
Data zmiany			
Nr telefonu			
Podpis			
Zastępca Oficera Bezpieczeństwa Systemów Łączności / Alternate COMSEC			
Nazwisko i imię			
Stopień		Rodz. wojsk	
Numer i data ważności Poświadczenia Bezpieczeństwa		Data wyznaczenia	
Data zmiany			
Nr telefonu			
Podpis			
Kierownik Kancelarii Kryptograficznej / Cryptocustodian			
Nazwisko i imię			
Stopień		Rodz. wojsk	
Numer i data ważności Poświadczenia Bezpieczeństwa		Data wyznaczenia	
Data zmiany			
Nr telefonu			
Podpis			
..... (**)			
Nazwisko i imię			
Stopień		Rodz. wojsk	
Numer i data ważności Poświadczenia Bezpieczeństwa		Data wyznaczenia	
Nr telefonu			
Podpis			
Potwierdzenie:			
m.p. (Podpis KJO)			

** - wpisać kolejno etatowy personel KK

Uwaga:

Na KWP nie nanosi się oznaczenia „KRYPTO”.

Wytyczne do sporządzania procedur zaopatrywania w materiały kryptograficzne

Procedury zaopatrywania powinny zawierać m.in. następujące informacje:

- 1) informacje ogólne:
 - a) nr KK JO zaopatrującej,
 - b) pełna nazwa i adres JO zaopatrywanej,
 - c) pełna nazwa i adres JO zaopatrującej, dane i adres (jeżeli inny) KK zaopatrującej (Zaświadczenie nr .../... o powołaniu/funkcjonowaniu KK, klauzula tajności przetwarzanych informacji),
 - d) zależność służbowa JO zaopatrywanej względem JO zaopatrującej (podległa/nadrzędna/równorzędna/niezależna służbowo),
 - e) przyczyna/powód zaopatrywania w materiały kryptograficzne (uzasadnienie),
 - f) typ/rodzaj/klauzule tajności materiałów kryptograficznych będących przedmiotem zaopatrywania oraz systemy łączności lub szyfrowo-kodowe, które będą zabezpieczane kryptograficznie,
 - g) prognozowany czas zaopatrywania w materiały kryptograficzne,
 - h) realizacja/zawieszenie realizacji/cofnięcie realizacji procedur zaopatrywania,
 - i) sprawowanie nadzoru nad materiałami kryptograficznymi w JO zaopatrywanej;
- 2) dostęp do materiałów kryptograficznych:
 - a) wymagania upoważniające do dostępu do materiałów kryptograficznych,
 - b) wykaz personelu OBSŁ JO zaopatrywanej,
 - c) zasady wydawania CUK dla użytkowników JO,
 - d) procedury wykonywania/wydawania materiałów kryptograficznych (krajowych, międzynarodowych),
 - e) przechowywanie materiałów kryptograficznych,
 - f) niszczenie materiałów kryptograficznych,
 - g) transport materiałów kryptograficznych,
 - h) postępowanie na wypadek zagrożenia,
 - i) odpowiedzialność osób funkcyjnych w zakresie prowadzenia urządzeń ewidencyjnych (formularzy),
 - j) podstawa opracowania procedur zaopatrywania,
 - k) akceptacja/uzgodnienie procedur zaopatrywania przez KJO zaopatrującą i zaopatrywaną,
 - l) wykaz osób funkcyjnych wraz z kierownikiem i zastępcą KJO zaopatrywanej upoważnionych do dostępu do materiałów kryptograficznych (załącznik/tabela),
 - m) wykaz urządzeń ewidencyjnych i dokumentacji dodatkowo prowadzonych przez jednostkę zaopatrującą (załącznik/tabela).

Procedury należy opracować w 2 egzemplarzach:

Egz. nr 1 – JO zaopatrywana

Egz. nr 2 – JO zaopatrująca

Uwaga:

- 1) na Procedurach zaopatrywania w materiały kryptograficzne nie nanosi się oznaczenia „KRYPTO”;
- 2) Procedury zaopatrywania podlegają uzgodnieniu z DKWOC oraz wymagają akceptacji przez Szefa KOGD.

WZÓR

Certyfikat Upoważnienia Kryptograficznego

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 ZAKRES¹⁾, 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 nieujawniania 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
* niepotrzebne skreślić

Formularz 104 PL

Instruktaż w zakresie bezpieczeństwa materiałów kryptograficznych

1. Akty prawne 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.

WZÓR

Książka ewidencji wydanych CUK

Lp.	nr CUK	st. imię i nazwisko	Cel wydania	Data wydania i podpis pobierającego	Data wydania i podpis przyjmującego	Uwagi
1	2	3	4	5	6	7

Uwaga:

Na książce ewidencji wydanych CUK nie nanosi się oznaczenia „KRYPTO”.

WZÓR

Grupowy Certyfikat Upoważnienia Kryptograficznego

GRUPOWY CERTYFIKAT UPOWAŻNIENIA KRYPTOGRAFICZNEGO	
CZEŚĆ I	
NUMER KOLEJNY:	
KLAUZULA TAJNOŚCI MATERIAŁÓW KRYPTOGRAFICZNYCH ORAZ ZAKRES¹⁾, DO KTÓREGO UPRAWNIENI MAJĄ DOSTĘP:	
OŚWIADCZENIE SKŁADANE W MOMENCIE PRZYZNANIA CERTYFIKATU: 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.	
	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 nieujawniania 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:

¹⁾ Należy szczegółowo określić wykaz materiałów kryptograficznych, do których nadaje się dostęp

* niepotrzebne skreślić

Dobór środków bezpieczeństwa fizycznego

CZĘŚĆ I.

INSTRUKCJA:

1. Proces doboru środków bezpieczeństwa fizycznego powinien zapewniać elastyczność ich stosowania w zależności od określonego poziomu zagrożeń, nieuprawnionym ujawnieniem lub utratą informacji niejawnych.
2. Środki bezpieczeństwa fizycznego określone w części III „Klasyfikacja środków bezpieczeństwa fizycznego” zostały podzielone na 13 kategorii, z których każda dotyczy określonego aspektu bezpieczeństwa fizycznego. Aby ułatwić odczytywanie informacji, wykaz środków został sporządzony w formie tabeli z przypisanymi im wartościami liczbowymi.
3. Etapy wyboru optymalnych i ekonomicznych kombinacji środków bezpieczeństwa fizycznego:
 - 1) pierwszym etapem procesu doboru środków bezpieczeństwa fizycznego jest odczytanie z tabeli w części II „Podstawowe wymagania bezpieczeństwa fizycznego” minimalnej wymaganej sumy punktów koniecznych do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiednich kombinacji środków bezpieczeństwa fizycznego. Liczba wymaganych do uzyskania punktów zależy od najwyższej klauzuli tajności informacji niejawnych przetwarzanych w danej lokalizacji oraz poziomu zagrożeń, określonego wcześniej zgodnie z przepisami rozporządzenia wydanego na podstawie art. 47 ust. 1 pkt 1 i 3-6 ustawy;
 - 2) drugim etapem jest odczytanie z tej samej tabeli w cz. II, odpowiadającej założonemu poziomowi ochrony informacji, minimalnej liczby punktów koniecznych do uzyskania w każdej z grup obejmującej kategorii wymaganych do zastosowania środków bezpieczeństwa fizycznego (oznaczonej „obowiązkowo”);
 - 3) trzecim etapem jest dokonanie wyboru określonych środków bezpieczeństwa fizycznego, przy którym należy posługiwać się tabelą z części III „Klasyfikacja środków bezpieczeństwa fizycznego”. W tej tabeli należy odczytać liczbę punktów odpowiadającą wybranemu środkowi bezpieczeństwa, zsumować ją w ramach kategorii i sumę podstawić w odpowiednie miejsce w tabeli „Podstawowe wymagania bezpieczeństwa fizycznego”.
4. Niezastosowanie danego środka jest jednoznaczne z przyznaniem za niego liczby punktów „0”. Przy dokonywaniu wyboru konieczne jest uwzględnienie wymagań określonych w zarządzeniu, jak też w samej tabeli z części III „Klasyfikacja środków bezpieczeństwa fizycznego”.
5. Dobór adekwatnych środków bezpieczeństwa fizycznego w konkretnym przypadku musi zapewnić uzyskanie zarówno minimalnej sumy punktów koniecznych do osiągnięcia założonego poziomu ochrony informacji niejawnych (w zależności od najwyższej klauzuli tajności informacji przetwarzanych w danej lokalizacji oraz poziomu zagrożeń), jak również uzyskanie minimalnej liczby punktów odpowiadających każdej z grup kategorii środków bezpieczeństwa fizycznego (oznaczonych jako „obowiązkowo”).
6. W przypadku, gdy liczba punktów uzyskanych po zastosowaniu środka należącego do grup kategorii oznaczonych jako „obowiązkowo” jest mniejsza od minimalnej wymaganej sumy punktów koniecznej do osiągnięcia założonego poziomu ochrony informacji niejawnych, należy zastosować środki z kategorii oznaczonych „dodatkowo” zapewniające uzyskanie minimalnej wymaganej sumy punktów w każdej z kategorii oznaczonych jako „obowiązkowo” oraz wymaganej sumy punktów.

