Warszawa, dnia 30 stycznia 2014 r.

Poz. 32

ZARZĄDZENIE MINISTRA SPRAWIEDLIWOŚCI

z dnia 23 stycznia 2014 r.

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

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

Rozdział 1
Postanowienia ogólne

§ 1.1. Zarządzenie określa:
1) dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;
2) zakres stosowania środków bezpieczeństwa fizycznego.

2. Zarządzenie stosuje się do jednostek organizacyjnych objętych zakresem działania Ministra Sprawiedliwości.

§ 2. Ilekroć w zarządzeniu jest mowa o:
1) ustawie – należy przez to rozumieć ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
2) rozporządzeniu – należy przez to rozumieć rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683).

Rozdział 2
Środki bezpieczeństwa fizycznego

§ 3.1. System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, w tym stref ochronnych, których kryteria tworzenia zostały określone w § 5 ust. 1 i 4 rozporządzenia, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych.

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

3. W zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy, o której mowa w § 3 ust. 6 rozporządzenia, 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.

4. Zarządzenie określa minimalne wymagania dotyczące zastosowania środków bezpieczeństwa fizycznego, o których mowa w ust. 3.

5. W celu zapewnienia poufności, integralności i dostępności – w rozumieniu rozporządzenia – jeżeli taka potrzeba wynika z analizy, o której mowa w § 3 ust. 6 rozporządzenia, można zastosować dodatkowo inne środki bezpieczeństwa fizycznego, niż wymienione w ust. 3.

6. Jeżeli wynika to z analizy, o której mowa w § 3 ust. 6 rozporządzenia, organizuje się dodatkowo system kontroli osób i przedmiotów. System obejmuje 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.

7. 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.

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

§ 4. Informacje niejawne przetwarza się z zastrzeżeniem § 5:
1) w przypadku klauzuli „ściśle tajne” lub „tajne” – w strefie ochronnej I lub II;
2) w przypadku klauzuli „poufne” – w strefie ochronnej I, II lub w mieszczącym się w strefie ochronnej III pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu, z zastrzeżeniem, że informacje te można przechowywać wyłącznie w strefie ochronnej I lub II;
3) w przypadku klauzuli „zastrzeżone” – w pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu.

§ 5.1. Informacje niejawne przetwarza się w systemach teleinformatycznych, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy:
1) w przypadku klauzuli „poufne” lub wyższej – w strefie ochronnej I lub II;
2) w przypadku klauzuli „zastrzeżone” – w pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu.

2. Przekazywanie informacji, o których mowa w ust. 3 pkt 1, odbywa się w strefie ochronnej, na podstawie wyników procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy.

3. 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 przypadku przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej – w strefie ochronnej I lub II;
2) w przypadku przetwarzania informacji niejawnych o klauzuli „zastrzeżone” – w strefie ochronnej I, II lub w mieszczącym się w strefie ochronnej III pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu.

4. 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.

§ 6. Pomieszczenia lub obszary, w których przetwarza się informacje niejawne, sprawdza się bezpośrednio przed rozpoczęciem i po zakończeniu w nich pracy w celu upewnienia się, czy informacje te zostały właściwie zabezpieczone, w sposób zapewniający poufność, integralność i dostępność przetwarzanych w nich informacji niejawnych.

§ 7.1. Informacje niejawne o klauzuli „poufne” lub wyższej przechowuje się w szafach przeznaczonych do przechowywania informacji niejawnych. Szafy umieszcza się w odpowiednio przystosowanych pomieszczeniach, znajdujących się w strefie ochronnej I lub II.

2. Klasyfikację i wymagania techniczne szaf stalowych służących do przechowywania informacji niejawnych określa załącznik nr 1 do zarządzenia.

3. Metodykę stosowania środków bezpieczeństwa fizycznego służących do zabezpieczenia pomieszczeń, w których są przechowywane informacje niejawne o klauzuli „poufne” lub wyższej oraz stref ochronnych I lub II, w których znajdują się te pomieszczenia, określa załącznik nr 2 do zarządzenia.

