

SPIS TREŚCI

Wstęp	1
1. Cyberprzestrzeń jako środowisko walki	9
1.1. Istota walki	10
1.2. Współczesny wymiar konfliktu zbrojnego i wojny	25
1.3. Cyberprzestrzeń jako domena operacyjna	34
2. Elementy bezpieczeństwa cyberprzestrzeni	51
2.1. Informacja i przestrzeń informacyjna	52
2.2. Systemy informacyjne i systemy krytyczne	65
2.3. Bezpieczeństwo informacji, informacyjne i teleinformatyczne ...	74
2.4. Wymagania stawiane przed systemami informacyjnymi i teleinformatycznymi	86
3. Charakterystyka zagrożeń bezpieczeństwa cyberprzestrzeni ...	95
3.1. Zagrożenia informacyjne	96
3.2. Zagrożenia informatyczne	110
3.3. Zagrożenia kinetyczne	121
3.4. Inwigilacja, szpiegostwo i rozpoznanie	126
4. Wyznaczniki działań w cyberprzestrzeni	135
4.1. Czynniki walki	138
4.2. Zasady i reguły walki	146
4.3. Siła, potęga i potencjał	158
5. Klasyfikacja działań w cyberprzestrzeni	163
5.1. Cele realizowane w cyberprzestrzeni	164
5.2. Poziomy działań	173
5.3. Elementy konfliktu w cyberprzestrzeni	179
5.4. Działania profilaktyczno-ochronne	185
5.5. Wykorzystanie cyberprzestrzeni w poglądach narodowych i NATO	194
5.6. Wykorzystanie cyberprzestrzeni według poglądów rosyjskich ...	201

6. System walki w cyberprzestrzeni	209
6.1. Charakterystyka systemu walki	210
6.2. Tworzenie systemu walki	215
6.3. Elementy systemu	219
Zakończenie	239
Bibliografia	241
Spis rysunków i tabel	255
Wstęp	259
1. Cyberprzestrzeń jako środowisko walki	261
1.1. Istota walki	261
1.2. Współczesny wymiar konfliktu zbrojnego wojny informacyjnej	262
1.3. Cyberprzestrzeń jako domena operacyjna	264
2. Elementy bezpieczeństwa cyberprzestrzeni	265
2.1. Informacja i przesłany informacyjny	265
2.2. Systemy informacyjne i systemy krytyczne	266
2.3. Bezpieczeństwo informacji, informacji i teleinformatyczne	267
2.4. Wymagania stawiane przed systemami informacyjnymi i teleinformatycznymi	268
2.5. Charakterystyka zagrożeń bezpieczeństwa cyberprzestrzeni	269
2.6. Zagrożenia informacyjne	270
2.7. Zagrożenia informacyjne	271
2.8. Zagrożenia kinetyczne	272
2.9. Inwigilacja, szpiegostwo i rozpoznawanie	273
3. Wymagalność działań w cyberprzestrzeni	274
3.1. Czynności walki	274
3.2. Zasady i reguły walki	275
3.3. Siła, potęga i potencjał	276
4. Klasyfikacja działań w cyberprzestrzeni	277
4.1. Cele realizowane w cyberprzestrzeni	277
4.2. Poziomy działania	278
4.3. Elementy konfliktu w cyberprzestrzeni	279
4.4. Działania profilaktyczno-ochronne	280
4.5. Wykorzystanie cyberprzestrzeni w poglądach	281
4.6. Wykorzystanie cyberprzestrzeni w NATO	282
4.7. Wykorzystanie cyberprzestrzeni według poglądów rosyjskich	283