

Spis treści

Wykaz skrótów i symboli.....	7
Wstęp	11
1. Metodologiczne podstawy badań i analiz zagrożeń informacji.....	13
2. Zagrożenia informacji w cyberprzestrzeni Rzeczypospolitej Polskiej	21
2.1. Określenie informacji, zagrożeń i bezpieczeństwa informacji	22
2.2. Identyfikacja i klasyfikacja zagrożeń informacji w cyberprzestrzeni Rzeczypospolitej Polskiej	25
3. Oprogramowanie złośliwe.....	31
3.1. Wirusy.....	33
3.2. Robaki sieciowe.....	40
3.3. Trojany	45
3.4. Bomba logiczna	51
3.5. Exploit.....	52
3.6. Dialery	53
3.7. SQL/URL Injections	54
3.8. Sztuczna inteligencja	54
3.9. Botnety	55
3.10. Spam i fałszywki.....	57
3.11. Objawy oprogramowania szkodliwego i profilaktyka przeciwdziałania.....	58
4. Sposoby, metody i formy ataków w cyberprzestrzeni.....	62
4.1. Ataki blokujące.....	63
4.2. Ataki kryptograficzne	69
4.3. Ataki podszywania się i oszustwa	75
4.4. Ataki z elementami inżynierii społecznej.....	79
4.5. Inne formy ataków	85
4.6. Oprogramowanie ułatwiające przeprowadzenie ataków	88
4.7. Scenariusz ataków w cyberprzestrzeni	91
4.8. Przykłady cyberataków w Cyberprzestrzeni Rzeczypospolitej Polskiej.....	95

5. Kategorie cyberprzestępstw.....	105
5.1. Określenie cyberprzestrzeni i cyberprzestępstwa	105
5.2. Kategorie cyberprzestępstw w ujęciu organizacji międzynarodowych	110
5.3. Kategorie cyberprzestępstw w Rzeczypospolitej Polskiej.....	112
6. Analiza stanu zagrożeń cyberprzestrzeni Rzeczypospolitej Polskiej.....	123
6.1. Stan zagrożeń cyberprzestrzeni Rzeczypospolitej Polskiej	124
6.2. Analiza współczesnych zagrożeń cyberprzestrzeni Rzeczypospolitej Polskiej	133
6.3. Przewidywane trendy rozwojowe współczesnych zagrożeń cyberprze- strzeni Rzeczypospolitej Polskiej	137
7. Cyberterroryzm zagrożeniem bezpieczeństwa informacji	145
7.1. Określenie i destrukcyjna rola cyberterroryzmu.....	145
7.2. Cele i obiekty ataków cyberterrorystycznych.....	149
7.3. Krytyczna infrastruktura teleinformatyczna Rzeczypospolitej Polskiej szczególnym obiektem zainteresowania cyberterroryzmu	150
7.3.1. Identyfikacja obiektów i celów ataku krytycznej infrastruktury te- leinformatycznej.....	151
7.3.2. Charakterystyka obiektów cyberataków krytycznej infrastruktury teleinformatycznej	155
8. Wojna informacyjna, cyberwojna.....	166
8.1. Określenie współczesnych wojen. Wojna informacyjna, cyberwojna	167
8.2. Charakter i warunki prowadzenia wojny informacyjnej.....	169
8.3. Elementy wojny informacyjnej.....	172
8.4. Współczesna wojna informacyjna, studium przypadku	174
Zakończenie	184
Bibliografia	186
Załączniki.....	191
Spis rysunków i tabel	204