Warszawa, dnia 12 grudnia 2017 r.

Poz. 227

Departament Ochrony Informacji Niejawnych

ZARZĄDZENIE Nr 59/MON
MINISTRA OBRONY NARODOWEJ

z dnia 11 grudnia 2017 r.

w sprawie doboru i stosowania środków bezpieczeństwa fizycznego do ochrony informacji niejawnych

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167 i 1948 oraz z 2017 r. poz. 935) zarządza się, co następuje:

Rozdział 1
Postanowienia ogólne

§ 1. Zarządzenie określa:

1) dobór i stosowanie środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;
2) dobór i stosowanie środków bezpieczeństwa fizycznego dla pomieszczeń kancelarii tajnych, pomieszczeń specjalnych, pomieszczeń wzmocnionych i pomieszczeń wydzielonych;
3) dobór i stosowanie środków bezpieczeństwa fizycznego miejsc, w których są przetwarzane informacje niejawne w jednostce organizacyjnej, w tym podczas ćwiczeń, kryzysu i wojny oraz w środkach mobilnych i w kancelariach mobilnych;
4) dobór i stosowanie środków bezpieczeństwa fizycznego miejsc, w których przetwarzane są informacje niejawne w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych w czasie realizacji zadań poza granicami kraju;
5) dobór i stosowanie środków bezpieczeństwa fizycznego miejsc, w których są przetwarzane informacje niejawne na okrętach i pomocniczych jednostkach pływających Marynarki Wojennej;

6) dobór i stosowanie środków bezpieczeństwa fizycznego do ochrony materiałów niejawnych na pokładach statków powietrznych Sił Zbrojnych Rzeczypospolitej Polskiej.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) jednostka organizacyjna – Ministerstwo Obrony Narodowej, jednostkę organizacyjną podległą Ministrowi Obrony Narodowej lub przez niego nadzorowaną;
2) pomieszczenie specjalne – pomieszczenie lub zespół pomieszczeń, przeznaczone do prowadzenia narad, odpraw, konferencji, prezentacji multimedialnych lub wideo-konferencji, związanych z przetwarzaniem informacji niejawnych o klauzulach „tajne" i „ściśle tajne";
3) pomieszczenie wzmocnione – pomieszczenie, w którym dopuszczalne jest przechowywanie materiałów niejawnych o klauzuli „tajne" i „ściśle tajne" poza urządzeniami do ich przechowywania;
4) elementy systemów teleinformatycznych – urządzenia służące do przetwarzania informacji niejawnych w systemach teleinformatycznych w szczególności: serwery, stacje robocze, terminale, drukarki, skanery, urządzenia wielofunkcyjne, a także ich elementy aktywne oraz pasywne, w szczególności routery, switche, modemy i patch-panele;
5) rozległe systemy teleinformatyczne - system teleinformatyczny funkcjonujący w więcej niż jednej jednostce organizacyjnej;
6) pomieszczenie wydzielone:
   a) pomieszczenie lub zespół pomieszczeń, w którym zainstalowano elementy systemów teleinformatycznych przetwarzających informacje niejawne o klauzuli „poufne" lub wyższej z wyłączeniem pomieszczeń, dla których charakterystyka techniczna zlokalizowanych w nich elementów systemów teleinformatycznych lub sposób ich instalacji zapewnia, że informacje niejawne nie są w nich przechowywane poza okresem aktywności uwierzytelnionego użytkownika,
   b) pomieszczenie lub zespół pomieszczeń, w którym zainstalowano newralgiczne elementy rozległych systemów teleinformatycznych, w szczególności serwery przetwarzające informacje niejawne o klauzuli „zastrzeżone" więcej niż jednej jednostki organizacyjnej;
7) personel bezpieczeństwa – osoby przeszkolone, nadzorowane, 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;

8) ustawa – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167 i 1948 oraz z 2017 r. poz. 935).

