

Spis treści

Wykaz skrótów	9
ROZDZIAŁ 1. WPROWADZENIE DO OCHRONY INFORMACJI NIEJAWNYCH	11
1.1. Geneza ochrony informacji niejawnych	13
1.2. Polskie prawo normujące ochronę informacji niejawnych	16
1.3. Podstawowe pojęcia i ustawowe definicje	22
1.4. Podmioty zobowiązane do ochrony informacji niejawnych	31
ROZDZIAŁ 2. MIEJSCE I ROLA PIONU OCHRONY W JEDNOSTCE ORGANIZACYJNEJ	33
2.1. Miejsce kierownika jednostki organizacyjnej w systemie ochrony informacji niejawnych	35
2.2. Rola pełnomocnika ochrony	41
2.3. Obowiązki kierownika kancelarii tajnej i jej personelu	45
2.4. Zadania inspektora bezpieczeństwa teleinformatycznego	48
ROZDZIAŁ 3. BEZPIECZEŃSTWO OSOBOWE	53
3.1. Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone”	55
3.2. Postępowania sprawdzające	58
3.2.1. Zwyczajne postępowanie sprawdzające	62
3.2.2. Poszerzone postępowanie sprawdzające	65
3.3. Przebieg postępowania sprawdzającego	68
3.4. Kolejne postępowanie sprawdzające	71
3.5. Kontrolne postępowanie sprawdzające	72
3.6. Postępowanie odwoławcze	74
3.7. Postępowanie skargowe	76
3.8. Przechowywanie i archiwizowanie akt postępowań sprawdzających	78
3.9. Szkolenia z zakresu ochrony informacji niejawnych	79
ROZDZIAŁ 4. ANALIZA RYZYKA W OCHRONIE INFORMACJI NIEJAWNYCH	83
4.1. Podstawowe pojęcia, metody, czynności w analizie ryzyka	86
4.2. Identyfikacja i wycena zasobów	88
4.3. Identyfikacja zagrożeń dla ochrony informacji niejawnych	90
4.4. Określenie poziomu podatności zasobu na wystąpienie zagrożenia	92
4.5. Szacowanie i ocena ryzyka	94
4.6. Ryzyko szczątkowe. Akceptacja ryzyka	95
4.7. Postępowanie z ryzykiem	95
4.8. Przykładowa metodologia analizy ryzyka	97

ROZDZIAŁ 5. ZABEZPIECZENIA FIZYCZNE INFORMACJI NIEJAWNYCH	105
5.1. Poziom zagrożenia.....	107
5.2. Środki bezpieczeństwa fizycznego.....	109
5.3. Strefy ochronne	112
5.4. Plan ochrony informacji niejawnych.....	114
ROZDZIAŁ 6. ORGANIZACJA OBIEGU INFORMACJI NIEJAWNYCH	117
6.1. Obieg dokumentów niejawnych w kancelarii tajnej	119
6.2. Organizacja obiegu informacji niejawnych poza kancelarią tajną	122
6.3. Oznaczanie dokumentów niejawnych	124
6.4. Przesyłanie dokumentów niejawnych	127
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	129
6.6. Instrukcja określająca sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne”	132
ROZDZIAŁ 7. BEZPIECZEŃSTWO TELEINFORMATYCZNE.....	135
7.1. Podstawowe zadania w bezpieczeństwie teleinformatycznym.....	137
7.2. Etapy funkcjonowania systemu teleinformatycznego.....	140
7.3. Analiza ryzyka w bezpieczeństwie teleinformatycznym	143
7.4. Dokumentacja bezpieczeństwa teleinformatycznego.....	144
7.4.1. Szczególne wymagania bezpieczeństwa (SWB)	145
7.4.2. Procedury bezpiecznej eksploatacji (PBE).....	147
7.5. Akredytacja bezpieczeństwa teleinformatycznego.....	148
7.6. Konsekwencje modernizacji systemów teleinformatycznych.....	151
ROZDZIAŁ 8. BEZPIECZEŃSTWO PRZEMYSŁOWE.....	153
8.1. Świadectwa bezpieczeństwa przemysłowego – stopnie i terminy ważności	155
8.2. Postępowanie bezpieczeństwa przemysłowego	159
8.3. Opłaty w postępowaniu bezpieczeństwa przemysłowego	164
8.4. Obowiązki przedsiębiorcy posiadającego świadectwo bezpieczeństwa przemysłowego	165
8.5. Kontrola ochrony informacji niejawnych u przedsiębiorcy podstawą decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego	166
8.6. Postępowanie odwoławcze i skargowe.....	168
8.7. Instrukcja bezpieczeństwa przemysłowego – obowiązek zamawiającego	168
ROZDZIAŁ 9. KONTROLA OCHRONY INFORMACJI NIEJAWNYCH.....	173
9.1. Kontrola wewnętrzna ochrony informacji niejawnych.....	175
9.2. Kontrola ochrony informacji niejawnych prowadzona przez ABW i SKW.....	179
9.2.1. Zakres kontroli	180
9.2.2. Program kontroli	181
9.2.3. Uprawnienia kontrolerów	182

9.3. Obowiązki i prawa instytucji i osób kontrolowanych.....	184
9.4. Dobra praktyka kontrolna.....	187
9.5. Zakończenie kontroli.....	188

ROZDZIAŁ 10. OCHRONA INFORMACJI NIEJAWNYCH W STOSUNKACH MIĘDZYNARODOWYCH 191

10.1. Zadania i rola krajowej władzy bezpieczeństwa	194
10.2. Organizacja ochrony informacji niejawnych międzynarodowych w jednostce organizacyjnej	195
10.2.1. Dostęp do informacji niejawnych międzynarodowych – poświadczenia bezpieczeństwa organizacji międzynarodowych	195
10.2.2. Utworzenie kancelarii tajnej międzynarodowej.....	197
10.2.3. Przetwarzanie informacji niejawnych międzynarodowych w systemach teleinformatycznych.....	199
10.2.4. Świadectwo bezpieczeństwa przemysłowego w obrocie międzynarodowym	200

ROZDZIAŁ 11. ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH 203

11.1. Naruszenie przepisów o ochronie informacji niejawnych.....	205
11.2. Odpowiedzialność wynikająca z ustawy o ochronie informacji niejawnych.....	207
11.3. Odpowiedzialność służbowa	207
11.4. Odpowiedzialność dyscyplinarna	208
11.5. Odpowiedzialność karna	208

Słownik pojęć.....	213
Bibliografia	221
Akty prawne.....	225
Zalecenia ABW i SKW	228
Inne źródła	228
Spis rysunków	229
Spis tabel	229

WZORY DOKUMENTÓW 231

Spis wzorów	233
-------------------	-----