

Spis treści

Podziękowania	9
Wstęp – dlaczego „bezpieczeństwo informacyjne”	11
1. Wprowadzenie do bezpieczeństwa informacyjnego i bezpieczeństwa informacji	17
Literatura	27
2. Wykorzystanie sieci i systemów teleinformatycznych do przestępstw o charakterze terrorystycznym	29
2.1. Zarys problemu	29
2.2. „State of the Art” w dziedzinie legislacji i nazewnictwa	33
2.3. Prognoza pesymistyczna – ataki terrorystyczne na sieci i systemy teleinformatyczne są skazane na powodzenie	36
2.4. Podsumowanie	40
Literatura	40
3. Ochrona informacji i obiektów w sieciach teleinformatycznych połączonych z systemami przemysłowymi – przegląd zagadnień	43
3.1. Wprowadzenie do zagrożeń i bezpieczeństwa systemów nadzorczo-sterujących infrastruktury przemysłowej	44
3.2. Systemy nadzoru i sterowania infrastruktury przemysłowej jako element infrastruktury krytycznej	48
3.3. Przegląd typów sieci przemysłowych	49
3.4. Łączenie sieci teleinformatycznych z systemami przemysłowymi – nowa jakość w dziedzinie bezpieczeństwa	54
3.5. Zalecenia NIST	56
Literatura	58

4. O zagrożeniach skutecznej ochrony informacji przetwarzanej w sieciach i systemach teleinformatycznych powodowanych nowomowa	60
4.1. Cybernetyka – nauka o sterowaniu i komunikacji	61
4.2. Podstawowe zasady działalności inżynierskiej a nowomowa	63
4.3. Podsumowanie	65
5. Modele ochrony informacji	67
5.1. Organizacja dostępu do informacji	68
5.2. Sterowanie dostępem do informacji	78
5.3. Model Grahama–Denninga	81
5.4. Model Belli–LaPaduli	84
5.5. Model Biby	92
5.6. Model Brewera–Nasha (chiński mur)	96
5.7. Model Clarka–Wilsona	100
5.8. Model Harrisona–Ruzzo–Ullmana (HRU)	103
5.8.1. Uogólnienie modelu HRU – model TAM	107
5.9. Podstawowe twierdzenie bezpieczeństwa	108
5.9.1. Konkretyzacja BST	115
5.10. Podsumowanie	115
Literatura	118
6. Dokumentowanie systemu ochrony informacji	120
6.1. Polityka bezpieczeństwa	121
6.2. Plan, instrukcje i procedury bezpieczeństwa informacyjnego	130
6.3. Plan zapewniania ciągłości działania	135
6.3.1. Opracowanie planu zapewniania ciągłości działania	137
6.3.2. Plany kryzysowe a plany zapewniania ciągłości działania	143
6.3.3. Wytyczne z norm i standardów do konstrukcji planów zapewniania ciągłości działania	145
Literatura	154
7. Zapewnianie informacyjnej ciągłości działania	155
7.1. Kopie bezpieczeństwa	159
7.2. Kopie bezpieczeństwa – infrastruktura i organizacja	162
7.3. Zdalna kopia bezpieczeństwa	165
7.4. Zapasowe ośrodki przetwarzania danych	167
Literatura	179
8. Szablon analizy i minimalizacji ryzyka na potrzeby ochrony informacji – wariant zasobowy	180
8.1. Ustalenie systemu ocen i sposobu oszacowania ryzyka	182
8.2. Identyfikacja środowiska	187
8.3. Identyfikacja zasobów	187
8.4. Identyfikacja zagrożeń	188
8.5. Identyfikacja podatności wykorzystywanych przez zagrożenia	189
8.6. Identyfikacja wielkości strat	191
8.7. Tabelaiczna prezentacja ryzyka i propozycja jego minimalizacji	191
8.8. Szacowanie ryzyka złożonego	192

Załącznik 1. Wzorzec dokumentacyjny Planu Zapewniania Ciągłości Działania dla systemów teleinformatycznych według dodatku A do wytycznych NIST SP 800-34	197
Załącznik 2. Zarządzanie ciągłością działania według PN-ISO/IEC-17799	203
Załącznik 3. Przykład struktury dokumentu Plan zapewniania ciągłości działania	208
Załącznik 4. Zasady przeprowadzenia sesji „burzy mózgów”	214
Załącznik 5. Przebieg sesji „burzy mózgów”	216