

Spis treści

TABLE OF CONTENTS	19
Część pierwsza	
ZAGADNIENIA OGÓLNE	
Rozdział I. ŚWIAT W OBLICZU CYFRYZACJI	33
1. Globalny stan cyfrowy	33
2. Wpływ technologii na rozwój cywilizacji	38
3. Cyborgizacja człowieka	39
4. Wpływ internetu na mózg człowieka	43
5. Zalety internetu	47
Rozdział II. KOMPUTER. SIECI KOMPUTEROWE. INTERNET	55
1. Komputer i jego oprogramowanie	55
1.1. Komputery	55
1.2. Definicja komputera	57
1.3. Klasyfikacja komputerów	59
1.4. Podstawy architektury komputerów	62
2. Oprogramowanie komputerowe	67
2.1. Algorytmy, programy i dane	67
2.2. Definicja oprogramowania	72
2.3. Metody dystrybucji oprogramowania	73
2.4. Licencje na oprogramowanie	74
2.5. Systemy operacyjne	75
2.6. Sterowniki urządzeń	79
2.7. Firmware	80
2.8. Oprogramowanie użytkowe	82
3. Sieci komputerowe. Internet	83
3.1. Klasyfikacja sieci komputerowych	84
3.2. Internet	85
3.3. DNS (Domain Name System). Zasady tworzenia domen adresowych	88
3.4. Adresy urządzeń komputerowych MAC (Medium Access Control)	91
3.5. Standard kompatybilności systemowej OSI (Open Systems Interconnection)	92
3.6. Urządzenia intersieciowe	97
3.7. Usługi internetowe	99
3.7.1. Protokół HTTP	100
3.7.2. Zasoby informacji w Internecie	101
3.8. Języki skryptowe	104
3.9. Eksploracja danych	106

Rozdział III. CELE I ZADANIA KRYMINALISTYKI CYFROWEJ	109
1. Ogólne zastosowanie kryminalistyki cyfrowej	109
2. Polska procedura karna w odniesieniu do kryminalistyki cyfrowej	113
3. Nowe przepisy międzynarodowe	114
4. Inne międzynarodowe standardy	120
5. Standardy i przewodniki najlepszych praktyk w Stanach Zjednoczonych Ameryki	122
6. Standardy i przewodniki najlepszych praktyk w Wielkiej Brytanii	126

Rozdział IV. CYBERPRZESTĘPCZOŚĆ W ŚWIELE BADAŃ

STATYSTYCZNO-KRYMINOLOGICZNYCH	129
1. Wzrost cyberprzestępczości w społeczeństwie 4.0	129
2. Statystyki cyberprzestępczości na świecie	131
3. Cyberbezpieczeństwo w Europie	137
4. Cyberprzestępczość w Unii Europejskiej	138
5. Wpływ ataków cybernetycznych na państwa europejskie	139
6. Skutki naruszeń cyberbezpieczeństwa	141
6.1. Skutki finansowe	141
6.2. Szkody dla reputacji przedsiębiorstwa	143
6.3. Naruszenia prywatności i danych	144
6.4. Konsekwencje dla bezpieczeństwa narodowego	146
7. Wyzwania i trendy w obszarze cyberbezpieczeństwa	148
8. Współpraca i wymiana informacji w zakresie cyberbezpieczeństwa	149
9. Krajowe strategie cyberbezpieczeństwa w wybranych krajach	152
9.1. Niemcy	153
9.2. Wielka Brytania	153
9.3. Francja	155
9.4. Estonia	157
9.5. Indie	158
10. Cyberbezpieczeństwo w Polsce	159
11. Uwarunkowania prawne w Polsce	161
12. Statystyki dotyczące cyberbezpieczeństwa w Polsce	163
13. Specyfika cyberbezpieczeństwa w Polsce na tle Europy	166
14. Działania Federacji Rosyjskiej zakłócające wybory do Parlamentu Europejskiego w 2024 roku	169

Literatura – część I	181
-----------------------------	-----

Część druga

CYFROWE ŹRÓDŁA INFORMACJI

Rozdział V. INFORMACJA JAKO PROBLEMOWA CECZA KOMUNIKACJI	209
1. Pojęcie informacji	209
2. Ogólna klasyfikacja informacji	215
3. Stres informacyjny	220
4. Bezpieczeństwo w ujęciu informatyki	226
5. Zagrożenia technologiczne	231
Rozdział VI. SPOŁECZNOŚCIOWE SERWISY INFORMATYCZNE	234
1. Zakres serwisów informatycznych	234
2. Znaczenie mediów społecznościowych	236
3. Korzystanie z mediów społecznościowych	239
4. Efekty mediów społecznościowych	243
5. Podejście skoncentrowane na platformie	245
6. Podejście zorientowane na użytkownika	246
7. Projekt badawczy API	250
8. Projekt badawczy darowizny danych	251
9. Śledzenie projektu badawczego	251
10. Decyzja o metodzie gromadzenia cyfrowych danych	252
11. Facebook	253

