

WSTĘP / 9

Rozdział I. INTERDYSCYPLINARNY CHARAKTER CYBERPRZESTĘPCZOŚCI / 15

1. Problem definicyjny / 15
2. Prawny aspekt cyberprzestępczości / 20
3. Techniczny aspekt cyberprzestępczości / 24
 - 3.1. Malware / 25
 - 3.2. Spam / 26
 - 3.3. Botnet / 27
 - 3.4. Kradzież tożsamości / 28
 - 3.5. Phishing / 29
 - 3.6. DDoS / 30
 - 3.7. Darknet / 30
 - 3.8. Kryptowaluty / 31
 - 3.9. Carding / 31
 - 3.10. Internet IPR / 32
 - 3.11. Hazard internetowy / 33
 - 3.12. Oszustwa na aukcjach internetowych / 33
 - 3.13. Oszustwa telekomunikacyjne / 33
4. Organizacyjny aspekt cyberprzestępczości / 34
5. Socjologiczny aspekt cyberprzestępczości / 37

Rozdział II. CHARAKTERYSTYKA RYNKU CYBERPRZESTĘPCZEGO / 40

1. Szacowanie skali zjawiska / 40
2. Struktury na rynku cyberprzestępczości / 43
3. Problem bezpieczeństwa transakcji / 50
4. Dojrzałość rynku / 52
 - 4.1. Elastyczność / 52
 - 4.2. Niezawodność i integralność / 53
 - 4.3. Dostępność / 53
 - 4.4. Specjalizacja / 53
 - 4.5. Stabilność / 54
5. Podsumowanie i prognozy przyszłości / 54

Rozdział III. EKONOMICZNA ANALIZA CYBERPRZESTĘPCZOŚCI / 58

1. Wstęp / 58
2. Behawioralne podstawy analizy / 60
3. Motywacja do podjęcia działań cyberprzestępczych / 64
4. Kontekst społeczny / 68
5. Koszty transakcyjne / 71
6. Transakcje / 75
 - 6.1. Specyficzność aktywów / 75
 - 6.2. Niepewność / 76
 - 6.3. Częstotliwość / 78
7. Problem pomiaru / 79
8. Integracja pionowa / 81
9. Wiarygodne zobowiązania / 84
10. Rozwiązanie bilateralne / 85
11. Zawodność rynku i cyberprzestępczość / 86
12. Ewolucja rynku cyberprzestępczego / 87

Rozdział IV. EKONOMETRYCZNA ANALIZA CYBERPRZESTĘPCZOŚCI / 94

1. Dotychczasowy stan wiedzy i przyczyny badania / 94
2. Jednorównaniowy liniowy model ekonometryczny / 99
 - 2.1. Budowa modelu ekonometrycznego / 99
 - 2.2. Testowanie modelu ekonometrycznego / 102
3. Czynniki, które nie wpływają na cyberprzestępczość / 104
4. Zmienne wpływające na cyberprzestępczość / 105
5. Prognozowanie na podstawie ekonometrycznego modelu cyberprzestępczości / 107
6. Znaczenie ekonometrii w badaniu cyberprzestępczości / 109

Rozdział V. ANALIZA PRZYPADKU DARKMARKET / 111

1. Wprowadzenie do studium przypadku / 111
2. Powstanie DarkMarket / 112
3. Działanie DarkMarket / 114
4. DarkMarket jako organizacja przestępcza / 117
5. Ryzyko i niepewność na rynku cyberprzestępczości / 121
6. Instytucja DarkMarket / 125
7. Konkurencja bez zasad / 126
8. Otoczenie rynkowe DarkMarket / 129
9. Interesariusze organizacji / 133
10. Strategia DarkMarket / 135
11. Analiza SWOT / 136
12. Twórcza destrukcja jako model rozwoju rynku cyberprzestępczości / 138
13. Organizacje cyberprzestępcze w przyszłości / 141
14. Wnioski ze studium przypadku / 142

ZAKOŃCZENIE / 145

BIBLIOGRAFIA / 147

SPIS RYSUNKÓW / 151

SPIS TABEL / 152