CZĘŚĆ II.

PODSTAWOWE WYMAGANIA BEZPIECZEŃSTWA FIZYCZNEGO

Najwyższa klauzula tajności informacji przetwarzanych w JO	Poziom zagrożenia		
	Niski	Średni	Wysoki
ŚCIŚLE TAJNE			
Obowiązkowo: kategorie K1+K2+K3+K4+K5	12	13	16
Obowiązkowo: kategorie K6+K7+K8+K9+K10	6	7	10
Dodatkowo: kategoria K11+K12+K13	4	5	6
Wymagana suma punktów	18	20	26
TAJNE			
Obowiązkowo: kategorie K1+K2+K3+K4+K5	8	9	10
Obowiązkowo: kategorie K6+K7+K8+K9+K10	4	5	5
Dodatkowo: kategoria K11+K12+K13	4	5	5
Wymagana suma punktów	12	14	15
POUFNE			
Obowiązkowo: kategorie K1+K2+K3+K4+K5	6	8	9
Obowiązkowo: kategorie K6+K7+K8+K9+K10	2	3	3
Dodatkowo: kategoria K11+K12+K13	3	3	4
Wymagana suma punktów	8	11	12

KATEGORIA K1: Szafy do przechowywania materiałów niejawnych

KATEGORIA K2: Konstrukcja ścian, stropów i podłóg pomieszczenia lub zespołu pomieszczeń

KATEGORIA K3: Drzwi do pomieszczenia

KATEGORIA K4: Okna pomieszczenia

KATEGORIA K5: Budynki

KATEGORIA K6: System kontroli dostępu do pomieszczeń (obszaru)

KATEGORIA K7: Kontrola osób nieposiadających stałego upoważnienia do wejścia na teren JO (interesantów)

KATEGORIA K8: Telewizyjny system nadzoru w budynku

KATEGORIA K9: System alarmowy

KATEGORIA K10: Personel ochrony

KATEGORIA K11: Ogrodzenie

KATEGORIA K12: System kontroli osób i pojazdów

KATEGORIA K13: Telewizyjny system nadzoru w terenie, na którym usytuowany jest budynek

CZĘŚĆ III.

KLASYFIKACJE ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

Kategoria K1: Szafy do przechowywania materiałów niejawnych

Punktacja	Funkcja lub cechy
Typ 3 4 pkt	Szafa stalowa spełniająca wymagania klasy C.
Typ 2 3 pkt	Szafa stalowa spełniająca wymagania klasy B.
Typ 1 2 pkt	Szafa stalowa spełniająca wymagania klasy A.

Kategoria K2: Konstrukcja ścian, stropów i podłóg pomieszczenia lub zespołu pomieszczeń

Uwaga! W przypadku zastosowania czujek inercyjnych na przegrodach budowlanych przyznaje się dodatkowo 2 pkt dla przegród budowlanych Typu 1 lub 2.

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Przegrody budowlane murowane o grubości co najmniej 22 cm lub konstrukcji betonowej o grubości nie mniejszej niż 15 cm lub z materiału zapewniającego zbliżony lub większy poziom wytrzymałości.
Typ 3 3 pkt	Przegrody budowlane murowane o grubości co najmniej 20 cm lub konstrukcji betonowej o grubości nie mniejszej niż 12 cm lub z materiału zapewniającego zbliżony lub większy poziom wytrzymałości.
Typ 2 2 pkt	Przegrody budowlane murowane o grubości co najmniej 16 cm lub konstrukcji betonowej o grubości nie mniejszej niż 10 cm lub z materiału zapewniającego zbliżony lub większy poziom wytrzymałości.
Typ 1 1 pkt	Przegrody budowlane murowane lub z materiału zapewniającego zbliżony lub większy poziom wytrzymałości.

Kategoria K3: Drzwi do pomieszczenia

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Drzwi o odporności na włamanie klasy nie niższej niż RC4 wg PN-EN 1627 oraz dodatkowo, wyposażone w zamek mechaniczny szyfrowy, co najmniej klasy B wg Polskiej Normy PN-EN 1300 co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętło 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. 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. Zamek

	powinien być wyposażony 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. Dopuszcza się stosowanie drzwi o zwiększonej odporności na włamanie klasy C wg PN - 90/B/92270 dodatkowo wyposażonych w zamek szyfrowy o parametrach opisanych powyżej.
Typ 3 3 pkt	Drzwi o odporności na włamanie klasy nie niższej niż RC1N wg PN-EN 1627 lub równorzędne.
Typ 2 2 pkt	Pełne drzwi wzmocnione wyposażone w blokady przeciwwyważeniowe i w co najmniej dwa zamki, w tym jeden zamek certyfikowany lub wkładka klasy C albo kat. 3 wg PN-EN 1627 lub równorzędne.
Typ 1 1 pkt	Drzwi drewniane z co najmniej jednym zamkiem.

Kategoria K4: Okna pomieszczenia

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Brak otworów okiennych lub certyfikowane okna antywłamaniowe spełniające wymagania klasy odporności nie niższej niż RC 3 określone w Polskiej Normie PN-EN 1627 z szybą o podwyższonej odporności na włamanie - co najmniej klasy P 3A według PN-EN 356 lub rolety antywłamaniowe spełniające wymagania klasy odporności nie niższej niż RC 3 określone w Polskiej Normie PN-EN 1627 lub okno wyposażone w jedno z poniższych zabezpieczeń: - kraty zapewniające wysoką odporność na włamanie* - siatki z drutu stalowego w ramie**
Typ 3 3 pkt	Certyfikowane okna 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 lub okno posiadające zabezpieczenie przed otwarciem od wewnątrz wraz z folią antywłamaniową
Typ 2 2 pkt	Niezabezpieczone okna pomieszczeń usytuowanych na pozostałych kondygnacjach z wyłączeniem piwnic, parteru, ostatniej kondygnacji i poddasza.
Typ 1 1 pkt	Niezabezpieczone okna pomieszczeń piwnic, parteru, ostatniej kondygnacji i poddasza.

Zabezpieczenia, o których mowa w Typ 4, stosuje się do okien, które stanowią granicę "obszaru chronionego", o którym mowa w przepisach dotyczących ochrony obiektów wojskowych oraz do okien, które nie stanowią granicy "obszaru chronionego", w przypadku gdy ich dolna krawędź znajduje się na wysokości poniżej 5 m od poziomu otaczającego terenu i/lub górna krawędź znajduje się na wysokości mniejszej niż 3 m od poziomu dachu.

* Kraty zainstalowane 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 i wzmocnionymi płaskownikami stalowymi o przekroju nie mniejszym niż 45 x 6 mm, usytuowanymi w poziomie, w odstępach nie większych niż 500 mm.

Uwaga! Kraty stanowiące wartość zabytkową nie podlegają demontażowi.

Mocowanie krat w otworze okiennym powinny spełniać następujące wymagania:

- a) kraty mocuje się na co najmniej dwóch (przeciwnych) krawędziach,
- b) kraty muszą być mocowane za pomocą kotw o średnicy nie mniejszej niż średnica pręta kraty, wmurowanych w ścianę na głębokość minimum 100 mm, kotwy powinny być rozmieszczone w odstępach nie większych niż co 480 mm. Kotwy powinny być niewidoczne.

Co najmniej jedna z krat w pomieszczeniu lub zespole pomieszczeń powinna być rozsuwana lub otwierana oraz zabezpieczona nie mniej niż jedną kłódką klasy nie niższej niż 5 wg normy PN-EN-12320.

**** Mocowanie siatek powinno spełniać następujące wymagania:**

- a) siatki mocuje się od zewnętrznej strony okien budynków,
- b) ramę siatki mocuje się minimum na trzech krawędziach,
- c) rama siatki musi być mocowana za pomocą kotw wmurowanych w ścianę.

Siatki z drutu stalowego w ramie nie można stosować do okien, które stanowią granicę "obszaru chronionego", o którym mowa w przepisach dotyczących ochrony obiektów wojskowych, a ich dolna krawędź znajduje się na wysokości poniżej 5 m od poziomu otaczającego terenu i/lub górna krawędź znajduje się na wysokości mniejszej niż 3 m od poziomu dachu.