Rozdział 2
Sposób określania poziomu zagrożeń

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

1) załącznika nr 1 do rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683 oraz z 2017 r. poz. 522);
2) informacji otrzymanych od Służby Kontrwywiadu Wojskowego, zwanej dalej „SKW", Żandarmerii Wojskowej, zwanej dalej „ŻW", Policji i osób funkcyjnych odpowiedzialnych za ochronę obiektów wojskowych, dotyczących ewentualnych zagrożeń związanych z działalnością obcych służb specjalnych, sabotażem, zamachem terrorystycznym lub innej działalności przestępczej;
3) wyników działalności kontrolnej i ocen stanu zabezpieczenia informacji niejawnych i przeglądów stanu ochrony fizycznej informacji niejawnych.

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

Rozdział 3
Dobór i stosowanie środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń

§. 5. 1. W zależności od poziomu zagrożeń, w miejscach, w których są przetwarzane informacje niejawne o klauzuli „poufne", „tajne" lub „ściśle tajne" stosuje się, adekwatne do poziomu zagrożeń środki bezpieczeństwa fizycznego dobrane według Załącznika nr 1 do zarządzenia.

2. Do przechowywania materiałów niejawnych wykorzystuje się niżej wymienione urządzenia:

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

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

3. Klasyfikację i wymagania techniczne urządzeń, o których mowa w ust. 2, określa Załącznik nr 2 do zarządzenia.

4. Wszystkie pomieszczenia, w których przetwarzane są informacje niejawne o klauzuli „poufne” lub wyższej powinny posiadać zabezpieczenie okien uniemożliwiające wgląd z zewnątrz.

5. Pomieszczenia wydzielone, w których przetwarzane są informacje niejawne o klauzuli „poufne”, powinny posiadać system kontroli dostępu, co najmniej Typ 2 w kat. K6 określony w części III Załącznika nr 1 do zarządzenia.

6. Pomieszczenia kancelarii tajnych powinny w szczególności spełniać wymagania:
1) określone w części III Załącznika nr 1:
   a) konstrukcja pomieszczenia – uzyskuje co najmniej 2 pkt w Kat. K2,
   b) drzwi do pomieszczenia – co najmniej Typ 3 w Kat. K3, wyposażone w dwa zamki, w tym jeden zamek szyfrowy określony w Typ 4 Kat. K3,
   c) okna pomieszczenia – Typ 4 Kat. K4;
2) kanały wentylacyjne i techniczne zabezpieczone w sposób uniemożliwiający przedostanie się do pomieszczenia z zewnątrz.

7. Pomieszczenia kancelarii tajnych, pomieszczenia wydzielone, pomieszczenia wzmocnione oraz pomieszczenia innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy, w których przetwarzane są informacje niejawne o klauzuli „poufne” lub wyższej, powinny posiadać system sygnalizacji pożaru.

8. Pomieszczenia kancelarii tajnych, pomieszczenia wydzielone, pomieszczenia wzmocnione oraz pomieszczenia innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy, w których przetwarzane są informacje niejawne o klauzuli „tajne” lub wyższej, powinny posiadać system alarmowy zbudowany z certyfikowanych urządzeń, spełniający wymagania określone w normie obronnej „NO-04-A004 Obiekty wojskowe. Systemy alarmowe”.

9. Materiały niejawne oznaczone klauzulą "poufne", "tajne" i "ściśle tajne" w innych niż określone w ust. 6 pomieszczeniach służbowych, nie spełniających kryteriów punktacji określonych w Załączniku nr 1 do zarządzenia, należy przechowywać w urządzeniach do przechowywania

materiałów niejawnych, o których mowa w ust. 2 oraz należy spełnić jeden z następujących warunków:

1) pomieszczenie jest wyposażone w system alarmowy określony w Typ 3 Kat. K9;

2) pomieszczenie jest chronione całodobowo przez personel bezpieczeństwa posiadający odpowiednie poświadczenie bezpieczeństwa;

3) strefa jest chroniona całodobowo przez personel bezpieczeństwa w formie posterunku lub patroli zorganizowanych w sposób wynikający z określonego poziomu zagrożeń, zgodnie z zasadami określonymi w Kat. K10 w części III Załącznika nr 1 do zarządzenia.