4. W zależności od klauzuli tajności przyznanej przechowywanym informacjom, stosuje się następujące szafy:
1) w przypadku klauzuli „ściśle tajne”, „tajne” lub „poufne”:
   a) szafy stalowe klasy C, o których mowa w załączniku nr 1 do zarządzenia w części III,
   lub
   b) szafy klasy S2 według Polskiej Normy PN-EN 14450 z 2 zamkami, o których mowa w załączniku nr 1 do zarządzenia w części III pkt 6;

2) w przypadku klauzuli „tajne” lub „poufne”:
   a) szafy stalowe klasy B, o których mowa w załączniku nr 1 do zarządzenia w części II,
   lub
   b) szafy klasy S1 według Polskiej Normy PN-EN 14450 z 2 zamkami, o których mowa w załączniku nr 1 do zarządzenia w części II pkt 6;
3) w przypadku klauzuli „poufne”:
   a) szafy stalowe klasy A, o których mowa w załączniku nr 1 do zarządzenia w części I,
   lub
   b) szafy klasy S1 według Polskiej Normy PN-EN 14450 z zamkiem, o którym mowa w załączniku nr 1 do zarządzenia w części I pkt 4.

5. Pomieszczenia, o których mowa w ust. 1, muszą spełniać następujące wymogi:
1) stropy i zewnętrzne ściany pomieszczenia są wykonane z materiału, którego wytrzymałość odpowiada co najmniej konstrukcji murowanej z cegły pełnej klasy 15 o grubości 250 mm;
2) ściany wewnętrzne pomieszczenia są wykonane zgodnie z metodyką podaną w załączniku nr 2 do zarządzenia w części I;
3) pomieszczenia są wyposażone w drzwi zgodnie z metodyką podaną w załączniku nr 2 do zarządzenia w części I;
4) występujące w pomieszczeniu otwory wentylacyjne, których powierzchnia przekracza 500 cm^2, zabezpiecza się siatką o grubości nie mniejszej niż 2 mm i o oczkach nie większych niż 10 x 10 mm, innym zabezpieczeniem posiadającym odporność na włamanie nie mniejszą niż siatka lub urządzeniami należącymi do systemu sygnalizacji włamania i napadu, sygnalizującymi próbę nieuprawnionego dostępu;
5) otwory okienne pomieszczenia zabezpiecza się odpowiednio środkami bezpieczeństwa fizycznego, zgodnie z metodyką podaną w załączniku nr 2 do zarządzenia w części II.

§ 8.1. Dopuszcza się w strefie ochronnej I lub II budowę pomieszczeń wzmocnionych, w których przechowuje się informacje niejawne o klauzuli „poufne” lub wyższej poza szafami, o których mowa w § 7 ust. 4.

2. Konstrukcja pomieszczenia, o którym mowa w ust. 1, musi zapewniać ochronę co najmniej taką, jaka została zapewniona w przypadku przechowywania informacji niejawnych w przeznaczonych do tego celu szafach, odpowiednio do klauzuli tajności przyznanej przechowywanym informacjom niejawnym.

§ 9. Informacje niejawne o klauzuli „zastrzeżone” przechowuje się w szafach, o których mowa w § 7 ust. 4, pomieszczeniu, o którym mowa w § 8, lub zamkniętym na klucz meblu biurowym.

§ 10.1. Granice stref ochronnych I lub II zabezpiecza się stałą barierą fizyczną, uniemożliwiającą niekontrolowany dostęp do obszaru tych stref.

2. Na wejściach do stref, o których mowa w ust. 1, organizuje się system kontroli dostępu, spełniający wymagania opisane w § 5 ust. 1 pkt 1 lit. c rozporządzenia, a w przypadku przechowywania w tych strefach informacji niejawnych o klauzuli „tajne” lub „ściśle tajne” – zapewniający dodatkowo:
   a) identyfikację i rejestrację każdej wchodzącej i wychodzącej osoby,
   b) rejestrację czasu wejścia i wyjścia każdej osoby,
   c) co najmniej 30-dniowy okres archiwizacji zarejestrowanych danych.

