Warszawa, dnia środa, 30 grudnia 2020 r.

Poz. 31

ZARZĄDZENIE NR 30/20
SZEFA CENTRALNEGO BIURA ANTYKORUPCYJNEGO

z dnia 29 grudnia 2020 r.

w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnej, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Centralnym Biurze Antykorupcyjnym

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) zarządza się, co następuje:

Rozdział 1.
Postanowienia ogólne

§ 1. 1. Zarządzenie określa:

1) sposób organizacji i funkcjonowania kancelarii tajnej, o której mowa w art. 42 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), zwanej dalej „ustawą”;

2) sposób i tryb przetwarzania informacji niejawnych;

3) dobór i stosowanie środków bezpieczeństwa fizycznego w Centralnym Biurze Antykorupcyjnym, zwanym dalej „CBA”.

2. Przepisy zarządzenia stosuje się do ochrony materiałów niejawnych.

3. Przepisy niniejszego zarządzenia stanowią również wykonanie obowiązków wynikających z art. 43 ust. 3 i 5 ustawy.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) dekretacja - odręczna adnotacja właściwego przełożonego na pierwszej stronie dokumentu lub w innej formie pisemnej informująca o sposobie dalszego postępowania, potwierdzona podpisem i datą;

2) delegatura - delegatura CBA, o której mowa w statucie CBA;

3) dokument niejawny - dokument, o którym mowa w art. 2 pkt 3 ustawy;

4) dziennik ewidencji – wszelkie zarejestrowane papierowe dzienniki, rejestry, skorowidze oraz książki służące do rejestrowania i dokumentowania obiegu dokumentów niejawnych, a także dzienniki prowadzone w systemie teleinformatycznym;

5) funkcjonariusz - funkcjonariusza lub pracownika CBA;

6) główna kancelaria tajna - wyodrębniona komórka w jednostce organizacyjnej, w której powołano pełnomocnika ochrony;

7) informatyczny nośnik danych - materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

8) instrukcja EDEN - Instrukcja zarządzania Elektronicznym Dziennikiem Ewidencji Niejawnej Centralnego Biura Antykorupcyjnego;

9) jednostka organizacyjna - jednostka organizacyjna, o której mowa w statucie CBA, inna niż delegatura;

10) jednostka rejestrująca – główna kancelaria tajna, oddział kancelarii tajnej w delegaturze lub stanowisko rejestracji w jednostce, o której mowa w pkt 9;

11) kancelaria ogólna - kancelaria, o której mowa w zarządzeniu nr 36/12 Szefa CBA z dnia 27 grudnia 2012 r. w sprawie wprowadzenia w Centralnym Biurze Antykorupcyjnym instrukcji kancelaryjnej (Dz. Urz. CBA poz. 47 i z 2019 r. poz.10);

12) kancelaria tajna – komórka, o której mowa w art. 42 ust. 1 ustawy, w skład której wchodzą jednostki rejestrujące;

13) komórka organizacyjna - wydział lub sekcja wyodrębnione w ramach jednostki organizacyjnej lub delegatury;

14) kopiowanie – w szczególności również wykonywanie odpisu, wypisu, wyciągu, wydruku, odwzorowania cyfrowego, nagrania lub tłumaczenia;

15) materiał niejawny – materiał, o którym mowa w art. 2 pkt 4 ustawy;

16) obieg wewnętrzny – obieg kancelaryjny materiałów w ramach jednej strefy ochronnej lub stref ochronnych bezpośrednio przylegających do siebie, w których przetwarza się informacje niejawne o klauzuli tajności nie niższej, niż klauzula przesyłki niejawnej;

17) obieg zewnętrzny - obieg niespełniający wymagań dla obiegu wewnętrznego;

18) pełnomocnik ochrony - pełnomocnik do spraw ochrony informacji niejawnych, o którym mowa w art. 14 ust. 2 ustawy, powołany w CBA;

19) pokwitowanie – potwierdzenie w dzienniku ewidencji, z czytelnym podaniem imienia i nazwiska, daty oraz podpisu, funkcjonariusza odbierającego dokument niejawny lub informacja w systemie teleinformatycznym potwierdzająca fakt odebrania dokumentu z wykorzystaniem mechanizmu elektronicznej akceptacji;

20) poziom zagrożeń - poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, o których mowa w art. 43 ust.4 ustawy;

21) przesyłka niejawna - list lub paczka zawierające materiał niejawny;

22) przetwarzanie informacji niejawnych - przetwarzanie, o którym mowa w art. 2 pkt 5 ustawy;

23) przewoźnik - podmiot, o którym mowa w § 2 ust. 1 rozporządzenia z dnia 7 grudnia 2011 r. Prezesa Rady Ministrów w sprawie sposobu nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. poz. 1603);

24) rozporządzenie o KT - rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. z 2017 r. poz. 1558);

25) rozporządzenie o oznaczaniu – rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. poz. 1692);

26) rozporządzenie o przewożeniu - rozporządzenie z dnia 7 grudnia 2011 r. Prezesa Rady Ministrów w sprawie sposobu nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. poz. 1603);

27) rozporządzenie w sprawie środków bezpieczeństwa fizycznego - rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2017 r. poz. 522);

28) służba ochrony - funkcjonariusze wyznaczeni do wykonywania zadań w zakresie ochrony fizycznej obiektów, a także przebywających w nich osób;

29) stanowisko rejestracji – jednostka rejestrująca utworzona w jednostce lub komórce organizacyjnej;

30) strefa ochronna – części obiektu użytkowanego przez CBA, wydzielone w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej, określone w planie ochrony;

31) system utajnionej łączności – system wymiany informacji niejawnych za pośrednictwem urządzeń kryptofaksowych.

§ 3. Pełnomocnik ochrony realizuje swoje zadania przy pomocy pionu ochrony, o którym mowa w art. 15 ust. 2 ustawy.

§ 4. Pełnomocnik ochrony może wydawać wytyczne w zakresie funkcjonowania kancelarii tajnej, obiegu informacji niejawnych, organizacji obsługi kancelaryjnej oraz sposobu prowadzenia dzienników ewidencji.

§ 5. Wytyczne, o których mowa w § 4 będą zamieszczane na Portalu Wewnętrznym Centralnego Biura Antykorupcyjnego.

Rozdział 2.
Organizacja obsługi kancelaryjnej

§ 6. 1. Kancelaria tajna, jest nadzorowana w zakresie merytorycznym przez pełnomocnika ochrony i odpowiedzialna za rejestrowanie, przechowywanie, wysyłanie, obieg i wydawanie materiałów niejawnych.

2. Obsługę kancelaryjną materiałów niejawnych zapewniają jednostki rejestrujące, obsługiwane przez osoby posiadające ukończone szkolenie z zakresu obsługi kancelaryjnej materiałów niejawnych.

3. Za ukończenie szkolenia, o którym mowa w ust. 2 uważa się zaliczenie egzaminu pisemnego.

4. Osoby prowadzące obsługę kancelaryjną materiałów niejawnych są zobowiązane do odbycia raz w roku szkolenia uzupełniającego z zakresu obsługi kancelaryjnej.

5. Jednostki rejestrujące prowadzą wykazy osób upoważnionych do dostępu do informacji niejawnych w obsługiwanej delegaturze, jednostce lub komórce organizacyjnej.

§ 7. 1. Wniosek w sprawie utworzenia oddziału kancelarii tajnej lub stanowiska rejestracji, kierownik jednostki organizacyjnej lub dyrektor delegatury składa do pełnomocnika ochrony w egzemplarzu pojedynczym. Tryb, o którym mowa w zdaniu pierwszym stosuje się odpowiednio dla funkcjonujących przed dniem wejścia w życie niniejszego zarządzenia jednostek rejestrujących.

2. We wniosku, o którym mowa w ust. 1, należy podać:

1) datę zatwierdzenia planu ochrony informacji niejawnych siedziby jednostki organizacyjnej lub delegatury, w której ma się znajdować jednostka rejestrująca;

2) nazwę komórki organizacyjnej, adres siedziby jednostki organizacyjnej lub delegatury, w której ma się znajdować jednostka rejestrująca, numer pomieszczenia;

3) imiona i nazwiska funkcjonariuszy przewidzianych do obsługi kancelaryjnej wraz z numerem aktualnego poświadczenia bezpieczeństwa i datą ważności, numerem aktualnego zaświadczenia ze szkolenia z zakresu ochrony informacji niejawnych, numerem zaświadczenia ze szkolenia z zakresu obsługi kancelaryjnej materiałów niejawnych.

3. Wzór wniosku, o którym mowa w ust. 1, stanowi załącznik nr 1.

§ 8. 1. Zatwierdzony wniosek, o którym mowa w § 7 ust. 1, wraz z nadanym przez Elektroniczny Dziennik Ewidencji Niejawnej, zwany dalej "EDEN" indywidualnym numerem jednostki rejestrującej, pełnomocnik ochrony przekazuje wnioskującemu kierownikowi jednostki organizacyjnej lub dyrektorowi delegatury, a jego kopię pozostawia w dokumentacji bieżących działań podejmowanych w zakresie ochrony informacji niejawnych.

2. W przypadku niezatwierdzenia wniosku, pełnomocnik ochrony odsyłając go, wskazuje przyczyny odmowy.

§ 9. 1. Czynności związane z obsługą jednostek rejestrujących, o których mowa w § 6 ust. 3, wykonują wyznaczeni funkcjonariusze jednostki organizacyjnej lub delegatury, w której zostały one zorganizowane, spełniający wymogi, o których mowa w § 10.

2. W zakresie obsługi jednostek rejestrujących funkcjonariusze, o których mowa w ust. 1, wykonują zadania pionu ochrony w rozumieniu ustawy, i w tym zakresie podlegają merytorycznemu nadzorowi pełnomocnika ochrony.

3. Pełnomocnik ochrony, w oparciu o wyniki przeprowadzonej kontroli stanu ochrony informacji niejawnych lub w ramach nadzoru realizowanego za pośrednictwem kierownika kancelarii tajnej, może wydać opinię co do oceny pracy merytorycznej funkcjonariusza wykonującego zadania związane z obsługą kancelaryjną w jednostce rejestrującej.

4. Kierownik jednostki organizacyjnej lub dyrektor delegatury, w której funkcjonuje jednostka rejestrująca, zobowiązany jest do bieżącej współpracy z pełnomocnikiem ochrony w zakresie określonym w ust. 2.

