

# Spis treści

<b>Wstęp</b> .....	9
<b>1. Wprowadzenie do ochrony informacji</b> .....	15
1.1. Prywatność, anonimowość, poufność, ... ..	19
1.2. Zagrożenia, podatności, zabezpieczenia, incydenty .....	22
1.2.1. Zagrożenia .....	22
1.2.2. Podatności .....	29
1.2.2.1. Security Content Automation Protocol (SCAP) .....	32
1.2.2.2. Cykl życia podatności oprogramowania .....	36
1.2.3. Zabezpieczenia .....	41
1.2.4. Incydenty i zarządzanie incydentami .....	50
1.2.4.1. Obsługa incydentów – podstawowe wytyczne norm i standardów .....	52
1.2.4.2. Zgłoszenie incydentu .....	55
1.2.4.3. Zasoby do obsługi incydentu .....	60
1.3. Elementy projektowania systemu bezpieczeństwa informacyjnego .....	64
1.3.1. Cykl życia systemu .....	65
1.3.2. Zarządzanie przedsięwzięciem projektowania i budowy systemu bezpieczeństwa informacyjnego .....	69
1.3.3. Etap analizy w cyklu rozwojowym systemu bezpieczeństwa informacyjnego .....	70
1.3.4. Etap projektowania w cyklu rozwojowym systemu bezpieczeństwa informacyjnego .....	72
1.3.5. Dokumentowanie prac projektowych .....	76
1.3.6. Dobre praktyki w projektowaniu wiarygodnych systemów .....	77
Literatura .....	82
<b>2. Modele ochrony informacji</b> .....	84
2.1. Organizacja dostępu do informacji .....	85
2.2. Sterowanie dostępem do informacji .....	95
2.3. Model Grahama–Denninga .....	99
2.4. Model Bella–LaPaduli .....	102
2.5. Model Biby .....	110
2.6. Model Brewera–Nasha (chiński mur) .....	115
2.7. Model Clarka–Wilsona .....	118

2.8. Model Harrisona–Ruzzo–Ullmana (HRU) .....	121
2.8.1. Uogólnienie modelu HRU – model TAM .....	125
2.9. Podstawowe Twierdzenie Bezpieczeństwa .....	126
2.9.1. Konkretyzacja BST .....	133
2.10. Podsumowanie .....	134
Literatura .....	136
<b>3. Zarządzanie ryzykiem .....</b>	<b>138</b>
3.1. Charakterystyka procesu zarządzania ryzykiem .....	141
3.2. Przegląd norm i standardów z zakresu zarządzania ryzykiem .....	145
3.2.1. Norma PN-ISO/IEC 27005:2010 .....	145
3.2.2. Standardy FIPS/NIST .....	147
3.2.3. ISO 31000 – rodzina norm dotyczących zarządzania ryzykiem .....	148
3.2.4. Rekomendacja D .....	150
3.3. Analiza ryzyka – identyfikacja zakresu, środowiska, zagrożeń i podatności .....	152
3.3.1. Identyfikacja zakresu i środowiska analizy ryzyka .....	152
3.3.2. Identyfikacja zagrożeń i podatności .....	159
3.4. Analiza ryzyka – szacowanie ryzyka .....	160
3.4.1. Oszacowanie ryzyka – metoda ilościowa .....	163
3.4.2. Oszacowanie ryzyka – metoda jakościowa .....	169
3.4.3. Burza mózgów – identyfikacje zagrożeń i podatności .....	189
3.4.4. Szacowanie ryzyka według normy PN-ISO/IEC-27005 .....	194
3.4.5. Szacowanie ryzyka według organizacji Microsoft® .....	199
3.4.6. Szacowanie ryzyka – analiza bezpieczeństwa dla systemów sterowania .....	201
3.5. Zmniejszanie wartości ryzyka .....	204
3.5.1. Kontrolowanie ryzyka przez stosowanie zabezpieczeń .....	206
3.6. Akceptacja ryzyka szacunkowego .....	210
3.6.1. Ryzyko akceptowalne i koszty postępowania z ryzykiem .....	212
3.7. Administrowanie ryzykiem .....	215
Literatura .....	222
<b>4. Dokumentowanie systemu ochrony informacji .....</b>	<b>224</b>
4.1. Polityka bezpieczeństwa .....	225
4.2. Plan, instrukcje i procedury bezpieczeństwa informacyjnego .....	234
4.3. Dokumentowanie przedsięwzięć zapewniania ciągłości działania organizacji .....	239
4.3.1. Plan zapewniania ciągłości działania – nazewnictwo i struktura .....	241
4.3.2. Przygotowanie planu zapewniania ciągłości działania .....	243
4.3.3. Plany kryzysowe a plany zapewniania ciągłości działania .....	248
4.3.4. Wytyczne z norm i standardów do konstrukcji planów zapewniania ciągłości działania .....	250
4.4. Przedsięwzięcia techniczne w zapewnianiu informacyjnej ciągłości działania .....	262
4.4.1. Kopie bezpieczeństwa .....	266
4.4.2. Kopie bezpieczeństwa – infrastruktura i organizacja .....	269
4.4.3. Zdalna kopia bezpieczeństwa .....	272
4.4.4. Zapasowe ośrodki przetwarzania danych .....	275
4.5. Przykłady struktury dokumentu <i>Plan zapewniania ciągłości działania</i> .....	279
4.5.1. Wariant 1 .....	279
4.5.2. Wariant 2 .....	282
4.5.3. Wariant 3 .....	284
Literatura .....	289