3. Strefę ochronną I lub II, w której znajdują się pomieszczenia, o których mowa w § 7 ust. 5 lub w § 8, organizuje się w ten sposób, że wejście do tych pomieszczeń jest możliwe wyłącznie po wejściu do tej strefy, z zastrzeżeniem ust. 4.

4. Pomieszczenia, o których mowa w § 7 ust. 5 lub § 8, mogą stanowić strefę ochronną I lub II, pod warunkiem sprawowania przez personel bezpieczeństwa, ochraniający te pomieszczenia, stałej kontroli nad strefą ochronną, z której jest możliwy wstęp do tych pomieszczeń lub w przypadku gdy w wyniku przeprowadzenia analizy, o której mowa w § 3 ust. 6 rozporządzenia, poziom zagrożenia został określony jako „niski”.

§ 11.1. Pomieszczenia, o których mowa w § 7 ust. 5 i § 8, zabezpiecza się przy pomocy systemu przeciwpożarowego.

2. Dla pomieszczeń, o których mowa w § 7 ust. 5 i § 8 oraz stref ochronnych, w których znajdują się te pomieszczenia, w zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy, o której mowa w § 3 ust. 6 rozporządzenia, stosuje się środki bezpieczeństwa fizycznego zgodnie z metodyką określoną w załączniku nr 2 do zarządzenia w części III.

§ 12. Serwery, rejestratory lub inne newralgiczne elementy należące do systemu kontroli dostępu, systemu sygnalizacji włamania i napadu, systemu dozoru wizyjnego lub systemu przeciwpożarowego, umieszcza się w pomieszczeniach lub obszarach wyposażonych w kontrolę dostępu.

§ 13. Klucze i kody dostępu do szaf, mebli biurowych, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, a także w których znajdują się urządzenia, o których mowa w § 12, 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.

Rozdział 3
Postanowienia końcowe

§ 14.1. System sygnalizacji włamania i napadu wykonany przed wejściem w życie zarządzenia, zgodny z wymaganiami co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E08390, zachowuje ważność.

2. Drzwi zamontowane przed wejściem w życie zarządzenia w pomieszczeniach, w których przechowuje się informacje niejawne o klauzuli „poufne" lub wyższej przy zastosowaniu szaf przeznaczonych do przechowywania informacji niejawnych, zachowują ważność, jeżeli co najmniej:
1) są wyposażone w zamek drzwiowy wielopunktowy oraz spełniają co najmniej wymagania, o których mowa w Polskiej Normie PN-90/B-92270;
2) w przypadku przechowywania informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" – są wyposażone w zamek drzwiowy dodatkowy, o którym mowa w Polskiej Normie PN-90/B-92270.

3. Szafy przeznaczone do przechowywania informacji niejawnych stosowane przed wejściem w życie zarządzenia zachowują ważność, jeżeli spełniają wymagania zawarte w załączniku nr 1 do zarządzenia.

4. Pomieszczenia wzmocnione służące do przechowywania informacji niejawnych, które zorganizowano przed wejściem w życie zarządzenia, zachowują ważność, jeżeli:
1) w przypadku przechowywania informacji niejawnych o klauzuli „poufne" – odpowiadają co najmniej klasie 0 odporności na włamanie według Polskiej Normy PN-EN 1143-1;
2) w przypadku przechowywania informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" – odpowiadają co najmniej klasie I odporności na włamanie według Polskiej Normy PN-EN 1143-1;
3) drzwi do pomieszczeń, o których mowa w pkt 1, są zabezpieczone dodatkowo odpowiednim zamkiem szyfrowym.

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

§ 15. W terminie określonym w § 10 rozporządzenia dostosowuje się kombinację środków bezpieczeństwa fizycznego do wymagań określonych w zarządzeniu.