§ 10. 1. Funkcjonariusze prowadzący obsługę kancelaryjną materiałów niejawnych, są zobowiązani:

1) posiadać poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „ściśle tajne”;

2) posiadać zaświadczenie o przeszkoleniu z zakresu ochrony informacji niejawnych;

3) posiadać zaświadczenie o przeszkoleniu w zakresie obsługi kancelaryjnej materiałów niejawnych, którego wzór stanowi załącznik nr 2;

4) posiadać, w zakresie obowiązków i odpowiedzialności, określenie zakresu zadań właściwych dla obsługi kancelaryjnej materiałów niejawnych jednostki organizacyjnej.

2. Funkcjonariusz prowadzący obsługę kancelaryjną materiałów niejawnych jest odpowiedzialny za rejestrowanie i dokumentowanie ich obiegu oraz wydawanie go osobom uprawnionym.

3. Funkcjonariusz prowadzący obsługę kancelaryjną materiałów niejawnych jest odpowiedzialny za organizację pracy w sposób zapewniający możliwość ustalenia w każdych okolicznościach, gdzie powinien znajdować się materiał niejawny pozostający w dyspozycji jednostki, delegatury bądź komórki organizacyjnej oraz kto z tym materiałem się zapoznał.

§ 11. 1. W przypadku konieczności wyznaczenia funkcjonariusza do okresowego przejęcia obowiązków w zakresie obsługi jednostki rejestrującej, kierownik jednostki organizacyjnej lub dyrektor delegatury jest zobowiązany zawnioskować do pełnomocnika ochrony o wyznaczenie osoby, podając informacje, o których mowa w § 7 ust. 2 pkt 3 zarządzenia.

2. Po zatwierdzeniu wniosku, o którym mowa w ust. 1, jest sporządzany w egzemplarzu pojedynczym protokół przejęcia obowiązków od funkcjonariusza prowadzącego obsługę jednostki rejestrującej oraz protokół przekazania niezbędnych dzienników ewidencji i pieczęci. Protokoły, o których mowa w zdaniu pierwszym, przechowuje się w jednostce rejestrującej, w której nastąpiło przekazanie.

3. Do funkcjonariusza przejmującego obowiązki w trybie, o którym mowa w ust. 1, stosuje się wymogi określone w § 10, z wyłączeniem ust. 1 pkt 4.

4. W przypadku braku możliwości sporządzenia protokołów, o których mowa w ust. 2, spowodowanej nagłą sytuacją losową, protokoły sporządza komisja wyznaczona przez kierownika jednostki organizacyjnej lub dyrektora delegatury.

5. W przypadku prowadzenia dzienników ewidencji w ramach systemu teleinformatycznego, funkcjonariuszowi, o którym mowa w ust. 1 zostają nadane uprawnienia w systemie zgodnie z instrukcją EDEN.

§ 12. 1. Kancelarią tajną kieruje wyznaczony funkcjonariusz jednostki organizacyjnej, o której mowa w § 6 ust. 2, zwany dalej "kierownikiem kancelarii tajnej".

2. Do zadań kierownika kancelarii tajnej należy w szczególności:

1) nadzór nad przestrzeganiem przepisów dotyczących obiegu materiałów niejawnych w głównej kancelarii tajnej;

2) opiniowanie wniosków w sprawach utworzenia, łączenia i likwidacji oddziałów kancelarii tajnej oraz stanowisk rejestracji;

3) nadzór i prowadzenie szkoleń z zakresu obsługi kancelaryjnej materiałów niejawnych;

4) nadzór merytoryczny nad jednostkami rejestrującymi, w szczególności w zakresie przestrzegania przepisów dotyczących ewidencjonowania i obiegu materiałów niejawnych;

5) doradztwo i konsultacje w zakresie funkcjonowania jednostek rejestrujących oraz obiegu materiałów niejawnych;

6) wykonywanie poleceń pełnomocnika ochrony.

§ 13. 1. W przypadku zmiany na stanowisku kierownika kancelarii tajnej albo jego faktycznej lub przewidywanej nieobecności trwającej nieprzerwanie ponad 60 dni, przejęcie obowiązków odbywa się na podstawie protokołu zdawczo-odbiorczego. Zapisy § 11 ust. 2 stosuje się odpowiednio.

2. W przypadku niemożności przekazania obowiązków kierownika kancelarii tajnej w sposób określony w ust.1, przekazanie przeprowadza komisja powołana według zasad określonych w § 17 ust. 1.

3. Protokół, o którym mowa w ust. 1, sporządza się w egzemplarzu pojedynczym i przechowuje w głównej kancelarii tajnej.

4. W przypadku nieobecności innej niż określona w ust. 1, kierownik kancelarii tajnej wyznacza pisemnie funkcjonariusza kancelarii tajnej lub, w porozumieniu z pełnomocnikiem ochrony, innego funkcjonariusza, który będzie go zastępował.

§ 14. Do zadań głównej kancelarii tajnej należy w szczególności:

1) prowadzenie obsługi kancelaryjnej materiałów niejawnych delegatur lub jednostek organizacyjnych, w których nie utworzono oddziału kancelarii tajnej lub stanowiska rejestracji;

2) prowadzenie rejestru dzienników ewidencji i teczek, zwanego dalej "RDEiT";

3) bieżąca kontrola właściwego oznaczania, zabezpieczania oraz ewidencjonowania przesyłek niejawnych przekazywanych za pośrednictwem kancelarii;

4) konsultacje i bieżąca pomoc w przedmiocie prawidłowego ewidencjonowania i oznaczania materiałów niejawnych;

5) udział w konwojowaniu materiałów niejawnych kierowanych do adresatów za pośrednictwem przewoźnika;

6) przechowywanie materiałów niejawnych, niestanowiących elementów składowych spraw prowadzonych w jednostce lub komórce organizacyjnej obsługiwanej przez główną kancelarię tajną;

7) odbieranie przesyłek niejawnych dostarczonych przez nadawcę bezpośrednio do CBA, jeżeli nie wskazał on na kopercie zewnętrznej lub wykazie przesyłek nadanych konkretnej jednostki lub komórki organizacyjnej CBA;

8) obsługa systemów utajnionej łączności;

9) prowadzenie szkoleń z zakresu obsługi kancelaryjnej materiałów niejawnych.

§ 15. Do zadań oddziału kancelarii tajnej należy:

1) prowadzenie obsługi kancelaryjnej materiałów niejawnych w delegaturze;

2) prowadzenie RDEiT dla oddziału kancelarii tajnej w delegaturze, zarejestrowanego w RDEiT, o którym mowa w § 14 pkt 2;

3) odbieranie przesyłek niejawnych dostarczonych bezpośrednio do siedziby oddziału kancelarii tajnej;

4) przekazywanie, przesyłek niejawnych bezpośrednio do adresata za pośrednictwem funkcjonariuszy delegatury, jeżeli nie jest uzasadnione korzystanie z usług przewoźnika;

5) wykonywanie odpowiednio zadań, o których mowa w § 14 pkt 4-6 i 8 w zakresie właściwości delegatury.

§ 16. Do zadań stanowiska rejestracji należy w szczególności:

1) prowadzenie obsługi kancelaryjnej materiałów niejawnych w jednostce lub komórce organizacyjnej;

2) przekazywanie przesyłek niejawnych bezpośrednio do adresata za pośrednictwem funkcjonariuszy jednostki lub komórki organizacyjnej, jeżeli kierownik jednostki organizacyjnej nie zdecyduje o skorzystaniu z usług przewoźnika

3) przekazywanie i odbieranie z głównej kancelarii tajnej lub oddziału kancelarii tajnej przesyłek niejawnych wysyłanych lub odbieranych od przewoźnika;

4) odbieranie przesyłek niejawnych, jeżeli jednostka lub komórka organizacyjna, w których to stanowisko zostało zorganizowane, została wskazana na kopercie zewnętrznej lub wykazie przesyłek nadanych;

5) wykonywanie odpowiednio zadań, o których mowa w § 14 pkt 4-6 i 8, w zakresie właściwości jednostki lub komórki organizacyjnej.

§ 17. 1. Do przeprowadzenia likwidacji lub przekształcenia jednostki rejestrującej, pełnomocnik ochrony powołuje komisję w liczbie co najmniej trzech osób.

2. Komisja, o której mowa w ust. 1 jest powoływana z urzędu lub na wniosek kierownika jednostki organizacyjnej lub dyrektora delegatury.

3. Zadania komisji określa każdorazowo pełnomocnik ochrony.

§ 18. 1. W CBA funkcjonuje kancelaria tajna międzynarodowa, której organizację określają przepisy odrębne.

2. Kierownik kancelarii tajnej pełni również funkcję kierownika kancelarii tajnej międzynarodowej.

Rozdział 3.
Obowiązki funkcjonariuszy uczestniczących w obiegu informacji niejawnych

§ 19. 1. Każdy funkcjonariusz ma obowiązek zapewnić należytą ochronę informacjom niejawnym odpowiednio do przyznanej im klauzuli tajności z zachowaniem atrybutów bezpieczeństwa informacji, a mianowicie poufności, integralności i dostępności informacji niejawnych.

2. Funkcjonariusz, który stwierdzi nieprawidłowości w zakresie przetwarzania informacji niejawnych, zobowiązany jest poinformować o nich kierownika jednostki organizacyjnej lub dyrektora delegatury w formie notatki służbowej za pośrednictwem bezpośredniego przełożonego. Notatkę, o której mowa w zdaniu pierwszym należy sporządzić niezwłocznie, nie później niż w ciągu trzech dni.

3. Kierownik jednostki organizacyjnej lub dyrektor delegatury:

1) sprawuje bieżący, bezpośredni nadzór nad właściwym zabezpieczeniem i ochroną materiałów niejawnych w podległej mu jednostce organizacyjnej;

2) jest zobowiązany do powiadomienia pełnomocnika ochrony o fakcie ujawnienia informacji niejawnych lub utraty materiału niejawnego w podległej mu jednostce organizacyjnej lub delegaturze oraz innych nieprawidłowościach dotyczących ochrony informacji niejawnych i podjęcia w tym zakresie czynności wyjaśniających;

3) w przypadku, o którym mowa w pkt. 2 oraz zarejestrowania materiału niejawnego w dzienniku ewidencji, należy wpisać w nim numer pisma, którym dokonano zgłoszenia stwierdzonego incydentu do pełnomocnika ochrony;

4) jest zobowiązany do informowania pełnomocnika ochrony o wszystkich zdarzeniach, które mogą mieć wpływ na obieg informacji niejawnych w podległej mu jednostce organizacyjnej lub delegaturze;

5) nie może bez porozumienia z pełnomocnikiem ochrony wprowadzać dodatkowych, szczególnych regulacji w zakresie funkcjonowania obiegu informacji niejawnych.

Rozdział 4.
Dzienniki ewidencji

§ 20. 1. Podstawowym dziennikiem ewidencji materiałów niejawnych w CBA jest „EDEN”, który funkcjonuje w systemie teleinformatycznym, spełniającym wymagania, o których mowa w art. 48 ustawy.

