Warszawa, dnia 21 marca 2018 r.

Poz. 28

O B W I E S Z C Z E N I E

M I N I S T R A F I N A N S Ó W

z dnia 17 stycznia 2018 r.

w sprawie ogłoszenia jednolitego tekstu zarządzenia Ministra Finansów w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych

1. Na podstawie art. 16 ust. 3 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2017 r. poz. 1523) ogłasza się w załączniku do niniejszego obwieszczenia jednolity tekst zarządzenia Nr 32 Ministra Finansów z dnia 27 lipca 2012 r. w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Fin. poz. 41), z uwzględnieniem zmian wprowadzonych:

1) zarządzeniem Ministra Rozwoju i Finansów z dnia 3 stycznia 2017 r. zmieniającym zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 12);
2) zarządzeniem Ministra Rozwoju i Finansów z dnia 17 maja 2017 r. zmieniającym zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 102);
3) zarządzeniem Ministra Rozwoju i Finansów z dnia 27 grudnia 2017 r. zmieniającym zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 271).

2. Podany w załączniku do niniejszego obwieszczenia tekst jednolity zarządzenia nie obejmuje:

1) § 2 zarządzenia Ministra Rozwoju i Finansów z dnia 3 stycznia 2017 r. zmieniającego zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 12), który stanowi:

„§ 2. Zarządzenie wchodzi w życie z dniem 1 marca 2017 r., z wyjątkiem § 1 pkt 1 i 2 w zakresie § 1 pkt 2a, który wchodzi w życie z dniem podpisania z mocą od dnia 2 grudnia 2016 r.”.

2) § 2 zarządzenia Ministra Rozwoju i Finansów z dnia 17 maja 2017 r. zmieniającego zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 102), który stanowi:

„§ 2. Zarządzenie wchodzi w życie z dniem podpisania.”;

3) § 2 zarządzenia Ministra Rozwoju i Finansów z dnia 27 grudnia 2017 r. zmieniającego zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 271), który stanowi:

„§ 2. Zarządzenie wchodzi w życie z dniem podpisania.”.

Minister Finansów: T. Czerwińska

Załącznik do obwieszczenia Ministra Finansów
z dnia 17 stycznia 2018 r. (poz. 28)

ZARZĄDZENIE NR 32

MINISTRA FINANSÓW [1)]

z dnia 27 lipca 2012 r.

w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167 i 1948, z 2017 r. poz. 935 oraz z 2018 r. poz. 106) zarządzam, co następuje:

§ 1. Zarządzenie określa dobór i zakres stosowania środków bezpieczeństwa fizycznego w:

1) Ministerstwie Finansów;

2)[2)] izbach administracji skarbowej;

2a)[3)] urzędach skarbowych;

2b)[3)] urzędach celno-skarbowych wraz z podległymi oddziałami celnymi;

3) (uchylony);[4)]

3a)[5)] Krajowej Informacji Skarbowej;

4) (uchylony);[6)]

5)[7)] Krajowej Szkole Skarbowości;

6)[8)] Centrum Informatyki Resortu Finansów;

7) *Centrum Informatyki Krajowej Administracji Skarbowej.*[9)]

---

1) Minister Finansów kieruje działami administracji rządowej - budżet, finanse publiczne i instytucje finansowe, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 10 stycznia 2018 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. poz. 92).

2) W brzmieniu ustalonym przez § 1 pkt 1 zarządzenia Ministra Rozwoju i Finansów z dnia 3 stycznia 2017 r. zmieniającego zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 12), które weszło w życie z dniem 1 marca 2017 r.

3) Dodany przez § 1 pkt 2 zarządzenia, o którym mowa w odnośniku 2; wszedł w życie z dniem 3 stycznia 2017 r. z mocą od 2 grudnia 2016 r.

4) Przez § 1 pkt 3 zarządzenia, o którym mowa w odnośniku 2.

5) Dodany przez § 1 pkt 4 zarządzenia, o którym mowa w odnośniku 2;

6) Przez § 1 pkt 5 zarządzenia, o którym mowa w odnośniku 2;

7) W brzmieniu ustalonym przez § 1 pkt 6 zarządzenia, o którym mowa w odnośniku 2.

8) W brzmieniu ustalonym przez § 1 zarządzenia z dnia 27 grudnia 2017 r. zmieniającego zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 271), które weszło w życie z dniem 27 grudnia 2017 r.

9) Dodany przez § 1 pkt 7 zarządzenia, o którym mowa w odnośniku 2; przepis o utworzeniu Centrum Informatyki Krajowej Administracji Skarbowej uchylony przez art. 2 pkt 3 ustawy z dnia 24 listopada 2017 r. o zmianie ustawy o Krajowej Administracji Skarbowej oraz ustawy – Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej (Dz. U. poz. 2409), która wejdzie w życie z dniem 1 stycznia 2019 r.; wszedł wżycie z dniem 1 stycznia 2018 r.

