Warszawa, dnia 19 czerwca 2012 r.

Poz. 683

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 29 maja 2012 r.

w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych

Na podstawie art. 47 ust. 1 pkt 1 i 3–6 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) zarządza się, co następuje:

§ 1. 1. Rozporządzenie określa:

1) podstawowe kryteria i sposób określania poziomu zagrożeń;

2) dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;

3) rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń;

4) podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;

5) zakres stosowania środków bezpieczeństwa fizycznego;

6) kryteria tworzenia stref ochronnych.

2. Przepisów rozporządzenia regulujących sprawy, o których mowa w ust. 1 pkt 2 i 5, nie stosuje się w jednostkach organizacyjnych organów wymienionych w art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą", oraz w stosunku do informacji niejawnych wchodzących w skład zasobu archiwalnego archiwów państwowych. W jednostkach organizacyjnych, o których mowa w art. 1 ust. 2 pkt 2 ustawy, nie stosuje się ponadto przepisów rozporządzenia regulujących sprawy, o których mowa w ust. 1 pkt 4 i 6.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) dostępności informacji niejawnej – należy przez to rozumieć właściwość określającą, że informacja niejawna jest możliwa do wykorzystania na żądanie podmiotu uprawnionego w określonym czasie;

2) integralności informacji niejawnej – należy przez to rozumieć właściwość określającą, że informacja niejawna nie została zmodyfikowana w sposób nieuprawniony;

3) poufności informacji niejawnej – należy przez to rozumieć właściwość określającą, że informacja niejawna nie jest ujawniana podmiotom do tego nieuprawnionym;

4) incydencie bezpieczeństwa – należy przez to rozumieć pojedyncze zdarzenie lub serię zdarzeń związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności.

§ 3. 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 związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zwany dalej „poziomem zagrożeń".

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

4. Poziom zagrożeń określa się jako wysoki, średni albo niski.

5. Przy określaniu poziomu zagrożeń uwzględnia się:

1) zagrożenia naturalne, wynikające z działania sił przyrody lub awarii urządzeń;

2) zagrożenia związane zarówno z umyślnym, jak i nieumyślnym zachowaniem człowieka.

6. W celu określenia poziomu zagrożeń przeprowadza się analizę, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych.

7. Poziom zagrożeń określa się przed rozpoczęciem przetwarzania informacji niejawnych, a także po każdej zmianie czynników, o których mowa w ust. 6.

8. Podstawowe kryteria i sposób określania poziomu zagrożeń zawiera załącznik nr 1 do rozporządzenia.

§ 4. 1. Cel, o którym mowa w § 3 ust. 1, osiąga się przez:

1) zapewnienie właściwego przetwarzania informacji niejawnych;

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

3) wykrywanie, udaremnianie lub powstrzymywanie działań nieuprawnionych;

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

2. Środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje niejawne, z zastrzeżeniem § 8 ust. 5.

3. 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 określonego w wyniku przeprowadzenia analizy, o której mowa w § 3 ust. 6, stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

1) personel bezpieczeństwa – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na alarmy lub sygnały awaryjne;

2) bariery fizyczne – środki chroniące granice miejsca, w którym są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;

3) szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;

4) system kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;

5) system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;

6) system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;

7) system kontroli osób i przedmiotów – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

4. W celu zapewnienia poufności, integralności i dostępności informacji niejawnych można zastosować również środki bezpieczeństwa fizycznego inne niż wymienione w ust. 3, jeżeli taka potrzeba wynika z analizy poziomu zagrożeń.

5. Jeżeli istnieje zagrożenie podglądu, także przypadkowego, informacji niejawnych, zarówno w świetle dziennym, jak i w warunkach sztucznego oświetlenia, podejmuje się działania w celu wyeliminowania takiego zagrożenia.

6. Elektroniczny system pomocniczy wspomagający ochronę informacji niejawnych powinien posiadać wydane przez dostawcę, z uwzględnieniem przepisów o systemie oceny zgodności, poświadczenie zgodności z wymogami określonymi w rozporządzeniu.

7. Metodykę doboru środków bezpieczeństwa fizycznego określa załącznik nr 2 do rozporządzenia.

§ 5. 1. Tworzy się następujące strefy ochronne:

1) strefę ochronną I – obejmującą pomieszczenie lub obszar, w których informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji; pomieszczenie lub obszar spełniają następujące wymagania:

   a) wyraźnie wskazana w planie ochrony najwyższa klauzula tajności przetwarzanych informacji niejawnych,

   b) wyraźnie określone i zabezpieczone granice,

   c) wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych,

   d) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. c, przetwarzane informacje niejawne zabezpiecza się przed możliwością dostępu do nich tych innych osób oraz zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne,

   e) wstęp możliwy jest wyłącznie ze strefy ochronnej;

2) strefę ochronną II – obejmującą pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji; pomieszczenie lub obszar spełniają następujące wymagania:

   a) wyraźnie określone i zabezpieczone granice,

   b) wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych,

   c) w przypadku konieczności wstępu osób innych niż te, o których mowa w lit. b, zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne,

   d) wstęp możliwy jest wyłącznie ze strefy ochronnej;

3) strefę ochronną III – obejmującą pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów;

4) specjalną strefę ochronną – umiejscowioną w obrębie strefy ochronnej I lub strefy ochronnej II, chronioną przed podsłuchem, spełniającą dodatkowo następujące wymagania:

   a) strefę wyposaża się w system sygnalizacji włamania i napadu,

   b) strefa pozostaje zamknięta, gdy nikogo w niej nie ma,

   c) w przypadku posiedzenia niejawnego strefa jest chroniona przed wstępem osób nieupoważnionych do udziału w tym posiedzeniu,

   d) strefa podlega regularnym inspekcjom przeprowadzanym według zaleceń Agencji Bezpieczeństwa Wewnętrznego albo Służby Kontrwywiadu Wojskowego, nie rzadziej niż raz w roku oraz po każdym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście mogło mieć miejsce,

   e) w strefie nie mogą znajdować się linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny, których umieszczenie nie zostało zaakceptowane w sposób określony w procedurach bezpieczeństwa, o których mowa w § 9 ust. 1 pkt 4.