2. Sposób zarządzania i funkcjonowania „EDEN” określa instrukcja EDEN zamieszczona na Portalu Wewnętrznym Centralnego Biura Antykorupcyjnego.

3. Do rejestrowania i wydawania dokumentów niejawnych przesyłanych za pośrednictwem systemu akredytowanego, o którym mowa w art. 48 ustawy, którego użytkownikiem końcowym jest Centralne Biuro Antykorupcyjne, o ile reguluje to dokumentacja bezpieczeństwa tego systemu, nie stosuje się ust. 1.

4. System, o którym mowa w ust.1 zapewnia:

1) integralność wpisów, polegającą na zabezpieczeniu przed wprowadzeniem nieautoryzowanych danych;

2) możliwość identyfikacji uprawnionych funkcjonariuszy i dokumentowanie wszystkich operacji dokonanych w systemie, szczególnie w zakresie modyfikacji rekordów;

3) możliwość dostępu do danych znajdujących się w systemie zgodnie z nadanymi uprawnieniami.

5. Zmiany treści zapisów w systemie odnotowywane są we właściwych metadanych.

6. Papierowymi dziennikami ewidencji przeznaczonymi do rejestrowania, obiegu i wydawania materiałów niejawnych są:

1) dziennik ewidencyjny;

2) rejestr wydanych przedmiotów (RWP);

3) książka doręczeń przesyłek miejscowych (KDPM);

4) wykaz przesyłek nadanych (WPN).

7. Wzory dzienników ewidencji, o których mowa w ust. 6, określa rozporządzenie o KT.

8. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych, w jednostkach organizacyjnych i delegaturach można prowadzić inne dzienniki ewidencji, niż wymienione w ust. 6, w szczególności dziennik podawczy, którego wzór określa załącznik nr 4.

9. Papierowe dzienniki ewidencji służące do dokumentowania obiegu materiałów niejawnych podlegają rejestracji w RDEiT, prowadzonym odpowiednio w głównej kancelarii tajnej lub w oddziale kancelarii tajnej. Wzór RDEiT określa rozporządzenie o KT.

10. Papierowe dzienniki ewidencji muszą być zszyte, opieczętowane, posiadać ponumerowane strony, a na końcu adnotację dotyczącą daty i miejscowości oraz liczby stron dziennika, potwierdzoną podpisem osoby wypełniającej.

11. Rejestracja w papierowych dziennikach ewidencji jest dokonywana tuszem lub atramentem w kolorze czarnym lub niebieskim. Wpisy oraz ich zmiany, dokonywane są przez osoby upoważnione do prowadzenia obsługi kancelaryjnej materiałów niejawnych. Zmiany wpisów są dokonywane kolorem czerwonym z podaniem daty oraz czytelnego podpisu osoby dokonującej zmiany. Wpisu o anulowaniu pozycji w ewidencji dokonuje się kolorem czerwonym podając przyczynę anulowania oraz datę i czytelny podpis osoby anulującej.

12. Wpisów dokonuje się czytelnie, zgodnie z tytułami kolumn dzienników ewidencji. Wycieranie i zamazywanie wpisów w dziennikach ewidencji jest zabronione.

13. Każdy papierowy dziennik ewidencji podlega zakończeniu poprzez dokonanie podkreślenia pod ostatnią zarejestrowaną pozycją tuszem lub atramentem w kolorze czerwonym i naniesienie adnotacji z informacją o pozycji, na której dziennik został zakończony, z datą i czytelnym podpisem osoby dokonującej adnotacji.

14. Papierowe dzienniki ewidencji prowadzone w systemie wieloletnim, w każdym roku kalendarzowym rozpoczynają się od pozycji 1 i podlegają zakończeniu w sposób, o którym mowa w ust. 13.

15. Jednostka rejestrująca jest zobowiązana zachować zdolność kontynuowania rejestracji w dziennikach papierowych na wypadek awarii systemu teleinformatycznego, a następnie po jej usunięciu uzupełnić dane w systemie, w celu przywrócenia ich ciągłości.

Rozdział 5.
Wytwarzanie, kopiowanie i rejestracja materiałów niejawnych

§ 21. 1. Materiały niejawne przetwarza się w pomieszczeniach znajdujących się w odpowiednich strefach ochronnych, z zastrzeżeniem § 38 ust. 4.

2. Przetwarzanie materiałów niejawnych w formie elektronicznej odbywa się wyłącznie w systemach teleinformatycznych, posiadających akredytację bezpieczeństwa teleinformatycznego, o której mowa art. 48 ustawy.

§ 22. 1. Materiał niejawny, bez względu na technikę wytworzenia, rejestruje się pod kolejnym numerem pozycji dziennika ewidencji, z zastrzeżeniem § 10 ust. 2 rozporządzenia o oznaczaniu.

2. Rejestracji podlega dokument niejawny podpisany lub parafowany, a także dokument elektroniczny, o którym mowa w § 2 pkt 3 rozporządzenia o oznaczaniu.

3. W numerze ewidencyjnym materiału niejawnego umieszcza się oznaczenie cyfrowe oznaczające indywidualny numer jednostki rejestrującej, o którym mowa w § 8 ust. 1 zarządzenia.

4. Dopuszcza się umieszczenie w numerze ewidencyjnym innych elementów ułatwiających ustalenie miejsca przechowywania dokumentu.

5. Funkcjonariusz jednostki rejestrującej ma prawo odmówić przyjęcia do rejestracji lub do wysłania materiału niejawnego, jeżeli nie zostały spełnione warunki formalne w zakresie jego wykonania lub oznaczenia, wynikające z rozporządzenia o oznaczaniu.

6. Materiały wadliwe, w szczególności w postaci wydruków, odbitek, matryc, kalek oraz brudnopisów powstałych w toku prac nad ostateczną wersją dokumentu niejawnego, jeżeli nie podlegają rejestracji, powinny zostać bezzwłocznie zniszczone w sposób uniemożliwiający ich odczytanie lub odtworzenie.

7. Wszelkie działania związane z oznaczaniem oraz umieszczaniem dodatkowych adnotacji na dokumencie elektronicznym, dokumentowane są zgodnie z rozporządzeniem o oznaczaniu.

§ 23. 1. Zezwolenie na kopiowanie materiału niejawnego wydaje w formie dekretacji:

1) Szef CBA lub jego Zastępca;

2) kierownik jednostki organizacyjnej lub dyrektor delegatury, jego zastępca lub upoważniony przez niego funkcjonariusz, w odniesieniu do materiałów niejawnych znajdujących się w kierowanej przez niego jednostce organizacyjnej lub delegaturze.

2. Zezwolenie na kopiowanie materiału niejawnego o klauzuli „poufne”, „zastrzeżone”, może wydać również kierownik komórki organizacyjnej lub jego zastępca, w odniesieniu do materiałów znajdujących się w kierowanej przez niego komórce.

§ 24. Zezwolenie, o którym mowa w § 23 odnotowywane jest bezpośrednio na dokumencie niejawnym, który ma być kopiowany lub w innej formie pisemnej, w szczególności, w odniesieniu do dokumentacji kartotecznej, ewidencyjnej, procesowej i archiwalnej oraz innych niż dokument niejawny materiałów niejawnych. Zezwolenie powinno zawierać:

1) imię i nazwisko funkcjonariusza lub wskazanie jednostki rejestrującej wyznaczonych do kopiowania;

2) zakres dokumentu, którego dotyczy zezwolenie;

3) liczbę egzemplarzy;

4) podmioty, którym mają być wydane poszczególne egzemplarze;

5) podpis sporządzającego wraz z datą.

§ 25. 1. Dokument niejawny powstały w wyniku kopiowania jest rejestrowany jako nowy dokument.

2. Obowiązek dopełnienia rejestracji we właściwej jednostce rejestrującej spoczywa na funkcjonariuszu wyznaczonym do kopiowania.

3. W przypadku kopiowania materiałów stanowiących zbiór dokumentów, zszytych i kolejno ponumerowanych, dopuszcza się możliwość rejestracji nowopowstałego dokumentu niejawnego pod jednym numerem ewidencyjnym.

4. W przypadku wyłączenia dokumentów ze zbioru przed kopiowaniem, należy każdy z pozostałych dokumentów zbioru traktować odrębnie i zarejestrować pod odrębną pozycją dziennika.

5. Dokument niejawny powstały w wyniku kopiowania, będący odwzorowaniem cyfrowym, należy zarejestrować jako egzemplarz pojedynczy, zapisany na jednym nośniku danych.

Rozdział 6.
Obieg materiałów niejawnych

§ 26. 1. Obieg materiałów niejawnych odnotowuje się w dziennikach ewidencji, które odzwierciedlają ich przekazywanie w obiegu wewnętrznym i zewnętrznym.

2. Zasady pakowania, nadawania, przewożenia oraz odbioru przesyłek niejawnych określają odrębne przepisy, z zastrzeżeniem przepisów niniejszego rozdziału.

§ 27. 1. W przypadku wystąpienia konieczności bezpośredniego przekazania przesyłki od nadawcy do adresata, jednostki organizacyjne lub delegatury dokonują przekazania we własnym zakresie, z zastrzeżeniem ust. 5.

2. Przekazywanie przesyłek niejawnych pomiędzy jednostkami organizacyjnymi lub delegaturami odbywa się za pośrednictwem przewoźnika lub bezpośrednio przez pisemnie upoważnionych funkcjonariuszy.

3. Upoważnienie do nadawania i odbioru przesyłek niejawnych bezpośrednio od podmiotów zewnętrznych i za pośrednictwem przewoźnika wydaje kierownik jednostki organizacyjnej lub dyrektor delegatury.

4. Kancelaria ogólna może pośredniczyć w przesyłaniu dokumentów oznaczonych klauzulą „zastrzeżone" i „poufne" za pośrednictwem przewoźnika, o którym mowa w § 2 ust. 1 pkt 4 rozporządzenia o przewożeniu.

5. Szczegółowy tryb przekazywania i przesyłania przesyłek pomiędzy nieruchomościami użytkowanymi przez CBA, zlokalizowanymi w granicach administracyjnych Warszawy a przewoźnikiem, określają wytyczne pełnomocnika ochrony.