Kategoria K5: Budynki

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Budynek o konstrukcji murowanej, betonowej lub innej o podobnych parametrach konstrukcyjnych, wolnostojący, użytkowany samodzielnie, usytuowany w terenie ogrodzonym i strzeżonym. Drzwi wejściowe do budynku objęte są stałym nadzorem służby ochronnej i systemem kontroli dostępu.
Typ 3 3 pkt	Budynek o konstrukcji murowanej, betonowej lub innej o podobnych parametrach konstrukcyjnych, wolnostojący, użytkowany wspólnie z innymi JO, usytuowany w terenie ogrodzonym i strzeżonym. Drzwi wejściowe do budynku objęte są stałym nadzorem służby ochronnej i systemem kontroli dostępu.
Typ 2 2 pkt	Budynek o konstrukcji murowanej, betonowej lub innej o podobnych parametrach konstrukcyjnych, w zabudowie zwartej. Drzwi wejściowe do budynku zamykane po opuszczeniu go przez personel.
Typ 1 1 pkt	Budynek o innej konstrukcji użytkowany samodzielnie lub wspólnie z innymi JO.

Kategoria K6: System kontroli dostępu do pomieszczeń (obszaru)

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Elektroniczny system kontroli dostępu osób. Umożliwia rejestrowanie i archiwizację wejścia/wyjścia (czasu przebywania) osoby, z wyszczególnieniem: imienia i nazwiska, daty i czasu. Jest zainstalowany w przejściach i posiada antipass-back lub inny system podobnie działający. System generuje alarmy i ostrzeżenia o próbie nieuprawnionego dostępu do kontrolowanej strefy. Obejmuje wejścia i wyjścia z kontrolowanej strefy.
Typ 3 3 pkt	Elektroniczny system kontroli dostępu osób. Umożliwia rejestrowanie i archiwizację wejścia/wyjścia (czasu przebywania) osoby, z wyszczególnieniem: imienia i nazwiska, daty i czasu. Obejmuje wejścia i wyjścia z kontrolowanej strefy.
Typ 2 2 pkt	Ewidencja dostępu osób obejmująca rejestrowanie i archiwizację wejścia/wyjścia (czasu przebywania) osoby do/z pomieszczenia, obszaru, strefy z wyszczególnieniem: imienia i nazwiska, daty i czasu.

Typ 1 1 pkt	System kontroli osób wykonywany bez wspomagania urządzeniami technicznymi i elektronicznymi. Ewidencja wejścia/wyjścia w dokumentacji służbowej obsługi biura przepustek, lokalnego centrum nadzoru (LCN) lub innej służby.
----------------	---

Kategoria K7: Kontrola osób nieposiadających stałego upoważnienia do wejścia na teren JO (interesantów)

Punktacja	Funkcja lub cechy
Typ 2 2 pkt	Nadzór nad gościem przez uprawnionego do przyjmowania interesantów żołnierza lub pracownika przez cały czas wizyty w obiekcie (obszarze). Wydanie przepustki (identyfikatora) i zaewidencjonowanie danych gościa w dokumentacji obsługi biura przepustek lub lokalnego centrum nadzoru (LCN).
Typ 1 1 pkt	Nadzór nad gościem przez uprawnionego do przyjmowania interesantów żołnierza lub pracownika przez cały czas wizyty w obiekcie (obszarze). Wydanie przepustki (identyfikatora) i zaewidencjonowanie danych gościa w dokumentacji obsługi biura przepustek lub lokalnego centrum nadzoru (LCN). Goście w przypadkach uzasadnionych rodzajem wykonywanych obowiązków mogą uzyskać prawo do wstępu na teren części obiektu (obszaru) po zaewidencjonowaniu, bez konieczności nadzoru ze strony uprawnionego do przyjmowania interesantów żołnierza lub pracownika.

Kategoria K8: Telewizyjny system nadzoru w budynku

Punktacja	Funkcja lub cechy
Typ 2 2 pkt	Wejścia do budynku oraz pomieszczeń lub stref, objęte są telewizyjnym systemem nadzoru z pełną rejestracją zdarzeń i wideodetekcją.
Typ 1 1 pkt	Wejścia do budynku lub pomieszczeń (stref), objęte są telewizyjnym systemem nadzoru z pełną rejestracją zdarzeń.

Kategoria K9: System alarmowy

Punktacja	Funkcja lub cechy
Typ 3 3 pkt	System alarmowy sygnalizujący nieuprawnione otwarcie drzwi wejściowych i okien, ruch w pomieszczeniach oraz próby napadu. W systemie wykorzystuje się dwa rodzaje czujek ruchu, których działanie opiera się na odmiennych zjawiskach fizycznych.
Typ 2 2 pkt	System alarmowy sygnalizujący nieuprawnione otwarcie drzwi wejściowych i okien, ruch w pomieszczeniach oraz próby napadu. W systemie wykorzystuje się czujki ruchu, których działanie opiera się na jednym rodzaju zjawiska fizycznego.
Typ 1 1 pkt	System alarmowy, sygnalizujący nieuprawnione otwarcie drzwi wejściowych i okien oraz próby napadu.

Kategoria K10: Personel ochrony

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Służba dyżurna i siły ochronne w systemie ciągłym i całodobowym. Ochrona jest realizowana na całym terenie obiektu przez służbę wartowniczą i patrole lub inne formacje ochronne.
Typ 3 3 pkt	Służba dyżurna i siły ochronne w systemie dziennym we wszystkie dni tygodnia. Ochrona jest realizowana na całym terenie obiektu przez służbę wartowniczą lub inne formacje ochronne.
Typ 2 2 pkt	Służba dyżurna i siły ochronne w systemie dziennym tylko w dni robocze. Ochrona jest realizowana na całym terenie obiektu przez służbę wartowniczą lub inne formacje ochronne.
Typ 1 1 pkt	Patrol interwencyjny realizowany przez pracowników specjalistycznej uzbrojonej formacji ochronnej.

W JO należy opracować procedury działania personelu ochrony na incydenty/sygnały alarmowe oraz sposób pełnienia służby uwzględniające w szczególności objęcie bezpośrednią ochroną fizyczną w postaci posterunku wystawianego przy budynku lub okresowe patrolowanie terenu wokół budynku, przy czym:

- przy wysokim poziomie zagrożeń - nie rzadziej niż raz w dzień i dwa razy w nocy. Czas reakcji wartowników/pracowników ochrony w przypadku wystąpienia sytuacji alarmowych i dotarcia do miejsca zdarzenia nie dłuższy niż 5 min,
- przy średnim poziomie zagrożeń - nie rzadziej niż raz w dzień i raz w nocy. Czas reakcji wartowników/pracowników ochrony w przypadku wystąpienia sytuacji alarmowych i dotarcia do miejsca zdarzenia nie dłuższy niż 10 min,
- przy niskim poziomie zagrożeń - nie rzadziej niż raz w nocy. Czas reakcji wartowników/pracowników ochrony w przypadku wystąpienia sytuacji alarmowych i dotarcia do miejsca zdarzenia nie dłuższy niż 10 min. Ponadto należy przyjąć zasadę, iż głównym celem interwencji personelu ochrony na incydenty/sygnały alarmowe jest odizolowanie miejsca/obszaru zagrożonego.

Kategoria K11: Ogrodzenie

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Jest wykonane z trwałych materiałów (stal, cegła, itp.). Minimalna wysokość zasadniczej części ogrodzenia wynosi co najmniej 2 m. Górna część na całej długości zabezpieczona jest przed przechodzeniem (np. poprzez zastosowanie ostrych elementów) lub jest wspomagane systemem alarmowym.
Typ 3 3 pkt	Jest wykonane ze stałych, lżejszych metalowych materiałów (np. siatka druciana). Minimalna wysokość ogrodzenia wynosi co najmniej 2 m.
Typ 2 2 pkt	Jest wykonane z trwałych materiałów, a wysokość ogrodzenia wynosi poniżej 2 m.
Typ 1 1 pkt	Wyznacza wyłącznie granice terenu i zapewnia minimalne zabezpieczenie przed nieuprawnionym dostępem.

Kategoria K12: System kontroli osób i pojazdów

Punktacja	Funkcja lub cechy
Tak = 1 pkt Nie = 0 pkt	Kontrola osób przy użyciu elektronicznego systemu kontroli dostępu (bramki, kołowroty, drzwi). Pojazdy kontrolowane na podstawie przepustek lub elektronicznego systemu kontroli dostępu pojazdów. Wjazd/wyjazd zabezpieczony szlabanem lub zamykaną bramą. Możliwość kontroli wnoszonego bagażu przy użyciu wykrywacza metali lub detektorów. Wjazd/wyjazd pojazdów nadzorowany przez telewizyjny system nadzoru.

