Warszawa, dnia 23 maja 2017 r.

Poz. 102

# Z A R Z Ą D Z E N I E

# M I N I S T R A  R O Z W O J U  I  F I N A N S Ó W [1)]

z dnia 17 maja 2017 r.

## zmieniające zarządzenia 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) zarządza się, co następuje:

**§ 1.** W zarządzeniu 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. Roz. i Fin. z 2016 r. poz. 9 oraz z 2017 r. poz. 12) wprowadza się następujące zmiany:

1) w § 3:
   a) po ust. 2 dodaje się ust. 2a w brzmieniu:

      „2a. 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. 3 otrzymuje brzmienie:

      „3. 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.”;

2) w załączniku do zarządzenia:
   a) w części I „Instrukcja” w ust. 10 uchyla się pkt 5,

---

[1)] Minister Rozwoju i Finansów kieruje działami administracji rządowej – budżet, finanse publiczne i instytucje finansowe na podstawie § 1 ust. 2 pkt 1, 2 i 4 rozporządzenia Prezesa Rady Ministrów z dnia 30 września 2016 r. w sprawie szczegółowego zakresu działania Ministra Rozwoju i Finansów (Dz. U. poz. 1595).

b) w części III „Klasyfikacja środków bezpieczeństwa fizycznego” w zakresie „KATEGORIA K4: Kontrola dostępu” tabela „Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu” otrzymuje brzmienie:

| **Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu** | |
|---|---|
| **Typ/ Punktacja** | **Funkcje lub cechy** |
| **Typ 4**<br><br>**4 pkt** | Elektroniczny automatyczny system kontroli dostępu:<br>1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru;<br>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;<br>3) zapewnia właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa;<br>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;<br>5) przekazuje sygnały ostrzeżeń i alarmów do stacji monitoringu obsługiwanej przez personel bezpieczeństwa. |
| **Typ 3**<br><br>**3 pkt** | Elektroniczny automatyczny system kontroli dostępu:<br>1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru;<br>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**<br>**2 pkt** | Dopuszcza się zastosowanie jednego z poniższych rozwiązań:<br>1) elektroniczny automatyczny system kontroli dostępu:<br>a) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru,<br>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,<br>c) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru strażnika;<br>2) system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający:<br>a) obecności personelu bezpieczeństwa,<br>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**<br>**1 pkt** | System tego typu może być stosowany do zabezpieczania obszarów, w których przetwarzane są informacje niejawne o najwyżej klauzuli „poufne”.<br>System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą:<br>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<br>2) kluczy wydawanych uprawnionym osobom. |

**§ 2.** Zarządzenie wchodzi w życie z dniem podpisania.

Minister Rozwoju i Finansów: wz. W. Janczyk