§ 28. 1. Przyjmowanie i przekazywanie przesyłek niejawnych przez jednostki rejestrujące polega na:

1) sprawdzeniu prawidłowości nazwy adresata i adresu;

2) sprawdzeniu zgodności odcisku pieczęci na opakowaniu z nazwą nadawcy, umieszczonej na wykazie przesyłek nadanych;

3) sprawdzeniu zgodności numerów na przesyłce z numerami na wykazie przesyłek nadanych lub w książce doręczeń przesyłek miejscowych;

4) sprawdzeniu poprawności zapakowania koperty zewnętrznej i wewnętrznej oraz czy nie zostały naruszone pieczęcie i opakowania;

5) otwarciu koperty zewnętrznej w celu ustalenia właściwego adresata;

6) niezwłocznym zarejestrowaniu i przekazaniu za pokwitowaniem w odpowiednim dzienniku ewidencji:

   a) w książce doręczeń przesyłek miejscowych lub dzienniku podawczym, w obiegu wewnętrznym, jeżeli na kopercie wewnętrznej jest wskazana jednostka lub komórka organizacyjna, lub delegatura która posiada własną jednostkę rejestrującą,

   b) w papierowym dzienniku ewidencyjnym, w przypadku gdy jednostka organizacyjna lub delegatura nie korzysta z EDEN.

2. Materiał niejawny mylnie skierowany, nie podlega rejestracji, lecz jest zwracany nadawcy, protokołem zwrotu, razem z jego pierwotnym opakowaniem. Wzór protokołu określa załącznik nr 5.

3. Szczególny sposób przyjmowania i przekazywania przesyłek niejawnych poza godzinami podstawowego czasu służby CBA, realizowany na terenie nieruchomości użytkowanej przez CBA, określa kierownik jednostki organizacyjnej lub dyrektor delegatury odpowiedzialny za ochronę tej nieruchomości.

§ 29. 1. Wysyłanie przesyłek niejawnych za pośrednictwem jednostek rejestrujących polega na:

1) zarejestrowaniu materiału niejawnego w odpowiednim dzienniku ewidencji;

2) zapakowaniu przesyłki;

3) sporządzeniu wykazu przesyłek nadanych lub wpisaniu do książki doręczeń przesyłek miejscowych.

2. W obiegu wewnętrznym materiały niejawne mogą być przekazywane w nieprzezroczystych okładkach lub teczkach.

3. Przekazywanie materiałów niejawnych, o których mowa w ust. 2, odbywa się za pokwitowaniem w książce doręczeń przesyłek miejscowych.

4. Przekazywanie materiałów niejawnych w obiegu zewnętrznym odbywa się na podstawie wykazu przesyłek nadanych.

5. Przekazywanie materiałów niejawnych pomiędzy jednostkami organizacyjnymi CBA w granicach administracyjnych miasta może odbywać się na podstawie książki doręczeń przesyłek miejscowych.

§ 30. 1. Przesyłki niejawne wysyłane za pośrednictwem przewoźnika, po wykonaniu czynności, o których mowa w § 28 ust. 1, przekazuje się do głównej kancelarii tajnej lub oddziału kancelarii tajnej, za pokwitowaniem w książce doręczeń przesyłek miejscowych.

2. W przypadku stanowisk rejestracji utworzonych w jednostkach organizacyjnych lub delegaturach, które znajdują się w innych granicach administracyjnych niż główna kancelaria tajna lub oddział kancelarii tajnej, przesyłki niejawne mogą być dostarczane bezpośrednio do przewoźnika.

§ 31. 1. W jednostkach rejestrujących nie otwiera się przesyłek niejawnych oznaczonych adnotacjami typu: „do rąk własnych". Są one przekazywane wyłącznie wskazanemu na kopercie adresatowi, który dokonuje czynności, o których mowa w § 32 ust. 1 pkt 1, z zastrzeżeniem § 32 ust. 2.

2. Na opakowaniu przesyłek, o których mowa w ust. 1, wpisuje się datę wpływu i numer, pod którym zarejestrowano przesyłkę, z zaznaczeniem w rubryce „uwagi/informacje uzupełniające" dziennika ewidencji adnotacji, że przesyłka była oznaczona „do rąk własnych".

3. W przypadku prowadzenia EDEN, uzupełnia się wszystkie pola niezbędne do zarejestrowania dokumentu, z zastrzeżeniem, o którym mowa w ust. 2.

4. W EDEN w polu opisu materiału niejawnego należy wpisać adnotację – „rejestracja wstępna", a następnie po otwarciu przesyłki uzupełnić informacje poprzez modyfikację rekordu.

5. W przypadku nieobecności adresata, o którym mowa w ust. 1, o przesyłce należy powiadomić przełożonego adresata lub funkcjonariusza upoważnionego przez adresata do odbioru, który podejmie decyzję w sprawie dalszego postępowania z przesyłką.

6. Z chwilą zwrotu do jednostki rejestrującej dokonuje się kompletnej rejestracji przesyłki niejawnej.

§ 32. 1. Rejestracja przesyłek niejawnych wpływających polega w szczególności na:

1) sprawdzeniu przez funkcjonariusza obsługującego jednostkę rejestrującą prawidłowości adresu oraz zgodności zawartości przesyłki z pisemnie zadeklarowaną zawartością;

2) opatrzeniu otrzymanego dokumentu niejawnego pieczęcią wpływu, wpisaniu kolejnego numeru z dziennika ewidencji oraz daty wpływu - bezpośrednio na dokumencie, a w przypadkach, o których mowa w § 30 ust. 1, w pierwszej kolejności na kopercie wewnętrznej.

2. W przypadkach braku możliwości otwarcia koperty wewnętrznej, o której mowa w § 31, czynności określone w ust. 1 przeprowadza osoba upoważniona

3. Fakt zapoznania się z dokumentem niejawnym o klauzuli „ściśle tajne", „tajne" funkcjonariusz potwierdza czytelnym podpisem i datą na karcie zapoznania się z dokumentem, którą dołącza się do dokumentu z chwilą jego rejestracji. Wzór karty zapoznania się z dokumentem określa rozporządzenie o KT.

4. W przypadku dokumentów o klauzuli „poufne", fakt zapoznania się z dokumentem można odnotować w karcie zapoznania się z dokumentem lub bezpośrednio na dokumencie.

5. W przypadku zszytego i zabezpieczonego pieczęcią zbioru dokumentów niejawnych zakłada się jedną kartę zapoznania się z dokumentem bądź jej funkcję może pełnić karta kontrolna prowadzona dla zbioru.

6. Obowiązek, o którym mowa w ust. 3 i 4 nie dotyczy dokumentów stanowiących ewidencję operacyjną.

7. Przekazywanie dokumentów, o których mowa w ust. 3, 4 i 5 w obiegu wewnętrznym następuje razem z kartą zapoznania się z dokumentem w celu zachowania kontynuacji wpisów.

8. W przypadku przekazywania dokumentów odbiorcom zewnętrznym, kartę zapoznania się z dokumentem pozostawia się w jednostce organizacyjnej.

9. Kartę zapoznania się z dokumentem, który został zarchiwizowany przechowuje się w jednostce rejestrującej zgodnie z przepisami odrębnymi

10. W przypadku zarejestrowania dokumentu niejawnego w EDEN kartę, o której mowa w ust. 7 archiwizuje się zgodnie z innymi przepisami.

§ 33. 1. W przypadku stwierdzenia uszkodzenia przesyłki niejawnej lub śladów jej otwierania, funkcjonariusz kwitujący odbiór przesyłki, sporządza w obecności doręczającego protokół uszkodzenia. Protokół sporządza się w dwóch egzemplarzach, po jednym dla każdej ze stron.

2. W przypadku stwierdzenia w przesyłce niejawnej wpływającej rozbieżności, dotyczących elementów, o których mowa w § 28 ust. 1 pkt 1 - 4:

1) funkcjonariusz prowadzący jednostkę rejestrującą sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki, z przeznaczeniem dla adresata oraz nadawcy;

2) funkcjonariusz prowadzący jednostkę rejestrującą dokonuje w odpowiednim dzienniku ewidencji zapisu o sporządzeniu protokołu.

3. W przypadku, gdy nadawca może bezpośrednio usunąć nieprawidłowości, dopuszcza się odstąpienie od sporządzenia protokołu, o którym mowa w ust. 2 pkt 1.

4. Po otrzymaniu protokołu z otwarcia przesyłki wychodzącej z CBA, sporządzonego przez instytucję zewnętrzną, kierownik kancelarii tajnej lub funkcjonariusz prowadzący oddział kancelarii tajnej:

1) przeprowadza czynności wyjaśniające lub zwraca się do odpowiedniej jednostki rejestrującej z prośbą o wyjaśnienie zaistniałej sytuacji i dokonanie adnotacji, o której mowa w ust. 2 pkt 2;

2) powiadamia pisemnie adresata o wynikach ustaleń.

5. W przypadku, gdy protokół, o którym mowa w ust. 4, wpłynie bezpośrednio do jednostki organizacyjnej lub delegatury, egzemplarz pisemnego powiadomienia, o którym mowa w ust. 4 pkt 2, przekazuje się niezwłocznie do wiadomości kierownika kancelarii tajnej.

6. Czynności, o których mowa w ust. 2 i 4 nie powinny wstrzymywać ani bez koniecznej potrzeby opóźniać toku sprawy, której przesyłka dotyczy.

§ 34. 1. Przekazanie lub udostępnienie materiału niejawnego kolejnemu funkcjonariuszowi następuje na podstawie dekretacji.

2. Fakt przejęcia materiału niejawnego, funkcjonariusz przejmujący jest zobowiązany pokwitować.

Rozdział 7.
Informatyczne nośniki danych

§ 35. 1. Informacje niejawne przetwarza się na informatycznych nośnikach danych zewidencjonowanych w RWP lub w EDEN.

2. Informatyczny nośnik danych podlega oznaczeniu zgodnie z przepisami rozporządzenia o oznaczaniu, poprzez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób na ich obudowie lub opakowaniu.

3. Informatyczny nośnik danych oznacza się dodatkowo w miarę możliwości hologramem.

4. Od obowiązków, o których mowa w ust. 1 i 2, można odstąpić w przypadku dysków twardych lub innych nośników trwale montowanych w urządzeniach technicznych, których usunięcie nie jest możliwe bez zniszczenia urządzenia. W tym przypadku rejestruje i oznacza się urządzenie.

5. W przypadku nośnika trwale połączonego z urządzeniem, klauzula tajności dotyczy całego urządzenia.

6. Klauzula tajności informatycznego nośnika danych zależy od najwyższej klauzuli informacji, które mają być na nim zapisane.

7. Obniżenie lub zniesienie klauzuli tajności informatycznego nośnika danych, z wyłączeniem nośnika wielokrotnego zapisu, możliwe jest w wyniku obniżenia lub zniesienia klauzuli tajności zapisanych na nim informacji.

8. Proces trwałego usuwania danych zapisanych na informatycznych nośnikach danych z wykorzystaniem specjalnych urządzeń lub oprogramowania, umożliwiający obniżenie lub zniesienie klauzuli tajności tego nośnika, określają procedury pełnomocnika ochrony zatwierdzane przez Szefa CBA.