11.1. Języki programowania Facebooka	255
11.2. Bezpieczeństwo informacji w Facebooku	256
12. Google	257
Rozdział VII. SZTUCZNA INTELIGENCJA	262
1. Istota sztucznej inteligencji	262
2. Technologia blockchain	268
3. Metody realizacji algorytmów uczących	271
3.1. Generowanie reguł za pomocą drzew decyzyjnych	271
3.2. Pozyskiwanie wiedzy za pomocą generowania „pokryć”	272
4. Pozyskiwanie wiedzy za pomocą sieci semantycznych	273
5. Sieci neuronowe	274
6. Model Q*	275
7. Empiryczne metody uzyskiwania informacji	277
8. Trudności w skonstruowaniu „inteligentnego” komputera	283
9. Perspektywy rozwoju maszyn przewyższających inteligencją człowieka	291
10. Sztuczna inteligencja w kryminalistyce	295
11. Rozszerzanie możliwości a granice dla funkcji celu	298
12. Polska i prace związane ze sztuczną inteligencją	300
13. Koordynacja Polityki AI	300
14. Negatywne skutki sztucznej inteligencji Microsoftu	301
14.1. Badania WIRED-u	301
14.2. Badania AlgorithmWatch i AI Forensics	305
15. Nowy akt Parlamentu Europejskiego w sprawie sztucznej inteligencji	314
15.1. Zakaz pewnych zastosowań	314
15.2. Wyjątki dla organów ścigania	314
15.3. Obowiązki dotyczące systemów wysokiego ryzyka	314
15.4. Wymogi przejrzystości	315
15.5. Kolejne kroki	315
15.6. Kontekst	315
Rozdział VIII. ELEKTRONICZNE METODY INWIGILACJI	317
1. Uwagi wstępne	317
2. Metody eksploracji danych sieci WEB	318
3. Eksploracja źródłowych danych internetowych dla potrzeb inwigilacji	322
3.1. <i>Web Semantic</i>	325
3.2. Architektura systemów eksploracji danych	330
3.2.1. Gromadzenie i przetwarzanie danych	330
3.2.2. Narzędzia <i>Data Mining</i>	331
3.2.3. <i>Oracle Data Mining (ODM)</i>	332
3.2.4. <i>SQL Server Data Mining Business Intelligence</i>	332
3.2.5. Zalety metod <i>Data/Web Mining</i>	333
3.2.6. Wady metod <i>Data/Web Mining</i>	333
4. Steganografia	334
4.1. Idea steganografii	334
4.2. Współczesne trendy rozwoju metod steganograficznych	338
4.3. Algorytmy steganografii wzorowane na łańcuchach molekuł DNA	339
4.4. Steganografia sieciowa	340
4.5. Steganografia w bezprzewodowych systemach mobilnych z rozproszonym widmem	342
4.6. Moc kryptograficzna steganogramów	344
4.7. Ilościowe miary oceny jakości steganogramów – entropia informatyczna	347
4.8. Inwigilacja przestępstw internetowych i wiarygodność dowodowa analiz steganografii	349
4.9. Wiarygodność dowodowa	351
5. Pegasus	354
6. Kontrola społeczeństwa, firm i organizacji w Chinach	358
Literatura – część II	361