Kategoria K13: Telewizyjny system nadzoru w terenie, na którym usytuowany jest budynek

Punktacja	Funkcja lub cechy
Typ 4 4 pkt	Cały teren lub granice obiektu objęte są telewizyjnym systemem nadzoru.
Typ 3 3 pkt	Zewnętrzne granice budynku objęte są telewizyjnym systemem nadzoru.
Typ 2 2 pkt	Część budynku, w tym wejścia, objęte są telewizyjnym systemem nadzoru.
Typ 1 1 pkt	Czynne wejście do budynku objęte jest telewizyjnym systemem nadzoru.

Klasyfikacja i wymagania techniczne dla urządzeń do przechowywania zasobów kryptograficznych zawierających informacje niejawne

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 (rygle 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 (rygle 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 zaślepiony otwór umożliwiający jej zakotwienie.
8. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, potwierdzający zgodność wyrobu z wymaganiami klasy A.
9. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:
 - 1) nazwę wyrobu;
 - 2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
 - 3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu;
 - 4) masę.

II.

Szafa stalowa klasy B

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 3 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone rygłem na czterech krawędziach.
4. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygle w średnicy min. 15 mm lub przekroju min. 175 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 (rygle 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; rygle przyzawiasowe mogą być stałe.
6. Mechanizm ryglowy w drzwiach musi być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grapie 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. Z szafą powinny być dostarczone dwa komplety kluczy;
 - 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 pokrętło i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Szafa powinna być wyposażona w klucz 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 zamknięte 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 (rygle 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

(rygle 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; rygle przyzawiasowe mogą być stałe.

6. Mechanizm ryglowy w drzwiach musi być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglowy, w tym:
 - 1) zamek mechaniczny kluczowy, co najmniej klasy B wg Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Z szafą powinny być dostarczone dwa komplety kluczy;
 - 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 pokrętło 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. 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 klucz 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 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.

IV.
Oznaczenie szaf stalowych

Każdą szafę, w której przechowywane są materiały niejawne, należy oznaczyć w sposób jednoznacznie wskazujący dane, pozwalające na identyfikację osoby odpowiedzialnej za przechowywane w niej materiały. W tym celu, stosuje się kartę informacyjną, której wzór został umieszczony poniżej.

Karta informacyjna na drzwi urządzeń do przechowywania materiałów niejawnych

CHROŃ INFORMACJE NIEJAWNE SZAFA nr fabryczny
Odpowiedzialny:
PRZED OPUSZCZENIEM MIEJSCA PRACY ZABEZPIECZ POWIERZONE CI MATERIAŁY NIEJAWNE

Wymagania konstrukcyjne oraz wymagania w zakresie zabezpieczenia fizycznego i technicznego kontenerów MKK, PKK oraz PKKs

1. Kontenery mające stanowić nowy sprzęt wojskowy muszą posiadać pozytywną opinię wydaną przez SKW potwierdzającą spełnienie wymagań z zakresu zabezpieczenia fizycznego i technicznego.
2. Kontenery powinny być wykonane z płyt warstwowych składających się z co najmniej dwóch warstw blach (stopów aluminiowych lub stali) o grubości minimum 1 mm każda z nich, konstrukcyjnie ze sobą połączonych, oddzielonych od siebie co najmniej 50 mm warstwą twardego niepalnego materiału izolacyjnego. Materiał ten musi charakteryzować się również niską higroskopijnością oraz dźwiękochłonnością (zgodnie z przepisami BHP w tym zakresie).
3. W przypadku wystąpienia innych rozwiązań konstrukcyjno-technicznych muszą one spełniać wymagania nie mniejsze niż określone w pkt 2. Przyjęte rozwiązanie techniczne potwierdzone powinno być, w zakresie spełniania wymagań odporności, stosownym dokumentem (certyfikat, deklaracja zgodności) wydanym przez uprawniony podmiot.
4. Płyty warstwowe na narożach powinny być zespawane i wyposażone w zaczepy transportowe umożliwiające mocowanie w czasie przewożenia różnymi środkami transportu oraz manewrowania.
5. Drzwi wejściowe główne do kontenera powinny:
 - 1) spełniać wymagania klasy odporności nie niższej niż RC2, określone w Polskiej Normie PN-EN1627, posiadać element samozatraskowy, uniemożliwiający pozostawienie pomieszczenia otwartego (np. elektro zaczep, elektro zwora) oraz dodatkowo wyposażone w zamek mechaniczny szyfrowy, co najmniej klasy B według Polskiej Normy PN-EN1300;
 - 2) być ryglowane od wewnątrz o konstrukcji uniemożliwiającej ich zablokowanie od zewnątrz (z wyłączeniem zamków), w czasie pracy personelu w kontenerze;
 - 3) być wyposażone w mechanizm samozamykający (domykający);
 - 4) być wyposażone w urządzenie umożliwiające podgląd bezpośredniego zewnętrznego otoczenia.
6. Kontenery powinny posiadać właz ewakuacyjny otwierany od wewnątrz.
7. Posiadane otwory urządzeń wentylacyjnych i klimatyzacyjnych powinny być zabezpieczone siatką stalową o grubości nie mniejszej niż 2 mm, o oczkach nie większych niż 20x20 mm lub powierzchni oczka nie większej niż 4 cm².
8. Kontenery powinny być wyposażone w system alarmowy z tym, że:
 - 1) powinien on sygnalizować nieuprawnione otwarcie drzwi wejściowych, włazu ewakuacyjnego i okien, ruch w pomieszczeniach oraz próby napadu;
 - 2) powinien spełniać wymagania techniczne i organizacyjne określone w stosowanej normie dotyczącej systemów alarmowych montowanych w obiektach wojskowych.
9. Kontenery powinny być wyposażone w system sygnalizacji przeciwpożarowej wewnętrznej i zewnętrznej.
10. W przypadku opcjonalnie zamontowanych okien powinny być one antywłamaniowe, certyfikowane (kwalifikowane) w zakresie spełniania wymagań klasy odporności nie niższej niż RC3, określone w Polskiej Normie PN-EN1627.
11. Dopuszcza się doposażenie kontenerów w innego typu sprzęt (urządzenia) wymagane na podstawie odrębnych przepisów.
12. W kontenerach, w których przewiduje się przyjmowanie interesantów należy wydzielić część kabiny przeznaczonej na czytelną (miejsce do zapoznawania się z materiałami

niejawnymi). Część kabiny należy fizycznie oddzielić poprzez zastosowanie stałej przegrody wewnętrznej. Przy zabudowie należy wziąć pod uwagę umożliwienie personelowi KK prowadzenie nadzoru nad osobą przebywającą w czytelni oraz sterowanie funkcją otwarcia drzwi wejściowych.

13. Czytelnia powinna być zorganizowana w takim miejscu, aby osoba zapoznająca się z materiałem niejawnym nie posiadała możliwości bezpośredniego dostępu do urządzeń do przechowywania informacji niejawnych, urządzeń do niszczenia materiałów niejawnych oraz systemów teleinformatycznych, z wyjątkiem tych, które przeznaczone są dla interesantów.

**Formularz z kodami dostępu, kodami systemu alarmowego do pomieszczeń kancelarii
kryptograficznej, urzędów 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:	
<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*

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/urzędzeniu

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	
** 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)		
Podlega ochronie przewidzianej dla materiałów niejawnych o klauzuli tajności *		

* klauzula tajności odpowiada najwyżej sklasyfikowanej informacji przechowywanej w pomieszczeniu/urzędzeniu

WZÓR

PLAN
PRZEPROWADZENIA INSPEKCJI KRYPTOGRAFICZNEJ

I. Temat inspekcji kryptograficznej:

Inspekcja kryptograficzna w

II. Cel inspekcji kryptograficznej:

1. Dokonać oceny funkcjonowania OBSŁ.
2.

III. Zakres inspekcji kryptograficznej:

BEZPIECZEŃSTWO ZASOBÓW KRYPTOGRAFICZNYCH

1. Sprawdzenie zaświadczenia o funkcjonowaniu/powołaniu KK.
2. Sprawdzenie posiadania przez personel OBSŁ, użytkowników 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/powołaniu KK.
3. Sprawdzenie prawidłowości wyznaczenia na stanowiska personelu OBSŁ oraz poprawności wystawiania KWP ww. personelu.
4. Sprawdzenie posiadanych kursów specjalistycznych personelu OBSŁ.
5. Analiza zawartości teczki z protokołami inspekcji kryptograficznych i innych form kontroli oraz sprawdzenie wykonania zaleceń w nich zawartych.
6. Sprawdzenie aktualności podstaw zaopatrywania innej JO w materiały kryptograficzne.
7. Sprawdzenie prawidłowości wydania oraz aktualności wydanych CUK.
8. Sprawdzenie poprawności ewidencji szkoleń w zakresie bezpieczeństwa materiałów kryptograficznych, (plany konspekty, lista obecności).
9. Sprawdzenie posiadania instrukcji pracy KK oraz instrukcji dotyczącej postępowania z zasobami kryptograficznymi w sytuacjach zagrożenia.
10. Porównanie opracowanych instrukcji dotyczących postępowania z zasobami kryptograficznymi w sytuacjach zagrożenia z planami ochrony danej JO.
11. Sprawdzenie funkcjonowania stref ochronnych oraz systemu sygnalizacji włamania i napadu (SSWiN) do pomieszczeń KK oraz innych pomieszczeń, w których eksploatowane są zasoby kryptograficzne.
12. Sprawdzenie systemu kontroli dostępu (SKD) do pomieszczeń KK oraz innych pomieszczeń, w których eksploatowane są zasoby kryptograficzne.
13. Sprawdzenie zabezpieczenia kluczy użytku bieżącego oraz kluczy zapasowych do pomieszczeń i urządzeń do przechowywania informacji niejawnych, w których przechowywane są zasoby kryptograficzne.