§ 16. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Sprawiedliwości:
Marek Biernacki

Załącznik Nr 1 do zarządzenia
Ministra Sprawiedliwości z dnia
23 stycznia 2014 r. (poz. 32)

KLASYFIKACJA I WYMAGANIA TECHNICZNE SZAF STALOWYCH SŁUŻĄCYCH DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH

I. Szafa stalowa klasy A

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 1 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone ryglem co najmniej na trzech krawędziach.
4. Szafa musi być wyposażona w zamek mechaniczny kluczowy, co najmniej klasy A według Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem.
5. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm^2, rozstaw rygli max. 450 mm).
6. Szafy dwuskrzydłowe powinny być wyposażone w mechanizm dźwigowy, umieszczony na skrzydle aktywnym, blokujący je na

co najmniej 3 krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm^2, rozstaw rygli max. 450 mm); skrzydło aktywne musi blokować skrzydło bierne na całej ich wysokości. W przypadku niezależnego zamykania obu skrzydeł każde z nich powinno być wyposażone w oddzielny mechanizm ryglujący.
7. Podstawa szafy musi posiadać te same rozmiary co wierzch. W szafie może znajdować się zaślepiony otwór umożliwiający jej zakotwienie.
8. Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, potwierdzający zgodność wyrobu z wymaganiami klasy A.
9. Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:
   1) nazwę wyrobu;
   2) nazwę i kod identyfikacyjny producenta, typ i numer modelu;
   3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu;
   4) masę.

II. Szafa stalowa klasy B

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

III. Szafa stalowa klasy C

1. Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane ze stali konstrukcyjnej wyższej jakości, o grubości min. 5 mm, a w przypadku konstrukcji wielopłaszczowej grubość płaszcza zewnętrznego powinna wynosić min. 3 mm. Połączenia korpusu szafy powinny zapewnić dostateczną sztywność.
2. Szafa może być wyposażona w zamykane skrytki.
3. Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone ryglem na czterech krawędziach.
4. Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygle w średnicy min. 15 mm lub przekroju min. 175 mm^2, rozstaw rygli max. 450 mm); rygiel przyzawiasowy może być stały.
5. Szafy dwuskrzydłowe powinny być wyposażone w mechanizm ryglowy, umieszczony na skrzydle aktywnym, blokujący je na co najmniej trzech krawędziach systemem ruchomym (rygle w średnicy min. 15 mm lub przekroju min. 175 mm^2, rozstaw rygli max. 450 mm); skrzydło aktywne musi blokować skrzydło bierne na całej ich wysokości. W przypadku niezależnego zamykania obu skrzydeł każde z nich powinno być wyposażone w oddzielny mechanizm ryglujący; rygle przyzawiasowe mogą być stałe.
6. Mechanizm ryglowy w drzwiach musi być zabezpieczony przed uruchomieniem dwoma zamkami posiadającymi wymagane w swojej grupie certyfikaty, oddzielnie blokującymi mechanizm ryglowy, w tym:
   1) zamek mechaniczny kluczowy, co najmniej klasy B według Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem;

2) zamek mechaniczny szyfrowy, co najmniej klasy B według Polskiej Normy PN-EN 1300 co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem (atakiem) radiologicznym (promieniowanie z radioaktywnego źródła nieprzekraczającego równowartości 10 curie, co – 60 z odległości 760 mm przez 20 godzin). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy od ustawiania szyfru. Dopuszcza się również stosowanie zamka elektronicznego szyfrowego, co najmniej klasy B według Polskiej Normy PN-EN 1300, pod warunkiem że zamek spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.

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

Załącznik Nr 2 do zarządzenia
Ministra Sprawiedliwości z dnia
23 stycznia 2014 r. (poz. 32)

METODYKA STOSOWANIA ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO SŁUŻĄCYCH DO ZABEZPIECZENIA POMIESZCZEŃ, W KTÓRYCH SĄ PRZECHOWYWANE INFORMACJE NIEJAWNE O KLAUZULI „POUFNE" LUB WYŻSZEJ ORAZ STREF OCHRONNYCH I LUB II, W KTÓRYCH ZNAJDUJĄ SIĘ TE POMIESZCZENIA

I. Środki bezpieczeństwa fizycznego, obejmujące konstrukcję ścian wewnętrznych i drzwi, stosowane do zabezpieczenia pomieszczeń, w których przechowuje się informacje niejawne o klauzuli „poufne" lub wyższej przy zastosowaniu szaf przeznaczonych do przechowywania informacji niejawnych.