10. Sposób zabezpieczenia sprzętu wojskowego, zwanego dalej „SpW", będącego materiałem niejawnym lub zawierającego materiały niejawne musi uwzględniać konieczność zapewnienia ich ochrony.

11. Sposób zabezpieczenia pomieszczeń, w których przechowywany jest SpW wyposażony w elementy zawierające informacje niejawne określają odrębne przepisy w zakresie ochrony SpW.

12. Pomieszczenia wydzielone, w których zlokalizowane są newralgiczne elementy systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" zabezpiecza się analogicznie jak pomieszczenia wydzielone, w których przetwarza się informacje niejawne o klauzuli „poufne".

§ 6. 1. Osoby, którym powierzono materiały niejawne po zakończeniu pracy mają obowiązek zabezpieczenia ich przed dostępem osób nieuprawnionych.

2. Kierownik jednostki organizacyjnej określa system zarządzania kluczami do miejsc przetwarzania informacji niejawnych oraz urządzeń do przechowywania materiałów niejawnych, a także zasady ustalania, zmiany i deponowania haseł lub kodów (szyfrów) w przypadku stosowania zamków szyfrowych.

3. Klucze zapasowe, kody zamków szyfrowych oraz kody systemu alarmowego do pomieszczeń, a także znajdujących się w tych pomieszczeniach urządzeń do przechowywania materiałów niejawnych, zapisane na formularzu, przechowuje się w sposób określony w planie ochrony informacji niejawnych. Wzór formularza określa Załącznik nr 3 do zarządzenia.

4. Zabrania się zapisywania przez użytkowników kodów zamków szyfrowych oraz kodów systemu alarmowego, z zastrzeżeniem ust. 3, oraz wynoszenia poza teren jednostki organizacyjnej kluczy, o których mowa w ust. 2 i 3. Wszelkie odstępstwa od tej zasady określa kierownik jednostki organizacyjnej.

5. Częstotliwość zmiany kodów zamków szyfrowych określa kierownik jednostki organizacyjnej, jednakże obligatoryjnie zmienia się je:

1) w urządzeniach i zamkach nowo instalowanych;
2) po każdej naprawie lub konserwacji zamka;
3) każdej zmianie składu osób znających kod;
4) w przypadku ujawnienia lub podejrzenia ujawnienia kodu osobie nieupoważnionej;
5) w urządzeniach, w których przechowywane są materiały niejawne o klauzuli „tajne" i „ściśle tajne" - nie rzadziej niż co 6 miesięcy.

6. W razie utraty lub zagubienia kluczy, o których mowa w ust. 2 i 3, należy wymienić zamki.

Rozdział 4
Dobór i stosowanie środków bezpieczeństwa fizycznego dla pomieszczeń specjalnych, pomieszczeń wzmocnionych i pomieszczeń wydzielonych

§ 7. Pomieszczenia specjalne powinny spełniać wymagania określone w § 15 ust. 3 rozporządzenia Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz. U. z 2016 r. poz. 1720) z uwzględnieniem, że:

1) szczegółowe wymagania w zakresie zabezpieczenia przed podsłuchem i podglądem oraz stosowania odpowiednich środków bezpieczeństwa fizycznego dla każdego z pomieszczeń określa SKW;
2) obowiązuje zakaz wnoszenia do nich przez osoby biorące udział w spotkaniu (naradzie, odprawie, konferencji) wszelkich urządzeń służących do przetwarzania obrazu lub dźwięku;
3) SKW prowadzi okresowe badania przeciwpodsłuchowe pomieszczeń oraz przeprowadza je doraźnie w miarę potrzeb, przed naradą, odprawą, konferencją, prezentacją multimedialną, wideokonferencją, a także po każdorazowym nieuprawnionym wejściu do strefy, podejrzeniu, że takie wejście mogło mieć miejsce, a także badania przeciwpodsłuchowe sprzętu będącego na wyposażeniu pomieszczenia, który powrócił po naprawie lub konserwacji;
4) pomieszczenie wyposażone jest w system kontroli dostępu, o którym mowa w kat. K6 w części III Załącznika nr 1 do zarządzenia.