14. Sprawdzenie dokonywania zmian ustawień kodów dostępu (kombinacji) w zamkach szyfrowych i SSWiN oraz sprawdzenie przechowywania tych kodów.
15. Sprawdzenie certyfikatów drzwi wejściowych do KK oraz urządzeń do przechowywania informacji niejawnych, w których przechowywane są zasoby kryptograficzne.
16. Sprawdzenie zabezpieczeń eksploatowanych produktów kryptograficznych, a także sprawdzenie przechowywania zapasowych produktów kryptograficznych.
17. Sprawdzenie stanu środków przeznaczonych do niszczenia oraz ewakuacji zasobów kryptograficznych.
18. Sprawdzenie zasad rutynowego niszczenia zasobów kryptograficznych, w tym dokumentów kryptograficznych, które przestały obowiązywać lub zostały wykorzystane, oraz kontrola postępowania z pozostałościami powstającymi w trakcie niszczenia.
19. Sprawdzenie realizacji czynności po wystąpieniu incydentów kryptograficznych.
20. Sprawdzenie u użytkowników sposobu przechowywania zasobów kryptograficznych.

PROWADZENIE EWIDENCJI ZASOBÓW KRYPTOGRAFICZNYCH

1. Sprawdzenie „Rejestru teczek materiałów kryptograficznych, dzienników i ksiąg ewidencyjnych”.
2. Sprawdzenie znajomości i przestrzegania przez kierownika KK oraz jego zastępcy umiejętności postępowania z zasobami kryptograficznymi, a także przestrzegania zasad ich ewidencji.
3. Sprawdzenie, czy prowadzona ewidencja odzwierciedla wszystkie posiadane zasoby 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 czy zasoby kryptograficzne, które zostały wykorzystane lub przestały obowiązywać są zniszczone zgodnie z obowiązującymi w tym zakresie przepisami.
7. Sprawdzanie prawidłowości wykonania protokołów zniszczonych zasobów kryptograficznych.
8. Sprawdzenie terminowego przesyłania do kancelarii zaopatrującej potwierdzeń zniszczenia zasobów kryptograficznych.
9. Sprawdzenie publikacji kryptograficznych zawierających wprowadzone zmiany i poprawki oraz czy są one właściwie ewidencjonowane.
10. Sprawdzenie poprawności oznakowania nośników danych.
11. Sprawdzenie posiadania w KK dokumentu określającego klasyfikację rzeczową akt kryptograficznych (wypisu z jrw/wykazu/rejestru JO dotyczącej KK).

BEZPIECZEŃSTWO SYSTEMÓW ŁĄCZNOŚCI

1. Sprawdzenie, czy w JO, w której przeprowadzana jest inspekcja kryptograficzna, są wytwarzane i przetwarzane, przy użyciu systemów łączności, zasoby kryptograficzne.
2. Sprawdzenie u użytkowników przestrzegania wymagań w zakresie ochrony zasobów kryptograficznych wytwarzanych i przetwarzanych w eksploatowanych systemach łączności, o których mowa w pkt 1.
3. Sprawdzenie, czy systemy łączności, o których mowa w pkt 1, posiadają zatwierdzoną aktualną dokumentację normującą ich funkcjonowanie.

4. Sprawdzenie, czy KJO wyznaczył personel odpowiedzialny za funkcjonowanie systemów łączności, o których mowa w pkt 1, zgodnie z dokumentacją, o której mowa w pkt 3.
5. Sprawdzenie czy dokumentacja, o której mowa w pkt 3, jest właściwie aktualizowana (czy istnieją aneksy).
6. Sprawdzenie czy wszystkie osoby wytwarzające dokumenty (wg. DEWD) znajdują się na liście użytkowników uprawnionych do pracy w systemie łączności.
7. Sprawdzenie czy administrator systemu teleinformatycznego prowadzi okresowe szkolenia użytkowników z zakresu użytkowania systemu teleinformatycznego.
8. Sprawdzenie czy procedury deponowania IND są realizowane zgodnie z zapisami dokumentacji bezpieczeństwa systemu łączności.
9. Sprawdzenie czy DEWD jest prowadzony właściwie.

IV. Termin przeprowadzenia inspekcji kryptograficznej:

Inspekcja kryptograficzna przeprowadzona zostanie w dniach20.... r.

V. Skład komisji:

Przewodniczący: -

Członkowie: -

-

VI. Sposób przedstawienia wyników inspekcji kryptograficznej:

Na podstawie ustaleń inspekcji kryptograficznej sporządzony zostanie protokół z inspekcji kryptograficznej przedstawiony KJO zarządzającej inspekcję kryptograficzną.

Uwaga:

Na Planie przeprowadzenia inspekcji kryptograficznej nie nanosi się oznaczenia „KRYPTO”.

WZÓR

Upoważnienie do przeprowadzenia inspekcji kryptograficznej

.....
Miejscowość, dnia

.....
(nazwa organu zarządzającego inspekcję kryptograficzną)

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 JO inspekcji)

Upoważnienie niniejsze ważne jest za okazaniem legitymacji służbowej (dowodu osobistego).
Ważność upoważnienia upływa z dniem 20 ... r.

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

mp.
(pieczęć okrągła organu zarządzającego inspekcję kryptograficzną)

Ważność upoważnienia przedłuża się do dnia

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

mp.
(pieczęć okrągła organu zarządzającego inspekcję kryptograficzną)

....., dnia r.

WZÓR

PROTOKÓŁ Z INSPEKCJI KRYPTOGRAFICZNEJ

W

(nazwa jednostki (komórki) organizacyjnej)

I. Inspekcję kryptograficzną przeprowadziła komisja z w składzie:

(nazwa JO przeprowadzającej inspekcję)

- – przewodniczący;
-
-

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

III. Osoby funkcyjne z OBSŁ¹⁾:

- Oficer BSŁ -, na stanowisku od r. do r.;
(stopień, imię i nazwisko)
- Zastępca Oficera BSŁ -, na stanowisku od r. do r.;
(stopień, imię i nazwisko)
- Kierownik KK -, na stanowisku od r. do r.;

¹⁾ wymienić wszystkie osoby funkcyjne za okres objęty inspekcją kryptograficzną

(stopień, imię i nazwisko)

– Zastępca Kierownika KK -, na stanowisku od r. do r.;

(stopień, imię i nazwisko)

IV. Ogólna charakterystyka OBSŁ poddanego inspekcji kryptograficznej:

(m.in. główne zadania i przeznaczenie OBSŁ, w tym informacja o innych JO zaopatrywanych w materiały kryptograficzne)

V. Zagadnienia podlegające inspekcji kryptograficznej:

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
BEZPIECZEŃSTWO ZASOBÓW KRYPTOGRAFICZNYCH						
1.	Sprawdzenie zaświadczenia o funkcjonowaniu/powołaniu KK.	☐	☐	☐	☐	Sprawdzeniem objąć aktualność zapisów oraz spełnienie warunków wydanego zaświadczenia (dotyczy JO/KO, w których powołana jest KK).
2.	Sprawdzenie posiadania przez personel OBSŁ, użytkowników 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/powołaniu KK.	☐	☐	☐	☐	Sprawdzeniem objąć KJO i jego etatowego Zastępcę oraz osoby funkcyjne personelu OBSŁ, tj.: Oficera BSŁ i jego zastępcę, personel KK oraz użytkowników materiałów wydanych z KK za okres objęty inspekcją kryptograficzną, tj.: daty ważności poświadczeń bezpieczeństwa i certyfikatów NATO / UE, ich klauzule tajności oraz zaświadczenia stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych.