9. Informatyczne nośniki danych podlegają ochronie stosownej do klauzuli tajności, jaką zostały oznaczone.

Rozdział 8.
Środki bezpieczeństwa fizycznego

§ 36. 1. W ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego, w celu zapewnienia poufności, integralności i dostępności tych informacji.

2. W celu doboru adekwatnych środków bezpieczeństwa fizycznego określa się poziom zagrożeń.

3. Poziom zagrożeń określa się dla pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

4. Podstawowe kryteria i sposób określania poziomu zagrożeń oraz rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń określa rozporządzenie w sprawie środków bezpieczeństwa fizycznego.

5. Dokumentację określającą poziom zagrożeń, o której mowa w art. 43 ust. 4 ustawy, dla obiektów zajmowanych przez CBA opracowuje pełnomocnik ochrony, z zastrzeżeniem, że dla obiektów zajmowanych przez jednostkę organizacyjną, których lokalizacja jest niejawna oraz przez delegaturę, określa pełnomocnik we współpracy z kierownikiem tych jednostek lub dyrektorem delegatury.

6. Cel, o którym mowa w ust. 1, osiąga się przez:

1) zapewnienie właściwego przetwarzania informacji niejawnych;

2) umożliwienie zróżnicowania dostępu do informacji niejawnych dla funkcjonariuszy zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji niejawnych;

3) zapobieganie działaniom nieuprawnionym;

4) uniemożliwianie lub opóźnianie wtargnięcia osób nieuprawnionych w sposób niezauważony lub z użyciem siły do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

7. Środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje niejawne.

8. System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych. W zależności od poziomu zagrożeń, o którym mowa w ust. 2, stosuje się odpowiednią kombinację środków bezpieczeństwa fizycznego.

9. Metodykę doboru środków bezpieczeństwa fizycznego określa załącznik nr 6.

§ 37. 1. Szczegółowe wymagania w zakresie stosowania środków bezpieczeństwa fizycznego informacji niejawnych przetwarzanych przez CBA, określa plan ochrony informacji niejawnych w CBA.

2. Na plan, o którym mowa w ust. 1, składają się poszczególne plany ochrony informacji niejawnych opracowane oddzielnie dla każdego obiektu użytkowanego przez CBA, w którym przetwarzane są informacje niejawne.

3. Plany ochrony informacji niejawnych dla obiektów delegatur i obiektów jednostek organizacyjnych, których lokalizacja jest niejawna, opracowują kierownicy tych jednostek lub dyrektorzy delegatur.

4. Projekty planów, o których mowa w ust. 3 muszą uzyskać akceptację pełnomocnika ochrony.

5. Plany ochrony informacji niejawnych dla pozostałych obiektów CBA opracowuje pełnomocnik ochrony.

6. Plany ochrony informacji niejawnych dla poszczególnych obiektów wymagają zatwierdzenia przez Szefa CBA lub upoważnionego przez niego kierownika jednostki organizacyjnej.

§ 38. 1. Informacje niejawne o klauzuli „ściśle tajne”:

1) przetwarza się w strefie ochronnej I lub II z zastosowaniem jednego z poniższych środków uzupełniających:

a) stałej ochrony lub kontroli w nieregularnych odstępach czasu przez osoby wykonujące czynności związane z fizyczną ochroną obiektów, posiadające odpowiednie poświadczenie bezpieczeństwa, w szczególności z wykorzystaniem systemu dozoru wizyjnego z obowiązkową rejestracją, z rozdzielczością nie mniejszą niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni,

b) systemu sygnalizacji włamania i napadu z wykorzystaniem systemu dozoru wizyjnego, o którym mowa w lit. a;

2) przechowuje się w certyfikowanej szafie metalowej lub w odrębnie zamykanych skrytkach, będących jej częścią.

2. Informacje niejawne o klauzuli „tajne”:

1) przetwarza się w strefie ochronnej I lub II;

2) przechowuje się w certyfikowanej szafie metalowej lub w odrębnie zamykanych skrytkach, będących jej częścią.

3. Informacje niejawne o klauzuli „poufne”:

1) przetwarza się w strefie ochronnej I, II lub III;

2) przechowuje się w strefie ochronnej I lub II w certyfikowanej szafie metalowej lub w odrębnie zamykanych skrytkach, będących jej częścią.

4. Informacje niejawne o klauzuli „zastrzeżone” przetwarza się w pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu i przechowuje się w szafie metalowej lub zamkniętym na klucz meblu biurowym.

5. O ile jest to uzasadnione potrzebami służby, dopuszcza się przechowywanie materiałów niejawnych wchodzących w skład zasobu archiwalnego archiwum wyodrębnionego CBA, w niecertyfikowanych szafach metalowych, zestawach kartotecznych i na regałach, pod warunkiem zastosowania dodatkowych zabezpieczeń pomieszczenia, gwarantujących realizację celu, o którym mowa w § 36. Szczegółowy opis zastosowanych środków bezpieczeństwa podlega akceptacji pełnomocnika ochrony i stanowi element planu ochrony informacji niejawnych.

6. Przechowywanie materiałów niejawnych w tym informatycznych nośników danych, zewidencjonowanych na więcej niż jednego funkcjonariusza, w szafach metalowych nieposiadających wydzielonych skrytek jest dopuszczalne wyłącznie pod warunkiem odpowiedniego ich zabezpieczenia przed wglądem nieuprawnionych do tego innych użytkowników szafy.

7. Informatyczny nośnik danych stosowany do przetwarzania informacji niejawnych w systemie teleinformatycznym może być przechowywany poza certyfikowaną szafą metalową w przypadkach określonych w dokumentacji bezpieczeństwa tego systemu teleinformatycznego.

§ 39. 1. Szafy i pomieszczenia, w których przechowywane są materiały niejawne, po zakończeniu służby zamyka się i zabezpiecza zgodnie z planem ochrony informacji niejawnych.

2. Po zakończeniu służby funkcjonariusz, w którego dyspozycji znajdują się materiały niejawne, jest obowiązany sprawdzić prawidłowość zamknięcia szaf, skrytek, pojemników, bezpiecznych kopert i innych zabezpieczeń przewidzianych w planie ochrony informacji niejawnych oraz pomieszczeń, w których materiały te są przechowywane.

3. Przed otwarciem pomieszczeń oraz szaf, w których są przechowywane dokumenty niejawne, należy sprawdzić czy drzwi, zamki i inne zabezpieczenia nie noszą śladów uszkodzeń bądź śladów wskazujących na podejmowanie próby nieuprawnionego dostania się do nich.

4. Na polecenie kierownika jednostki organizacyjnej lub dyrektora delegatury, a w stosunku do kierowników jednostek organizacyjnych lub dyrektorów delegatur na polecenie Szefa CBA lub jego Zastępcy, otwarcia pomieszczeń, szaf lub skrytek służących do przechowywania materiałów niejawnych pod nieobecność ich dysponenta, dokonuje się w obecności co najmniej dwóch osób.

5. Na zasadach określonych w ust. 4 można dokonać zdjęcia zabezpieczenia przed wglądem, o którym mowa w § 38 ust. 6, a także uzyskać dostęp do informacji niejawnych zapisanych na informatycznym nośniku danych.

6. Czynności, o których mowa w ust. 4 i 5, dokumentuje się w formie protokołu, który zatwierdza osoba wydająca polecenie otwarcia. Po zatwierdzeniu protokół przechowuje się w jednostce rejestrującej. Z protokołem należy zapoznać dysponenta pomieszczenia, szafy lub komputera, który potwierdza ten fakt podpisem.

7. Klucze i hasła (kody) zamków szyfrowych zabezpieczające szafy, skrytki, pomieszczenia lub obszary, w których przetwarzane są informacje niejawne udostępnia się wyłącznie osobom uprawnionym, a w przypadku realizowania czynności, o których mowa w ust. 4, z hasłem (kodem) zamka szyfrowego zapoznaje się wyłącznie jeden z jej uczestników, wyznaczony przez osobę wydającą polecenie otwarcia, którego wskazuje się w treści protokołu, o którym mowa w ust. 6.

8. W przypadku utraty kluczy od pomieszczeń, szaf, pojemników i innych miejsc przechowywania materiałów niejawnych, funkcjonariusz zawiadamia o tym fakcie bezpośredniego przełożonego. Powiadomiony przełożony niezwłocznie podejmuje działania zmierzające do prawidłowego zabezpieczenia materiałów przechowywanych w szafach metalowych bądź pomieszczeniach, do których klucze utracono, oraz zawiadamia o utracie i podjętych działaniach kierownika jednostki. Kierownik jednostki organizacyjnej lub dyrektor delegatury przeprowadza wyjaśnienia, o których informuje pełnomocnika ochrony.

9. W przypadku stosowania haseł (kodów) zamków szyfrowych do zabezpieczania szaf, w których przechowywane są materiały niejawne, powinny być one zmieniane co najmniej raz w roku, a także w sytuacji:

1) utraty uprawnień do użytkowania szafy, skrytki lub pomieszczenia zabezpieczanego zamkiem szyfrowym;

2) stwierdzenia lub podejrzenia utraty poufności hasła (kodu);

3) naprawy uszkodzonego zamka szyfrowego lub jego konserwacji;

4) przewidzianej w planie ochrony.

10. Po przeprowadzeniu czynności, o których mowa w ust. 4, zmiany, o której mowa w ust. 9 dokonuje niezwłocznie osoba uprawniona do użytkowania otwartego pomieszczenia, szafy metalowej lub skrytki.

11. Jeśli osoba uprawniona do użytkowania miejsca przechowywania materiałów niejawnych, o której mowa w ust. 10, zapoznała się z hasłem (kodem) zamka szyfrowego w związku z realizacją czynności, o których mowa w ust. 4, to jego zmiana jest obligatoryjna wyłącznie w przypadku, gdy wystąpią przesłanki dla takiej zmiany wskazane w ust. 9.

12. W planie ochrony informacji niejawnych określa się szczegółowe zasady:

1) przyznawania uprawnień do użytkowania szaf i pomieszczeń, w których przetwarzane są informacje niejawne;

2) zdawania, przechowywania i wydawania kluczy do szaf i pomieszczeń, w których przetwarzane są informacje niejawne, z uwzględnieniem zasad dotyczących kluczy do użytku bieżącego oraz kluczy zapasowych;

3) stosowania haseł (kodów) do zamków szyfrowych zabezpieczających miejsca przechowywania materiałów niejawnych oraz deponowania i udostępniania dokumentów zawierających ich treść.