§ 8. Pomieszczenia wzmocnione powinny w szczególności spełniać wymagania:

1) określone w Załączniku nr 1 do zarządzenia:
   a) konstrukcja pomieszczenia określona w Typ 4 Kat. K2,
   b) drzwi do pomieszczenia określone w Typ 4 Kat. K3,
   c) okna pomieszczenia określone w Typ 4 Kat. K4,

d) system alarmowy określony w Typ 3 Kat. K9;

2) konstrukcja stropów i podłóg - w przypadku, gdy ściany zewnętrzne lub stropy stanowią granicę strefy ochronnej, powinny być wykonane z materiałów niepalnych i spełniać wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej klasy 15 o grubości nie mniejszej niż 25 cm dla ścian lub dla stropów o konstrukcji żelbetowej o minimalnej dopuszczalnej grubości przy danej rozpiętości stropu nie mniejszej jednak niż 15 cm;

3) kanały wentylacyjne i techniczne zabezpieczone w sposób uniemożliwiający przedostanie się do pomieszczenia z zewnątrz.

§ 9. 1. Pomieszczenia wydzielone, w których przetwarzane są informacje niejawne o klauzuli „tajne" i „ściśle tajne" powinny spełniać wymagania określone w § 8 oraz posiadać system kontroli dostępu co najmniej Typ 2 w kat. K6 określony w części III Załącznika nr 1 do zarządzenia.

2. Dla pomieszczeń wydzielonych, w których przetwarzane są informacje niejawne o klauzuli „poufne" środki bezpieczeństwa fizycznego dobiera się na podstawie Załącznika nr 1 do zarządzenia.

Rozdział 5

Dobór i stosowanie środków bezpieczeństwa fizycznego miejsc, w których są przetwarzane informacje niejawne podczas ćwiczeń, kryzysu i wojny oraz w środkach mobilnych i w kancelariach mobilnych

§ 10. Środki bezpieczeństwa fizycznego, określone w rozdziale 3, stosuje się również w czasie ćwiczeń, kryzysu i wojny o ile przepisy niniejszego rozdziału nie stanowią inaczej.

§ 11. 1. Miejsca, w szczególności pomieszczenia lub obszary i rejony, w których będą przetwarzane informacje niejawne organizuje się w strefie ochronnej:

1) w przypadku działań prowadzonych w miejscu stałej dyslokacji w pomieszczeniach zabezpieczonych środkami, o których mowa w rozdziale 3 przy zachowaniu gradacji środków bezpieczeństwa fizycznego w zależności od poziomu zagrożeń;

2) w przypadku działań prowadzonych poza miejscem, o którym mowa w pkt 1, w rejonie działań, przy czym:

   a) miejsce, w którym przetwarza się informacje niejawne chroni się i w miarę potrzeb oznacza,

b) w przypadku przechowywania materiałów niejawnych o klauzuli „ściśle tajne” i „tajne” poza urządzeniami, o których mowa w § 5 ust. 2, materiały niejawne pozostają pod nadzorem osoby, której je powierzono,

c) miejsca, w których przetwarza się informacje niejawne zabezpiecza się przed podglądem z zewnątrz,

d) materiały niejawne przechowuje się w urządzeniach do przechowywania materiałów niejawnych lub w inny sposób gwarantujący bezpieczeństwo informacji niejawnych,

e) zapewnia się całodobową ochronę fizyczną miejsc przetwarzania informacji niejawnych.

2. W przypadku gdy materiały niejawne pozostają bez nadzoru osób, środek transportu lub kancelaria mobilna powinny zostać zamknięte i objęte stałą ochroną fizyczną lub ochroną techniczną nadzorowaną przez personel bezpieczeństwa.

3. W przypadku, o którym mowa w ust. 2, oraz gdy środek transportu lub kancelaria mobilna są wyposażone w urządzenia do przechowywania materiałów niejawnych, powinny one zostać obowiązkowo w nich zamknięte.

