

Wykaz skrótów

ROZDZIAŁ 1. WPROWADZENIE DO OCHRONY INFORMACJI NIEJAWNYCH

- 1.1. Geneza ochrony informacji niejawnych
- 1.2. Polskie prawo normujące ochronę informacji niejawnych
- 1.3. Podstawowe pojęcia i ustawowe definicje
- 1.4. Podmioty zobowiązane do ochrony informacji niejawnych

ROZDZIAŁ 2. MIEJSCE I ROLA PIONU OCHRONY W JEDNOSTCE ORGANIZACYJNEJ

- 2.1. Miejsce kierownika jednostki organizacyjnej w systemie ochrony informacji niejawnych
- 2.2. Rola pełnomocnika ochrony
- 2.3. Obowiązki kierownika kancelarii tajnej i jej personelu
- 2.4. Zadania inspektora bezpieczeństwa teleinformatycznego

ROZDZIAŁ 3. BEZPIECZEŃSTWO OSOBOWE

- 3.1. Upoważnienie do dostępu do informacji niejawnych o klauzuli "zastrzeżone"
- 3.2. Postępowania sprawdzające
 - 3.2.1. Zwykłe postępowanie sprawdzające
 - 3.2.2. Poszerzone postępowanie sprawdzające
- 3.3. Przebieg postępowania sprawdzającego
- 3.4. Kolejne postępowanie sprawdzające
- 3.5. Kontrolne postępowanie sprawdzające
- 3.6. Postępowanie odwoławcze
- 3.7. Postępowanie skargowe
- 3.8. Przechowywanie i archiwizowanie akt postępowań sprawdzających
- 3.9. Szkolenia z zakresu ochrony informacji niejawnych

ROZDZIAŁ 4. ANALIZA RYZYKA W OCHRONIE INFORMACJI NIEJAWNYCH

- 4.1. Podstawowe pojęcia, metody, czynności w analizie ryzyka
- 4.2. Identyfikacja i wycena zasobów
- 4.3. Identyfikacja zagrożeń dla ochrony informacji niejawnych
- 4.4. Określenie poziomu podatności zasobu na wystąpienie zagrożenia
- 4.5. Szacowanie i ocena ryzyka
- 4.6. Ryzyko szczątkowe. Akceptacja ryzyka
- 4.7. Postępowanie z ryzykiem
- 4.8. Przykładowa metodologia analizy ryzyka

ROZDZIAŁ 5. ZABEZPIECZENIA FIZYCZNE INFORMACJI NIEJAWNYCH

- 5.1. Poziom zagrożenia
- 5.2. Środki bezpieczeństwa fizycznego
- 5.3. Strefy ochronne
- 5.4. Plan ochrony informacji niejawnych

ROZDZIAŁ 6. ORGANIZACJA OBIEGU INFORMACJI NIEJAWNYCH

- 6.1. Obieg dokumentów niejawnych w kancelarii tajnej
- 6.2. Organizacja obiegu informacji niejawnych poza kancelarią tajną
- 6.3. Oznaczanie dokumentów niejawnych

- 6.4. Przesyłanie dokumentów niejawnych
- 6.5. Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli "zastrzeżone" oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony
- 6.6. Instrukcja określająca sposób i tryb przetwarzania informacji niejawnych o klauzuli "poufne"

ROZDZIAŁ 7. BEZPIECZEŃSTWO TELEINFORMATYCZNE

- 7.1. Podstawowe zadania w bezpieczeństwie teleinformatycznym
- 7.2. Etapy funkcjonowania systemu teleinformatycznego
- 7.3. Analiza ryzyka w bezpieczeństwie teleinformatycznym!
- 7.4. Dokumentacja bezpieczeństwa teleinformatycznego
 - 7.4.1. Szczegółne wymagania bezpieczeństwa (SWB)
 - 7.4.2. Procedury bezpiecznej eksploatacji (PBE)
- 7.5. Akredytacja bezpieczeństwa teleinformatycznego
- 7.6. Konsekwencje modernizacji systemów teleinformatycznych

ROZDZIAŁ 8. BEZPIECZEŃSTWO PRZEMYSŁOWE

- 8.1. Świadectwa bezpieczeństwa przemysłowego - stopnie i terminy ważności
- 8.2. Postępowanie bezpieczeństwa przemysłowego
- 8.3. Opłaty w postępowaniu bezpieczeństwa przemysłowego
- 8.4. Obowiązki przedsiębiorcy posiadającego świadectwo bezpieczeństwa przemysłowego
- 8.5. Kontrola ochrony informacji niejawnych u przedsiębiorcy podstawą decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego
- 8.6. Postępowanie odwoławcze i skargowe
- 8.7. Instrukcja bezpieczeństwa przemysłowego - obowiązek zamawiającego

ROZDZIAŁ 9. KONTROLA OCHRONY INFORMACJI NIEJAWNYCH

- 9.1. Kontrola wewnętrzna ochrony informacji niejawnych
- 9.2. Kontrola ochrony informacji niejawnych prowadzona przez ABW i SKW
 - 9.2.1. Zakres kontroli
 - 9.2.2. Program kontroli
 - 9.2.3. Uprawnienia kontrolerów
- 9.3. Obowiązki i prawa instytucji i osób kontrolowanych
- 9.4. Dobra praktyka kontrolna
- 9.5. Zakończenie kontroli

ROZDZIAŁ 10. OCHRONA INFORMACJI NIEJAWNYCH W STOSUNKACH MIĘDZYNARODOWYCH

- 10.1. Zadania i rola krajowej władzy bezpieczeństwa
- 10.2. Organizacja ochrony informacji niejawnych międzynarodowych w jednostce organizacyjnej
 - 10.2.1. Dostęp do informacji niejawnych międzynarodowych - poświadczenia bezpieczeństwa organizacji międzynarodowych
 - 10.2.2. Utworzenie kancelarii tajnej międzynarodowej
 - 10.2.3. Przetwarzanie informacji niejawnych międzynarodowych w systemach teleinformatycznych
 - 10.2.4. Świadectwo bezpieczeństwa przemysłowego w obrocie międzynarodowym

ROZDZIAŁ 11. ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

- 11.1. Naruszenie przepisów o ochronie informacji niejawnych
- 11.2. Odpowiedzialność wynikająca z ustawy o ochronie informacji niejawnych
- 11.3. Odpowiedzialność służbowa
- 11.4. Odpowiedzialność dyscyplinarna
- 11.5. Odpowiedzialność karna

Słownik pojęć

Bibliografia

Akty prawne

Zalecenia ABW i SKW

Inne źródła

Spis rysunków

Spis tabel

WZORY DOKUMENTÓW

Spis wzorów