§ 2. Ilekroć w zarządzeniu jest mowa o:

1) poziomie zagrożeń – rozumie się przez to poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą, zgodnie z § 3 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683 oraz z 2017 r. poz. 522), zwanego dalej „rozporządzeniem”;
2) strefie ochronnej – rozumie się przez to pomieszczenie lub obszar zorganizowane, według kryteriów, określonych w § 5 rozporządzenia, w celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych;
3) ustawie – rozumie się przez to ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

§ 3. 1. System bezpieczeństwa fizycznego obejmuje środki bezpieczeństwa fizycznego, których zakres stosowania uzależniony jest od poziomu zagrożeń. W skład środków bezpieczeństwa fizycznego wchodzą:

1) rozwiązania organizacyjne;
2) wyposażenie i urządzenia służące ochronie informacji niejawnych;
3) elektroniczne systemy pomocnicze wspomagające ochronę informacji niejawnych.

2. W zależności od poziomu zagrożeń 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.

2a)[10] Elektroniczne systemy pomocnicze wspomagające ochronę informacji niejawnych należy wykonywać zgodnie z zasadami sztuki inżynierskiej i aktualnym poziomem wiedzy technicznej, opisanym w szczególności w odpowiednich Polskich Normach.

3.[11] Elektroniczne systemy pomocnicze wspomagające ochronę informacji niejawnych powinny posiadać wydane przez dostawcę, z uwzględnieniem przepisów o systemie oceny zgodności, poświadczenia zgodności z wymogami określonymi w zarządzeniu.

4. 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.

5. Dopuszcza się stosowanie dodatkowo środków bezpieczeństwa fizycznego innych niż wymienione w ust. 1, jeżeli z analizy poziomu zagrożeń wynika taka potrzeba.

6. 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.

7. Szczegółową metodykę doboru środków bezpieczeństwa fizycznego określa załącznik do zarządzenia.

---

[10] Dodany przez § 1 pkt 1 lit. a zarządzenia Ministra Rozwoju i Finansów z dnia 17 maja 2017 r. zmieniającego zarządzenie w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. Urz. Min. Roz. i Fin. poz. 102), które weszło w życie z dniem 17 maja 2017 r.

[11] W brzmieniu ustalonym przez § 1 pkt 1 lit. b zarządzenia, o którym mowa w odnośniku 10.

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

2. 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[12)], 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.

3. 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.

4. Informacje niejawne o klauzuli „poufne” przetwarza się w strefie ochronnej I, II lub III i przechowuje się w strefie ochronnej I lub w strefie ochronnej II, w szafie metalowej lub w pomieszczeniu wzmocnionym.

5. 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.

§ 5. 1. W systemach teleinformatycznych przetwarza się informacje niejawne:

1) o klauzuli „poufne” lub wyższej – w strefie ochronnej I lub w strefie ochronnej II i przekazuje się w strefie ochronnej;
2) o klauzuli „zastrzeżone” – w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu.

2. Przetwarzanie informacji niejawnych w części mobilnej zasobów systemu teleinformatycznego odbywa się w sposób określony w dokumentacji bezpieczeństwa systemu teleinformatycznego.

[12)] Zgodnie z § 5 ust. 3 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683).

3. Serwery, systemy zarządzania siecią, kontrolery sieciowe i inne newralgiczne elementy systemów teleinformatycznych umieszcza się:

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.

4. W systemach teleinformatycznych, o których mowa w ust. 1–3, przetwarzanie informacji niejawnych odbywa się w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

§ 6. 1. Dobór środków bezpieczeństwa fizycznego oraz organizację stref ochronnych należy dostosować do wymagań określonych w zarządzeniu w terminie 36 miesięcy od dnia wejścia w życie zarządzenia.

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

§ 7. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do zarządzenia Nr 32 Ministra Finansów
z dnia 27 lipca 2012 r.

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. W częściach II–IV przedstawiono opcje zapewniające wielopoziomową ochronę informacji niejawnych.
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.
6. 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").
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 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.

8. Za zastosowanie produktów, które posiadają ważne certyfikaty wydane przed wejściem w życie zarządzenia, 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:

    1) PN-EN 1627 – Okna, drzwi, żaluzje. Odporność na włamanie. Wymagania i klasyfikacja.

    2) PN-EN 14450 – Pomieszczenia i urządzenia do przechowywania wartości. Wymagania, klasyfikacja i metody badań odporności na włamanie. Pojemniki bezpieczne i szafy.

    3) PN-EN 1300 – Pomieszczenia i urządzenia do przechowywania wartości. Klasyfikacja zamków o wysokim stopniu zabezpieczenia z punktu widzenia odporności na nieuprawnione otwarcie.

    4) PN-EN 50131-1 – Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Wymagania systemowe.