W zależności od sposobu sprawowania przez personel bezpieczeństwa ochrony nad strefą ochronną, w której znajduje się pomieszczenie (vide: część III pkt 2), stosuje się odpowiednią konstrukcję ścian wewnętrznych pomieszczenia oraz drzwi do pomieszczeń.

SPOSÓB SPRAWOWANIA OCHRONY	
Całodobowa ochrona strefy ochronnej	**Ochrona strefy ochronnej tylko podczas godzin pracy w tej strefie**
Wewnętrzne ściany pomieszczenia są wykonane z materiału, którego wytrzymałość odpowiada co najmniej: 1) w przypadku klauzuli „tajne" i „ściśle tajne" – konstrukcji murowanej z cegły pełnej klasy 15, o grubości 120 mm; 2) w przypadku klauzuli „poufne" – konstrukcji z profili metalowych z zamontowanymi obustronnie płytami kartonowo-gipsowymi, o grubości 120 mm.	Wewnętrzne ściany pomieszczenia są wykonane z materiału, którego wytrzymałość odpowiada co najmniej konstrukcji murowanej z cegły pełnej klasy 15, o następującej grubości: 1) w przypadku klauzuli „tajne" i „ściśle tajne" – o grubości 250 mm; 2) w przypadku klauzuli „poufne" – o grubości 120 mm.
Drzwi do pomieszczenia spełniają co najmniej wymagania klasy RC3 określone w Polskiej Normie PN-EN 1627.	Drzwi do pomieszczenia spełniają co najmniej wymagania klasy RC4 określone w Polskiej Normie PN-EN 1627.

Drzwi do pomieszczenia muszą posiadać zamek kluczowy w klasie 7 według Polskiej Normy PN-EN 12209 oraz.– w przypadku klauzuli „tajne" lub „ściśle tajne" – dodatkowy zamek kluczowy w klasie 5 lub 7 według Polskiej Normy PN-EN 12209.

II. Środki bezpieczeństwa fizycznego stosowane do zabezpieczenia otworów okiennych pomieszczeń, w których przechowuje się informacje niejawne o klauzuli „poufne" lub wyższej przy zastosowaniu szaf przeznaczonych do przechowywania informacji niejawnych.

W zależności od występujących warunków, do zabezpieczenia otworu okiennego pomieszczenia stosuje się odpowiednie środki bezpieczeństwa fizycznego.

1. W przypadku gdy są zachowane wszystkie poniższe warunki:
   1) odległość od dolnej krawędzi otworu okiennego do poziomu gruntu wynosi przynajmniej 5 m;
   2) odległość od górnej krawędzi otworu okiennego do dolnej krawędzi dachu wynosi przynajmniej 3 m;
   3) w pobliżu otworu okiennego nie znajdują się obiekty (np. drzewo, inny obiekt budowlany), wyposażenie budynku (np. drabina, rynna) lub elementy jego budowy architektonicznej (np. gzymsy, balkony, balustrady, wysunięte części budynku), ułatwiające potencjalny dostęp do otworu okiennego,

otwór okienny zabezpiecza się oknem spełniającym co najmniej wymagania klasy 1 określone w Polskiej Normie PN-EN 1627, wyposażonym w stalową siatką wykonaną z drutu stalowego lub innego materiału o podobnej wytrzymałości na włamanie, o średnicy nie mniejszej niż 2 mm i o oczkach nie większych niż 20 mm na 20 mm.

Dopuszcza się stosowanie innych środków bezpieczeństwa fizycznego niż opisane powyżej, pod warunkiem zapewnienia co najmniej takiej samej odporności na włamanie.

W przypadku zastosowania siatki rozsuwanej lub otwieranej (lub podobnego rozwiązania technicznego), siatkę (lub inny element podobnego rozwiązania technicznego) zabezpiecza się co najmniej jedną kłódką, zapewniającą odporność na włamanie nie mniejszą niż ta siatka (lub inny element podobnego rozwiązania technicznego).