Rozdział 9.
Zadania kontrolne i sprawozdawczość

§ 40. 1. W przypadku uzyskania informacji o nieprawidłowościach w zakresie ochrony informacji niejawnych, w tym także w ramach zgłoszenia, o którym mowa w § 19 ust. 3 pkt 2 i 4, pełnomocnik ochrony podejmuje czynności mające na celu wyjaśnienie zaistniałych okoliczności, podlegające rejestracji w repertorium spraw dotyczących naruszenia przepisów ochrony informacji niejawnych.

2. Do czynności, o których mowa w ust. 1, stosuje się odpowiednio przepisy wewnętrzne CBA dotyczące zasad i trybu przeprowadzania kontroli stanu ochrony informacji niejawnych w CBA, w zakresie uprawnień kontrolera.

3. W każdej jednostce organizacyjnej i delegaturze przeprowadza się co roku inwentaryzację materiałów niejawnych, której zakres i sposób przeprowadzenia określa każdorazowo pełnomocnik ochrony.

4. Do przeprowadzenia inwentaryzacji materiałów niejawnych kierownik jednostki organizacyjnej lub dyrektor delegatury powołuje komisję inwentaryzacyjną.

5. Funkcjonariusze jednostki organizacyjnej, w której powołano pełnomocnika ochrony przeprowadzają weryfikację wyników inwentaryzacji w danej jednostce organizacyjnej lub delegaturze, lub komórce organizacyjnej nie rzadziej niż raz na trzy lata, na zasadach określonych przez pełnomocnika ochrony.

6. Pełnomocnik ochrony przedstawia do zatwierdzenia Szefowi CBA raport z przeprowadzonej weryfikacji inwentaryzacji.

Rozdział 10.
Postanowienia końcowe

§ 41. 1. Zaświadczenia o przeszkoleniu z zakresu obsługi kancelaryjnej wydane przed wejściem w życie niniejszego zarządzenia zachowują ważność.

2. Treść planów ochrony dostosowuje się do wymagań określonych w niniejszym zarządzeniu w terminie do 30 czerwca 2021 r.

3. Wnioski, o których mowa w § 7 ust. 1 należy złożyć w terminie 14 dni od dnia wejścia w życie zarządzenia.

§ 42. Traci moc zarządzenie nr 34/12 Szefa Centralnego Biura Antykorupcyjnego z dnia 26 listopada 2012 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Centralnym Biurze Antykorupcyjnym (Dz. Urz. CBA z 2012 r. poz. 45).

§ 43. Zarządzenie wchodzi w życie z dniem 1 stycznia 2021 r.

Szef Centralnego Biura Antykorupcyjnego

Andrzej Stróżny

Załącznik Nr 1 do Zarządzenia Nr 30/20
Szefa Centralnego Biura Antykorupcyjnego
z dnia 29 grudnia 2020 r.

WZÓR WNIOSKU
WNIOSEK

1. O utworzenie głównej kancelarii tajnej/oddziału kancelarii tajnej/stanowiska rejestracji*;
2. o zmianę na stanowisku funkcjonariusza prowadzącego obsługę kancelaryjną*;
3. o likwidację/ przekształcenie oddziału kancelarii tajnej/stanowiska rejestracji*;
4. o wyznaczenie funkcjonariusza przewidzianego do okresowej obsługi kancelaryjnej □;
5. inne……
……
…….....

w

……

jednostka/ komórka organizacyjna Centralnego Biura Antykorupcyjnego

……., mieszcząca się w siedzibie……., w pomieszczeniu nr…….

posiadającej zatwierdzony plan ochrony z dnia

…….....

w którym do prowadzenia obsługi kancelaryjnej materiałów niejawnych o klauzulach: ściśle tajne/tajne/poufne/zastrzeżone*, zostali wyznaczenia następujący funkcjonariusze:

1.

	Imię i nazwisko funkcjonariusza przewidzianego do obsługi kancelaryjnej	Nr poświadczenia bezpieczeństwa, data ważności i klauzula tajności	Nr zaświadczenia ze szkolenia z zakresu ochrony informacji niejawnych	Nr zaświadczenia ze szkolenia z zakresu obsługi kancelaryjnej materiałów niejawnych
1.				
2.				
3.				

2. do okresowej obsługi kancelaryjnej materiałów niejawnych o klauzulach: ściśle tajne/tajne/poufne/zastrzeżone*, zostali wyznaczenia następujący funkcjonariusze:

	Imię i nazwisko funkcjonariusza przewidzianego do okresowej obsługi kancelaryjnej	Nr poświadczenia bezpieczeństwa, data ważności i klauzula tajności	Nr zaświadczenia ze szkolenia z zakresu ochrony informacji niejawnych	Nr zaświadczenia ze szkolenia z zakresu obsługi kancelaryjnej materiałów niejawnych
1.				

……

(miejscowość i data)

(pieczęć i podpis kierownika jednostki organizacyjnej/dyrektora delegatury)

OPINIA

………
………
………..

....
(data i podpis kierownika kancelarii tajnej)

ZATWIERDZAM

………………………………
(data, podpis i pieczęć pełnomocnika ochrony)

*niepotrzebne skreślić

UWAGI

………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………
………

………………………………………………
(data i podpis pełnomocnika ochrony)

Załącznik Nr 2 do Zarządzenia Nr 30/20
Szefa Centralnego Biura Antykorupcyjnego
z dnia 29 grudnia 2020 r.

WZÓR ZAŚWIADCZENIA

ZAŚWIADCZENIE NR …….

o odbyciu przeszkolenia w zakresie obsługi kancelaryjnej materiałów niejawnych

wydane przez Pełnomocnika do Spraw Ochrony Informacji Niejawnych

w Centralnym Biurze Antykorupcyjnym

Pani/Panu ***……..,***

na podstawie § 10 ust. 1 pkt 3 Zarządzenia Nr …..

Szefa Centralnego Biura Antykorupcyjnego

z dnia ……..

w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnej oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Centralnym Biurze Antykorupcyjnym.

Warszawa, dnia …… r.

.....
(pieczęć i podpis pełnomocnika ochrony)

Załącznik Nr 3 do Zarządzenia Nr 30/20
Szefa Centralnego Biura Antykorupcyjnego
z dnia 29 grudnia 2020 r.

WZÓR PROTOKOŁU ZDAWCZO-ODBIORCZEGO

……..

……. Miejsce i data wytworzenia

Nazwa delegatury/jednostki organizacyjnej

PROTOKÓŁ ZDAWCZO-ODBIORCZY

Egzemplarz pojedynczy

Na polecenie…….……..

(imię i nazwisko kierownika jednostki/komórki organizacyjnej)

dokonano przekazania obowiązków w dniu…… oraz:

dzienników ewidencji:

1. numer dziennika, liczba kart, klauzula,
2. numer dziennika, liczba kart, klauzula,
3. numer dziennika, liczba kart, klauzula,

dokumentów:

1. numer ewidencyjny dokumentu, klauzula, liczba stron,
2. numer ewidencyjny dokumentu, klauzula, liczba stron,
3. numer ewidencyjny dokumentu, klauzula, liczba stron,

pieczęci:

1. ……..
2. ……

Przekazujący obowiązki: Przejmujący obowiązki:

……..

…….

(imię i nazwisko, podpis) (imię i nazwisko, podpis)

Zatwierdzam

……..

(imię i nazwisko, podpis dyrektora delegatury/kierownika jednostki/komórki organizacyjnej)

Załącznik Nr 4 do Zarządzenia Nr 30/20
Szefa Centralnego Biura Antykorupcyjnego
z dnia 29 grudnia 2020 r.

WZÓR DZIENNIKA PODAWCZEGO

.....
(pieczęć nagłówkowa)
(numer z ewidencji)

DZIENNIK PODAWCZY

.....
(komórka organizacyjna)

Rozpoczęto dn. .....

Od pozycji nr .....

Zakończono dn. .....

Na pozycji nr.....

Oznaczenie klauzuli	Numer kolejny zapisu	Data wpływu	Nadawca	Numer przesyłki	Dokąd skierowano	Data i godzina odbioru	Pokwitowanie odbioru	Uwagi

Załącznik Nr 5 do Zarządzenia Nr 30/20
Szefa Centralnego Biura Antykorupcyjnego
z dnia 29 grudnia 2020 r.

WZÓR PROTOKOŁU ZWROTU MATERIAŁU NIEJAWNEGO MYLNIE SKIEROWANEGO

……...
(miejscowość i data)

Egzemplarz nr ___

PROTOKÓŁ ZWROTU MATERIAŁU NIEJAWNEGO MYLNIE SKIEROWANEGO

Dnia ……. do głównej kancelarii tajnej/stanowiska rejestracji/oddziału kancelarii tajnej w Delegaturze CBA w …….* wpłynął mylnie skierowany materiał niejawny.

Numer wykazu/nr KDPM ww. materiału - _____

Adresat ww. materiału- _____

Nieprawidłowość stwierdzono bez otwarcia przesyłki/po otwarciu koperty zewnętrznej/po otwarciu koperty wewnętrznej, otwarciu przesyłki*.

Opis innych istotnych okoliczności (w przypadku wystąpienia) .....

……..
…….....
.....

Jednocześnie oświadczam, że ww. materiał nie został zarejestrowany w głównej kancelarii tajnej/ stanowisku rejestracji/oddziale kancelarii tajnej Delegatury CBA w…….*

……
(imię i nazwisko, podpis i pieczęć kierownika jednostki organizacyjnej/dyrektora delegatury)

*niepotrzebne skreślić

Załącznik nr 1 *- pierwotne opakowanie dokumentu niejawnego.*

Załącznik Nr 6 do Zarządzenia Nr 30/20

Szefa Centralnego Biura Antykorupcyjnego

z dnia 29 grudnia 2020 r.

WZÓR METODYKI DOBORU ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO
Metodyka doboru środków bezpieczeństwa fizycznego

Część I. Instrukcja:

1. Proces doboru środków bezpieczeństwa fizycznego powinien zapewniać elastyczność ich stosowania w zależności od określonego poziomu zagrożeń.

2. Poniżej przedstawiono metody wyboru najbardziej odpowiednich i ekonomicznych kombinacji środków bezpieczeństwa fizycznego.

3. Środki bezpieczeństwa fizycznego określone w części III „Klasyfikacja środków bezpieczeństwa fizycznego" zostały podzielone na 6 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.

4. Pierwszym etapem procesu doboru środków bezpieczeństwa fizycznego jest odczytanie

z tabeli w części II „Podstawowe wymagania bezpieczeństwa fizycznego" minimalnej łącznej sumy punktów wymaganych 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.

5. 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").

