SPIS TREŚCI

Wstęp 9
Spis pojęć i skrótów 13
Definicje i oznaczenia 15

Rozdział I: Notacja i opracowanie koncepcji 17
1. Globalne nawigacyjne systemy satelitarne 23
2. Struktura odbiornika GNSS 25
2.1. Klasyfikacja odbiorników GNSS 25
2.1.1. Klasyfikacja według typu sygnału 25
2.1.2. Klasyfikacja według liczby częstotliwości 25
2.1.3. Klasyfikacja według liczby używanych systemów 25
2.2. Kształtowanie częstotliwości nośnej 26
2.3. Koncepcja GNSS PNT – cyberataki na odbiorniki GNSS 30
3. *Jamming* GNSS 36
4. *Meakoning* GNSS 37
5. *Spoofing* GNSS 38
6. Klasyfikacja *spooferów* 39
6.1. *Spoofery* z anteną pojedynczą asynchroniczne 40
6.2. *Spoofery* z anteną pojedynczą synchroniczne 40
6.3. Ogólny HackRF One 41
7. Klasyfikacja systemów wykrywania *spoofingu* (SWS) 41
7.1. SWS z anteną statyczną 41
7.1.1. SWS jako analizator siły sygnału 42
7.1.2. SWS jako analizator SNR (stosunek sygnału do szumu) 42
7.1.3. SWS jako monitorowanie jakości sygnału 43
7.1.4. SWS jako monitorowanie czasu 43
7.2. SWS z ruchomą anteną pojedynczą 43
7.3. SWS z obrotową anteną pojedynczą 43
7.4. SWS z podwójną anteną 44
8. Podstawowa technologia walki elektronicznej z *jammingiem* i *spoofingiem* 44

Rozdział II: Konfiguracja sprzętu i oprogramowania 45
1. *Jammer* i *antyjamming* 45
1.1. Pojazdy bezzałogowe 46
1.2. Interferencja z pojazdami bezzałogowymi 48
1.3. Ekranowanie anteny UV w celu ochrony przed *spoofingiem* i/lub *jammingiem* GNSS 50
1.4. Dyfrakcja Fresnela na krawędzi pierścienia ekranującego 52
1.5. Redukcja dyfrakcji na krawędzi pierścienia ekranującego 52
1.6. Eksperymentalne badanie ekranowania anteny odbiornika 55
2. *Meakoning* i wykrywanie *meakoningu* 56
3. *Spoofing* i wykrywanie *spoofingu* 58
3.1. *Spoofery* działające na zasadzie symulatorów sygnałów GNSS 59
3.2. *Spoofery* działające na zasadzie sygnału odbiornika GNSS 62

Rozdział III: Analiza porównawcza metod wykrywania *spoofingu* 65
1. Metoda przeciwdziałania *spoofingowi* 65
2. Rozszerzony algorytm wykrywania *spoofingu* GNSS 68
3. Detekcja *spoofingu* GNSS z użyciem jednej – statycznej lub obracającej się anteny 76
3.1. GNSS *spoofera* i ofiary 77
3.2. Wykrywanie *spoofingu* 79
3.3. Dopuszczalny błąd zmierzonej wartości poziomu morza 80
3.4. Detekcja *spoofingu* GNSS z użyciem jednej anteny bazująca na pomiarach współrzędnych poruszającej się ofiary w dwóch punktach na trasie 82
3.5. Detekcja *spoofingu* GNSS za pomocą obracającej się anteny 85
4. Kompas satelitarny detektorem *spoofingu* GNSS 88

Rozdział IV: Badania systemu wykrywania *spoofingu* 93
1. Klasyfikacja i analiza scenariuszy *spoofingu* 93
2. Badania symulacyjne na podstawie rezultatów pomiarów badań statystycznych 96

3. Badania eksperymentalne 100
3.1. Wyniki badań statycznych z zastosowaniem dwóch odbiorników GNSS i *repeatera* sygnału GNSS jako *spoofera* 104
3.2. Badania doświadczalne z użyciem jednej – statycznej lub obracającej się anteny 111
3.3. Wyniki badań dynamicznych z zastosowaniem jednego odbiornika GNSS i *repeatera* sygnału GNSS jako *spoofera* 114
3.4. Wyniki statycznych badań podatności odbiornika GNSS i systemu komunikacji radiowej HackRF One jako *spoofera* 119

Rozdział V: Systemy nawigacji inercyjnej i filtrowanie danych 123
1. Filtr Kalmana 125
1.1. Algorytm filtrowania Kalmana 128
2. Filtr „średniej ruchomej" 130
3. GNSS jako jeden z głównych środków korekcji IMU 131

Zakończenie 133
Streszczenie 135
Summary 137
Bibliografia 139
Spis tabel i rysunków 145
Załącznik. *STANDARD NMEA 0183* 149