2. Pomieszczenie lub obszar w każdej strefie ochronnej, w których praca nie odbywa się w systemie całodobowym, sprawdza się bezpośrednio po zakończeniu pracy w celu upewnienia się, że informacje niejawne zostały właściwie zabezpieczone.

3. W strefie ochronnej I lub w strefie ochronnej II można utworzyć pomieszczenie wzmocnione. Konstrukcja pomieszczenia powinna zapewniać ochronę równoważną ochronie zapewnianej przez odpowiednie szafy przeznaczone do przechowywania informacji niejawnych o tej samej klauzuli tajności. W pomieszczeniu wzmocnionym dopuszczalne jest przechowywanie informacji niejawnych poza odpowiednimi szafami.

4. Strefę ochronną I, strefę ochronną II lub specjalną strefę ochronną można utworzyć tymczasowo w strefie ochronnej III w celu odbycia posiedzenia niejawnego.

§ 6. Klucze i kody dostępu do szaf, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, mogą być udostępnione tylko tym osobom, którym posiadanie kluczy lub znajomość kodów są niezbędne do wykonywania obowiązków służbowych. Kody zmienia się co najmniej raz w roku, a także w przypadku:

1) każdej zmiany składu osób znających kod;

2) zaistnienia podejrzenia, że osoba nieuprawniona mogła poznać kod;

3) gdy zamek poddano konserwacji lub naprawie.

§ 7. 1. Informacje niejawne o klauzuli „ściśle tajne” przetwarza się w strefie ochronnej I lub w strefie ochronnej II i przechowuje się w szafie metalowej spełniającej co najmniej wymagania klasy odporności na włamanie S2, określone w Polskiej Normie PN-EN 14450 lub nowszej, lub w pomieszczeniu wzmocnionym, z zastosowaniem jednego z poniższych środków uzupełniających:

1) stała ochrona lub kontrola w nieregularnych odstępach czasu przez pracownika personelu bezpieczeństwa posiadającego odpowiednie poświadczenie bezpieczeństwa, w szczególności z wykorzystaniem systemu dozoru wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni;

2) system sygnalizacji włamania i napadu obsługiwany przez personel bezpieczeństwa z wykorzystaniem systemu dozoru wizyjnego, o którym mowa w pkt 1.

2. Informacje niejawne o klauzuli „tajne” przetwarza się w strefie ochronnej I lub w strefie ochronnej II i przechowuje się w szafie metalowej spełniającej co najmniej wymagania klasy odporności na włamanie S1, określone w Polskiej Normie PN-EN 14450 lub nowszej, lub w pomieszczeniu wzmocnionym.

3. Informacje niejawne o klauzuli „poufne”:

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

2) przechowuje się w strefie ochronnej I lub w strefie ochronnej II w szafie metalowej lub w pomieszczeniu wzmocnionym.

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

§ 8. 1. Przetwarzanie informacji niejawnych o klauzuli „poufne” lub wyższej w systemach teleinformatycznych odbywa się w strefie ochronnej I lub w strefie ochronnej II, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

2. Przekazywanie informacji, o których mowa w ust. 1, odbywa się w strefie ochronnej, na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

3. Przetwarzanie informacji niejawnych o klauzuli „zastrzeżone” w systemach teleinformatycznych odbywa się w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

4. Serwery, systemy zarządzania siecią, kontrolery sieciowe i inne newralgiczne elementy systemów teleinformatycznych umieszcza się, z uwzględnieniem wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy, w następujący sposób:

1) w strefie ochronnej w przypadku przetwarzania informacji niejawnych o klauzuli „zastrzeżone”;

2) w strefie ochronnej I lub w strefie ochronnej II, w przypadku przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej.

5. Przetwarzanie informacji niejawnych w części mobilnej zasobów systemu teleinformatycznego odbywa się na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy, w sposób określony w dokumentacji bezpieczeństwa systemu teleinformatycznego.

§ 9. 1. Kierownik jednostki organizacyjnej zatwierdza plan ochrony informacji niejawnych, który zawiera:

1) opis stref ochronnych, pomieszczeń lub obszarów, o których mowa w § 7 ust. 4, w tym określenie ich granic i wprowadzonego systemu kontroli dostępu;

2) procedury zarządzania uprawnieniami do wejścia, wyjścia i przebywania w strefach ochronnych;

3) opis zastosowanych środków bezpieczeństwa fizycznego uwzględniający certyfikaty, o których mowa w art. 46 pkt 4 ustawy, oraz poświadczenia, o których mowa w § 4 ust. 6;

4) procedury bezpieczeństwa dla strefy ochronnej I, strefy ochronnej II oraz specjalnej strefy ochronnej, określające w szczególności:

   a) klauzule tajności informacji niejawnych przetwarzanych w strefie,

   b) sposób sprawowania nadzoru przez osoby uprawnione w przypadku przebywania w strefie osób nieposiadających stałego upoważnienia do wstępu oraz sposób zabezpieczania przetwarzanych informacji niejawnych przed możliwością nieuprawnionego dostępu tych osób,

   c) w przypadku specjalnej strefy ochronnej, sposób akceptacji umieszczania linii komunikacyjnych, telefonów, innych urządzeń komunikacyjnych, sprzętu elektrycznego lub elektronicznego, znajdujących się w strefie;

5) procedury zarządzania kluczami i kodami dostępu do szaf, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne;

6) procedury reagowania osób odpowiedzialnych za ochronę informacji niejawnych oraz personelu bezpieczeństwa w przypadku zagrożenia utratą lub ujawnieniem informacji niejawnych;

7) plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych, w celu zapobieżenia utracie poufności, integralności lub dostępności informacji niejawnych.

2. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych plan, o którym mowa w ust. 1, może zawierać dodatkowe elementy.

§ 10. 1. W terminie 3 lat od dnia wejścia w życie rozporządzenia określa się poziom zagrożeń, opracowuje dokumenty, o których mowa w § 9, i dostosowuje się kombinację środków bezpieczeństwa fizycznego oraz organizację stref ochronnych do wymagań określonych w rozporządzeniu.

2. Certyfikaty i tabliczki znamionowe przyznane wyposażeniu i urządzeniom służącym ochronie informacji niejawnych, wydane przed dniem wejścia w życie rozporządzenia, zachowują ważność.

