

Spis treści

Wykaz skrótów	11
Przedmowa	17
ROZDZIAŁ I	
Wpływ najnowszych technologii na ewolucję przestępczości oraz ich znaczenie w ujęciu kryminalistycznym i procesowym. Sztuczna inteligencja oraz ataki z wykorzystaniem złośliwego oprogramowania (phishing, spoofing, ransomware)	21
Patryk Zięba, Wojciech Kozłowski	
1.1. Wprowadzenie	21
1.2. AI oraz technika łączenia obrazów typu deepfake	22
1.2.1. AI – Artificial Intelligence	22
1.2.2. Technika łączenia obrazów typu deepfake	29
1.3. Phishing, spoofing, ransomware	31
1.3.1. Phishing	31
1.3.2. Spoofing	38
1.3.3. Ransomware	42
1.4. Zakończenie	46
Bibliografia	48

ROZDZIAŁ II

Phishing w polskim prawie karnym. Analiza wraz z oceną skuteczności regulacji w zwalczaniu przestępstw polegających na podszywaniu się i wyludzaniu danych z instrumentalnym wykorzystaniem sieci i systemów teleinformatycznych na gruncie art. 286 § 1 KK, art. 287 § 1 KK oraz art. 190a § 2 KK	52
--	----

Aneta Fraser, Maciej Pająk

2.1. Wprowadzenie	52
2.2. Phishing – charakterystyka i skala zjawiska	55
2.2.1. Aspekty techniczne zjawiska phishingu – terminologia	55
2.2.2. Liczba popełnianych cyberoszustw – skala zjawiska phishingu	59
2.3. Cyberoszustwo – perspektywa unijna i krajowa	62
2.3.1. Cyberoszustwo – perspektywa unijna	62
2.3.2. Cyberoszustwo (art. 286 § 1 KK i art. 287 § 1 KK) – perspektywa krajowa	66
2.4. Podszywanie się, kradzież tożsamości – perspektywa krajowa	71
2.5. Zakończenie	82
Bibliografia	84

ROZDZIAŁ III

Prawnokarna ochrona przed przestępstwami motywowanymi nienawiścią popełnianymi w Internecie w świetle przepisów obowiązujących oraz planowanej nowelizacji	89
--	----

Mateusz Kazanowski, Aleksander Panasiuk

3.1. Wprowadzenie	89
3.2. Przestępstwa z nienawiści	90
3.3. Rozszerzenie ochrony prawnokarnej na dodatkowe kryteria dyskryminacyjne	95
3.4. Realizacja międzynarodowych standardów ścigania przestępstw z nienawiści	101
3.5. Nienawiść w świecie cyfrowym	105
3.6. Zakończenie	111
Bibliografia	113

ROZDZIAŁ IV

Cyberatak na infrastrukturę krytyczną jako przestępstwo o charakterze terrorystycznym	118
---	-----

Zuzanna Grześkowiak

4.1. Wprowadzenie	118
4.2. Istota terroryzmu i cyberterroryzmu	120
4.3. Przestępstwo o charakterze terrorystycznym	124

4.4. Cyberprzestępstwo o charakterze terrorystycznym	127
4.5. Rodzaje cyberataków na infrastrukturę krytyczną i ich kwalifikacja prawna	130
4.6. Zakończenie	136
Bibliografia	137

ROZDZIAŁ V

Przymusowe odblokowywanie informatycznych nośników danych, Biometria i tradycyjne metody autoryzacji	140
Damian Robert Jaworski	
5.1. Wprowadzenie	140
5.2. <i>Right to Digital Silence</i>	142
5.3. Prawa i obowiązki wybranych uczestników postępowania karnego	149
5.4. Przymuszenie do odblokowania urządzenia przy użyciu metody pamięciowej	155
5.5. Przymuszenie do odblokowania urządzenia przy użyciu metody biometrycznej	156
5.6. Wykorzystanie zwłok do odblokowania informatycznego nośnika danych	158
5.7. Konsekwencje dowodowe	159
5.8. Aktualne możliwości „ominięcia” zakazu oraz wniosek <i>de lege ferenda</i>	161
5.9. Zakończenie	165
Bibliografia	168