§ 12. Przetwarzanie informacji niejawnych w części mobilnej zasobów systemu teleinformatycznego odbywa się na podstawie wyników procesu szacowania ryzyka, o których mowa w art. 49 ust. 1 ustawy, w sposób określony w dokumentacji bezpieczeństwa systemu teleinformatycznego, przy spełnieniu wymagań w zakresie bezpieczeństwa fizycznego, o których mowa w § 11.

§ 13. 1. Poza rejonami stanowisk dowodzenia, w trakcie prowadzenia działań bojowych, ćwiczeń lub w sytuacjach kryzysowych, materiały niejawne wykorzystuje się i chroni zgodnie z przyjętą taktyką działania wojsk.

2. Taktyka działania wojsk musi uwzględniać postępowanie z materiałami niejawnymi wchodzącymi w skład wyposażenia i uzbrojenia, w tym podczas przemieszczenia i działań poza miejscem stałej dyslokacji, zwanego dalej „MSD”.

Rozdział 6

Dobór i stosowanie środków bezpieczeństwa fizycznego miejsc, w których przetwarzane są informacje niejawne w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych w czasie realizacji zadań poza granicami kraju

§ 14. 1. Miejsca, w których przetwarzane są informacje niejawne zabezpiecza się zgodnie z przepisami rozdziału 3, a w przypadku braku możliwości spełnienia tych wymogów należy:

1) stosować standardy zabezpieczeń fizycznych nie niższe niż obowiązujące w jednostce (organizacji) międzynarodowej, w której funkcjonuje dana jednostka organizacyjna lub wydzielony pododdział w ramach jednostki (organizacji) międzynarodowej;
2) przechowywać materiały niejawne w urządzeniach, o których mowa w § 5 ust. 2;
3) poinformować Szefa SKW o zastosowanych standardach zabezpieczeń fizycznych.

2. Kancelarie tajne lub inne niż kancelaria tajna komórki organizacyjne odpowiedzialne za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy organizuje się w trwałych pomieszczeniach, schronach lub kancelarii mobilnej.

3. Wszelkie odstępstwa w zakresie zabezpieczeń pomieszczeń kancelarii tajnych wymagają zgody Szefa SKW.

4. Dopuszcza się zastosowanie odstępstw od standardów zabezpieczeń fizycznych w czasie realizacji zadań poza granicami kraju, bez uzgodnienia i akceptacji Szefa SKW, jeżeli uzyskanie ww. zgody nie jest możliwe ze względu na konieczność natychmiastowego działania poza granicami kraju oraz braku możliwości uzgodnień wynikających z charakteru działań. Zastosowanie odstępstw musi każdorazowo być poprzedzone wnikliwą analizą zagrożeń oraz uzyskać akceptację kierownika jednostki organizacyjnej (Dowódcy Polskiego Kontyngentu Wojskowego/polskiej jednostki wojskowej), który w przypadku nieuzasadnionego wprowadzenia odstępstw ponosi odpowiedzialność zgodnie z przepisami o ochronie informacji niejawnych.

Rozdział 7

Dobór i stosowanie środków bezpieczeństwa fizycznego miejsc, w których przetwarzane są informacje niejawne na okrętach i pomocniczych jednostkach pływających Marynarki Wojennej

§ 15. 1. Kancelarię tajną lub inną niż kancelaria tajna komórkę organizacyjną odpowiedzialną za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy, pomieszczenie wydzielone na okręcie i pomocniczej jednostce pływającej organizuje się w pomieszczeniach spełniających następujące warunki bezpieczeństwa:
1) oddzielonych od innych pomieszczeń trwałymi ścianami uniemożliwiających przedostanie się do wewnątrz;
2) nie posiadających 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 kat. K3).

2. Pomieszczenia kancelarii tajnej (pomieszczenia innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy) oraz pomieszczenie wydzielone powinny być chronione ogólnookrętową (lub zintegrowaną z zainstalowanym systemem alarmowym) instalacją przeciwpożarową.