2. W przypadku gdy są zachowane wszystkie poniższe warunki:
   1) odległość od dolnej krawędzi otworu okiennego do poziomu gruntu wynosi przynajmniej 5 m;
   2) w pobliżu otworu okiennego, do poziomu wyznaczonego dolną krawędzią tego otworu, nie znajdują się obiekty (np. drzewo, inny obiekt budowlany), wyposażenie budynku (np. drabina, rynna) lub elementy jego budowy architektonicznej (np. gzymsy, balkony, balustrady, wysunięte części budynku), ułatwiające potencjalny dostęp do otworu okiennego;
   3) otwór okienny pozostaje pod stałą obserwacją personelu bezpieczeństwa ochraniającego strefę ochronną, w której znajduje się pomieszczenie,

otwór okienny zabezpiecza się przy pomocy środków bezpieczeństwa fizycznego opisanych w pkt 1.

3. W przypadku gdy nie są zachowane warunki opisane w pkt 1 ppkt 1–3 i w pkt 2 ppkt 1–3, do zabezpieczenia otworu okiennego stosuje się środki bezpieczeństwa fizycznego (np. okna, kraty, rolety), które spełniają co najmniej wymagania klasy RC4 określone w Polskiej Normie PN-EN 1627.

W jednostkach organizacyjnych, w których obszar przyległy do fasady budynku z otworem okiennym jest pod stałą kontrolą personelu bezpieczeństwa ochraniającego strefę ochronną, w której znajduje się pomieszczenie, dopuszcza się także stosowanie środków bezpieczeństwa fizycznego w postaci okna spełniającego co najmniej wymagania klasy 1 określone w Polskiej Normie PN-EN 1627, zabezpieczonego kratą stalową z prętów o średnicy co najmniej 14 mm i o oczkach nie większych niż 150 mm na 150 mm.

W przypadku zastosowania krat rozsuwanych lub otwieranych, kraty zabezpiecza się co najmniej jedną kłódką klasy 5 według Polskiej Normy PN-EN 12320.

III. Środki bezpieczeństwa fizycznego, obejmujące system sygnalizacji włamania i napadu, personel bezpieczeństwa oraz system dozoru wizyjnego, stosowane dla pomieszczeń, w którym przechowuje się informacje niejawne o klauzuli „poufne" lub wyższej oraz stref ochronnych I lub II, w których znajdują się te pomieszczenia.

Uwaga:

Dotyczy pomieszczeń z szafami przeznaczonych do przechowywania informacji niejawnych i pomieszczeń wzmocnionych.

W zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy, o której mowa w § 3 ust. 6 rozporządzenia, stosuje się odpowiednio niżej wymienione środki bezpieczeństwa fizycznego.

1. System sygnalizacji włamania i napadu.

System sygnalizacji włamania i napadu musi spełniać co najmniej wymagania systemu stopnia 3 określone w Polskiej Normie PN-EN 50131-1.

Jako podstawowe urządzenia do sygnalizacji naruszenia obszaru stosuje się czujki ruchu. Jeżeli wynika to z analizy, o której mowa w § 3 ust. 6 rozporządzenia, stosuje się odpowiednio również inne, dodatkowe urządzenia należące do systemu sygnalizacji włamania i napadu, zapewniające: sygnalizację otwarcia okien, drzwi i innych zamknięć, sygnalizację penetracji okien, drzwi i innych zamknięć bez ich otwierania lub sygnalizację penetracji ścian i stropów.

POZIOM ZAGROŻEŃ		
NISKI	**ŚREDNI**	**WYSOKI**
Podczas godzin pracy w strefie ochronnej – sygnalizacja wystąpienia w tej strefie zdarzeń zagrażających bezpieczeństwu informacji niejawnych		
Po zakończeniu pracy w pomieszczeniu – sygnalizacja naruszenia obszaru tego pomieszczenia.	Po zakończeniu pracy w strefie ochronnej – sygnalizacja naruszenia obszaru tej strefy.	

2. Personel bezpieczeństwa.

Przez posterunek stały rozumie się posterunek personelu bezpieczeństwa stacjonujący w budynku lub obiekcie, w którym znajduje się pomieszczenie z przechowywanymi informacjami niejawnymi, sprawujący stałą ochronę nad strefą ochronną.