²⁾ opisać w kolumnie: Ustalenia / Uwagi / Rozbieżności

³⁾ opisać w kolumnie: Ustalenia / Uwagi / Rozbieżności

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
3.	Sprawdzenie prawidłowości wyznaczenia na stanowiska personelu OBSŁ oraz poprawności wystawiania KWP ww. personelu.	☐	☐	☐	☐	<i>Sprawdzeniu podlega:</i> <i>Rozwiązanie organizacyjno-etatowe dotyczące posiadania etatowej komórki organizacyjnej funkcjonującej w JO, odpowiedzialnej za obieg zasobów kryptograficznych.</i> <i>Podstawa wyznaczenia (R-z/Decyzja KJO) na stanowisko Oficera BSL, jego zastępcy i personelu KK oraz ciągłość pełnienia obowiązków ww. personelu, w tym protokołu przekazania obowiązków na stanowisku kierownika KK.</i>
4.	Sprawdzenie posiadanych kursów specjalistycznych personelu OBSŁ.	☐	☐	☐	☐	<i>Sprawdzeniem objąć zaświadczenia/świadectwa ukończenia kursów specjalistycznych wymaganych na zajmowanych stanowiskach służbowych.</i>
5.	Analiza zawartości teczki z protokołami inspekcji kryptograficznych i innych form kontroli oraz sprawdzenie wykonania zaleceń w nich zawartych.	☐	☐	☐	☐	<i>Sprawdzeniem objąć informacje o realizacji zaleceń oraz ich wykonanie.</i>
6.	Sprawdzenie aktualności podstaw zaopatrywania innej JO w materiały kryptograficzne	☐	☐	☐	☐	
7.	Sprawdzenie prawidłowości wydania oraz aktualności wydanych CUK.	☐	☐	☐	☐	<i>Sprawdzeniem objąć:</i> <i>Podstawę wydania CUK.</i> <i>Poprawność zakresu CUK do udostępnianych materiałów kryptograficznych.</i> <i>Poprawność wypełniania formularza CUK oraz aktualność zapisów w nim zawartych.</i> <i>Poprawność ewidencji CUK.</i> <i>Poprawność niszczenia formularzy CUK.</i>

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
8.	Sprawdzenie poprawności ewidencji szkoleń w zakresie bezpieczeństwa materiałów kryptograficznych, (plany konspekty, lista obecności).	☐	☐	☐	☐	<i>Sprawdzeniem objąć:</i> 1. Książkę ewidencji wydanych CUK. 2. Podstawę przeprowadzenia szkolenia (np. plany konspekty). 3. Potwierdzenie przeprowadzenia szkolenia (np. listy obecności).
9.	Sprawdzenie posiadania instrukcji postępowania z zasobami kryptograficznymi w sytuacjach zagrożenia oraz instrukcji pracy KK.	☐	☐	☐	☐	<i>Sprawdzeniu podlegają m.in.:</i> 1. Zawarte w instrukcjach procedury dotyczące niszczenia, ewakuacji i postępowania z zasobami kryptograficznymi na wypadek zagrożenia. 2. Możliwość realizacji ww. procedur w warunkach funkcjonowania JO/KO. 3. Znajomość przez personel OBSŁ instrukcji oraz zadań z nich wynikających.
10.	Porównanie opracowanych instrukcji dotyczących postępowania z zasobami kryptograficznymi w sytuacjach zagrożenia z planami ochrony danej JO.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in.:</i> 1. Spójność zapisów dotyczących ewakuacji KK. 2. Praktyczne działanie personelu ochrony. 3. Czas reakcji wartowników/pracowników ochrony w przypadku wystąpienia sytuacji alarmowych i dotarcia do miejsca zdarzenia.

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
11.	Sprawdzenie funkcjonowania stref ochronnych oraz systemu sygnalizacji włamania i napadu (SSWiN) do pomieszczeń KK oraz innych pomieszczeń w których eksploatowane są zasoby kryptograficzne.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in.:</i> <i>Wyznaczenie stref ochronnych zgodnie z Planem ochrony informacji niejawnych.</i> <i>Deklaracja zgodności SSWiN oraz częstotliwość jego konserwacji (umowa na konserwację).</i> <i>Wyznaczenie administratora SSWiN (podstawa, posiadane uprawnienia).</i> <i>Analiza rejestrów SSWiN przez personel OBSŁ i potwierdzenie jej wykonania (np. w książce meldunków).</i>
12.	Sprawdzenie systemu kontroli dostępu (SKD) do pomieszczeń KK oraz innych pomieszczeń, w których eksploatowane są zasoby kryptograficzne.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in.:</i> <i>Okres przechowywania rejestrów SKD.</i> <i>Analiza rejestrów SKD przez personel OBSŁ i potwierdzenie jej wykonania (np. w książce meldunków).</i>
13.	Sprawdzenie zabezpieczenia kluczy użytku bieżącego oraz kluczy zapasowych do pomieszczeń i urządzeń do przechowywania informacji niejawnych, w których przechowywane są zasoby kryptograficzne.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in. okres rotacji oraz ciągłość przechowywania kluczy zapasowych.</i>
14.	Sprawdzenie dokonywania zmian ustawień kodów dostępu (kombinacji) w zamkach szyfrowych i SSWiN oraz sprawdzenie przechowywania kodów do zamków szyfrowych.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in. okres zmian ustawień oraz ciągłość przechowywania kodów do zamków szyfrowych.</i>

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
15.	Sprawdzenie certyfikatów drzwi wejściowych do KK oraz urządzeń do przechowywania informacji niejawnych, w których przechowywane są zasoby kryptograficzne.	☐	☐	☐	☐	
16.	Sprawdzenie zabezpieczeń eksploatowanych produktów kryptograficznych, a także sprawdzenie przechowywania zapasowych produktów kryptograficznych.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in. wizualny stan produktów kryptograficznych w tym plomb na obudowach w zakresie prób manipulacji/penetracji (wymienić typy oraz nr fabryczne sprawdzanych urządzeń).</i>
17.	Sprawdzenie stanu środków przeznaczonych do niszczenia oraz ewakuacji zasobów kryptograficznych.	☐	☐	☐	☐	<i>Sprawdzeniu podlegają m.in.:</i> 1. <i>Środki do niszczenia (niszczarki, narzędzia dewastacyjne).</i> 2. <i>Środki do ewakuacji (worki, pojemniki, skrzynie oraz sposób ich zabezpieczenia i oznaczenia).</i>
18.	Sprawdzenie zasad rutynowego niszczenia zasobów kryptograficznych, w tym dokumentów kryptograficznych, które przestały obowiązywać lub zostały wykorzystane, oraz kontrola postępowania z pozostałościami powstającymi w trakcie niszczenia.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in. przestrzeganie terminów niszczenia (kasowania)</i>
19.	Sprawdzenie realizacji czynności po wystąpieniu incydentów kryptograficznych.	☐	☐	☐	☐	
20.	Sprawdzenie u użytkowników sposobu przechowywania zasobów kryptograficznych.	☐	☐	☐	☐	<i>W przypadku odstępstw, sprawdzeniu podlega m.in. zgoda KJO na przechowywanie zasobów kryptograficznych w pomieszczeniach służbowych niespełniających warunków.</i>

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
PROWADZENIE EWIDENCJI ZASOBÓW KRYPTOGRAFICZNYCH						
1.	Sprawdzenie „Rejestru teczek materiałów kryptograficznych, dzienników i ksiąg ewidencyjnych”.	☐	☐	☐	☐	
2.	Sprawdzenie znajomości i przestrzegania przez personel KK umiejętności postępowania z zasobami kryptograficznymi, a także przestrzegania zasad ich ewidencji.	☐	☐	☐	☐	
3.	Sprawdzenie, czy prowadzona ewidencja odzwierciedla wszystkie posiadane zasoby kryptograficzne.	☐	☐	☐	☐	<i>Sprawdzeniu podlega m.in.:</i> <i>1. Roczny raport o stanie posiadanych zasobów kryptograficznych.</i> <i>2. Wykaz zaopatrywanych KK.</i> <i>3. Raporty przekazania materiałów kryptograficznych, w tym dotyczące przekazania odrębnego.</i> <i>4. Sprawdzenie poprawności prowadzenia ewidencji w DSI.</i>
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.	☐	☐	☐	☐	

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
6.	Sprawdzenie czy zasoby kryptograficzne, które zostały wykorzystane lub przestały obowiązywać są zniszczone zgodnie z obowiązującymi w tym zakresie przepisami.	☐	☐	☐	☐	
7.	Sprawdzanie prawidłowości wykonania protokołów zniszczonych zasobów kryptograficznych.	☐	☐	☐	☐	
8.	Sprawdzenie terminowego przesyłania do kancelarii zaopatrującej potwierdzeń zniszczenia zasobów kryptograficznych.	☐	☐	☐	☐	
9.	Sprawdzenie publikacji kryptograficznych zawierających wprowadzone zmiany i poprawki oraz czy są one właściwie ewidencjonowane.	☐	☐	☐	☐	
10.	Sprawdzenie poprawności oznakowania nośników informacji.	☐	☐	☐	☐	
11.	Sprawdzenie posiadania w KK dokumentu określającego klasyfikację rzeczową akt kryptograficznych (wypisu z jrw wykazu/rejestru JO dotyczącej KK).	☐	☐	☐	☐	

