

SPIS TREŚCI

Wstęp	5
Introduction.	11
1. Bezpieczeństwo na płaszczyźnie informacyjnej.	17
1.1. Od danych do informacji – z teorii problemu. Informacja a społeczeństwo .	17
1.2. Strategia, źródła i rodzaje informacji strategicznych	29
1.3. Koncepcja systemu informatycznego jako istotnego ogniwa strategii organizacji	35
1.4. Istota bezpieczeństwa informacyjnego	41
1.5. Rosnąca rola bezpieczeństwa informacyjnego w państwie i podmiotach gospodarczych oraz wśród obywateli	45
1.6. Zasady bezpieczeństwa informacyjnego	50
1.7. Kształtowanie bezpieczeństwa informacyjnego.	55
1.8. Zarządzanie bezpieczeństwem informacyjnym	57
1.9. Ocena poziomu analizowanego bezpieczeństwa informacyjnego	62
2. Zapewnienie bezpieczeństwa informacyjnego.	65
2.1. Sposoby pozyskania informacji - elementy wojny informacyjnej	65
2.2. Analiza wybranych mechanizmów wojny informacyjnej, cyberterroryzmu i przestępczości komputerowej	74
2.3. Polityka bezpieczeństwa informacji.	89
2.4. Jak kształtować bezpieczeństwo informacyjne	94
3. Cyberterroryzm i przestępczość komputerowa.	103
3.1. Cyberterroryzm – definicja i zakres	103

3.2. Przemoc komputerowa.	106
3.3. Cyberterroryzm i przemoc komputerowa jako zagrożenie bezpieczeństwa	109
4. Współczesne zagrożenia cybernetyczne a teleinformatyczne rezerwy (zasoby) strategiczne państwa polskiego.	115
4.1. Potencjał teleinformatyczny.	115
4.2. Teleinformatyka na potrzeby obronności i bezpieczeństwa.	116
4.3. Sieci komputerowe, systemy, sprzęt i oprogramowanie jako zasoby IT państwa	120
4.4. Wiedza, specjaliści, firmy jako potencjał infrastruktury krytycznej	125
4.5. Współczesne zagrożenia przemoc komputerowej, cyberterroryzmu, cyberwojny	131
4.6. Wykorzystanie potencjału teleinformatycznego organizacji i instytucji odpowiedzialnych za zapewnienie bezpieczeństwa	135
4.7. Polska w systemie bezpieczeństwa teleinformatycznego UE i NATO	141
4.8. Identyfikacja strategicznych rezerw (zasobów) teleinformatycznych jako potencjału cyberbezpieczeństwa	156
5. Biometria w służbie bezpieczeństwa informacji	165
5.1. Podstawy biometrii	165
5.2. Identyfikacja biometryczna człowieka – podział i przykłady	167
5.3. Zastosowanie wybranych rozwiązań biometrycznych	182
6. Kryptografia na potrzeby bezpieczeństwa informacji	191
6.1. Wprowadzenie do kryptografii	191
6.2. Maszyny i inne rozwiązania szyfrujące	196
6.3. Wpływ kryptografii na losy konfliktów zbrojnych	204
6.4. Kryptologia, kryptografia i kryptoanaliza.	211
6.5. Przykłady praktycznych zastosowań – kryptografia symetryczna i asymetryczna.	216
7. Rola i zadania administratora systemu (sieci) informatycznego.	233
Zakończenie.	241
Conclusion	247
Bibliografia	251