§ 11. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[1)]

Prezes Rady Ministrów: *D. Tusk*

[1)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 114, poz. 765).

Załączniki do rozporządzenia Rady Ministrów
z dnia 29 maja 2012 r. (poz. 683)

Załącznik nr 1

PODSTAWOWE KRYTERIA I SPOSÓB OKREŚLANIA POZIOMU ZAGROŻEŃ

I. Wstęp

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego, należy określić poziom zagrożeń nieuprawnionym ujawnieniem lub utratą informacji niejawnych. Określenie poziomu zagrożeń jest indywidualną oceną znaczenia czynników, o których mowa w § 3 ust. 6 rozporządzenia, mogących mieć wpływ na bezpieczeństwo informacji niejawnych w konkretnej jednostce organizacyjnej. Z uwagi na specyfikę, zakres i różnorodność zadań realizowanych przez podmioty podlegające przepisom ustawy, ocena przedstawionych czynników leży w sferze odpowiedzialności kierownika jednostki organizacyjnej, w której informacje niejawne są przetwarzane. Każdy z wymienionych czynników powinien zostać poddany wnikliwej analizie pod kątem jego znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych. Ocena poziomu zagrożeń uwzględniająca klauzule tajności przetwarzanych informacji będzie determinowała stosowanie odpowiednich środków bezpieczeństwa fizycznego, o których mowa w tabeli II „Podstawowe wymagania bezpieczeństwa fizycznego" załącznika nr 2 „Metodyka doboru środków bezpieczeństwa fizycznego".

Przy określaniu poziomu zagrożeń oceniane jest znaczenie czynnika dla bezpieczeństwa informacji niejawnych w konkretnej jednostce organizacyjnej, a nie sam czynnik jako taki.

II. Objaśnienia

1. Poziom zagrożeń ustala się na podstawie wyboru „Oceny istotności czynnika" mającego wpływ na ujawnienie lub utratę informacji niejawnych w jednostce organizacyjnej. Z uzasadnienia oceny (sporządzonej według wskazań przedstawionych w „Tabeli oceny istotności czynników zagrożeń") powinno wynikać, jakie znaczenie dla jednostki organizacyjnej ma konkretny czynnik (czy jest bardzo istotny, czy mało istotny), a nie to, w jaki sposób czy za pomocą jakich środków bezpieczeństwa fizycznego zabezpieczono informacje niejawne. Wynik analizy dokonanej w konkretnej jednostce organizacyjnej ma znaczenie dla określenia poziomu zagrożeń w zależności od tego, czy wskazane w „Tabeli

oceny istotności czynników zagrożeń" czynniki bierze się pod uwagę jako: „bardzo istotne", „istotne" albo „mało istotne" dla zagrożenia ujawnieniem lub utratą informacji niejawnych.

2. W kolumnie 2 „Tabeli oceny istotności czynników zagrożeń" wskazano czynniki mające lub mogące mieć wpływ na bezpieczeństwo informacji niejawnych.

3. Każdy z czynników podlega indywidualnej ocenie pod kątem znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych w konkretnej jednostce organizacyjnej, tj. powinien zostać oceniony jako czynnik, który ma: „bardzo istotne znaczenie", „istotne znaczenie" lub „małe znaczenie". Wybór należy uzasadnić. Wyjątek stanowi czynnik 1, „Klauzula przetwarzanych informacji", gdzie wskazano, że dla informacji o klauzuli „ściśle tajne" czynnik ten ma „bardzo istotne znaczenie" (w rubryce „Uzasadnienie" należy wpisać, że w jednostce są przetwarzane informacje o tej klauzuli tajności).

4. Wartości punktowe przypisano odpowiednio „ocenie istotności" (a nie czynnikom jako takim), tj. czynnik oceniony jako „bardzo istotny" – 8 pkt, „istotny" – 4 pkt, „mało istotny" – 1 pkt. Liczba punktów nie podlega modyfikacji.

5. W celu dokonania oceny czynnika należy kierować się „Wskazaniami", przedstawionymi w kolumnie 7. Informacje tu przedstawione wskażą mierniki ocen.

6. Liczbę punktów z kolumn 3 – 5 („Ocena istotności czynnika") należy podsumować. Uzyskany wynik wskaże poziom zagrożenia, zgodnie ze skalą określoną w „Tabeli do określania poziomu zagrożeń":

   – do 16 pkt – poziom niski,

   – od 17 do 32 pkt – poziom średni,

   – powyżej 32 pkt – poziom wysoki.

TABELA OCENY ISTOTNOŚCI CZYNNIKÓW ZAGROŻEŃ

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE	WSKAZÓWKI
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)		
1	2	3	4	5	6	7
1	Klauzula tajności przetwarzanych informacji niejawnych					Analizie podlegają wszystkie klauzule tajności wszystkich przetwarzanych informacji niejawnych. Przy ocenie istotności czynnika stosuje się zasadę: im wyższe klauzule tajności przetwarzanych informacji, tym czynnik ma istotniejsze znaczenie. Dla informacji niejawnych o klauzuli „ściśle tajne” wartość oceny jest stała i wynosi 8 pkt (czynnik ma „bardzo istotne” znaczenie). W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
2	Liczba materiałów niejawnych					Przy ocenie istotności czynnika należy brać pod uwagę wszystkie materiały niejawne zarejestrowane w urządzeniach ewidencyjnych, pozostające w faktycznej dyspozycji jednostki organizacyjnej. W uzasadnieniu należy odnieść się do przybliżonej ogólnej liczby wszystkich materiałów, stosując zasadę: im więcej informacji niejawnych o najwyższych klauzulach tajności, tym czynnik ma istotniejsze znaczenie. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

1	2	3	4	5	6	7
3	Postać informacji niejawnych					Przy ocenie należy brać pod uwagę ogólną liczbę przetwarzanych informacji niejawnych, stosując zasadę, że im więcej informacji przetwarzanych w systemach teleinformatycznych (w stosunku do ogólnej liczby materiałów) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
4	Liczba osób					Przy ocenie istotności tego czynnika należy uwzględnić pracowników jednostki organizacyjnej mających lub mogących mieć dostęp do informacji niejawnych, tj. osoby zajmujące stanowiska, wykonujące zadania lub prace zlecone związane z dostępem do takich informacji, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych. Im więcej osób (w stosunku do liczby zatrudnionych) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
5	Lokalizacja					Na wzrost oceny istotności tego czynnika ma wpływ np. to, że budynek użytkowany jest wspólnie z innymi podmiotami lub budynek jest w zabudowie zwartej (np. budynek, którego ściany przylegają do innego budynku). Na wzrost oceny istotności czynnika ma wpływ także najbliższe sąsiedztwo np.: obiekty przedstawicielstw i podmiotów zagranicznych, hotele, obiekty sportowe i hale widowiskowe, ogólnodostępne parkingi, garaże, zakłady przemysłowe i instalacje stanowiące zagrożenie dla życia lub zdrowia.