PRZESTĘPCZE WYKORZYSTANIE TECHNIKI CYFROWEJ

Rozdział IX. DARK WEB JAKO ŹRÓDŁO INFORMACJI O PRZESTĘPCZOŚCI	371
1. Istota dark webu	371
2. Historia dark webu	375
3. Zawartość dark web: zalety i wady	377
3.1. Handel narkotykami	379
3.2. Pornografia	380
4. Terroryzm	383
5. Pranie pieniędzy	384
6. Zamieszanie jurysdykcyjne	385
7. Kwestie etyczne	386
8. Wspieranie wartości demokratycznych	386
9. Omijanie nadzoru	388
10. Policja w dark web	389
11. Dziennikarstwo prasowe	390
12. W stronę radykalnej krytyki kryminologicznej	390
13. Rekomendacje dotyczące polityki	391
Rozdział X. PRZESTĘPCZOŚĆ KOMPUTEROWA	394
1. Wpływ nowych technologii na przestępczość	394
2. Nowe rodzaje przestępstw	402
3. Nowe kierunki badań kryminalistycznych w świetle zagrożeń cybernetycznych	411
Rozdział XI. RODZAJE CYBERPRZESTĘPCZOŚCI	421
Rozdział XII. OGÓLNY MECHANIZM DZIAŁANIA RANSOMWARE	431
1. Początki i ewolucja oprogramowania ransomware	431
2. Fazy działania ransomware	443
3. Typowe wektory ataku i rozprzestrzeniania się	445
3.1. Złośliwe wiadomości e-mail (phishing)	445
3.2. Podatności w oprogramowaniu	447
4. Inne metody	448
5. Szyfrowanie danych	448
6. Przykłady znaczących ataków ransomware	450
6.1. Atak WannaCry na NHS (National Health Service)	450
6.2. Atak na Maersk	451
6.3. Atak na Colonial Pipeline Company	451
6.4. Atak na instytucje rządowe w Kostaryce	451
7. Przestępcze wykorzystanie ransomware	452
7.1. Ransomware jako narzędzie cyberprzestępczości	452
7.2. Wpływ na ofiary i gospodarkę	453
8. Działania po wykryciu ataku ransomware	454
9. Narzędzia i metody odzyskiwania zaszyfrowanych danych	455
10. Przypadki udanego odzyskiwania danych bez płacenia okupu	456
10.1. WannaKey	456
10.2. Petya Sector Extractor	456
10.3. TeslaDecoder	457
10.4. RannohDecryptor	457
11. Przyszłość ransomware	457
12. Rola sztucznej inteligencji i uczenia maszynowego w walce z ransomware	459
13. Przegląd technik wykrywania ransomware dla celów profilaktycznych	461
14. Strategie zapobiegania infekcjom ransomware	463
Rozdział XIII. ZŁOŚLIWE OPROGRAMOWANIE (MALWARE)	464
1. Wirus	465
2. Koń trojański	465
3. Robak	465
4. Keylogger	466

5. Spyware	466
6. Adware	466
7. Rootkit	467
8. Bot	467
Rozdział XIV. OGÓLNE UWAGI O HAKERSTWIE I ZŁYCH BOTACH	468
Rozdział XV. ZWIĄZKI PRZESTĘPCY Z OFIARĄ	477
1. Model ofiary	477
2. Relacje między ofiarą a sprawcą	488
Literatura – część III	493

Część czwarta

ZAKRES MOŻLIWOŚCI BADAWCZYCH KRYMINALISTYKI CYFROWEJ

Rozdział XVI. WPROWADZENIE DO PROBLEMATYKI METOD OPTOELEKTRONICZNYCH	511
1. Falki i funkcje skalujące	513
1.1. Falki i funkcje skalujące jednowymiarowe	513
1.1.1. Warunki analizy wielorozdzielczej	520
1.1.2. Podprzestrzeń aproksymacji.	522
1.1.3. Podprzestrzeń szczegółów	523
1.1.4. Transformata falkowa sygnałów.	527
1.1.5. Falki dwuwymiarowe	529
1.1.6. Falki w postaci krzywych β -sklejanych	531
1.1.6.1. Dyskretny algorytm analizy	533
2. Falkowy detektor krawędzi	536
2.1. Detekcja krawędzi i nieortogonalna transformata falkowa	537
2.2. Kryteria dla optymalnego dostrajania krawędzi	542
2.3. Filtr krawędzi bazujący na falkach	544
2.4. Dyskretna transformata falkowa	549
2.4.1. Dyskretna 1-D transformata falkowa	550
2.4.2. Odwrotna dyskretna transformata falkowa	552
3. Metoda falkowa detekcji krawędzi	553
3.1. Matematyczny model funkcji krawędzi	554
3.2. Całkowa transformata falkowa Haara-Gaussa	556
3.3. Cechy charakterystyczne obiektów w przestrzeni obrazowej	559
3.3.1. Momenty geometryczne	561
3.3.2. Niezmienniki i znormalizowane momenty centralne	562
3.3.3. Lokalizacja obiektów	563
3.3.4. Symulacja funkcji krawędzi rzeczywistej	565
3.4. Transformata falkowa obrazów z wykorzystaniem krzywych β -sklejanych	567
3.4.1. Detekcja i śledzenie krawędzi.	570
3.4.2. Ekstrakcja lokalnych maksimów transformaty falkowej	570
3.4.3. Śledzenie konturu	571
3.4.4. Cechy charakterystyczne linii konturowej obiektu. Deskryptory Fouriera.	572
4. Filtry i falki Gabora	573
4.1. Filtry Gabora	575
4.2. Falki Gabora	577
4.3. System segmentacji tekstury	583
4.4. Idea mikrooptycznego multifalkowego filtra	584
4.5. Proces segmentacji tekstur	586
4.6. Falkowy fraktalny wymiar	587
4.6.1. Fraktalny wymiar bazujący na falkach	589
4.6.2. Definicja wymiaru fraktala na bazie falek	589
4.6.3. Implementacja falki na rozmiarze fraktala	591
4.6.4. Macierz współwystąpień poziomów szarości	591
4.6.5. System wykrywania obiektów	592
5. Rozpoznawanie obrazów ucha z zastosowaniem transformaty falkowej	595
5.1. Proces wstępnej obróbki	595