3. W pomieszczeniu kancelarii tajnej (pomieszczeniach innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy), pomieszczeniu wydzielonym instaluje się systemy alarmowe spełniające wymagania określone co najmniej w Typ 1 Kat. K9 w części III Załącznika nr 1 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, materiały niejawne przechowuje się w kancelarii tajnej okrętu lub innych niż kancelaria tajna komórkach organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy.

6. Na okrętach, na których nie ma kancelarii tajnej lub innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy, materiały niejawne na czas niezbędny do realizacji zadania przechowuje się w kabinie dowódcy okrętu (lub innym pomieszczeniu określonym przez dowódcę okrętu), wyposażonej w urządzenia do przechowywania materiałów niejawnych.

7. Przetwarzanie informacji niejawnych poza kancelarią tajną (inną niż kancelaria tajna komórką organizacyjną odpowiedzialną za przetwarzanie materiałów niejawnych w rozumieniu art. 44 ustawy) jest dopuszczalne – za zgodą i na zasadach określonych przez dowódcę okrętu.

8. W przypadku ryzyka przejęcia okrętu przez przeciwnika lub innego zagrożenia dowódca okrętu nakazuje pełną kasację danych i oprogramowania oraz zniszczenie innych materiałów zawierające informacje niejawne. Okręty wyposaża się w miarę możliwości technicznych w urządzenia lub środki do natychmiastowego niszczenia materiałów niejawnych.

Rozdział 8

Dobór i stosowanie środków bezpieczeństwa fizycznego do ochrony materiałów niejawnych na pokładach statków powietrznych Sił Zbrojnych Rzeczypospolitej Polskiej

§ 16. 1. Kierownik jednostki organizacyjnej odpowiada za organizację ochrony materiałów niejawnych na pokładach statków powietrznych, która ma na celu zapewnienie stałego nadzoru nad nimi.

2. W jednostce organizacyjnej, w której stacjonują statki powietrzne, za ochronę materiałów niejawnych znajdujących się na wyposażeniu tych statków powietrznych, odpowiedzialny jest kierownik tej jednostki organizacyjnej, który stosuje środki ochrony fizycznej uniemożliwiające ujawnienie informacji niejawnych.

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

4. Po wylądowaniu na innym lotnisku wojskowym na terenie kraju, za ochronę informacji niejawnych znajdujących się na pokładzie statku powietrznego, odpowiedzialny jest dowódca bazy, w której wylądował statek powietrzny.

5. W przypadku lądowania na terenie kraju na lotniskach cywilnych lub poza MSD, w szczególności: lądowanie awaryjne, lądowanie w miejscu przygodnym, lądowanie w ramach zadań poszukiwawczo-ratowniczych, za ochronę materiałów niejawnych 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 członkowskich Organizacji Traktatu Północnoatlantyckiego, zwanej dalej „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 są 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 informacji niejawnych 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 materiałów niejawnych, 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. W przypadku zagrożenia dowódca statku powietrznego dokonuje dostępnymi środkami pełnej kasacji danych

i oprogramowania oraz niszczy inne materiały zawierające informacje niejawne. Statki powietrzne wyposaża się w miarę możliwości technicznych w urządzenia lub środki do natychmiastowego niszczenia materiałów niejawnych.

Rozdział 9

Postanowienia szczególne

§ 17. 1. W razie okoliczności trudnych do przewidzenia, w szczególności w czasie kryzysu, wojny lub stanów nadzwyczajnych, w których typowe sposoby ochrony materiałów niejawnych mogą być niemożliwe do wykorzystania lub ich użycie pogorszy bezpieczeństwo informacji kierownik jednostki organizacyjnej 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. W przypadku nieuzasadnionego wprowadzenia odstępstw, kierownik jednostki organizacyjnej ponosi odpowiedzialność zgodnie z przepisami o ochronie informacji niejawnych.

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

3. W warunkach bojowych, kiedy kontakt z kierownikiem jednostki organizacyjnej jest niemożliwy lub może spowodować zagrożenie, sposób ochrony materiałów niejawnych określa dowódca pododdziału (równorzędny), a w przypadku jego braku osoba będąca w posiadaniu materiałów niejawnych.