1	2	3	4	5	6	7
6	Dostęp osób do budynku					Na wzrost oceny istotności tego czynnika ma wpływ możliwość swobodnego poruszania się po budynku osób niebędących pracownikami jednostki organizacyjnej, np. gości, interesantów (w obiektach użyteczności publicznej).
7	Inne czynniki*)					Poziom zagrożeń powinien uwzględniać inne czynniki wynikające ze specyfiki jednostki organizacyjnej, niewykazane powyżej, a mogące mieć wpływ na ochronę informacji niejawnych, np.: działanie obcych służb specjalnych, sabotaż, zamach terrorystyczny, kradzież lub inna działalność przestępcza, pożar, działanie sił przyrody (np. obszar zagrożony powodzią) lub szkody górnicze.
Suma punktów						

*) Jeśli kierownik jednostki organizacyjnej uzna, że w jego jednostce występują inne niż wymienione w wierszach 1 – 6 tabeli czynniki mające wpływ na zagrożenie ujawnieniem lub utratą informacji niejawnych, powinien je określić, stanowisko uzasadnić (informacje zamieszcza się w rubryce „Uzasadnienie”), a następnie dokonać oceny istotności tych czynników. Ocenie podlegają wszystkie inne czynniki łącznie. Oznacza to, że jeśli w jednostce występuje tylko jeden z wymienionych czynników, należy go ocenić jako „bardzo istotny”, „istotny” lub „mało istotny” dla zagrożenia ujawnieniem lub utratą informacji niejawnych. Jeśli w jednostce występują dwa lub więcej czynników z tej grupy, należy oszacować je łącznie i ocenić wpływ tych czynników na ocenę zagrożenia ujawnieniem lub utratą informacji niejawnych. W sytuacji gdy np. jeden z „innych” czynników został oceniony jako „bardzo istotny”, a drugi jako „mało istotny”, należy wskazać ocenę o najwyższym znaczeniu (w tym przypadku ocena istotności „Innych czynników” zostałaby wskazana na poziomie „bardzo istotnym”). W sytuacji gdy kierownik jednostki organizacyjnej uzna, że w jego jednostce czynniki wymienione w tabeli są nieistotne lub ich występowanie jest mało realne (np. zagrożenie ze strony obcych służb specjalnych) czynnik 7. powinien zostać oceniony jako „mało istotny”.

TABELA DO OKREŚLANIA POZIOMU ZAGROŻEŃ

POZIOM ZAGROŻEŃ		
NISKI	ŚREDNI	WYSOKI
7 pkt – 16 pkt	17 pkt – 32 pkt	powyżej 32 pkt

Załącznik nr 2

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. W § 4 – 8 rozporządzenia ustalone zostały podstawowe wymagania doboru środków bezpieczeństwa fizycznego.
2. Poniżej przedstawiono metody wyboru najbardziej odpowiednich i ekonomicznych kombinacji środków bezpieczeństwa fizycznego.
3. W częściach II – IV przedstawiono opcje zapewniające wielopoziomową ochronę informacji niejawnych oraz spełniające wymagania określone w § 4 – 8 rozporządzenia.
4. 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.
5. 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 przepisem § 3 rozporządzenia.
6. Drugim etapem jest odczytanie z tej samej tabeli w części 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”).
7. 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 i wpisać ją w odpowiednie miejsce w tabeli w części IV „Punktacja zastosowanych środków bezpieczeństwa fizycznego”. Niezastosowanie danego środka jest jednoznaczne z przyznaniem za niego liczby

punktów „0”. Przy dokonywaniu wyboru konieczne jest uwzględnienie wymagań określonych w rozporządzeniu, 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.

8. Za zastosowanie produktów, które posiadają ważne certyfikaty wydane przed wejściem w życie niniejszego rozporządzenia, przyznaje się liczbę punktów odpowiednio do spełnianych przez nie wymagań określonych w tabeli z części III „Klasyfikacja środków bezpieczeństwa fizycznego”.
9. Przykładowe rozwiązanie dla średniego poziomu zagrożeń i najwyższej klauzuli informacji niejawnych „tajne” zawarte jest w części V.
10. Spis norm użytych w metodyce:

– PN-EN 1627 – Okna, drzwi, żaluzje. Odporność na włamanie. Wymagania i klasyfikacja.
– PN-EN 14450 – Pomieszczenia i urządzenia do przechowywania wartości. Wymagania, klasyfikacja i metody badań odporności na włamanie. Pojemniki bezpieczne i szafy.
– PN-EN 1300 – Pomieszczenia i urządzenia do przechowywania wartości. Klasyfikacja zamków o wysokim stopniu zabezpieczenia z punktu widzenia odporności na nieuprawnione otwarcie.
– PN-EN 50131-1 – Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Wymagania systemowe.
– PN-EN 50133-1 – Systemy alarmowe. Systemy kontroli dostępu. Część 1: Wymagania systemowe.
– PN-EN 12209 – Okucia budowlane. Zamki. Zamki mechaniczne wraz z zaczepami. Wymagania i metody badań.

– PN-EN 1143-1 – Pomieszczenia i urządzenia do przechowywania wartości. Wymagania, klasyfikacja i metody badań odporności na włamanie. Część 1: Szafy, szafy ATM, pomieszczenia i drzwi do pomieszczeń.

