Biuro Pełnomocnika
ds. Ochrony Informacji Niejawnych

Warszawa, 22 grudnia 2010 r.

BPOIN 0150/201/no/148072

Według rozdzielnika

Szanowni Państwo Dyrektorzy,

Uprzejmie informuję, że ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., Nr 182, poz. 1228) wprowadza w zakresie bezpieczeństwa teleinformatycznego następujące nowe dyspozycje:

1. Systemy teleinformatyczne przeznaczone do przetwarzania informacji niejawnych podlegają akredytacji. Udziela jej kierownik jednostki organizacyjnej w przypadku systemów przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" lub właściwa służba ochrony państwa w przypadku pozostałych klauzul. Akredytacji udziela się na czas określony, nie dłuższy niż 5 lat.

2. Urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez ABW albo SKW (bez względu na klauzulę). Dotychczas obowiązujące przepisy ograniczały ten wymóg do klauzuli „poufne" i wyższych.

3. Do zadań pełnomocnika ochrony, należy zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka. Proces szacowania ryzyka, zgodnie z zapisami ustawy, stanowi nieodłączny element projektu systemu teleinformatycznego oraz podstawę dokonania wszelkich zmian w systemie.

4. Ustawa sankcjonuje obowiązującą dotychczas praktykę niełączenia funkcji administratora systemu i inspektora bezpieczeństwa teleinformatycznego.

5. Kontrola stanu zabezpieczenia informacji niejawnych może, w uzasadnionych przypadkach, obejmować kontrolę systemów nieprzeznaczonych do przetwarzania informacji niejawnych (potocznie – „systemy jawne"). Wystarczającą podstawą jest uprawdopodobnienie w znacznym stopniu podejrzenia możliwości przetwarzania informacji niejawnych w tych systemach.

Z wyrazami szacunku,

Monika Sudar
Dyrektor