5.2. Ekstrakcja cech charakterystycznych i klasyfikacja	596
5.3. Wyniki eksperymentu	597
6. Rozpoznawanie obrazów z filtrami korelacyjnymi	598
7. Korelacyjne rozpoznawanie obrazów	601
7.1. Klasyczny korelator	603
7.2. Falkowy korelator różnic obrazów dyfrakcyjnych	605
7.3. Znormalizowany korelator	612
7.4. Zmodyfikowany znormalizowany korelator	617
7.5. Zmodyfikowany korelator dopasowany brzegowo	618
7.6. Akustooptyczny korelator	626
Rozdział XVII. ROLA SZTUCZNYCH SIECI NEURONOWYCH W ROZPOZNAWANIU OBRAZÓW DLA CELÓW KRYMINALISTYKI	628
1. Transformata Fouriera	630
1.1. Jednowymiarowa transformata Fouriera	630
1.2. Dwuwymiarowa transformata Fouriera	630
1.3. Własności transformaty Fouriera	633
1.4. Obraz $p(x, y)$ i jego transformata Fouriera $\mathfrak{F}$	637
1.5. Rozdzielczość próbkowania	638
1.6. Dyskretna transformata Fouriera funkcji 2-D	639
1.7. Regularna maczyca danych	642
1.8. Maczyce danych o losowo ułożonej strukturze	642
1.9. Soczewka realizująca transformatę Fouriera	643
1.10. Sztuczna sieć neuronowa realizująca dyskretną transformatę Fouriera	647
2. Ekstraktory cech charakterystycznych	654
2.1. Detektor pierścieniowo-klinowy	654
2.2. Holograficzny detektor pierścieniowo-klinowy	657
2.2.1. Równoległe przetwarzanie sygnałów w zoptymalizowanym KGH	663
2.2.2. Optymalizacja holograficznego detektora pierścieniowo-klinowego	664
2.2.3. Analiza teorii zbiorów przybliżonych z dyskretnymi atrybutami	667
2.2.4. Relacja nierozróżnialności w zbiorach przybliżonych z atrybutami ciągłymi	668
2.2.5. Optymalizacja wielokryterialna	674
2.2.6. Zastosowanie zmodyfikowanej metody optymalizacji w rozpoznawaniu obrazów	677
2.3. Ekstraktor neuronowy pełniący funkcje DPK	682
3. Klasyfikacja w przestrzeni cech charakterystycznych	684
3.1. Klasyfikacja w modelu niepewności probabilistycznej	689
3.2. Sztuczne sieci neuronowe w roli klasyfikatorów	691
3.2.1. Probabilistyczne sieci neuronowe	691
3.2.2. Testowanie jakości systemu klasyfikacji	692
3.2.3. Wielowarstwowe perceptrony	697
3.3. Klasyfikator przybliżonej konfiguracji	699
4. Optoelektroniczne rozpoznawanie obrazów	704
4.1. Jednokanałowy optoelektroniczny system rozpoznania	707
4.2. Dwukanałowy optoelektroniczny system rozpoznawania obrazów	709
4.3. Neuronowe rozpoznawanie obrazów	711
4.4. Automatyczne rozpoznawanie odcisków palców w przestrzeni Fouriera	715
4.5. Algorytm różnicy uporządkowania pierścieniowego w klasyfikowaniu pism	723
5. Rozpoznawanie w przestrzeni obrazowej	725
5.1. Detekcja twarzy z wykorzystaniem sieci neuronowych	730
5.1.1. System detekcji twarzy	731
5.1.2. Łączenie pokrywających się detekcji	736
5.1.3. Arbitraż pomiędzy wieloma sieciami	737
5.1.4. Porównanie z innymi systemami	739
6. Rozpoznawanie orientacji głowy za pomocą sieci neuronowych	740
6.1. Architektura systemu	741
6.2. Sieci LLM	743
6.3. Ustalanie orientacji twarzy	744
6.4. Ekstrakcja cech z wykorzystanie filtrów Gabora	745