4. W przypadku zagrożenia dowódca pododdziału (równorzędny), a w przypadku jego braku osoba będąca w posiadaniu materiałów niejawnych dokonuje, dostępnymi środkami, pełnej kasacji danych i oprogramowania oraz niszczy inne materiały zawierające informacje niejawne.

§ 18. W szczególnie uzasadnionych przypadkach uniemożliwiających spełnienie któregokolwiek z warunków, o których mowa w § 5, po przedstawieniu pozytywnej opinii pełnomocnika ochrony szczebla bezpośrednio nadrzędnego oraz Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych, zgodę na zastosowanie alternatywnych środków bezpieczeństwa udziela Szef SKW.

§ 19. W jednostce organizacyjnej, w której są przetwarzane informacje niejawne międzynarodowe uwzględnia się postanowienia obowiązujących umów i porozumień międzynarodowych oraz wytycznych Szefa Agencji Bezpieczeństwa Wewnętrznego.

Rozdział 10

Postanowienia przejściowe i końcowe

§ 20. Zastosowany przed wejściem w życie niniejszego zarządzenia system środków bezpieczeństwa fizycznego, obejmujący rozwiązania organizacyjne, a także wyposażenie pomieszczeń 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.

§ 21. Zezwala się na dalsze stosowanie urządzeń do przechowywania dokumentów niejawnych, spełniających wymagania zawarte w dotychczasowym zarządzeniu Nr 57/MON Ministra Obrony Narodowej z dnia 16 grudnia 2011 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 oraz doboru i stosowania środków bezpieczeństwa fizycznego (Dz. Urz. Min. Obr. Nar. poz. 402).

§ 22. Przepisów zarządzenia nie stosuje się do kancelarii kryptograficznych, dla których dobór środków bezpieczeństwa fizycznego reguluje odrębne zarządzenie.

§ 23. Zarządzenie wchodzi w życie z dniem 1 stycznia 2018 r.

Minister Obrony Narodowej: *A. Macierewicz*

Załączniki do zarządzenia Nr 59 /MON
Ministra Obrony Narodowej
z dnia 11 grudnia 2017 r. (poz. 227)

Załącznik nr 1

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[1)];

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 kategorie 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.

7. Do ochrony informacji niejawnych należy stosować systemy zabezpieczeń technicznych spełniające wymagania „Normy Obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe”.

[1)] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683 oraz z 2017 r. poz. 522).

CZĘŚĆ II.

PODSTAWOWE WYMAGANIA BEZPIECZEŃSTWA FIZYCZNEGO

Najwyższa klauzula tajności informacji przetwarzanych w jednostce organizacyjnej	**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
Suma punktów	22	25	32
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
Suma punktów	16	19	20
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
Suma punktów	11	14	16

KATEGORIA K1: Szafy do przechowywania materiałów niejawnych
KATEGORIA K2: Konstrukcja pomieszczenia
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 jednostki organizacyjnej (interesantów)
KATEGORIA K8: Telewizyjny system nadzoru w budynku
KATEGORIA K9: System alarmowy
KATEGORIA K10: Personel bezpieczeństwa
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 pomieszczenia

Uwaga! W przypadku zastosowania czujki inercyjnej 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 pomieszczenia wykonane są z cegły pełnej klasy 15 o grubości co najmniej 25 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 pomieszczenia wykonane są z cegły pełnej klasy 15 o grubości co najmniej 22 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 pomieszczenia wykonane są z cegły pełnej klasy 15 o grubości co najmniej 18 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 wykonane z cegły 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 lub równorzędne 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 pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem (atakiem) radiologicznym (promieniowanie z radioaktywnego źródła nieprzekraczającego równowartości 10 curie, co - 60 z odległości 760 mm przez 20 godzin). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. 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.
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

Uwaga! Kraty stanowiące wartość zabytkową nie podlegają demontażowi.