<b>5. Badanie i ocena stanu ochrony informacji</b> .....	290
5.1. Diagnostyka techniczna .....	293
5.2. Testowanie jako element diagnostyki technicznej .....	295
5.3. Testy penetracyjne jako szczególny przypadek testowania .....	300
5.4. Audyt jako szczególny przypadek badania jakości systemu ochrony informacji .....	302
5.5. Metodyka LP-A .....	311
Literatura .....	316
<b>6. Standardy i normy bezpieczeństwa informacyjnego</b> .....	318
6.1. Standardy i normy i wspierające projektowanie i wytwarzanie bezpiecznych produktów oraz systemów .....	320
6.1.1. Common Criteria i norma ISO/IEC 15408 .....	320
6.1.2. Publikacje specjalne NIST serii 800 .....	331
6.1.3. CIS Critical Security Controls .....	332
6.2. Standardy i normy wspierające zarządzanie bezpieczeństwem informacji .....	335
6.2.1. COBIT™ – dobre praktyki w zakresie ładu informatycznego .....	335
6.2.2. Zarządzanie bezpieczeństwem informacji – standard BS 7799 i normy serii ISO/IEC 2700x .....	340
6.2.2.1. Przegląd zawartości normy ISO/IEC 27002:2013 .....	342
6.2.2.2. Przegląd zawartości normy ISO/IEC 27001:2013 .....	342
6.3. Inne normy i standardy wspomagające ocenę oraz zarządzanie bezpieczeństwem informacyjnym .....	347
6.3.1. Norma ISO/IEC 21827 i SSE-CMM® – System Security Engineering Capability Maturity Model .....	347
6.3.2. ITIL – IT Infrastructure Library .....	349
Literatura .....	353
<b>7. Polityka informowania – oddziaływanie przekazem informacji</b> .....	354
7.1. Bezpieczeństwo informacyjne w dokumentach rangi państwowej .....	354
7.2. Komunikacja strategiczna .....	358
7.3. Definicje Komunikacji strategicznej .....	360
7.4. Charakterystyka Komunikacji strategicznej .....	362
7.5. Główne kontrowersje dotyczące Komunikacji strategicznej .....	365
7.6. Relacje Komunikacji strategicznej .....	369
7.6.1. Relacje Komunikacji strategicznej z operacjami informacyjnymi i psychologicznymi .....	370
7.6.2. Relacje Komunikacji strategicznej z dyplomacją publiczną .....	371
7.6.3. Relacje Komunikacji strategicznej z działalnością prasowo-informacyjną .....	372
7.7. Strategia Komunikacyjna – uwagi ogólne .....	373
Literatura .....	376
<b>Załącznik. Metodyka LP-A przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego</b> .....	378
Wykaz używanych terminów i symboli graficznych .....	378
Wstęp .....	380
<b>Z1. Skład Zespołu audytowego, kwalifikacje jego członków i zakresy kompetencji</b> .....	383
<b>Z2. Wyposażenie narzędziowe Zespołu audytowego</b> .....	386
Z.2.1. Kwestionariusze ankietowe .....	386
Z.2.2. Szablony edycyjne dokumentów .....	387

Z.2.3. Skanery bezpieczeństwa .....	387
Z.2.4. Skanery konfiguracji .....	388
Z.2.5. Skanery inwentaryzacyjne .....	388
Z.2.6. Zestawy narzędzi do badań technicznych .....	389
<b>Z3. Procesy audytowe .....</b>	<b>390</b>
<b>Z4. Specyfikacja dokumentów audytowych .....</b>	<b>396</b>
Z.4.1. Tabele IPO .....	396
Z.4.2. Specyfikacja zbiorcza dokumentów .....	404
<b>Z5. Diagramy przepływu danych .....</b>	<b>408</b>
<b>Z6. Rzetelne praktyki .....</b>	<b>415</b>
Z.6.1. Rzetelne praktyki stosowane na ścieżce formalnej .....	415
Z.6.2. Rzetelne praktyki stosowane na ścieżce technicznej .....	416
<b>Podsumowanie .....</b>	<b>417</b>
<b>Indeks .....</b>	<b>418</b>