

Spis treści

Podziękowania	6
Wstęp	7
Rozdział 1. O informacji, bezpieczeństwie i systemie ochrony	9
1.1. O informacji.....	10
1.2. O bezpieczeństwie	11
1.3. O systemie ochrony informacji*	14
Rozdział 2. O procesach	25
2.1. Procesy biznesowe w analizie ryzyka.....	26
Rozdział 3. O zasobach, ich inwentaryzacji i klasyfikacji	31
3.1. Inwentaryzacja zasobów teleinformatycznych.....	31
3.2. Klasyfikacja zasobów teleinformatycznych	32
3.3. Ocena wartości zasobów informacyjnych	35
Rozdział 4. O zagrożeniach i podatnościach	39
4.1. Rozważania o zagrożeniach.....	40
4.2. Jak szukać zagrożeń – pytania i podpowiedzi	49
4.3. Burza mózgów – przykład techniki identyfikacji zagrożeń	53
4.3.1. Generowanie zagrożeń/scenariuszy	56
4.3.2. Redukcja zbioru zagrożeń	56
4.3.3. Nadawanie priorytetów scenariuszom.....	56
4.4. Podatności.....	57
Rozdział 5. O pomiarach bezpieczeństwa teleinformatycznego	59
5.1. Pomiar.....	61
5.2. Elementy formalnej teorii pomiaru*.....	62
5.3. Omówienie wymagań definicji pomiaru	64
5.3.1. Określenie przedmiotu pomiaru	64
5.3.2. Przyporządkowanie liczb (miar)	64
5.3.3. Obiektywność.....	65
5.3.4. Empiryczność	66
5.4. Uwagi końcowe o „mierzeniu” bezpieczeństwa.....	66

Rozdział 6. O ryzyku i zarządzaniu ryzykiem	69
6.1. Ryzyko a problemy decyzyjne*	71
6.2. Charakterystyka procesu zarządzania ryzykiem.....	76
6.3. Analiza ryzyka – identyfikacja zagrożeń, podatności i środowiska	78
6.4. Identyfikacja wymagań dotyczących poziomu ochrony.....	81
6.5. Analiza ryzyka – szacowanie ryzyka.....	83
6.5.1. Oszacowanie ryzyka – metoda ilościowa (studium przypadku)	86
6.5.2. Oszacowanie ryzyka – metoda jakościowa (wytyczne raportu technicznego ISO/IEC TR 13335-3).....	91
6.5.3. Szacowanie ryzyka – analiza bezpieczeństwa systemów sterowania	99
6.6. Reakcja na ryzyko	102
6.6.1. Kontrolowanie ryzyka poprzez stosowanie zabezpieczeń	104
6.6.2. Akceptacja ryzyka szacunkowego.....	109
6.6.3. Ryzyko akceptowalne i koszty postępowania z ryzykiem	111
6.7. Administrowanie ryzykiem	115
6.7.1. Zadania, czynności i zakresy kompetencji – organizacja procesu zarządzania ryzykiem.....	117
6.8. Podsumowanie rozważań o analizie ryzyka	122
Rozdział 7. O testowaniu i audycie.....	125
7.1. Przegląd rodzajów badań.....	125
7.2. Ocena bezpieczeństwa teleinformatycznego	127
7.3. Audyt	129
7.4. Audyt i certyfikowanie SZBI	142
Rozdział 8. O standardach.....	149
8.1. Common Criteria i norma ISO/IEC 15408.....	151
8.2. COBIT™ – standard ładu informatycznego.....	161
8.3. BS 7799 i norma PN-ISO/IEC 27001:2007: Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania	164
8.3.1. Zawartość normy PN-ISO/IEC 27001:2007: Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.....	166
8.3.2. System zarządzania bezpieczeństwem informacji (SZBI).....	169
8.3.3. Normatywny zbiór zabezpieczeń – załącznik A normy PN-ISO/IEC 27001/73	
Rozdział 9. O projektowaniu	177
9.1. Cykl życia systemu bezpieczeństwa teleinformatycznego.....	178
9.2. Zarządzanie projektowaniem i budową systemu bezpieczeństwa teleinformatycznego	181
9.3. System bezpieczeństwa teleinformatycznego – koncepcja	183
9.3.1. Kompleksowość i dekompozycja.....	184

9.3.2. Przesłanki budowy „w głąb” systemu ochrony	188
9.4. Architektura systemu bezpieczeństwa teleinformatycznego	188
9.5. Analiza i projektowanie systemu bezpieczeństwa teleinformatycznego	192
9.5.1. Etap analizy	192
9.5.2. Etap projektowania	193
9.5.3. Wzorce projektowe	196
9.6. Ograniczenia procesu projektowania	197
9.7. Dokumentowanie prac projektowych	197
Załącznik. Metodyka L-RAC analizy i kontrolowania ryzyka w zakresie bezpieczeństwa teleinformatycznego.....	201
Literatura	279
Skorowidz	285