

Spis treści

Wstęp.....	9
-------------------	----------

Rozdział 1

Powstanie i rozwój technologii oraz systemów komputerowych.....	11
--	-----------

1.1. Historia i rozwój komputerów oraz sieci komputerowych	11
1.2. Znaczenie protokołu TCP/IP i jego pochodnych dla działania sieci komputerowych.....	22
1.3. Pierwsze regulacje prawne w zakresie zwalczania cyberprzestępczości.....	25

Rozdział 2

Ogólna charakterystyka przestępczości komputerowej	35
---	-----------

2.1. Rozwój i charakterystyka przestępczości komputerowej	35
2.2. Klasyfikacja przestępstw komputerowych	44

Rozdział 3

Regulacje prawne w przedmiocie ochrony praw autorskich i informacji.....	53
---	-----------

3.1. Ochrona praw do programów komputerowych	53
3.2. Regulacje prawne w zakresie powielania topografii układów scalonych	61
3.3. Rozwiązania prawne w zakresie karalności sprawców przestępstw komputerowych w Polsce	63

Rozdział 4

Ochrona obrotu gospodarczego	89
---	-----------

4.1. Zagadnienia ogólne	89
4.2. Definicja i przesłanki jej kształtowania.....	90
4.3. Przestępczość gospodarcza w środowisku komputerowym	91
4.4. Odpowiedzialność sprawcy w polskim systemie prawnym.....	96

4.5. Oszustwo komputerowe	103
4.6. Oszustwo telekomunikacyjne	110
4.7. Fałszerstwo komputerowe.....	115
4.8. Kradzież czasu pracy komputera	124

Rozdział 5

Techniki popełniania przestępstw z wykorzystaniem komputera	127
5.1. Atak komputerowy.....	127
5.2. Niszczenie danych i programów komputerowych.....	138
5.3. Sabotaż i szantaż komputerowy.....	151
5.4. Nieuprawnione wejście do systemu komputerowego.....	155
5.5. Podśluch komputerowy	170
5.6. Szpiegostwo komputerowe	177
5.7. Cyberterrozym	182

Rozdział 6

Metodyka ujawniania i zwalczania przestępstw komputerowych.....	185
6.1. Ujawnianie przestępstw komputerowych i gospodarczych.....	185
6.2. Źródła pierwszych informacji o przestępstwie	186
6.3. Reakcja organów ścigania na zawiadomienie o popełnieniu przestępstwa.....	188
6.4. Formy i cele postępowania.....	190
6.4.1. Czynności sprawdzające.....	190
6.4.2. Dochodzenie w niezbędnym zakresie	191
6.4.3. Dochodzenie w sprawach o przestępstwa komputerowe i pranie brudnych pieniędzy	193
6.4.4. Śledztwo w sprawach o przestępstwa komputerowe	196
6.5. Zabezpieczenie miejsca zdarzenia	198
6.6. Oględziny – ujawnianie i zabezpieczanie śladów	200
6.7. Przeszukanie i zabezpieczenie dowodów przestępstwa	201
6.7.1. Organizacja i zasady działania grupy operacyjno-rozpoznawczej.....	201
6.7.2. Poszukiwanie narzędzi i środków służących popełnieniu przestępstwa	202
6.7.2.1. Przygotowanie przeszukania.....	203
6.7.2.2. Przeszukanie miejsca zdarzenia	207
6.7.2.3. Przeszukanie przestrzeni komputera.....	208
6.7.2.4. Czynności końcowe	210

6.8. Przesłuchanie świadków i uprawnienia pokrzywdzonych	211
6.8.1. Stadia i taktyka przesłuchania świadków	211
6.8.2. Problematyka zeznań świadka – zestaw pytań	212
6.8.3. Uprawnienia pokrzywdzonych	213
6.9. Biegli i ekspertyzy	214
6.9.1. Biegły jako opiniodawca lub konsultant	214
6.9.2. Rola ekspertyzy kryminalistycznej i wiadomości specjalnych	216
6.9.3. Schemat ekspertyzy	216
6.9.4. Rodzaje ekspertyz	217
6.10. Czynności operacyjno-rozpoznawcze	220
6.11. Przesłuchanie podejrzanego	224
6.12. Okazanie osób i rzeczy	226
6.13. Konfrontacja	227
6.14. Zatrzymanie podejrzanego	228
6.15. Eksperyment procesowo-kryminalistyczny	230
6.16. Wniesienie aktu oskarżenia	231

Rozdział 7

Sprawca przestępstwa komputerowego	235
---	------------

Rozdział 8

Zapobieganie przestępczości komputerowej	251
---	------------

8.1. Przeciwdziałanie piractwu komputerowemu	251
8.2. Prawne podstawy modelu zwalczania przestępczości komputerowej	267
8.3. Techniczno-organizacyjne podstawy modelu zwalczania przestępczości komputerowej	278

Wnioski	291
----------------------	------------

Bibliografia	299
---------------------------	------------

Słowniczek pojęć informatycznych	317
---	------------

Wykaz skrótów	323
----------------------------	------------