6. 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". 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". Dobór adekwatnych środków bezpieczeństwa fizycznego w konkretnym przypadku musi zapewnić uzyskanie zarówno minimalnej łącznej sumy punktów wymaganych 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"). W przypadku, gdy liczba punktów uzyskanych po zastosowaniu środka należącego do grup kategorii oznaczonych jako „obowiązkowo" jest mniejsza od minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych, należy zastosować środki z kategorii oznaczonych „dodatkowo" zapewniające uzyskanie minimalnej łącznej sumy punktów.

7. Ilekroć w części III „Klasyfikacja środków bezpieczeństwa fizycznego" mowa jest o:

a) obiekcie, należy przez to rozumieć nieruchomość posiadaną przez CBA, o granicach, których przebieg określono w zatwierdzonym dla tego obiektu planie ochrony informacji niejawnych,

b) budynku, należy przez to rozumieć również kompleks przylegających do siebie budynków,

c) kratach, należy przez to rozumieć kraty stalowe wewnętrzne (w przypadku zabezpieczania okien piwnicy mogą to być kraty zewnętrzne, nieuchylne), trwale zakotwiczone do budynku, o prętach, których przekrój poprzeczny ma powierzchnię nie mniejszą od powierzchni okręgu o promieniu

16 mm, których rozstaw jest nie większy niż 15cm na 15 cm,

d) pomieszczeniach, należy przez to rozumieć pomieszczenia, których stropy mają wytrzymałość na przebicie zbliżoną lub wyższą od wytrzymałości ścian tych pomieszczeń.

8. Przy przypisywaniu liczby punktów za zastosowanie określonego środka z danej kategorii lub z danej grupy w obrębie kategorii należy brać pod uwagę zastosowany lub planowany do stosowania środek najniżej punktowany (zasada „najsłabszego ogniwa"). W przypadku kategorii „K2". Pomieszczenia", w odniesieniu do ścian oraz drzwi, dozwolone jest, aby przy wyborze najsłabszego ogniwa, kierować się oceną odnoszącą się do całego kompleksu pomieszczeń lub ciągów komunikacyjnych, które są zabezpieczane jako całość i jako całość oceniane. Można wówczas pominąć przypisywanie punktacji ścianom bądź drzwiom znajdującym się w obrębie tego kompleksu, ponieważ nie wpływają one na zabezpieczenie jego całości. Zasady tej nie można stosować w odniesieniu do okien.

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	9	11	12
Obowiązkowo: kategorie K4+K5*	6	7	7
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	19	23	24
TAJNE			
Obowiązkowo: kategorie K1+K2+K3	8	9	10
Obowiązkowo: kategorie K4+K5*	4	5	5
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	16	19	20
POUFNE			
Obowiązkowo: kategorie K1+K2+K3	6	8	9
Obowiązkowo: kategorie K4+K5*	2	3	3
Dodatkowo: kategoria K6	3	3	4
Łącznie suma punktów	11	14	16
ZASTRZEŻONE			
Obowiązkowo: kategorie K1+K2+K3	4	4	4
Dodatkowo: kategoria K4+K5 lub K6	1	2	2
Łącznie suma punktów	5	6	6

* żadna wartość nie może być równa 0

Część III: Klasyfikacje środków bezpieczeństwa fizycznego

Kategoria K1: Urządzenia do przechowywania materiałów niejawnych

Punktacja	Funkcja lub cechy
7 pkt	Szafa spełniająca wymagania klasy odporności na włamanie 0 określone w Polskiej Normie PN-EN 1143-1 zabezpieczona dwoma zamkami.
6 pkt	Szafa spełniająca wymagania klasy odporności na włamanie S2 określone w Polskiej Normie PN-EN 14450 zabezpieczona co najmniej jednym zamkiem.
5 pkt	Szafa spełniająca wymagania klasy odporności na włamanie S1 określone w Polskiej Normie PN-EN 14450 zabezpieczona co najmniej jednym zamkiem.
4 pkt	Szafa metalowa certyfikowana zabezpieczona co najmniej jednym zamkiem.
1 pkt	Szafy metalowe, meble biurowe zamykane na klucz.

Kategoria K2: Pomieszczenia

Środek bezpieczeństwa K2S1 – konstrukcja ścian.

Punktacja	Funkcja lub cechy
4 pkt	Ściany wykonane są z cegły o grubości co najmniej 35 cm lub materiału zapewniającego zbliżony lub większy poziom wytrzymałości (np. z żelbetonu o grubości co najmniej 15 cm) albo wykonane z elementów, które wraz z ich łączeniami posiadają certyfikat odporności na włamanie w klasie nie niższej niż RC4 wg PN-EN 1627.
3 pkt	Ściany wykonane są z cegły o grubości co najmniej 20 cm lub materiału zapewniającego zbliżony poziom wytrzymałości (np. z żelbetonu o grubości co najmniej 12 cm lub z innych lżejszych materiałów wzmocnionych konstrukcją stalową np. ramami lub kratą) albo wykonane z elementów, które wraz z ich łączeniami posiadają certyfikat odporności na włamanie w klasie nie niższej niż RC3 wg PN-EN 1627.
2 pkt	Ściany wykonane są z cegły o grubości co najmniej 12 cm lub materiału zapewniającego zbliżony poziom wytrzymałości (np. z żelbetonu o grubości co najmniej 10 cm lub z innych lżejszych materiałów wzmocnionych konstrukcją stalową np. ramami lub kratą) albo wykonane z elementów, które wraz z ich łączeniami posiadają certyfikat odporności na włamanie w klasie nie niższej niż RC2 wg PN-EN 1627.
1 pkt	Ściany mają grubość mniejszą niż 12 cm lub wykonane są z lekkiego materiału (drewno, pustak, szkło, itp.).

Środek bezpieczeństwa K2S2 – drzwi.

Punktacja	Funkcja lub cechy
4 pkt	Drzwi o odporności na włamanie klasy RC4 lub wyższej wg PN-EN 1627.
3 pkt	Drzwi o odporności na włamanie klasy RC3 wg PN-EN 1627.
2 pkt	Drzwi o odporności na włamanie klasy RC2 wg PN-EN 1627.
1 pkt	Drzwi pełne, np. drewniane, z co najmniej jednym zamkiem.

Środek bezpieczeństwa K2S3 – okna.

Punktacja	Funkcja lub cechy
5 pkt	Okna, których dolna krawędź znajduje się na wysokości powyżej 5 m od poziomu otaczającego terenu i są zabezpieczone kratą lub które posiadają odporność na włamanie w klasie co najmniej RC3 wg PN-EN 1627 i są zabezpieczone przed podglądem z zewnątrz, a budynek jest usytuowany na terenie ogrodzonym i strzeżonym.
4 pkt	Okna, których dolna krawędź znajduje się na wysokości powyżej 5 m od poziomu otaczającego terenu i są zabezpieczone przed podglądem, a budynek jest usytuowany na terenie ogrodzonym i strzeżonym lub okna, których dolna krawędź znajduje się na wysokości powyżej 5 m od poziomu otaczającego terenu i są zabezpieczone kratą lub które posiadają odporność na włamanie w klasie co najmniej RC3 wg PN-EN 1627 i są zabezpieczone przed podglądem z zewnątrz, lub okna, których dolna krawędź znajduje się na wysokości poniżej 5 m od poziomu otaczającego terenu i są zabezpieczone kratą lub które posiadają odporność na włamanie w klasie co najmniej RC3 wg PN-EN 1627 i są zabezpieczone przed podglądem z zewnątrz a budynek jest usytuowany na terenie ogrodzonym i strzeżonym.
3 pkt	Okna, których dolna krawędź znajduje się na wysokości powyżej 5 m od poziomu otaczającego terenu i są zabezpieczone przed podglądem lub okna, których dolna krawędź znajduje się na wysokości poniżej 5 m od poziomu otaczającego terenu i są zabezpieczone kratą lub które posiadają odporność na włamanie w klasie co najmniej RC3 wg PN-EN 1627 i są zabezpieczone przed podglądem z zewnątrz, lub okna, których dolna krawędź znajduje się na wysokości poniżej 5 m i są zabezpieczone przed podglądem a budynek jest usytuowany na terenie ogrodzonym i strzeżonym, z ogrodzeniem o wysokości co najmniej 2 m, wykonanym z trwałych materiałów.

2 pkt	Okna, których dolna krawędź znajduje się na wysokości poniżej 5 m od poziomu otaczającego terenu i są zabezpieczone przed podglądem z zewnątrz, a budynek jest usytuowany na terenie ogrodzonym i strzeżonym.

Kategoria K3: Budynek

Punktacja	Funkcja lub cechy
5 pkt	Budynek wolnostojący, samodzielnie użytkowany, usytuowany w terenie ogrodzonym i strzeżonym. Drzwi wejściowe do budynku objęte są stałym bezpośrednim nadzorem służby ochrony CBA lub z obustronnym elektronicznym systemem kontroli dostępu.
4 pkt	Budynek wolnostojący, samodzielnie użytkowany, usytuowany w terenie ogrodzonym i strzeżonym. Drzwi wejściowe do budynku okresowo zamykane, a w okresie pozostawania otwartymi bezpośrednio nadzorowane przez służbę ochrony CBA.
3 pkt	Budynek wolnostojący, samodzielnie użytkowany, którego ściany w obrysie budynku w jego części nieogrodzonej wykonane są z cegły o grubości co najmniej 12 cm lub materiału zapewniającego zbliżony poziom wytrzymałości lub z elementów, które wraz z ich łączeniami posiadają certyfikat odporności na włamanie w klasie nie niższej niż RC2 wg PN-EN 1627. Drzwi wejściowe do budynku dostępne z terenu ogrodzonego, będącego w wyłącznej dyspozycji CBA objęte są stałym bezpośrednim nadzorem służby ochrony CBA lub z obustronnym elektronicznym systemem kontroli dostępu lub drzwi wejściowe do budynku dostępne z terenu nieogrodzonego, wyposażone są w obustronny elektroniczny systemem kontroli dostępu oraz objęte są bezpośrednim nadzorem służby ochrony CBA lub okresowo zamykane.
2 pkt	Budynek zajmowany przez CBA i inne podmioty. Osobne wejścia z zewnątrz do części budynku zajmowanej przez CBA dostępne są z terenu ogrodzonego, będącego w wyłącznej dyspozycji CBA, są objęte obustronnie systemem kontroli dostępu lub okresowo zamykane, a w okresie pozostawania otwartym bezpośrednio nadzorowane przez służbę ochrony CBA. Brak przejść wewnątrz budynku pomiędzy częścią zajmowaną przez CBA a pozostałą częścią budynku. Ściany w obrysie budynku w jego części zajmowanej przez CBA oraz wewnątrz budynku, wyznaczające granicę obiektu zajmowanego przez CBA wykonane są z cegły o grubości co najmniej 12 cm lub materiału zapewniającego zbliżony poziom wytrzymałości lub wykonane z kraty lub z elementów, które wraz z ich łączeniami posiadają certyfikat odporności na włamanie w klasie nie niższej niż RC2 wg PN-EN 1627 oraz zabezpieczone za pomocą czujek wzbudzających alarm w systemie sygnalizacji włamania i napadu w przypadku próby przebicia.
1 pkt	Budynek zajmowany przez CBA i inne podmioty. Wejścia z zewnątrz do części budynku zajmowanej przez CBA oraz wejścia wewnątrz budynku do jego części zajmowanej przez CBA objęte są obustronnie systemem kontroli dostępu lub okresowo zamykane, a w okresie pozostawania otwartymi bezpośrednio nadzorowane przez służbę ochrony CBA. Ściany w obrysie budynku w jego części zajmowanej przez CBA oraz wewnątrz budynku, wyznaczające granicę obiektu zajmowanego przez CBA wykonane są z cegły o grubości co najmniej 12 cm lub materiału zapewniającego zbliżony poziom wytrzymałości lub wykonane z kraty lub elementów, które wraz z ich łączeniami posiadają certyfikat odporności na włamanie w klasie nie niższej niż RC2 wg PN-EN 1627 oraz zabezpieczone za pomocą czujek wzbudzających alarm w systemie sygnalizacji włamania i napadu w przypadku próby przebicia.