Przez grupę interwencyjną rozumie się personel bezpieczeństwa, w szczególności nie stacjonujący w ww. budynku lub obiekcie, którego zadaniem nie jest sprawowanie stałej ochrony nad pomieszczeniem lub strefą ochronną, lecz podejmowanie odpowiednich działań w przypadku wezwania.

Rozwiązania podane w poniższej tabeli określają minimalne wymagania co do sposobu organizacji ochrony sprawowanej przez personel bezpieczeństwa.

W przypadku poziomu zagrożenia „niski" lub „średni" można również przyjąć wariant całodobowej ochrony strefy bezpieczeństwa (działania grupy interwencyjnej przejmuje posterunek stały).

W przypadku poziomu zagrożenia „wysoki" stosuje się wyłącznie całodobową ochronę strefy bezpieczeństwa.

<table>
<tr><th colspan="3">POZIOM ZAGROŻEŃ</th></tr>
<tr><th>NISKI</th><th>ŚREDNI</th><th>WYSOKI</th></tr>
<tr><td colspan="2">Podczas godzin pracy w strefie ochronnej – ochrona tej strefy sprawowana przez posterunek stały.
Podejmowanie przez personel bezpieczeństwa odpowiednich działań w przypadku wystąpienia w tej strefie zdarzeń zagrażających bezpieczeństwu informacji niejawnych.</td><td rowspan="3">Całodobowa ochrona strefy ochronnej sprawowana przez posterunek stały, zorganizowany w sposób przedstawiony poniżej.
Monitorowanie przez jedną z osób z personelu bezpieczeństwa sygnałów z systemu dozoru wizyjnego.
Pozostałe osoby z personelu bezpieczeństwa:
– podejmowanie odpowiednich działań w przypadku wystąpienia w strefie ochronnej zdarzeń zagrażających bezpieczeństwu informacji niejawnych lub alarmu,
– odbywanie po godzinach pracy w strefie ochronnej okresowych patroli w obszarze przyległym do tej strefy.</td></tr>
<tr><td rowspan="2">Po godzinach pracy w strefie ochronnej – przybycie grupy interwencyjnej w przypadku wystąpienia alarmu w tym pomieszczeniu.</td><td>Podczas godzin pracy w strefie ochronnej – monitorowanie przez personel bezpieczeństwa sygnałów z systemu dozoru wizyjnego.</td></tr>
<tr><td>Po godzinach pracy w strefie ochronnej – przybycie grupy interwencyjnej w przypadku wystąpienia alarmu w tej strefie.</td></tr>
</table>

3. System dozoru wizyjnego.

W przypadku gdy obserwacja wejść do strefy ochronnej lub obszarów przyległych do tej strefy nie jest prowadzona bezpośrednio przez personel bezpieczeństwa, system dozoru wizyjnego ma zapewnić ich zdalną obserwację.

W przypadku prowadzenia bezpośredniej obserwacji, system można stosować jako środek uzupełniający.

W przypadku przechowywania informacji niejawnych o klauzuli „tajne" lub „ściśle tajne", system dozoru wizyjnego ma zapewniać całodobową rejestrację obrazu obejmującego wejście do pomieszczenia, o jakości pozwalającej na jednoznaczną identyfikację osoby oraz co najmniej 30-dniowy okres archiwizacji zarejestrowanego materiału. Dopuszcza się rejestrację poklatkową lub rejestrację w przypadku detekcji ruchu.

<table>
<tr><th colspan="3">POZIOM ZAGROŻEŃ</th></tr>
<tr><th>NISKI</th><th>ŚREDNI</th><th>WYSOKI</th></tr>
<tr><td colspan="3">W przypadku przechowywania informacji niejawnych o klauzuli „tajne" lub „ściśle tajne" – rejestracja obrazu z kamery obejmującego wejście do pomieszczenia.</td></tr>
<tr><td></td><td colspan="2">Obserwacja wejścia do strefy ochronnej.</td></tr>
<tr><td></td><td></td><td>Obserwacja obszarów przyległych do strefy ochronnej, w szczególności w bezpośrednim otoczeniu otworów okiennych tej strefy i wejść do niej.</td></tr>
</table>