

SPIS TREŚCI

Wstęp	5
1. INFORMACJA, JEJ BEZPIECZEŃSTWO I ZARZĄDZANIE	8
1.1. Interpretacja pojęcia „informacja”	9
1.2. Bezpieczeństwo informacyjne	21
1.3. Zarządzanie bezpieczeństwem informacyjnym	26
2. WYBRANE ASPEKTY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACYJNYM	35
2.1. Polityka bezpieczeństwa	37
2.1.1. Polityka bezpieczeństwa informacji	40
2.1.2. Koncepcja bezpieczeństwa informacyjnego	43
2.2. Ochrona danych	45
2.2.1. Dostęp do informacji – sterowanie dostępem	47
2.2.2. Transmisja informacji	52
2.2.2.1. Kryptografia	53
2.2.2.2. Podpis cyfrowy	56
2.2.3. Przechowywanie informacji	59
2.3. Ochrona techniczna	61
2.3.1. Ochrona fizyczna	63
2.3.2. Zabezpieczenie przed promieniowaniem	67
2.4. Współdziałanie menadżera ds. bezpieczeństwa z pozostałymi menadżerami	69
3. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	77
3.1. Terminologia systemu bezpieczeństwa informacji i systemu bezpieczeństwa informatycznego	78
3.2. Model PDCA stosowany w systemie zarządzania bezpieczeństwem informacji	84
3.3. Ogólne podstawy zarządzania systemem bezpieczeństwa informacji	86
3.3.1. Ustanowienie i zarządzania SZBI.....	87
3.3.2. Wdrożenie i eksploatacja SZBI	89
3.3.3. Monitorowanie i przegląd SZBI	91
3.3.4. Utrzymanie i doskonalenie SZBI.....	92
3.4. Ogólny model zarządzania systemem bezpieczeństwa informatycznego	92
4. WYBRANE ASPEKTY AUDYTU	100
4.1. Audyt – cele, definicje i terminy	101
4.2. Rodzaje audytów	105

4.3. Zasady audytowania	107
4.4. Zarządzanie programem audytu	109
4.5. Działania audytowe	113
4.5.1. Algorytm przeprowadzania audytu	113
4.5.2. Inicjowanie audytu	115
4.5.3. Przeprowadzenie przeglądu dokumentów	118
4.5.4. Przygotowanie działań audytowanych na miejscu	121
4.5.5. Przeprowadzenie działań audytowanych	123
4.5.6. Zakończenie audytu	127
4.5.7. Przeprowadzenie działań poaudytowych	131
4.6. Audyt wewnętrzny	132
4.7. Audyt zewnętrzny	135
4.8. Audyt bezpieczeństwa informacji	137
4.9. Słownik podstawowych pojęć z zakresu audytu	143
Zakończenie	145
Bibliografia	147