ROZDZIAŁ VI

Kryminalistyczna analiza podpisu biometrycznego oraz określenie wieku dokumentów kwestionowanych - wybrane możliwości badawcze	171
Jerzy Utrata, Mateusz Kowalcze	
6.1. Wprowadzenie	171
6.2. Zagadnienia podstawowe	172
6.3. Możliwości analizy podpisów biometrycznych	174
6.3.1. Pismo ręczne i odręczny podpis wystawcy dokumentu	174
6.3.2. Graficzno-porównawcza metoda analizy pisma ręcznego	176
6.3.3. Podpis elektroniczny i jego rodzaje	177
6.3.4. Podpis biometryczny i możliwości jego analizy	178
6.4. Możliwości określenia bezwzględnego wieku dokumentu	180
6.4.1. Szacowanie zapisów długopisowych metodą Walerego Agińskiego	181
6.4.2. Ograniczenia metody szacowania zapisów długopisowych Walerego Agińskiego	181

6.5. Możliwości określenia względnego wieku dokumentu	183
6.5.1. Nieniszczące metody określenia względnego wieku dokumentu	184
6.5.2. Niszczące metody określenia względnego wieku dokumentu	186
6.6. Zakończenie	187
Bibliografia	189

ROZDZIAŁ VII

Dostęp do informacji objętych tajemnicą bankową jako instrument zwalczania cyberprzestępczości – aktualne problemy i propozycje zmian	191
Piotr Preneta	
7.1. Wprowadzenie	191
7.2. Kompetencje prokuratora do pozyskania informacji objętych tajemnicą bankową	193
7.3. Uprawnienia finansowych organów postępowania przygotowawczego	204
7.4. Przeszukanie zdalne rachunku bankowego	207
7.5. Zakończenie	208
Bibliografia	210

ROZDZIAŁ VIII

Potrzeba systemowej regulacji czynności operacyjno-rozpoznawczych – analiza projektu ustawy z roku 2008 w kontekście aktualnych wyzwań społecznych i technologicznych	213
Kornelia Gilarska, Mateusz Kazanowski, Natalia Kostera	
8.1. Wprowadzenie	213
8.2. Geneza i cel projektu	217
8.3. Projekt ustawy a ingerencja w prawa człowieka	221
8.4. Kontratyp czynności operacyjno-rozpoznawczych	225
8.5. Perspektywy na przyszłość	229
8.6. Zakończenie	231
Bibliografia	233

ROZDZIAŁ IX

Wykorzystanie instytucji wspólnych zespołów śledczych (Joint Investigation Teams – JIT) w zwalczaniu zorganizowanej cyberprzestępczości	237
Monika Świrta	
9.1. Wprowadzenie	237
9.2. Charakterystyka wspólnych zespołów śledczych działających przy zaangażowaniu Eurojust	239
9.3. Powołanie i ogólne zasady funkcjonowania wspólnego zespołu śledczego działającego przy zaangażowaniu Eurojust	242
9.4. Korzyści wynikające z instytucji wspólnych zespołów śledczych działających przy zaangażowaniu Eurojust	248
9.5. Wady wynikające z instytucji wspólnych zespołów śledczych działających przy zaangażowaniu Eurojust	251
9.6. Wspólny zespół śledczy a zwalczanie zorganizowanej międzynarodowej cyberprzestępczości	253
9.7. Zakończenie	256
Bibliografia	258

ROZDZIAŁ X

Przeprowadzenie posiedzenia jawnego przy użyciu urządzeń technicznych umożliwiających jego przeprowadzenie na odległość w postępowaniu cywilnym – aspekty normatywne i praktyczne	260
Kamil Nahler	
10.1. Wprowadzenie	260
10.2. Zagadnienia podstawowe – geneza, przesłanki stosowania, ryzyka związane z wyznaczeniem rozprawy w formie zdalnej	261
10.3. Zagadnienia systemowo-proceduralne	265
10.4. Zagadnienia szczegółowo-proceduralne	267
10.5. Zakończenie	272
Bibliografia	273

O autorach	275
------------	-----