Spis treści

Wykaz skrótów 8
Wstęp 11

ROZDZIAŁ 1. OCHRONA INFORMACJI I JEJ CHARAKTER 13
1. Przesłanki uchwalenia nowej ustawy o ochronie informacji niejawnych 15
2. Zasady i wartości uzasadniające ograniczenie konstytucyjnych wolności i praw przysługujących jednostce 17
2.1. Konstytucyjne gwarancje wolności informacyjnej 17
2.2. Granice wolności informacyjnej 19
2.2.1. Zasada wyłączności ustawy 20
2.2.2. Proporcjonalność ograniczeń 21
2.2.3. Obowiązek zachowania istoty praw i wolności 22
2.2.4. Wartości (przesłanki) będące podstawą ograniczenia wolności i praw jednostki 24
3. Ustawowe zdefiniowanie ochrony informacji niejawnych 27
3.1. Ochrona informacji i jej źródeł 27
3.1.1. Informacja jawna 28
3.1.2. Informacja niejawna 29
3.1.2.1. Klauzula „ściśle tajne" 30
3.1.2.2. Klauzula „tajne" 37
3.1.2.3. Klauzula „poufne" 40
3.1.2.4. Klauzula „zastrzeżone" 41
3.2. Autonomiczny charakter pojęcia „szkoda dla Rzeczypospolitej Polskiej" na gruncie uoin 42

ROZDZIAŁ 2. INFORMACJE NIEJAWNE A PRAWO DOSTĘPU DO INFORMACJI PUBLICZNEJ 47
1. Przesłanki sądowej oceny zasadności objęcia konkretnych informacji klauzulą tajności 49
2. Prawo dostępu do informacji publicznej 51
3. Specyfika sposobu identyfikacji źródeł informacji publicznej 55
4. Sądowa weryfikacja zasadności nadania informacji klauzuli tajności w świetle udostępnienia informacji publicznej 57

ROZDZIAŁ 3. KOMPLETNOŚĆ SYSTEMU OCHRONY INFORMACJI 69
1. Założenia modelowe systemu ochrony informacji niejawnych 71
2. Ukształtowanie prawnych podstaw systemu 71
3. Rozporządzenie jako akt wykonawczy 80
4. Konstrukcja upoważnienia zawarta w art. 47 ust. 1 uoin 83

ROZDZIAŁ 4. ZARZĄDZANIE RYZYKIEM I CIĄGŁOŚCIĄ DZIAŁANIA W PROCESACH TELEINFORMATYCZNEGO PRZETWARZANIA INFORMACJI NIEJAWNYCH 87

1. Optymalizacja jako czynnik skutecznej ochrony informacji niejawnych 89

2. Zarządzanie ryzykiem związanym z przetwarzaniem informacji niejawnych 93

2.1. Specyfika procesu szacowania ryzyka związanego z przetwarzaniem informacji niejawnych w systemach teleinformatycznych 96

2.1.1. Procedura szacowania ryzyka 98

2.1.1.1. Szacowanie wstępne (etap projektowania systemu teleinformatycznego) 98

2.1.1.2. Kolejne etapy szacowania ryzyka, postępowanie z ryzykiem, ocena ryzyka – wdrażanie i eksploatacja systemu 107

2.1.2. Przegląd i monitorowanie ryzyk i czynników ryzyka – etap eksploatacji i wycofywania systemu 109

3. Zarządzanie ciągłością działania jako element skutecznego i racjonalnego systemu bezpieczeństwa danych niejawnych 109

3.1. Podstawowe założenia dotyczące zarządzania ciągłością działania 110

3.2. Zastosowanie standardów zarządzania ciągłością działania (BCM) w procesie zabezpieczania informacji niejawnych 112

3.2.1. Identyfikacja kluczowych i krytycznych procesów i zasobów 116

3.2.2. Struktura organizacyjna odpowiedzialna za BCM 118

3.2.3. Dokumentowanie BCM 120

3.2.4. Testowanie strategii przetrwania i planów ciągłości działania 123

ROZDZIAŁ 5. DOBÓR ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO W PROCESACH PRZETWARZANIA INFORMACJI NIEJAWNYCH 127

1. Tryb i zasady stosowania elementów bezpieczeństwa fizycznego informacji niejawnych 129

1.1. Ustawowe przesłanki ochrony fizycznej informacji niejawnych 129

1.2. Zasady organizacji i funkcjonowania kancelarii tajnych 129

1.2.1. Zadania kancelarii tajnej 131

1.2.2. Funkcjonowanie kancelarii w strukturze pionu ochrony 132

2. Tryb i zasady obiegu informacji niejawnych 133

2.1. Czynności kancelaryjne związane z przetwarzaniem informacji niejawnych 133

2.1.1. Oznaczanie materiałów, umieszczanie, zmiana i znoszenie klauzul tajności 136

2.1.2. Nadawanie, przyjmowanie, przewożenie, wydawanie i ochrona materiałów 146

2.1.3. Niszczenie dokumentacji niejawnej 156

3. Wdrażanie i stosowanie środków bezpieczeństwa fizycznego 157

3.1. Analiza poziomu zagrożeń 157

3.2. Identyfikacja stref ochronnych 164

3.3. Identyfikacja i zakres stosowania zabezpieczeń fizycznych 165

3.3.1. Metodyka doboru środków bezpieczeństwa fizycznego 166

3.4. Bezpieczeństwo fizyczne infrastruktury teleinformatycznej 171

3.5. Wymagania dotyczące prowadzenia dokumentacji związanej z bezpieczeństwem fizycznym..... 172
3.6. Kierunek zmian dotyczących techniczno-organizacyjnych środków stosowanych w obszarze bezpieczeństwa fizycznego..... 174

ROZDZIAŁ 6. WARUNKI NADZOROWANIA IMPLEMENTACJI ŚRODKÓW BEZPIECZEŃSTWA PRZEZ ABW I SKW 181

1. Warunki procedury akredytacyjnej systemu teleinformatycznego, akceptacji środków bezpieczeństwa fizycznego oraz uzyskania świadectwa bezpieczeństwa przemysłowego 183
1.1. Akredytacja systemu teleinformatycznego 183
1.1.1. Akredytacja w ramach postępowania bezpieczeństwa przemysłowego..... 185
1.2. Akceptacja środków bezpieczeństwa fizycznego..... 187
1.2.1. Akceptacja środków bezpieczeństwa fizycznego w ramach postępowania bezpieczeństwa przemysłowego..... 187

2. Postępowanie odwoławcze i skargowe związane z wdrożeniem zabezpieczeń w systemach teleinformatycznych i środków bezpieczeństwa fizycznego 188

Podsumowanie 191
Bibliografia..... 193
Wykaz aktów prawnych i dokumentów urzędowych..... 198

ZAŁĄCZNIKI..... 201

Skorowidz..... 241