Część II. Podstawowe wymagania bezpieczeństwa fizycznego

Najwyższa klauzula tajności informacji przetwarzanych w jednostce organizacyjnej	**Poziom zagrożeń**		
	Niski	**Średni**	**Wysoki**
ŚCIŚLE TAJNE			
Obowiązkowo: kategorie K1+K2+K3*	10	11	13
Obowiązkowo: kategorie K4+K5**	6	7	7
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	20	23	25
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	2	2	2
Dodatkowo: kategoria K4, K5 lub K6	-	1	2
Łącznie suma punktów	2	3	4

* tylko jedna z wartości może być równa 0.
** żadna z wartości nie może być mniejsza od 2.
*** żadna z wartości nie może być równa 0.

Część III. Klasyfikacja środków bezpieczeństwa fizycznego

KATEGORIA K1: Szafy do przechowywania informacji niejawnych

Środek bezpieczeństwa K1S1 – Konstrukcja szafy

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie 0 określone w Polskiej Normie PN-EN 1143-1; 2) jest zabezpieczona dwoma zamkami typu 3 lub 4 z Kategorii K1S2.
Typ 3 **3 pkt**	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie S2 określone w Polskiej Normie PN-EN 14450; 2) jest zabezpieczona zamkiem typu 3 lub 4 z Kategorii K1S2.
Typ 2 **2 pkt**	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie S1 określone w Polskiej Normie PN-EN 14450; 2) jest zabezpieczona zamkiem typu 2 lub 3 z Kategorii K1S2.
Typ 1 **1 pkt**	Szafa charakteryzuje się następującymi cechami: 1) jest to zamykany na klucz mebel biurowy, niewyposażony w żadne szczególne funkcje zabezpieczające, ale charakteryzujący się umiarkowaną odpornością na nieuprawnione próby otwarcia; 2) jest zabezpieczona zamkiem typu 1 lub 2 z Kategorii K1S2.

Środek bezpieczeństwa K1S2 – Zamek do szafy

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, które nie są powszechnie dostępne. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy 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; 2) zamek elektroniczny szyfrowy 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**	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, dostępnymi powszechnie dla profesjonalistów. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy 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; 2) zamek elektroniczny szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.

Typ 2 **2 pkt**	Zamek charakteryzuje się odpornością na sprawne działania osoby nieuprawnionej, posługującej się zwykłymi, powszechnie dostępnymi środkami. Zamek spełnia co najmniej wymagania klasy A określone w Polskiej Normie PN-EN 1300.
Typ 1 **1 pkt**	Zamek charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia i może być wykorzystywany wyłącznie w szafach typu 1. Zamek spełnia co najmniej wymagania kategorii 4 określone w Polskiej Normie PN-EN 12209.

KATEGORIA K2: Pomieszczenia

Kategoria K2 opisuje pomieszczenia, w których informacje niejawne przechowywane są w szafach opisanych w kategorii K1, i nie dotyczy pomieszczeń wzmocnionych, o których mowa w § 5 ust. 3 rozporządzenia.

O zaklasyfikowaniu pomieszczenia do danego typu decyduje najsłabszy element (ściana, podłoga, strop, drzwi, okna).

Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na próby wymuszenia otwarcia oraz otwarcia z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało ze zbrojonego betonu o grubości 15 cm lub materiału o podobnej wytrzymałości; 4) drzwi i okna spełniają co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 4 z Kategorii K2S2.
Typ 3 **3 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą różnorodnych narzędzi ręcznych; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało z cegły lekkiej o grubości 25 cm lub materiału o podobnej wytrzymałości; 4) drzwi i okna spełniają co najmniej wymagania klasy 3 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 2 lub 3 z Kategorii K2S2.

Typ 2 **2 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia względną odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą ograniczonej liczby narzędzi ręcznych; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało z cegły lekkiej o grubości 15 cm lub materiału o podobnej wytrzymałości albo ze sklejki oraz płyty gipsowej na ramie wspierającej; 4) drzwi i okna spełniają co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 1 lub 2 z Kategorii K2S2. Okna nie muszą spełniać powyższych wymagań, jeżeli: – dolna krawędź okna znajduje się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą), – nie znajdują się na ostatnim piętrze, – w pobliżu nie znajduje się żaden element (np. rynna, drabina, drzewo) ułatwiający potencjalny dostęp i penetrację.
Typ 1 **1 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) jest to pomieszczenie lub pokój biurowy, który może zostać zamknięty (w przypadku pozostawienia bez nadzoru), zapewniający poziom bezpieczeństwa odpowiedni dla materiałów tam przechowywanych; 2) zbudowane zostało z cegły lekkiej, gipsokartonu, drewna, płyt pilśniowych lub innego materiału o podobnej wytrzymałości; 3) drzwi i okna spełniają co najmniej wymagania klasy 1 określone w Polskiej Normie PN-EN 1627. Uwaga: Jeżeli wymagane jest, by takie pomieszczenie było zabezpieczone przed długotrwałymi potajemnymi próbami uzyskania dostępu (na przykład w nocy lub podczas weekendu), standard drzwi i ich zamków oraz standard zabezpieczenia okien powinien być odpowiednio wyższy, adekwatnie do poziomu zagrożeń.

Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Zamek spełniający co najmniej wymagania klasy 7 określone w Polskiej Normie PN-EN 12209.
Typ 3 **3 pkt**	Zamek spełniający co najmniej wymagania klasy 5 określone w Polskiej Normie PN-EN 12209.
Typ 2 **2 pkt**	Zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209.
Typ 1 **1 pkt**	Zamek spełniający co najmniej wymagania klasy 3 określone w Polskiej Normie PN-EN 12209.

KATEGORIA K3: Budynki

O zaklasyfikowaniu budynku do danego typu decyduje najsłabszy jego element zewnętrzny.

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **5 pkt**	Budynek charakteryzuje się wytrzymałą konstrukcją i następującymi cechami: 1) zapewnia wysoki poziom odporności na próby włamania; 2) ściany, podłoga i strop są wykonane ze zbrojonego betonu lub podobnego materiału; 3) drzwi są wykonane ze stali wzmacnianej lub drewna pokrytego blachą stalową; 4) rama, mocowanie i szyby okien zapewniają zabezpieczenie przed fizycznym włamaniem, a ich powierzchnia jest jak najmniejsza.

