

Spis treści

Wykaz skrótów.....	7
Wprowadzenie	11
1. Zagrożenia informacji i systemów teleinformatycznych.....	15
1.1. Oprogramowanie złośliwe	17
1.1.1. Wirusy.....	17
1.1.2. Robaki sieciowe.....	18
1.1.3. Konie trojańskie.....	19
1.1.4. Dialery	20
1.1.5. Botnety.....	20
1.1.6. Spam i fałszywki.....	21
1.2. Cyberprzestępstwa	22
1.2.1. Kategorie przestępstw w cyberprzestrzeni	22
1.2.2. Stan zagrożeń i incydentów w cyberprzestrzeni Rzeczypospolitej Polskiej	28
1.3. Cyberterroryzm	31
1.3.1. Formy i metody ataków	33
1.3.2. Przykłady cyberataków w Rzeczypospolitej Polskiej	37
2. Metody ochrony informacji przed zagrożeniami w cyberprzestrzeni	39
2.1. Metody administracyjno-organizacyjne.....	40
2.1.1. Określenie potrzeb w zakresie bezpieczeństwa informacji organizacji	42
2.1.2. Określanie uwarunkowań i otoczenia bezpieczeństwa informacji or- ganizacji	45
2.1.3. Określanie funkcjonalności bezpieczeństwa informacji organizacji	51
2.1.4. Poszukiwanie i wybór właściwego rozwiązania bezpieczeństwa in- formacji organizacji	52
2.1.5. Opracowanie rozwiązania bezpieczeństwa informacji organizacji	54
2.1.6. Wdrożenie rozwiązania bezpieczeństwa informacji organizacji	57
2.2. Podstawy prawne i normalizacyjne bezpieczeństwa informacji organizacji	58
2.2.1. Bezpieczeństwo informacji niejawnych	58
2.2.2. Bezpieczeństwo danych wrażliwych	66
2.2.3. Bezpieczeństwo informacji w różnych aktach prawnych i dokumen- tach w państwie.....	73
2.2.4. Normalizacja i standaryzacja w bezpieczeństwie informacji organizacji.....	77

2.3. Metody techniczne.....	90
2.3.1. Metody kryptograficzne.....	91
2.3.2. Metody programowo-sprzętowe.....	99
2.3.3. Metody ochrony elektromagnetycznej	112
2.3.4. Elektroniczne systemy ochrony fizycznej obiektów i zasobów teleinformatycznych organizacji.....	115
2.4. Metody fizyczne.....	115
2.4.1. Systemy sygnalizacji włamania i napadu	118
2.4.2. Systemy sygnalizacji pożarów.....	130
2.4.3. Systemy telewizji użytkowej.....	132
2.4.4. Systemy kontroli dostępu	133
2.4.5. Systemy inteligentnych budynków.....	134
2.4.6. Bezpieczeństwo fizyczne informacji niejawnej.....	136
3. Systemy monitorowania i reagowania na zagrożenia cyberprzestrzeni	139
3.1. Uwarunkowania monitorowania i reagowania na zagrożenia cyberprzestrzeni	139
3.2. System ostrzegania i reagowania na zagrożenia cyberprzestrzeni	141
3.3. Funkcjonowanie systemu ostrzegania i reagowania na zagrożenia cyberprzestrzeni.....	147
4. Działania edukacyjne w zakresie bezpieczeństwa informacji i systemów teleinformatycznych	149
5. Podstawy prawne ochrony informacji i systemów teleinformatycznych.....	154
5.1. Strategie cyberbezpieczeństwa Unii Europejskiej i NATO	154
5.2. Podstawy prawne cyberbezpieczeństwa Rzeczypospolitej Polskiej.....	162
6. Zarządzanie bezpieczeństwem informacji organizacji	171
6.1. Określenie i zakres zarządzania bezpieczeństwem informacji organizacji ...	171
6.2. Elementy procesu zarządzania bezpieczeństwem informacji organizacji	172
6.3. Procesy zarządzania bezpieczeństwem informacji organizacji	176
6.4. System Zarządzania Bezpieczeństwem Informacji organizacji.....	182
Zakończenie	186
Literatura.....	188
Wykaz tablic i rysunków.....	192
Skorowidz	194