Kategoria K4: Kontrola dostępu

Środek bezpieczeństwa K4S1 – system kontroli dostępu od pomieszczeń (obszaru).

Punktacja	Funkcja lub cechy
4 pkt	Elektroniczny system kontroli dostępu osób. Umożliwia rejestr i archiwizację wejścia/wyjścia (czasu przebywania) osoby, z wyszczególnieniem: imienia i nazwiska, daty, godziny i minuty. Zainstalowany w drzwiach i posiada funkcję anti-passback lub inny system podobnie działający. System generuje alarmy i ostrzeżenia o nieuprawnionym lub nieprawidłowym dostępie do kontrolowanej strefy. Obejmuje co najmniej wszystkie znajdujące się w budynku wejścia i wyjścia ze stref ochronnych oraz wszystkie wejścia i wyjścia z budynku.
3 pkt	Elektroniczny system kontroli dostępu osób. Umożliwia rejestr i archiwizację wejścia/wyjścia (czasu przebywania) osoby, z wyszczególnieniem: imienia i nazwiska, daty, godziny i minuty. System generuje alarmy i ostrzeżenia o nieuprawnionym lub nieprawidłowym dostępie do kontrolowanej strefy. Obejmuje co najmniej wszystkie znajdujące się w budynku wejścia i wyjścia ze stref ochronnych oraz wszystkie wejścia i wyjścia z budynku.
2 pkt	Elektroniczny system kontroli dostępu osób. Umożliwia rejestr i archiwizację wejścia/wyjścia (czasu przebywania) osoby, z wyszczególnieniem: imienia i nazwiska, daty, godziny i minuty. Obejmuje co najmniej wszystkie znajdujące się w budynku wejścia i wyjścia ze stref ochronnych oraz wszystkie wejścia i wyjścia z budynku.
1 pkt.	System kontroli osób wykonywany bez wspomagania urządzeniami technicznymi i elektronicznymi. Ewidencja wejścia/wyjścia realizowana na bieżąco w papierowej dokumentacji służbowej, obejmuje co najmniej wszystkie znajdujące się w budynku wejścia i wyjścia ze stref ochronnych.

Środek bezpieczeństwa K4S2 – system telewizji dozorowej w budynku.

Punktacja	Funkcja lub cechy
3 pkt	Wejścia do budynku, ciągi komunikacyjne oraz wejścia do pomieszczeń objęte są telewizją dozorową.
2 pkt	Wejścia do budynku oraz ciągi komunikacyjne w budynku objęte są telewizją dozorową.
1 pkt	Wejścia do budynku objęte są telewizją dozorową.

Środek bezpieczeństwa K4S3 – kontrola gości.

Punktacja	Funkcja lub cechy
4 pkt	Nadzór nad gościem przez wyznaczonego funkcjonariusza lub pracownika przez cały czas wizyty w obiekcie (obszarze). Wydanie przepustki (identyfikatora) i zaewidencjonowanie danych gościa w dokumentacji służbowej służby ochrony obiektu.
3 pkt	Nadzór nad gościem przez wyznaczonego funkcjonariusza lub pracownika przez cały czas wizyty w obiekcie (obszarze). Wydanie przepustki (identyfikatora) i zaewidencjonowanie danych gościa w dokumentacji służbowej służby ochrony obiektu. W uzasadnionych przypadkach, goście mogą uzyskać prawo do wstępu na teren obiektu po zaewidencjonowaniu ich danych w dokumentacji służbowej służby ochrony CBA obiektu, bez konieczności realizowania wobec nich w określonej części obiektu stałej, bezpośredniej asysty ze strony funkcjonariusza lub pracownika CBA, a zasady wyrażania zgody na odstąpienie od asysty są uregulowane w przepisach obowiązujących w obiekcie .
1 pkt	Goście mogą uzyskać prawo do wstępu na teren obiektu (obszaru) po zaewidencjonowaniu, bez konieczności realizowania asysty ze strony funkcjonariusza lub pracownika.

Kategoria K5: System alarmowy i personel bezpieczeństwa

Środek bezpieczeństwa K5S1 – system sygnalizacji włamania i napadu.

Punktacja	Funkcja lub cechy
4 pkt	Posiada stopień 3 lub wyższy zgodnie z PN-EN 50131-1. Obejmuje ochroną co najmniej wszystkie pomieszczenia, w których są przechowywane materiały niejawne. Całodobowo monitorowany przez służbę ochrony CBA obiektu, której co najmniej jeden funkcjonariusz przebywa stale w granicach chronionego obiektu.
3 pkt	Posiada stopień 3 lub wyższy zgodnie z PN-EN 50131-1. Obejmuje ochroną co najmniej wszystkie pomieszczenia, w których są przechowywane materiały niejawne. Całodobowo monitorowany przez służbę ochrony CBA obiektu i pracowników specjalistycznej uzbrojonej formacji ochronnej, lub posiada stopień 2 zgodnie z PN-EN 50131-1. Obejmuje ochroną co najmniej wszystkie pomieszczenia, w których są przechowywane materiały niejawne. Całodobowo monitorowany przez służbę ochrony CBA obiektu, której co najmniej jeden funkcjonariusz przebywa stale w granicach chronionego obiektu.
2 pkt	Posiada stopień 2 lub wyższy zgodnie z PN-EN 50131-1 lub równorzędny. Obejmuje ochroną co najmniej wszystkie pomieszczenia, w których są przechowywane materiały niejawne. Całodobowo monitorowany przez służbę ochrony CBA obiektu lub pracowników specjalistycznej uzbrojonej formacji ochronnej.
1 pkt	Obejmuje ochroną pomieszczenia lub obszar w budynku wolnostojącym, samodzielnie użytkowanym. Całodobowo monitorowany przez służbę ochrony CBA lub pracowników specjalistycznej uzbrojonej formacji ochronnej.

Środek bezpieczeństwa K5S2 – personel bezpieczeństwa.

Punktacja	Funkcja lub cechy
6 pkt	Służba ochrony CBA w systemie ciągłym i całodobowo, której co najmniej jeden funkcjonariusz przebywa stale, całodobowo w granicach chronionego obiektu, realizując zadania ochronne na terenie całego obiektu.
3 pkt	Służba ochrony CBA w systemie ciągłym i całodobowo, której co najmniej jeden funkcjonariusz przebywa w granicach chronionego obiektu w godzinach urzędowania CBA we wszystkie w dni robocze, realizując zadania ochronne na terenie całego obiektu. Po godzinach urzędowania co najmniej jeden funkcjonariusz CBA pozostający w stałej gotowości do podjęcia interwencji w chronionym obiekcie, we współdziałaniu i ze wsparciem pracowników specjalistycznej uzbrojonej formacji ochronnej lub innych służb (np. Policji, Żandarmerii Wojskowej itp.)
1 pkt	Służba ochrony CBA w systemie ciągłym i całodobowo, której co najmniej jeden funkcjonariusz CBA pozostaje w stałej gotowości do podjęcia interwencji, we współdziałaniu i ze wsparciem pracowników specjalistycznej uzbrojonej formacji ochronnej lub innych jednostek organizacyjnych (np. Policji, Żandarmerii Wojskowej itp.), w chronionym obiekcie, w którym nie funkcjonują godziny urzędowania CBA, w trakcie których przyjmowani byliby goście lub przyjmowana byłaby nieuzgodniona wcześniej korespondencja.

Kategoria K6: Granice

Środek bezpieczeństwa K6S1 – ogrodzenie.

Punktacja	Funkcja lub cechy
4 pkt	Jest wykonane z trwałych materiałów (stal, cegła, itp.). Minimalna wysokość całego ogrodzenia wynosi co najmniej 2 m. Górna część na całej długości zabezpieczona jest przed przechodzeniem (np. poprzez zastosowanie ostrych elementów) lub jest wspomagane elektronicznymi urządzeniami monitorująco-sygnalizacyjnymi (np. kamerami, detektorami ruchu, itp.) Bramy, furtki i drzwi zewnętrzne posiadają zbliżoną trwałość co ogrodzenie.
3 pkt	Jest wykonane ze stałych, lżejszych metalowych materiałów (np. siatka druciana). Minimalna wysokość całego ogrodzenia wynosi co najmniej 2 m. Bramy, furtki i drzwi zewnętrzne posiadają zbliżoną trwałość co ogrodzenie.
2 pkt	Jest wykonane z trwałych materiałów, a wysokość poniżej 2 m. Bramy, furtki i drzwi zewnętrzne posiadają zbliżoną trwałość co ogrodzenie.
1 pkt	Wyznacza wyłącznie granice terenu i zapewnia minimalne zabezpieczenie przed nieuprawnionym dostępem.

Środek bezpieczeństwa K6S2 – system kontroli osób i pojazdów.

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

Środek bezpieczeństwa K6S3 – System telewizji dozorowej w terenie, na którym usytuowany jest budynek.

Punktacja	Funkcja lub cechy
4 pkt	Cały teren obiektu objęty jest systemem telewizji dozorowej.
3 pkt	Część obiektu, w tym wszystkie budynki obiektu (elewacje i każde z wejść) objęte są systemem telewizji dozorowej.
2 pkt	Część obiektu, w tym wszystkie wejścia do każdego z użytkowanych budynków, objęta jest systemem telewizji dozorowej.
1 pkt	Czynne wejścia do każdego z użytkowanych budynków obiektu objęte są systemem telewizji dozorowej.