

Spis treści

Przedmowa 7

Podziękowania 9

O autorze 11

Rozdział 1. Informacje ogólne i podstawowe akty prawne 13

1.1. Informacje ogólne 13

1.2. Podstawowe akty prawne 14

1.3. Prawa i obowiązki biegłych w postępowaniu przed organami sprawiedliwości 15

1.3.1. Odpowiedzialność karna biegłego 17

1.3.2. Odpowiedzialność cywilna biegłego 18

1.3.3. Biegły funkcjonariuszem publicznym 20

1.3.4. Ubezpieczenie odpowiedzialności cywilnej biegłego 20

1.4. Wymogi formalnoprawne opinii 21

1.5. Ekspertyza lub opinia prywatna 22

Rozdział 2. Informatyka sądowa 25

2.1. Licencje oprogramowania open source 25

2.2. Dowód elektroniczny i jego zabezpieczanie 26

2.3. Informatyka śledcza 27

2.3.1. Sprzęt komputerowy do badań 29

2.3.2. Oprogramowanie do badań 38

2.3.3. Wykonanie kopii binarnej 45

2.3.4. Badania post mortem 48

2.3.5. Live forensic 52

2.3.6. Analizy w środowisku big data 55

2.3.7. Technologia triage	58
2.3.8. Dobre praktyki badania nośników w informatyce śledczej	59
2.4. Badania systemów teleinformatycznych	60
2.4.1. Badania oprogramowania	64
2.4.2. Badania penetracyjne (pentesty)	65
2.5. Analiza projektów informatycznych	69
2.5.1. Metodyki zarządzania projektami	70
2.5.2. Opis realizacji systemu i jego funkcjonalności	71
2.5.3. Zastosowane technologie kształtujące koszt i zaawansowanie projektu (czasochłonność projektu)	71

Rozdział 3. Analiza śledcza i powłamaniowa 75

3.1. Informacje ogólne	75
3.1.1. Przygotowanie stanowiska badawczego	76
3.2. Analiza zawartości nośników i systemu plików	78
3.2.1. Tablica MFT	79
3.3. Analiza rejestru systemowego	84
3.4. Inwigilacja	86
3.4.1. Ślady działalności w sieci lokalnej i Internecie	88
3.5. Ukrywanie śladów aktywności	90
3.6. Wykrywanie złośliwego oprogramowania	92
3.6.1. Wykrywanie złośliwego oprogramowania	93
3.6.2. Postępowanie ze szkodliwym oprogramowaniem	94
3.6.3. Środowisko do analizy i analiza	95
3.7. Analiza zdarzeń w osi czasu	96
3.8. Analiza aplikacji	99
3.9. Automatyzacja analizy śledczej	101

Rozdział 4. Wycena systemów komputerowych 103

Rozdział 5. Prawa autorskie do programów komputerowych 109

- 5.1. Najczęściej występujące typy licencji 110
- 5.2. System operacyjny Windows firmy Microsoft 112
- 5.3. Systemy operacyjne LINUX 114
- 5.4. Inne systemy operacyjne (Apple itp.) 115
- 5.5. Aplikacje typu CAD/CAM, inżynierskie 115
- 5.6. Inne aplikacje użytkowe 115

Rozdział 6. Opiniowanie sądowo-informatyczne 117

- 6.1. Postanowienie o zasięgnięciu opinii. Dowód z opinii biegłego 117
- 6.2. Struktura opinii sądowo-informatycznej 119
 - 6.2.1. Struktura opinii dotyczących badań nośników i informatyki śledczej 120
 - 6.2.2. Struktura opinii dotycząca oceny systemów komputerowych i teleinformatycznych 125
 - 6.2.3. Struktura opinii/ekspertyzy z zakresu wyceny systemów teleinformatycznych 125
- 6.3. Metodyka pracy biegłego 139
- 6.4. Opisy czynności i ich dokumentowanie 139
- 6.5. Wnioski z ekspertyzy, opinii 142
- 6.6. Opinia uzupełniająca 143
- 6.7. Opinia ustna, wezwanie biegłego 144
- 6.8. Ocena pracy biegłego 144

Rozdział 7. Opiniowanie z zakresu elektroniki 147

- 7.1. Sprzęt i oprogramowanie do badań 147
- 7.2. Struktura opinii z zakresu elektroniki 155
 - 7.2.1. Struktura opinii dotyczącej elektroniki 155

7.2.2. Struktura opinii dotyczących metrologii/miernictwa elektrycznego i elektronicznego 160

7.2.3. Struktura opinii dotyczącej badań nośników i informatyki śledczej 166

7.3. Sprzęt do badania urządzeń mobilnych 171

7.4. Oprogramowanie do badania urządzeń mobilnych 187

Rozdział 8. Przykłady opinii sądowych z zakresu informatyki 203

8.1. Ochrona dóbr osobistych 204

8.2. Włamanie do systemu teleinformatycznego 210

8.3. Kradzież z włamaniem na rachunek bankowy 228

8.4. Badanie w sprawie o czyn z art. 200 § 1k.k. 246

8.5. Badanie oprogramowania 261

8.6. Analiza dokumentacji projektowej 289

Rozdział 9. Przykłady opinii sądowych z zakresu elektroniki 307

9.1. Wady fizyczne sprzętu radiowego 308

9.2. Ocena uszkodzenia laptopa 318

9.3. Ocena wady fabrycznej laptopa 330

9.4. Badanie w sprawie o czyn z art. 297 § 1 k.k. 341

9.5. Badanie w sprawie o czyn z art. 286 § 1 k.k. 351

9.6. Badanie w sprawie o czyn z art. 200a § 2 k.k. 369

9.7. Wycena systemu teleinformatycznego 381

Rozdział 10. Zakończenie 395

Dodatek A. Adresy WWW 397

Dodatek B. Sądy okręgowe 401

Dodatek C. Prokuratury okręgowe 403

Dodatek D. Komendy wojewódzkie policji 409

Dodatek E. Urzędy marszałkowskie 411

Bibliografia 413