6.5. Dopasowywanie elipsy do segmentowanej twarzy	746
6.6. Rozpoznawanie orientacji głowy	747
7. Transformata Hougha w rozpoznawaniu obrazów	748
7.1. Podstawowe definicje obrazu rastrowego	750
7.2. Transformata Hougha w detekcji krzywych płaskich z obrazów 2-D	751
7.2.1. Transformata Hougha linii prostej	751
7.2.2. Transformata Hougha kilku linii prostych	752
7.2.3. Transformata Hougha prostej figury	753
7.2.4. Odwrotna transformata Hougha kilku linii prostych	754
7.2.5. Wykrywanie okręgów	756
7.2.6. Wykrywanie innych krzywych analitycznych płaskich	758
7.3. Grafowe metody opisu sceny	758
Rozdział XVIII. INTERNET JAKO MIEJSCE ZDARZENIA	766
1. Rozwój Internetu	766
2. Przestępcze wykorzystanie sieci internetowych	767
Rozdział XIX. PRZESZUKANIE ONLINE	773
1. Istota przeszukania <i>online</i>	774
2. Techniczna realizacja przeszukania <i>online</i>	774
Literatura – część IV	779

Część piąta

WYMIAR SPRAWIEDLIWOŚCI WOBEC PRZESTĘPCZOŚCI CYFROWEJ

Rozdział XX. DOWODY CYFROWE	799
1. Pojęcie dowodu cyfrowego	799
2. Identyfikacja dowodów cyfrowych	804
3. Analiza danych elektronicznych	815
4. Filtry danych/produktów roboczych	821
5. Swap file data	822
6. Pliki tymczasowe	822
7. Dane ukryte	823
8. Slack space	823
9. Unallocated space	825
10. Defragmentacja	825
11. Swap file/swap space	826
12. Usunięte pliki	826
13. Analiza kryminalistyczna danych internetowych	827
14. Internetowe pliki cookie	827
15. Podstawy prawne zajęcia i zabezpieczenia danych cyfrowych	828
Rozdział XXI. SĄDOWE BADANIA DOWODÓW ELEKTRONICZNYCH	841
1. Cele badań	841
2. Projekt badawczy	842
3. Metodologia badań	843
4. Przebieg badań	844
5. Dystrybucja ankiet	845
6. Kwestionariusz i uczestnicy wywiadu	845
7. Definicja dowodu cyfrowego	849
8. Znajomość procesu informatyki śledczej i ICT	850
9. Problemy sędziów z dowodem cyfrowym	852
10. Standard jakości	853
11. Cyfrowy dowód w sądzie	854
12. Podsumowanie wyników ankiety	854
13. Wyniki wywiadu	856
14. Uczestnicy wywiadu	856
15. Uwierzytelnianie dowodów cyfrowych	856
16. Uwierzytelnianie poczty elektronicznej	857
17. Uwierzytelnianie stron internetowych	858

18. Uwierzytelnianie i wpływ sieci społecznościowych	859
19. Uwierzytelnianie map Google	859
20. Rola testu Dauberta	860
21. Rola sędziów	860
22. Biegli i specjaliści	864
23. Ekspertzy zewnętrzni	865
24. Wiedza w porównaniu z innymi sędziami	866
25. E-discovery	866
26. Podsumowanie ustaleń z wywiadu	868
27. Implikacje	869
28. Plan edukacyjny	870
29. Podsumowanie	872

Rozdział XXII. ZABEZPIECZENIE DOWODÓW ELEKTRONICZNYCH 875

Rozdział XXIII. GRANICE ZASTOSOWANIA PROGRAMÓW KOMPUTEROWYCH W ODNIESIENIU DO POLITYKI KARNEJ 877

Literatura – część V 881

Część szósta

Z PRAKTYKI NAUKOWO-BADAWCZEJ KRYMINALISTYKI CYFROWEJ

Rozdział XXIV. INTELIGENTNY SYSTEM WSPOMAGANIA DECYZJI OPARTY NA ALGORYTMICZNEJ ANALIZIE OBRAZU W DZIAŁANIACH SŁUŻB WYMIARU SPRAWIEDLIWOŚCI 901