Typ 3 **3 pkt**	Budynek charakteryzuje się następującymi cechami: 1) zapewnia średni poziom odporności na próby włamania; 2) stanowi wytrzymałą konstrukcję, zazwyczaj z cegły lub pustaków, opartą na ścianach szczelinowych lub podobnej budowie; 3) okna i drzwi są wykonane w standardzie odpowiadającym standardowi budynku w zakresie odporności na włamanie. Okna nie muszą być zabezpieczone w powyższy sposób, jeżeli: – dolne krawędzie okien znajdują się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą), – nie można uzyskać do nich dostępu z dachu lub z wykorzystaniem znajdującego się w pobliżu elementu (rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację. Uwaga: jako Typ 3 może również zostać sklasyfikowany budynek zbudowany z zastosowaniem nowoczesnych technologii budowlanych, z wykorzystaniem prefabrykowanych paneli lub ramy stalowej i szkła bądź podobnych materiałów.
Typ 2 **2 pkt**	Budynek charakteryzuje się następującymi cechami: 1) zapewnia średni poziom odporności na próby włamania; 2) stanowi lekką konstrukcję, zazwyczaj z pojedynczego rzędu cegieł lub lekkich bloczków, bądź jest to wytrzymałe pomieszczenie biurowe przystosowane do transportu; 3) okna i drzwi są wykonane w standardzie odpowiadającym standardowi budynku w zakresie odporności na włamanie. Okna nie muszą być zabezpieczone w powyższy sposób, jeżeli: – dolne krawędzie okien znajdują się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą), – nie można uzyskać do nich dostępu z dachu lub z wykorzystaniem znajdującego się w pobliżu elementu (np. rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację.
Typ 1 **1 pkt**	Budynek jest lekką konstrukcją przeznaczoną do ochrony zawartości i osób znajdujących się wewnątrz tylko przed działaniem czynników zewnętrznych (deszcz, wiatr itd.).

KATEGORIA K4: Kontrola dostępu

Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 3, a w klasie dostępu B – określone w normie PN-EN 50133-1; 2) jest to automatyczny system zapewniający właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa; 3) jest stosowany w połączeniu z barierą dostępu uniemożliwiającą powrót, działającą na zasadzie uniemożliwiającej otwarcie danego przejścia kontrolowanego, jeżeli wcześniej nie nastąpiło wyjście ze strefy, do której zamierza się wejść, bądź bez uprzedniego wejścia do poprzedzającej go strefy; 4) sygnały ostrzeżeń i alarmów z systemu przekazywane są do stacji monitoringu obsługiwanej przez personel bezpieczeństwa; 5) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru.
Typ 3 **3 pkt**	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 3, a w klasie dostępu B – określone w normie PN-EN 50133-1; 2) wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa; 3) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru.
Typ 2 **2 pkt**	Dopuszcza się zastosowanie jednego z poniższych rozwiązań: 1. elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 2, a w klasie dostępu B – określone w normie PN-EN 50133-1; 2) wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru strażnika; 3) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru; lub 2. system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający: 1) obecności personelu bezpieczeństwa; 2) zastosowania fotografii lub systemu wstępu na podstawie unikalnych przepustek; w zależności od ustaleń związanych z przyznawaniem wstępu akceptowane mogą być również inne dokumenty identyfikacyjne, na przykład legitymacja służbowa.

Typ 1 **1 pkt**	System tego typu może być stosowany do zabezpieczania obszarów, w których przetwarzane są informacje niejawne najwyżej o klauzuli „poufne”. System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą: 1. kodów – spełnia co najmniej wymagania systemu w klasie rozpoznania 1, a w klasie dostępu B – określone w normie PN-EN 50133-1; lub 2. kluczy wydawanych uprawnionym osobom.

Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)

Typ/ Punktacja	**Funkcje lub cechy**
Eskorta **3 pkt**	Kontrolę interesantów organizuje się w następujący sposób: 1) wprowadzani interesanci przez cały czas swojej wizyty przebywają pod nadzorem osoby uprawnionej lub pracownika, z którym związana jest ich wizyta; 2) jeżeli interesanci muszą odwiedzić kilka różnych działów lub pracowników, powinni formalnie przechodzić spod nadzoru jednej osoby pod nadzór innej, z zapewnieniem wszelkiej dokumentacji dotyczącej takiej wizyty i zmiany towarzyszących osób uprawnionych; 3) interesanci są zobligowani do noszenia odpowiedniego identyfikatora odróżniającego ich od pracowników.
Przepustka **1 pkt**	Kontrolę interesantów organizuje się w następujący sposób: 1) interesanci mogą uzyskać prawo wstępu na dany obszar bez konieczności nadzoru osoby uprawnionej; 2) interesanci są zobligowani do noszenia plakietki z przepustką, która ich identyfikuje jako osoby nieposiadające stałego upoważnienia do wejścia na obszar jednostki organizacyjnej, i tym samym odróżnia ich od pracowników. Uwaga: należy pamiętać, że system oparty na wydawaniu interesantom przepustek jest skuteczny, jeżeli wszyscy pracownicy jednostki organizacyjnej również noszą identyfikatory.

KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania

Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa

Typ/ Punktacja	Funkcje lub cechy
Typ 5 **5 pkt**	Personel bezpieczeństwa organizuje się w następujący sposób: 1) personel bezpieczeństwa składa się z osób zatrudnionych w jednostce organizacyjnej; 2) organizuje się częsty, wewnętrzny patrol kontrolujący wnętrze budynku po losowo wybranych trasach i przeprowadzany w nieregularnych odstępach czasu, jednak nie rzadziej niż co dwie godziny; 3) strażnicy mają przydzielone określone zadania do wykonania podczas patrolu.
Typ 4 **4 pkt**	Personel bezpieczeństwa organizuje się w następujący sposób: 1) personel bezpieczeństwa składa się z osób zatrudnionych w jednostce organizacyjnej; 2) organizuje się wewnętrzny patrol kontrolujący wnętrze budynku po losowo wybranych trasach i przeprowadzany w nieregularnych odstępach czasu nieprzekraczających 6 godzin, co umożliwia odbycie 2 lub 3 patroli w nocy i przeprowadzenie okresowych kontroli zabezpieczeń podczas weekendów lub dni wolnych od pracy.
Typ 3 **3 pkt**	Personel bezpieczeństwa organizuje się w następujący sposób: 1) zadania personelu bezpieczeństwa mogą wykonywać pracownicy firmy zewnętrznej; 2) patrol ograniczony jest do kontroli terenu i jego granic, podczas którego strażnicy sprawdzają zabezpieczenia budynków, ale nie mają do nich dostępu; 3) częstotliwość patroli powinna zależeć od środowiska operacyjnego i poziomu zagrożenia.
Typ 2 **2 pkt**	Personel bezpieczeństwa organizuje się w następujący sposób: 1) w jednostce organizacyjnej funkcjonują strażnicy „stacjonarni”, którzy nie są zobowiązani do przeprowadzania patroli, ale są zatrudnieni do przebywania w pomieszczeniu kontroli zdarzeń lub w stróżówce oraz do sprawdzania podejrzanych zdarzeń i wzywania pomocy, gdy jest to wymagane; 2) zadania mogą wykonywać pracownicy firmy zewnętrznej.