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 siatki z drutu stalowego w ramie** lub kraty zapewniające wysoką odporność na włamanie*.
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 jedno z poniższych zabezpieczeń: - siatka z drutu stalowego w ramie**, - 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.
Typ1 1 pkt.	Niezabezpieczone okna pomieszczeń piwnic, parteru, ostatniej kondygnacji i poddasza.

* 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.

Kraty stosuje się 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.

Mocowanie krat w otworze okiennym powinny spełniać następujące wymagania:

a) kraty mocuje się minimum na trzech 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 powinny 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.

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 jednostkami organizacyjnymi, 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 okresowo zamykane.
Typ 1 1 pkt.	Budynek o innej konstrukcji użytkowany samodzielnie lub wspólnie z innymi jednostkami organizacyjnymi.

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 jednostki organizacyjnej (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 1pkt.	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 i wideodetekcją.

Kategoria K9: System alarmowy

Punktacja	Funkcja lub cechy
Typ 3 3 pkt.	System alarmowy, spełniający wymagania techniczne i organizacyjne określone w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe. System alarmowy sygnalizujący nieuprawnione otwarcie drzwi wejściowych i okien, ruch w pomieszczeniach oraz próby napadu.

Typ 2 2 pkt.	System alarmowy, spełniający wymagania techniczne i organizacyjne określone w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe. 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, spełniający wymagania techniczne i organizacyjne określone w normie obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe. System alarmowy, sygnalizujący nieuprawnione otwarcie drzwi wejściowych i okien oraz próby napadu.

Kategoria K10: Personel bezpieczeństwa

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 jednostce organizacyjnej należy opracować procedury działania personelu bezpieczeństwa 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:

a) 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,
b) 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,
c) 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 bezpieczeństwa 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.

Załącznik nr 2

KLASYFIKACJA I WYMAGANIA TECHNICZNE DLA URZĄDZEŃ DO PRZECHOWYWANIA MATERIAŁÓW NIEJAWNYCH

I. Szafa stalowa klasy A

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

II. Szafa stalowa klasy B

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

1300, pod warunkiem że zamek spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.

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

III. Szafa stalowa klasy C

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

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

Załącznik nr 3

Formularz z kodami dostępu i kodami systemu alarmowego do pomieszczeń kancelarii tajnych, a także do znajdujących się w tych pomieszczeniach urządzeń do przechowywania materiałów niejawnych

strona 1

Podlega ochronie przewidzianej
dla informacji niejawnych o klauzuli
tajności** .. ……..
Egz. Nr. ……...

KOD DO POMIESZCZENIA NR* …….

SZAFA NR FABRYCZNY* ……

SZAFA KLASY ……

POMIESZCZENIE ZNAJDUJE SIĘ W STREFIE OCHRONNEJ ……..

ADRES: …….....

.....

PRAWO POBRANIA POSIADAJĄ:

1. .....
(stopień, imię i nazwisko)
2. .....
(stopień, imię i nazwisko)
3. .....
(stopień, imię i nazwisko)
4. .....
(stopień, imię i nazwisko)

(miejsce zagięcia kartki)

.....

Podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności** …… str. 1/2

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

KOMBINACJA ZAMKA SZYFROWEGO	Podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności** .. …….. Egz. Nr. ……...

FORMULARZ TEN POWINIEN BYĆ ZGIĘTY W POŁOWIE I ODPOWIEDNIO ZAMKNIĘTY W NIEPRZEZROCZYSTEJ KOPERCIE

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

KOD SYSTEMU ALARMOWEGO: **

KOMBINACJA/***

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

** **JEŚLI KOMBINACJA ZACZYNA SIĘ PRZEKRĘCENIEM POKRĘTŁA ZAMKA SZYFROWEGO W LEWO, ZACZYNAMY OPIS OD POZYCJI 1.**

JEŚLI KOMBINACJA ZACZYNA SIĘ PRZEKRĘCANIEM POKRĘTŁA ZAMKA SZYFROWEGO W PRAWO, ZACZYNAMY OPIS OD POZYCJI 2.

*** **WYPEŁNIAĆ MIĘKKIM OŁÓWKIEM.**

(miejsce zagięcia kartki)

[redacted]

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