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
BEZPIECZEŃSTWO SYSTEMÓW ŁĄCZNOŚCI						
1.	Sprawdzenie, czy w JO ⁴⁾ , w której przeprowadzana jest inspekcja kryptograficzna, są wytwarzane i przetwarzane, przy użyciu systemów łączności, zasoby kryptograficzne.	☐	☐	☐	☐	Wymienić nazwy JO oraz systemów łączności
2.	Sprawdzenie u użytkowników przestrzegania wymagań w zakresie ochrony zasobów kryptograficznych wytwarzanych i przetwarzanych w eksploatowanych systemach łączności, o których mowa w pkt 1.	☐	☐	☐	☐	
3.	Sprawdzenie, czy systemy łączności, o których mowa w pkt 1, posiadają zatwierdzoną aktualną dokumentację normującą ich funkcjonowanie.	☐	☐	☐	☐	Sprawdzeniu podlega dokumentacja wymieniona w zaleceniach SKW dotyczących zarządzania materiałami kryptograficznymi.
4.	Sprawdzenie, czy KJO wyznaczył personel odpowiedzialny za funkcjonowanie systemów łączności, o których mowa w pkt 1, zgodnie z dokumentacją, o której mowa w pkt 3.	☐	☐	☐	☐	

⁴⁾ dotyczy również innych JO dla których OBSŁ jest jednocześnie OBSŁ, w której przeprowadzana jest inspekcja kryptograficzna.

LP	Zagadnienie podlegające sprawdzeniu	Wynik				Ustalenia / Uwagi / Rozbieżności
		Spełnia	Nie spełnia ²⁾	Nie dotyczy	Rozbieżność ³⁾	
5.	Sprawdzenie czy dokumentacja, o której mowa w pkt 3 jest właściwie aktualizowana (czy istnieją aneksy).	☐	☐	☐	☐	
6.	Sprawdzenie czy wszystkie osoby wytwarzające dokumenty (wg DEWD) znajdują się na liście użytkowników uprawnionych do pracy w systemie łączności.	☐	☐	☐	☐	
7.	Sprawdzenie czy administrator systemu teleinformatycznego prowadzi okresowe szkolenia użytkowników z zakresu użytkowania systemu teleinformatycznego.	☐	☐	☐	☐	
8.	Sprawdzenie czy procedury deponowania IND są realizowane zgodnie z zapisami dokumentacji bezpieczeństwa systemu łączności.	☐	☐	☐	☐	
9.	Sprawdzenie czy DEWD jest prowadzony właściwie.	☐	☐	☐	☐	

VI. Ustalenia inspekcji kryptograficznej:

(opis ustaleń inspekcji kryptograficznej na podstawie zagadnień podlegających inspekcji kryptograficznej)

VII. Podsumowanie.

(ogólna ocena wyników inspekcji kryptograficznej)

VIII. Wnioski i zalecenia.

(przedstawić wnioski i zalecenia wynikające z ustaleń inspekcji kryptograficznej, w chronologii wynikającej z opisu ustaleń)

KJO, w której przeprowadzono inspekcję kryptograficzną, zobowiązuje się niezwłocznie do podjęcia działań celem usunięcia nieprawidłowości opisanych w niniejszym protokole, z jednoczesnym powiadomieniem o podjętych działaniach nadrzędny OBSŁ oraz KOGD w terminie do 30 dni, od dnia sporządzenia niniejszego protokołu.

**KIEROWNIK
JEDNOSTKI ORGANIZACYJNEJ**

.....

(stopień, imię i nazwisko)

**PRZEWODNICZĄCY
INSPEKCJI KRYPTOGRAFICZNEJ**

.....

(stopień, imię i nazwisko)

Wykonano w egz. pojedynczym

Sporządził:

Uwaga:

Na Protokole z inspekcji kryptograficznej nie nanosi się oznaczenia „KRYPTO”.

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 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

WZÓR

DZIENNIK EWIDENCJI SZYFROGRAMÓW

Data założenia r.

Data zakończenia r.

Lewa strona

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

Prawa strona

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

WZÓR

Książka doręczeń przesylek miejscowych

[illegible]

WZÓR

Książka depozytu zasobów kryptograficznych

[illegible]

WZÓR

Karta ewidencyjna dokumentu kryptograficznego (formularz AF 54 A PL)

<i>(KLAUZULA TAJNOŚCI właściwa po wypełnieniu)</i>											
										KRYPTO	
										<i>Strona ze stron</i>	
CZĘŚĆ A Dane wchodzące			KLAUZULA: TAJNOSCI	Pełna nazwa:				Nazwa skrócona:		Kancelaria	
Rejestr / edycja	Numer seryjny		Ilość	Otrzymane od	Numer formularza	Data odbioru	Data ważności	Zniszczenie	Inwentaryzacja	Uwagi	
	Początkowy	Końcowy									
CZĘŚĆ B Dane wychodzące											
Rejestr / edycja	Ilość	Numer seryjny		Dyspozycje		Dyspozycje		Dyspozycje		Zniszczenie lokalne	Zniszczenie zbiorcze
		od	do	Kancelaria	Dane	Kancelaria	Dane	Kancelaria	Dane		
<i>(KLAUZULA TAJNOŚCI właściwa po wypełnieniu)</i>											
Skrócona nazwa:											

(KLAUZULA TAJNOŚCI właściwa po wypełnieniu)

KRYPTO

Strona ze stron

[illegible]

(KLAUZULA TAJNOŚCI właściwa po wypełnieniu)

Skrócona nazwa:

WZÓR

Karta ewidencyjna produktu kryptograficznego (formularz AF 54 B PL)

[illegible]

[illegible]

WZÓR

Karta ewidencyjna publikacji, wydawnictw kryptograficznych oraz dokumentacji technicznej systemów i produktów kryptograficznych (formularz AF 54 C PL)

[illegible]

FORMULARZ AF 54 C PL

WZÓR

Formularz AF 147 PL

.....(rok)

KRYPTO[illegible]

WZÓR

Raport materiału kryptograficznego (formularz SF 153 (PL))

COMSEC MATERIAL REPORT									
RAPORT MATERIAŁU KRYPTOGRAFICZNEGO									
1.	TRANSFER PRZEKAZANIE	INVENTORY INWENTARYZ ACJA	DESTRUCTION ZNISZCZENIE	HAND RECEIPT PRZEKAZANIE ODRĘCZNE	OTHER: INNE:				
2. FROM: ACCT NO. OD: KANCELARIA NR:				3. DATE OF REPORT (Year, Month, Day) Data wykonania (rok, miesiąc, dzień)		4. OUTGOING NUMBER Numer wychodzący			
				5. DATE OF TRANSACTION (Year, Month, Day) Data transakcji (rok, miesiąc, dzień)		6. INCOMING NUMBER Numer wchodzący			
7. TO: ACCT NO. DO: KANCELARIA NR:				8. ACCOUNTING LEGEND CODES (ALC): Kod rozliczalności					
				1. Accountable by Serial Number Rozliczane poprzez numer seryjny 2. Accountable by Quantity Rozliczane ilościowo 4. Initial receipt required, controlled in accordance with service/agency directives Wymagane stworzenie posiadania – otrzymano z innego źródła 6. Continuously accountable to COR via EKMS Rozliczane do COR poprzez EKMS 7. Continuous local accountability within EKMS Rozliczane lokalnie bez EKMS					
9.	SHORT TITLE SIGNATOR Nazwa skrócona	EDITION Edycja	10. QTY Ilość	11. ACCOUNTING NUMBERS Numer seryjny / identyfikacyjny		12. ALC Indeks	13. STATUS/ LINK INFO / DEST Uwagi / przeznaczenie		
	• • •								
14.	THE MATERIAL HAS BEEN: (X-one) Materiał został (zaznaczyć "X" we właściwym polu)		RECEIVED Odebrany	INVENTORIED Zinventaryzowany	DESTROYED Zniszczony	VOIDED Unieważniony			
15.	AUTHORIZED RECIPIENT Upoważniony odbiorca			16. (X-one) Wstawić X we właściwym polu		WITNESS Świadek		OTHER Inny	
a. Signature Podpis			b. Grade Stopień		a. Signature Podpis			b. Grade Stopień	
c. Typed or Stamped Name Nazwisko i imię (drukowane litery)			d. Service Nazwa JO		c. Typed or Stamped Name Nazwisko i imię (drukowane litery)			d. Service Nazwa JO	
17. FOR DEPARTMENT OR AGENCY USE: Do wiadomości – podać nazwę JO									
Page of Stronaz.....									