Typ 1 **1 pkt**	Personel bezpieczeństwa organizuje się w następujący sposób: 1) w jednostce organizacyjnej funkcjonują strażnicy „sporadyczni”, którzy są zatrudnieni do odwiedzania terenu nocą i podczas weekendów w celu przeprowadzenia podstawowej kontroli ogrodzenia; 2) strażnicy nie mają uprawnień dostępu do danego obiektu lub budynku, ale w przypadku podejrzenia włamania zareagują poprzez wezwanie osoby posiadającej klucze.

Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania

Typ/ Punktacja	**Funkcje lub cechy**
Typ 4 **4 pkt**	System charakteryzuje się następującymi cechami: 1) spełnia wymagania systemu stopnia 4 określone w normie PN-EN 50131-1; 2) obejmuje ochroną cały obszar, w tym szafy służące do przechowywania informacji niejawnych i sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, c) penetrację ścian, sufitów i podłóg, d) poruszanie się w chronionym obszarze (pułapkowo – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia), e) atak na szafy służące do przechowywania informacji niejawnych; 3) stosowany jest wraz z systemem dozoru wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni, nie obejmującym pomieszczeń służących wyłącznie jako pomieszczenia przeznaczone do spotkań; 4) stan systemu sygnalizacji napadu i włamania oraz systemu dozoru wizyjnego, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. Uwaga: 4 pkt przyznaje się również w przypadku obszarów, w których przez 24 godziny na dobę przebywają pracownicy.

Typ 3 **3 pkt**	System charakteryzuje się następującymi cechami: 1) spełnia co najmniej wymagania systemu stopnia 3 określone w normie PN-EN 50131-1; 2) obejmuje ochroną otwory wejściowe i wnętrze obszaru oraz sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, c) poruszanie się w chronionym obszarze (pułapkowo – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia), d) atak na szafy służące do przechowywania informacji niejawnych; 3) stan systemu, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. Uwaga: 3 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 4.
Typ 2 **2 pkt**	System charakteryzuje się następującymi cechami: 1) spełnia co najmniej wymagania systemu stopnia 2 określone w normie PN-EN 50131-1 i zapewnia identyfikację użytkowników włączających i wyłączających system lub jego część; 2) obejmuje ochroną miejsca, w których informacje niejawne są przechowywane oraz całą granicę obszaru (okna, drzwi i inne otwory) i sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) poruszanie się w chronionym obszarze (pułapkowo – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia); 3) stan systemu, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. Uwaga: 2 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 3.

Typ 1 **1 pkt**	System charakteryzuje się następującymi cechami: 1) spełnia co najmniej wymagania systemu stopnia 1 określone w normie PN-EN 50131-1; 2) obejmuje ochroną miejsca, w których informacje niejawne są przechowywane i sygnalizuje co najmniej: a) otwarcie drzwi do chronionego obszaru, b) poruszanie się w chronionym obszarze (pułapkowo – nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia). Uwaga: 1 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 2.

KATEGORIA K6: Granice

Środek bezpieczeństwa K6S1 – Ogrodzenie

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Ogrodzenie charakteryzuje się następującymi cechami: 1) zapewnia wysoki poziom zabezpieczenia, maksymalnie utrudnia i opóźnia działania profesjonalnego i zdeterminowanego intruza/włamywacza, który dysponuje szeroką wiedzą i zaawansowanymi narzędziami; 2) projekt i konstrukcja ogrodzenia zapewniają wysoki poziom odporności na ataki dokonywane poprzez wspinanie się na ogrodzenie lub wyłamanie ogrodzenia; 3) minimalna wysokość wynosi 250 cm; 4) górna część jest zabezpieczona z obu stron przed wspinaniem się i przechodzeniem przez ogrodzenie; 5) zapewnia łatwe monitorowanie; 6) jest przeważnie wspomagane innymi systemami zabezpieczenia ogrodzenia, takimi jak system dozoru wizyjnego, system wykrywania naruszenia ogrodzenia; 7) jeśli to możliwe, między budynkami a ogrodzeniem zachowana jest wolna przestrzeń o szerokości 25 m.
Typ 3 **3 pkt**	Ogrodzenie charakteryzuje się następującymi cechami: 1) zapewnia średni poziom zabezpieczenia, jest zaprojektowane w celu utrudnienia i opóźnienia działań dobrze przygotowanego intruza/włamywacza, który dysponuje ograniczoną liczbą narzędzi ręcznych; 2) projekt i konstrukcja ogrodzenia zapewniają odporność na próby wspinania się na ogrodzenie lub wyłamanie ogrodzenia; 3) minimalna wysokość wynosi 250 cm; 4) górna część jest zabezpieczona przed wspinaniem się i przechodzeniem przez ogrodzenie; 5) zapewnia łatwe monitorowanie; 6) jeśli to możliwe, między budynkami a ogrodzeniem zachowana jest wolna przestrzeń o szerokości 25 m.
Typ 2 **2 pkt**	Ogrodzenie charakteryzuje się następującymi cechami: 1) zabezpiecza przed włamaniem, zapewnia umiarkowany poziom odporności na próby wspinania się na ogrodzenie lub wyłamanie ogrodzenia przez nieprofesjonalnego włamywacza/intruza, niedysponującego określonymi umiejętnościami i posługującego się powszechnie dostępnymi, typowymi narzędziami; 2) minimalna wysokość wynosi 250 cm.