1. Wybrane zadania Służby Więziennej	901
2. Zakłócenie funkcjonowania jednostki organizacyjnej	903
2.1. Regulacje prawne	904
2.2. Zakres i definicje	905
2.3. Zakazane praktyki w zakresie sztucznej inteligencji	905
2.4. Systemy sztucznej inteligencji wysokiego ryzyka	906
2.5. Obowiązki w zakresie przejrzystości w odniesieniu do określonych systemów sztucznej inteligencji	908
3. Opis techniczny narzędzia	908
3.1. Architektura systemu	908
3.2. Opis sprzętu i oprogramowania	910
3.3. Skalowalność	913
3.4. Skuteczność	914
3.5. Funkcjonalności i parametry techniczne	915
4. Miejsce zastosowania	918
4.1. Identyfikacja miejsca instalacji narzędzia w jednostce Służby Więziennej	918
4.2. Procedura doboru rozwiązania do jednostki Służby Więziennej	919
4.3. Określenie parametrów rozwiązania w jednostce Służby Więziennej	920
4.4. Dokumentacja narzędzia w Służbie Więziennej	921
4.4.1. Dokumentacja lokalna w jednostce Służby Więziennej	921
4.4.2. Dokumentacja w Centralnym Zarządzie Służby Więziennej	921
5. Procedura instalacji narzędzia w jednostce Służby Więziennej	922
5.1. Przygotowanie konfiguracji skryptu	922
5.2. Uruchomienie usługi systemowej	923
5.3. Instalacja systemu	924
5.4. Douczanie systemu	929
5.5. Wykonywanie kopii plików wykorzystywanych w projekcie	932
6. Procedury obsługi dla poszczególnych poziomów dostępu	933
6.1. Poziom dostępu – Obserwator / Monitorowy	933
6.1.1. Praca w systemie	934
6.1.1.1. Uruchomienie systemu	935
6.1.1.2. Wylogowywanie	936
6.2. Poziom dostępu – Dowódca	936
6.2.1. Praca w systemie	937
6.2.1.1. Uruchomienie systemu	938

6.2.1.2. Przycisk „Pobierz dziennik zdarzeń”	939
6.2.1.3. Wylogowywanie	939
6.3. Poziom dostępu – Administrator systemu	939
6.3.1. Uruchomienie systemu	939
6.3.2. Praca w systemie	941
6.3.2.1. Ustawienia	941
6.3.2.2. Uruchomienie systemu	948
6.3.2.3. Wylogowywanie	949
6.4. Procedury awaryjne (reset, błędy, procedury naprawcze itp.)	949
6.5. Formatki, raporty, systemowe wzory dokumentów	950
6.6. Procedury okresowego przeglądu narzędzia	951
6.6.1. Regularne resetowanie systemu	951
6.6.2. Procedura restartu systemu	952
6.6.2.1. Serwer graficzny	952
6.6.2.2. Serwer webowy	952
6.6.3. Przeglądanie kamer	955
6.6.4. Sprawdzanie dziennika zdarzeń	955
7. Procedury aktualizacji lub douczania narzędzia	955
7.1. Przygotowanie nagrań do wprowadzenia do bazy danych narzędzia	956
7.2. Przygotowanie konfiguracji skryptu	956
7.3. Uruchomienie douczania istniejącego modelu sieci	957
7.4. Wprowadzenie scenariuszy alternatywnych do bazy więziennictwa	957
8. Opis infrastrukturalny	962
9. Oprogramowanie i kody źródłowe	962
9.1. Charakterystyka algorytmów ekstrakcji wiedzy ze strumieni wideo	962
9.2. Charakterystyka algorytmów podejmowania decyzji	963
9.3. Implementacja modułu podejmowania decyzji	963
Rozdział XXV. PRAWDZIWOŚĆ ZEZNAŃ NA PODSTAWIE ANALIZ WSKAŹNIKÓW EMOCJI	965
Rozdział XXVI. TECHNOLOGIE INFORMATYCZNE W SŁUŻBIE ANALIZY KRYMINALNEJ	974
1. Kontekst	974
2. Domeny danych	974
3. Financial Trail	975
4. Inżynieria inteligencji decyzyjnej	976
5. Technologie wizualizacji grafów w sercu rozwiązania	976
6. Otwarta architektura rozwiązania	976
7. Od dużych do małych i głębokich danych	977
8. Rozszerzenie bazy użytkowników	977
9. Matic	979
Rozdział XXVII. TELEINFORMATYCZNY MODEL WSPOMAGANIA IDENTYFIKACJI OFIAR KATASTROF I ATAKÓW TERRORYSTYCZNYCH	981
1. Protokół identyfikacji ofiar katastrof	981
2. Cele realizowane w procedurze identyfikacji masowych ofiar	982
3. Istotna rola w badaniach oględzin miejsca zdarzenia	982
4. Regulacje prawne w procedurze DVI	983
5. Schemat postępowania w przebiegu identyfikacji	983
6. Wyniki badań IDvictim	984
Rozdział XXVIII. ISWOT – SYSTEM WYKRYWANIA OSÓB UKRYTYCH W ŚRODKACH TRANSPORTU	985
1. Uwagi wprowadzające	985
2. Spełnienie osiągniętych celów, analiza czynnikowa wyników	985
3. Technologie krytyczne w projekcie ISWOT	986
4. Uzyskane wymagania funkcjonalne systemu	986
5. Podsystem chemiczny	987
6. Systemy wykrywania osób ukrytych w samochodach	989

