Warszawa, dnia 13 marca 2017 r.

Poz. 522

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 22 lutego 2017 r.

zmieniające rozporządzenie 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. z 2016 r. poz. 1167 i 1948) zarządza się, co następuje:

§ 1. W rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683) wprowadza się następujące zmiany:

1) w § 4:

a) po ust. 5 dodaje się ust. 5a w brzmieniu:

„5a. 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.”,

b) ust. 6 otrzymuje brzmienie:

„6. 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 rozporządzeniu.”;

2) w załączniku nr 2 do rozporządzenia:

a) w części I w pkt 10 uchyla się tiret piąte,

b) w części III tabela „KATEGORIA K4: Kontrola dostępu Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu” otrzymuje brzmienie określone w załączniku do niniejszego rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów: *B. Szydło*

Załącznik do rozporządzenia Rady Ministrów
z dnia 22 lutego 2017 r. (poz. 522)

KATEGORIA K4: Kontrola dostępu

Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu

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 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 mogą być akceptowane również inne dokumenty identyfikacyjne, np. legitymacja służbowa.

Typ 1 **1 pkt**	System tego typu może być stosowany do zabezpieczania obszarów, w których są przetwarzane 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 – 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.