Typ 1 **1 pkt**	Ogrodzenie jest zaprojektowane bez uwzględnienia żadnych szczególnych wymagań w zakresie bezpieczeństwa; takie ogrodzenie służy wyłącznie do wyznaczenia granic terenu i zapewnienia minimalnego zabezpieczenia przed osobami innymi niż zdeterminowany włamywacz/intruz.

Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu

Typ/ Punktacja	**Funkcje lub cechy**
TAK=1 pkt **NIE=0 pkt**	Bramy i wejścia są zbudowane zgodnie z tym samym standardem bezpieczeństwa co ogrodzenie oraz zapewniona jest kontrola dostępu. Uwaga: skuteczność każdego ogrodzenia zależy w dużym stopniu od poziomu bezpieczeństwa zapewnionego przy punktach dostępu umieszczonych w ogrodzeniu.

Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu

Typ/ Punktacja	**Funkcje lub cechy**
TAK=1 pkt **NIE=0 pkt**	Elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	System: 1) jest stosowany przy ogrodzeniu w celu zwiększenia poziomu bezpieczeństwa zapewnionego przez ogrodzenie; 2) jest instalowany w formie zamaskowanych urządzeń bądź też widocznego sprzętu, co działa jak czynnik odstraszający. Ponieważ może wywoływać fałszywe alarmy, to należy go stosować tylko w połączeniu z systemem weryfikacji alarmu, takim jak na przykład system dozoru wizyjnego.

Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	Oświetlenie jest czynnikiem odstraszającym potencjalnych intruzów, jak również zapewniającym widoczność wymaganą, aby można było skutecznie – bezpośrednio (personel bezpieczeństwa) lub pośrednio (dozór wizyjny) – kontrolować obszar. Charakteryzuje się następującymi cechami: 1) standard oświetlenia jest zgodny z minimalnymi wymaganiami określonymi dla systemu dozoru wizyjnego (jeżeli taki system zastosowano); 2) instalacja oświetlenia uwzględnia warunki terenu.

Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt **NIE=0 pkt**	System z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni.

Część IV. Punktacja zastosowanych środków bezpieczeństwa fizycznego

ŚRODEK BEZPIECZEŃSTWA	PKT
KATEGORIA K1: Szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa (K1S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	
KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3 = 5, 3, 2 lub 1 pkt)	
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 3 lub 1 pkt)	
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	

KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie **PUNKTY=K1+K2+K3+K4+K5+K6**	

Część V. Przykład:

Minimalna liczba punktów do osiągnięcia dla średniego poziomu zagrożeń i najwyższej klauzuli informacji niejawnych „tajne”, wskazana w tabeli „Podstawowe wymagania bezpieczeństwa fizycznego”, wynosi 19.

Suma 19 punktów musi obowiązkowo składać się z dwóch elementów:

– sumy punktów za zastosowanie środków z kategorii 1, 2 oraz 3, która musi wynieść minimum 9 punktów,

– sumy punktów za zastosowanie środków z kategorii 4 oraz 5, która musi wynieść minimum 5 punktów, przy czym liczba punktów za każdy ze składników musi być większa od 0.

W przypadku nieuzyskania wymaganej liczby 19 punktów – należy zastosować środki z kategorii 6, aby uzyskać dodatkowo do 5 punktów.

Dobór środków bezpieczeństwa fizycznego:

KATEGORIA K1: Szafy do przechowywania informacji niejawnych

Środek bezpieczeństwa K1S1 – Konstrukcja szafy: typ 3

Dla informacji o klauzuli „tajne” konieczne jest zastosowanie szafy typu 2, 3 lub 4. Szafa musi być zabezpieczona zamkiem typu 2, 3 lub 4. Wybierając typ 3 uzyskuje się 3 punkty i taką liczbę wpisać należy w odpowiednie miejsce w tabeli pomocniczej.

K1S1 = 3 pkt

Środek bezpieczeństwa K1S2 – Zamek do szafy: typ 2

Do szafy typu 3 konieczne jest zastosowanie zamka typu 2, 3 lub 4.

K1S2 = 2 pkt

Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2) = 6 pkt

KATEGORIA K2: Pomieszczenia

Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia: typ 2

K2S1 = 2 pkt

Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia: typ 1

K2S2 = 1 pkt

Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2) = 2 pkt

KATEGORIA K3: Budynki: typ 2

Liczba punktów za kategorię K3 = 2 pkt

Łączna liczba punktów za kategorie K1, K2 i K3 = 10 pkt – jest większa od wymaganej do osiągnięcia (9 pkt)

KATEGORIA K4: Kontrola dostępu

Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu: typ 4

K4S1 = 4 pkt

Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów): typ Eskorta

K4S2 = 3 pkt

Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2) = 7 pkt

KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania

Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa: typ 1

K5S1 = 1 pkt

Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania: typ 2

K5S2 = 2 pkt

Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2) = 3 pkt

Łączna liczba punktów za kategorie K4 i K5 = 10 pkt – jest większa od wymaganej do osiągnięcia (5 pkt)

Łączna liczba punktów za kategorie K1, K2, K3, K4 i K5 = 20 pkt – jest większa od wymaganej do osiągnięcia (19 pkt) – w związku z tym nie jest konieczne stosowanie dodatkowych środków bezpieczeństwa z kategorii K6. Jednak w rozpatrywanym przypadku zastosowane zostało ogrodzenie Typu 1 oraz kontrola w punktach dostępu, co uwzględnia się dodając 2 punkty do ostatecznego wyniku = 22 pkt.

Poniżej – wypełniona na podstawie podanego przykładu tabela „Punktacji zastosowanych środków bezpieczeństwa fizycznego”

ŚRODEK BEZPIECZEŃSTWA	**PUNKTACJA**
KATEGORIA K1: Szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa (K1S1 = 4, 3, 2 lub 1 pkt)	3

Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	2
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	6
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	2
Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	2
KATEGORIA K3: Budynki	
Liczba punktów za kategorię K3 (K3 = 5, 3, 2 lub 1 pkt)	2
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4, 3, 2 lub 1 pkt)	4
Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 3 lub 1 pkt)	3
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	7
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	2
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	3
KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4, 3, 2 lub 1 pkt)	1

Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	1
Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	0
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	2
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie: PUNKTY=K1+K2+K3+K4+K5+K6	22