Rozdział XXIX. MOBILNY PUNKT DYSTRYBUCYJNY INFRASTRUKTURY TELEINFORMATYCZNEJ (MPDIT)	991
Rozdział XXX. AISEARCHER	996
Literatura – część VI	1001

Część siódma

INFORMATYKA POLICYJNA

Rozdział XXXI. TECHNOLOGIA KOMPUTEROWA W SŁUŻBIE POLICJI	1007
1. Rozpowszechnienie i skuteczność technologii nadzoru	1007
2. Automatyczne czytniki tablic rejestracyjnych (Automatic License Plate Readers)	1008
3. Urządzenia do śledzenia pojazdów	1009
4. Obserwacja powietrzna	1010
5. Monitoring wizyjny	1010
6. Obserwator strzałów	1011
7. Czujniki inteligentnego domu	1012
8. Przejroczysta technologia	1013
9. Nadzór nad komunikacją	1013
10. Stingray	1014
11. Prawo nadzoru	1015
Rozdział XXXII. KRAJOWY SYSTEM INFORMACYJNY POLICJI	1016
1. Zagadnienia ogólne	1016
2. Charakterystyka KSIP	1020
3. Moduły KSIP – nowe możliwości dla Policji	1024
3.1. System wspomagania dowodzenia Policji (SWD)	1024
3.2. Podsystem POSIGRAF	1027
3.3. Aplikacja BROŃ I LICENCJE	1028
4. Aplikacja OPIS	1029
5. Aplikacja do wprowadzania i uzupełniania danych w zakresie obszaru informacyjnego RZECZ	1030
6. Aplikacja do wykonywania statystyk i typowań	1032
7. Aplikacja sprawdzenia w trybie PKR-1	1032
8. Moduł wspierający pracę dyżurnego	1033
9. AFIS	1034
10. GENOM	1034
11. BIULETYN	1035
12. Współpraca KSIP z Systemem Meldunku Informacyjnego	1035
13. Interfejsy z innymi systemami	1036
Rozdział XXXIII. SYSTEM INFORMACYJNY SCHENGEN	1037
1. Istota SIS	1037
2. Organy współpracujące z SIS	1041
3. Zakres czasowy	1042
4. Zabezpieczenia	1042
5. SIS II	1043
6. Krajowy System Informatyczny	1044
7. Biuro Międzynarodowej Współpracy Policji KGP (dawniej Biuro SIRENE)	1050
Rozdział XXXIV. MIĘDZYNARODOWA WSPÓŁPRACA POLICJI	1051
1. Współpraca policji w przeszłości	1051
2. Cele, zadania i struktura organizacyjna Interpolu	1055
3. System Interpolu do wykrywania broni i materiałów wybuchowych	1071
4. Współpraca międzynarodowa w ramach Interpolu	1073
5. Europejska współpraca policji	1082
Rozdział XXXV. KRAJOWE CENTRUM INFORMACJI KRYMINALNYCH	1087
1. Podstawy prawne	1087
2. Zadania KCIK	1089

3. Funkcje KCIK	1090
4. Opis systemu	1090
5. System bezpieczeństwa KCIK	1095
Rozdział XXXVI. INNE SYSTEMY INFORMATYKI POLICYJNEJ	1097
1. System Informacji Operacyjnych	1097
2. Elektroniczny Rejestr Czynności Dochodzeniowo-Śledczych	1100
3. System Elektronicznej Sprawozdawczości w Policji	1101
Literatura – część VII	1103