FORMULARZ SF 153 (PL)

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 poniższą zasadą. Podczas sporządzania raportów niejawnych nie nadaje się numerów z DEWD.

Formularz SF 153 (PL) oznaczony jest klauzulą:

- 1) przekazania lub przyjęcia produktu kryptograficznego – JAWNE;
- 2) przekazania lub przyjęcia publikacji – JAWNE;
- 3) przekazania lub przyjęcia dokumentów kryptograficznych – ZASTRZEŻONE;
- 4) lokalne posiadanie – POUFNE, jeśli zawiera tylko produkty kryptograficzne to – ZASTRZEŻONE;
- 5) zniszczenie – ZASTRZEŻONE;
- 6) przekazanie odręczne:
 - a) produktu kryptograficznego – JAWNE,
 - b) publikacji – JAWNE,
 - c) dokumentów kryptograficznych – ZASTRZEŻONE.

WZÓR

Wykaz przesyłek (formularz AF 69 PL)

WYKAZ PRZESYLEK						
ORGANIZACJA/JEDNOSTKA WYSYLAJĄCA /ADRES, NR KANCELarii:					NUMER WYKAZU PRZESYLEK:	
ORGANIZACJA/JEDNOSTKA ODBIERAJĄCA /ADRES, NR KANCELarii:					ILOŚĆ PRZESYLEK:	
LP.	ILOŚĆ PRZESYLEK	NUMER PRZESYŁKI	KLAUZULA	WAGA (KG)	OD/NR KANCELarii	DO/NR KANCELarii
INSTRUKCJE SPECJALNE:						
NAZWISKO/STOPIEŃ/PODPIS OSOBY PAKUJĄCEJ:				CZAS/DATA WYSYŁKI:		
				CZAS/DATA ODBIORU:		
NAZWISKO/STOPIEŃ/PODPIS KURIERA:				NAZWISKO/STOPIEŃ/PODPIS OSOBY ODBIERAJĄCEJ:		

WZÓR

Rejestr interesantów

JO				Budynek JO		Pomieszczenie JO			
Data	Stopień	Imię i nazwisko	Nazwa i numer dokumentu tożsamości	Miejsce wizyty	Podpis	Czas wejścia	Czas wyjścia	Upoważnienie wydane przez KJO	
								Imię i nazwisko	Podpis

Uwaga:

Na rejestrze interesantów nie nanosi się oznaczenia „KRYPTO”.

WZÓR

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

.....
Miejscowość, dnia

KRYPTO

PROTOKÓŁ ZNISZCZENIA ZASOBÓW 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 bezpieczeństwa)
-
(stopień wojskowy, imię i nazwisko; klauzula tajności, numer i data ważności poświadczenia bezpieczeństwa)

zakwalifikowała niżej wymienione zasoby kryptograficzne do zniszczenia:

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

Imiona, nazwiska oraz podpisy:
przewodniczący:

— -

członkowie:

— -

— -

Zasoby kryptograficzne wymienione w pozycjach zostały zniszczone:

- 1) wstępnie* w dniu przez
(określenie sposobu zniszczenia zasobu)

Pojemnik ze zniszczonymi wstępnie zasobami opieczętowano pieczęcią okrągłą numerową do teczek pracy nr

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

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

- 2) ostatecznie* w dniu przez
(określenie sposobu zniszczenia zasobu)

Imiona, nazwiska oraz podpisy:
przewodniczący:

— -

członkowie:

— -

— -

* niepotrzebne skreślić

Wymagania konstrukcyjne oraz wymagania w zakresie zabezpieczenia fizycznego i technicznego kontenerów PKKs-2

1. Kontenery PKKs-2 mające stanowić nowy sprzęt wojskowy muszą posiadać pozytywną opinię wydaną przez SKW potwierdzającą spełnienie wymagań z zakresu zabezpieczenia fizycznego i technicznego.
2. Ściany zewnętrzne i wewnętrzne kontenera PKKs-2 powinny być wykonane z blach (stopów aluminium lub stali) o grubości minimum 1 mm każda z nich. W przypadku ścian wewnętrznych dopuszcza się inny materiał (polipropylen, laminat itp.) pod warunkiem zachowania równoważnej sztywności i odporności na uszkodzenia. Wypełnienie ścian powinien stanowić niepalny, dźwiękochłonny, materiał izolacyjny, o niskiej higroskopijności.
3. W przypadku wystąpienia innych rozwiązań konstrukcyjno-technicznych muszą one spełniać wymagania nie mniejsze niż określone w pkt 2. Przyjęte rozwiązanie techniczne potwierdzone powinno być, w zakresie spełniania wymagań odporności, stosownym dokumentem (certyfikat, deklaracja zgodności) wydanym przez uprawniony podmiot.
4. Drzwi wejściowe do kontenera PKKs-2 powinny:
 - 1) spełniać wymagania klasy odporności nie niższej niż RC2, określone w Polskiej Normie PN-EN1627, posiadać element samozatraskowy, uniemożliwiający pozostawienie pomieszczenia otwartego (np. elektro zaczep, elektro zwora);
 - 2) być wyposażone w dwa patentowe zamki mechaniczne kluczowe wielopunktowe, spełniające 7 klasę odporności na wiercenie wg. PN-EN 12209:2016-04 oraz klasę C odporności na włamanie wg. KT/401/IMP/2009, w tym jeden spełniający funkcję zamka głównego ryglującego drzwi w minimum trzech punktach (ryglowane od strony zawiasów stałe);
 - 3) być wyposażone w mechanizm samozamykający (domykający);
5. W przypadku opcjonalnie zamontowanych okien powinny być one antywłamaniowe, certyfikowane (kwalifikowane) w zakresie spełniania wymagań klasy odporności nie niższej niż RC3, określone w Polskiej Normie PN-EN1627. Okna powinny być nieotwieralne i zabezpieczone przed wglądem do wnętrza oraz posiadać demontowane elementy służące do ich maskowania.
6. Kontenery PKKs-2 powinny posiadać właz ewakuacyjny otwierany na zewnątrz.
7. Kontenery PKKs-2 powinny być wyposażone w system alarmowy, który:
 - 1) sygnalizuje nieuprawnione otwarcie drzwi wejściowych, włazu ewakuacyjnego i okien, ruch w pomieszczeniach oraz próby napadu;
 - 2) odblokowuje i blokuje dostęp do PKKs-2;
 - 3) umożliwia rejestrację wszelkich zdarzeń, w tym wejścia/wyjścia, nieprawidłowości pracy systemu alarmowego lub spadek napięcia źródła zasilania poniżej poziomu wymaganego dla poprawnej pracy systemu;
 - 4) zapewnia pamięć zdarzeń przez co najmniej 90 dni licząc od ostatnio zarejestrowanego zdarzenia;
 - 5) spełnia wymagania normy:
 - a) PN-EN-50130:2012 Systemy alarmowe, dla urządzeń instalowanych w pomieszczeniach zamkniętych nieogrzewanych i ogrzewanych z przerwami,
 - b) PN-EN-50131-1:2009 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: wymagania systemowe, wraz z aktualizacją PN-EN-50131-1/A1:2010;

- 6) uwzględnia zapisy Wymagań Eksploatacyjno-Technicznych dla XIX grupy SpW Systemy i urządzenia specjalistyczne do ochrony obiektów.
8. Kontenery PKKs-2 powinny być wyposażone w system ostrzegania składający się z czujek wykrywających:
- 1) pożar lub dym – dopuszcza się stosowanie dwóch odrębnych czujników;
 - 2) tlenek i dwutlenek węgla – w stężeniu wykraczającym ponad dopuszczalny poziom.
- Czujki systemu ostrzegania powinny być zintegrowane z systemem alarmowym.
9. Kontenery PKKs-2 powinny być wyposażone w system monitorowania wizyjnego i kontroli dostępu (instalację wideodomofonu), zapewniający:
- 1) komunikację głosową z interesantem;
 - 2) wizualną identyfikację interesanta;
 - 3) otwarcie drzwi.
10. Dopuszcza się doposażenie kontenerów PKKs-2 w innego typu sprzęt (urządzenia) wymagane na podstawie odrębnych przepisów.
11. W przypadku konieczności uruchomienia w kontenerze PKKs-2 systemu łączności służącego do przetwarzania informacji niejawnych, kontener doposaża się w urządzenia posiadające odpowiedni poziom TPZU, zgodnie z Zaleceniami Ogólnymi Służby Kontrwywiadu Wojskowego w zakresie zapewnienia ochrony elektromagnetycznej systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych ZOBT-500A oraz instaluje zgodnie z zasadami zawartymi w Selection and Installation of Equipment for the Processing of Classified Information SDIP-29/3.