    5) (uchylony).[13)]

    6) PN-EN 12209 – Okucia budowlane. Zamki. Zamki mechaniczne wraz z zaczepami. Wymagania i metody badań.

    7) 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.

13) Przez § 1 pkt 2 lit. a zarządzenia, o którym mowa w odnośniku 10.

Część II. Podstawowe wymagania bezpieczeństwa fizycznego

Najwyższa klauzula tajności informacji przetwarzanych w jednostce organizacyjnej	**Poziom zagrożeń**[4)]		
	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

K1 – Szafy do przechowywania informacji niejawnych

K2 – Pomieszczenia

K3 – Budynki

K4 – Kontrola dostępu

K5 – Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania

K6 – Granice

4) Poziom zagrożeń określa się na podstawie rozporządzenia, o którym mowa w odnośniku 3.

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 narzędziamii 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 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 znajduje 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 wykorzystując znajdujący się w pobliżu element (np. rynna, drabina, drzewo) ułatwiający 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[14)]	
Typ/ Punktacja	**Funkcje lub cechy**
Typ 4 **4 pkt**	Elektroniczny automatyczny system kontroli dostępu: 1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru; 2) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku powiązania odczytu identyfikatora (karty, klucza itp.) z wprowadzeniem informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN) lub powiązania odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.) z wprowadzeniem informacji zapamiętanej, lub powiązania odczytu identyfikatora z odczytem cech biometrycznych, a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia; 3) zapewnia właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa; 4) 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, albo bez uprzedniego wejścia do poprzedzającej go strefy; 5) przekazuje sygnały ostrzeżeń i alarmów do stacji monitoringu obsługiwanej przez personel bezpieczeństwa.
Typ 3 **3 pkt**	Elektroniczny automatyczny system kontroli dostępu: 1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru; 2) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku powiązania odczytu identyfikatora (karty, klucza itp.) z wprowadzeniem informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN) lub powiązania odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.) z wprowadzeniem informacji zapamiętanej, lub powiązania odczytu identyfikatora z odczytem cech biometrycznych, a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia; 3) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa.
Typ 2 **2 pkt**	Dopuszcza się zastosowanie jednego z poniższych rozwiązań: 1) elektroniczny automatyczny system kontroli dostępu: a) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru, b) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku powiązania odczytu identyfikatora (karty, klucza itp.) lub odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.), a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia, c) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru strażnika; 2) system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający: a) obecności personelu bezpieczeństwa, b) 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 o najwyżej klauzuli „poufne”. System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą: 1) kodów – weryfikowanych przez elektroniczny automatyczny system kontroli dostępu, w którym rozpoznanie następuje w wyniku wprowadzenia informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN), a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia, lub 2) kluczy wydawanych uprawnionym osobom.

[14)] Tabela w brzmieniu ustalonym przez § 1 pkt 2 lit. b zarządzenia, o którym mowa w odnośniku 10.

Środek bezpieczeństwa K4S2 – Kontrola osób nie posiadających 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 odnośnej dokumentacji 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 nie posiadające 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 nie przekraczających 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 z rozdzielczością nie mniejszą 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 zarządzenia, 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 zarządzenia, 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 zarządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określone 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, nie dysponującego 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 z rozdzielczością nie mniejszą 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 nie posiadających 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 (K1+K2+K3),
- ✓ sumy punktów za zastosowanie środków z kategorii 4 oraz 5, która musi wynieść minimum 5 punktów (K4+K5), przy czym liczba punktów za każdy ze składników musi być większa od 0.

W przypadku nie uzyskania wymaganej liczby 19 punktów – należy zastosować środki z kategorii 6 (K6), aby uzyskać dodatkowo do 5 punktów.

Dobór środków bezpieczeństwa fizycznego:

A. KATEGORIA K1: Szafy do przechowywania informacji niejawnych
1. 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
2. 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

B. KATEGORIA K2: Pomieszczenia
1. Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia: typ 2
   K2S1 = 2 pkt
2. 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

C. 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)

D. KATEGORIA K4: Kontrola dostępu
1. Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu: typ 4
   K4S1 = 4 pkt
2. Środek bezpieczeństwa K4S2 – Kontrola osób nie posiadających 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

E. KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania
1. Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa: typ 1
   K5S1 = 1 pkt
2. 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, a zatem:

F. KATEGORIA K6: Granice

1. Środek bezpieczeństwa K6S1 – Ogrodzenie: typ 1
   K6S1 = 1 pkt
2. Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu: Tak
   K6S2 = 1 pkt

co zostało uwzględnione do ostatecznego wyniku wynoszącego 22 pkt.

Poniżej – wypełniona na podstawie podanego przykładu tabela „Punktacji 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)	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 = 5, 3, 2 lub 1 pkt)	**2**
Suma Kategorii K1+K2+K3	**10**
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 nie posiadających 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 a kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	**3**
Suma Kategorii K4+K5	**10**
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**