

SPIS TREŚCI

Wstęp	5
Rozdział 1	
Zagrożenia informacyjne w cyberprzestrzeni – dezinformacja i propaganda	
<i>Piotr DELA</i>	11
Rozdział 2	
Odpieranie ataku ransomware przez wykrywanie akcji payloadu	
<i>Adam E. PATKOWSKI</i>	31
Rozdział 3	
Automatyzacja zapytań deanonimizacyjnych w sieci Bitcoin	
<i>Przemysław RODWALD, Nicola KOŁAKOWSKA</i>	49
Rozdział 4	
Ochrona zasobów informacyjnych przed atakami wrogich podmiotów zorganizowana na podstawie uznanych wzorców, baz wiedzy i standardów – zarys metodyki	
<i>Krzysztof LIDERMAN</i>	67
Rozdział 5	
Ekstrakcja dowodów z urządzeń IoT z wykorzystaniem metody Chip-off	
<i>Michał GMUREK, Sasha SHEREMETOV, Igor LOSKUTOV</i>	89
Rozdział 6	
Trendy występujące na rynku kryptoaktywów	
<i>Jacek CHARATYNOWICZ</i>	101
Rozdział 7	
Osint i wojna czyli mocno subiektywny przegląd źródeł informacji	
<i>Krzysztof WOJCIECHOWSKI</i>	119
Rozdział 8	
O stanowczości opinii biegłego	
<i>Maciej SZMIT</i>	149
Rozdział 9	
Forensic analysis of flash memory using X-RAY and Logic Analyser	
<i>Sasha SHEREMETOV, Igor LOSKUTOV, Michał GMUREK</i>	157

Rozdział 10

Działania w cyberprzestrzeni podczas konfliktów hybrydowych – wnioski z wojny na Ukrainie

Jakub SYTA165

Rozdział 11

Winnti: Is the gaming industry in actual danger? Analysis of the operation of the largest organised cybercriminal syndicate targeting video game producers

Marek Piotr STOLARSKI187

Rozdział 12

Czy polski ekosystem prawny jest przyjazny dla stworzeń mitycznych i bytów nadprzyrodzonych?

Wojtak PLISZAK221

Rozdział 13

Genealogia na usługach oszustów i wymiaru sprawiedliwości

Joanna LUBIERSKA237

Rozdział 14

Narzędzia hackerskie – aspekty karne i techniczne

Filip RADONIEWICZ251

Rozdział 15

Credential stuffing

Kamil KOŁODZIEJCZYK273

Załącznik

Operations Analysis of Crypto-assets in Terrorist Financing

CFLW Intelligence Services287