Część ósma

ZAPOBIEGANIE ZAGROŻENIOM CYWILIZACJI CYFROWEJ

Rozdział XXXVII. SYSTEMY CYBERBEZPIECZEŃSTWA W POLSCE	1109
1. Ogólne zagadnienia krajowego systemu bezpieczeństwa	1109
2. Policja wobec zagrożeń cyfrowych	1116
3. Działania strategiczne wojska w cyberprzestrzeni	1117

Rozdział XXXVIII. DZIAŁANIA UNII EUROPEJSKIEJ W ZAKRESIE CYBERBEZPIECZEŃSTWA	1119
1. Przepisy dotyczące cyberbezpieczeństwa w Unii Europejskiej	1119
2. Organizacje i instytucje cybernetyczne	1122

Rozdział XXXIX. INFORMATYKA W PROGRAMOWANIU PROFILAKTYKI KRYMINALNEJ	1127
1. Prognozowanie a tworzenie polityki: kilka nauk z makroekonomii	1127
2. Krótka historia prognozowania w sprawach wymiaru sprawiedliwości	1128
3. Teoria tworzenia polityki	1130
4. Dokładność prognoz	1131
5. Uczestnictwo w procesie tworzenia polityki	1132
6. Zapotrzebowanie na prognozy w zakresie wymiaru sprawiedliwości	1133
7. Regresja parametryczna	1135
8. Widzenie komputerowe i uczenie maszynowe	1136
9. Przestrzenne aspekty prognozowania przestępczości	1139
10. Obecnie używane technologie w dziedzinie wykrywania i przewidywania przestępstw	1145
11. Porównawcze badanie różnych metod przewidywania	1145
12. Modele widzenia komputerowego w połączeniu z technikami uczenia maszynowego i uczenia głębokiego	1146
13. Pomysł nowego oprogramowania	1148

Rozdział XL. EDUKACJA SPOŁECZEŃSTWA W ZAKRESIE BEZPIECZEŃSTWA CYFROWEGO	1151
1. Ogólna problematyka	1151
2. Badania nad zwiększeniem bezpieczeństwa komunikatorów internetowych	1158

Rozdział XLI. ZAPOBIEGANIE PRZECIĄŻENIU INFORMACYJNEMU	1160
1. Metabolizm informacyjny	1160
2. Definicja przeciążenia	1161
3. Informacyjny zalew	1162
4. Techniki informatyczne	1166
5. Popularyzacja nauki	1168
6. Cyberhigiena	1173

Rozdział XLII. ANALIZA MALWARE – JAKO DZIAŁANIE PROFILAKTYCZNE	1177
1. Analiza wirusa Avaddon	1177
1.1. Infiltracja	1178
1.2. Działanie	1179
1.3. Sposoby odzyskania danych	1179
1.4. Analiza statyczna	1179
1.5. Analiza dynamiczna	1184

1.6. Weryfikacja stanu systemu po przeprowadzonym ataku	1186
1.7. Mechanizm kryptograficzny	1189
1.8. Sposób działania wirusa	1194
2. Profilaktyczne aspekty analizy wirusa CryptXXX	1197
2.1. Analiza struktury zaszyfrowanych plików	1197
2.2. Analiza statyczna	1199
2.3. Analiza dynamiczna	1199
2.4. Sposób działania wirusa	1204
Rozdział XLIII. PRZECIWDZIAŁANIE PRZESTĘPCZOŚCI KOMPUTEROWEJ	1206
1. Metody działania hakerów	1206
2. Odpowiedzialność karna dysponentów	1209
3. Bezpieczeństwo systemów komputerowych	1211
Rozdział XLIV. OBRONA PRZED OSZUSTWAMI, FAŁSZERSTWAMI I MANIPULACJAMI W ŚWIECIE CYFROWYM	1223
1. Przygotowanie do oszustwa	1223
2. Oszustwo a manipulacja	1225
3. Anti-Phishing Working Group	1231
4. Oszustwa loteryjne	1234
5. Oszustwa nigeryjskie	1235
6. Oszustwa matrymonialne	1235
7. Oszustwa domenowe	1235
8. Oszustwa firm reklamowych i agencji interaktywnych	1236
9. Oszustwa w portalach społecznościowych	1236
10. Fałszywe oferty pracy	1236
11. Oszustwa związane z telemarketingiem	1237
12. Oszustwa SMS-owe	1237
13. Oszustwa mailingowe	1238
14. Fałszerstwa i oszustwa jako zagrożenie bezpieczeństwa	1238
Literatura – część VIII	1245
Wykaz terminów angielskich z zakresu kryminalistyki cyfrowej	1263