

SPIS TREŚCI

Wykaz skrótów	13
Wstęp	17

ROZDZIAŁ I

Ogólna charakterystyka zjawiska i kategoryzacja oszustw w handlu internetowym oraz bankowości elektronicznej	27
1. Wprowadzenie do problematyki	27
2. Pojęcie i charakterystyka oszustw w handlu internetowym i bankowości elektronicznej	38
2.1. Klasyfikacja sposobów oszustw	41
2.2. Pojęcie oszustwa w ujęciu prawnoporównawczym	46
2.3. Pojęcie oszustwa komputerowego w ujęciu komparatystycznym (modele odpowiedzialności)	55
2.4. Pojęcie oszustwa na gruncie polskiego ustawodawstwa	61
2.5. Oszustwo tożsamościowe a kradzież tożsamości	64
2.6. Oszustwa i inne przestępstwa związane z kartami płatniczymi	68
3. Kryminologiczny obraz zjawiska	71
3.1. <i>Modus operandi</i> sprawców	74
3.2. Charakterystyka sprawcy	86
3.3. Statystyczne ujęcie rozmiarów przestępczości	93
3.4. Rozpoznane zagrożenia w Polsce	99
4. Metody przeciwdziałania zagrożeniom związanym z oszustwami i innymi przestępstwami w handlu internetowym i bankowości elektronicznej	108
4.1. Inicjatywy legislacyjne w zakresie karalności i przeciwdziałania oszustwom w Internecie i przestępstwom związanym z elektronicznymi środkami płatniczymi	108
4.2. Systemy autoryzacji transakcji płatniczych oraz pozaprawnokarne środki przeciwdziałania i profilaktyki	118
5. Wnioski	124

ROZDZIAŁ II

Karnoprawna reakcja na zjawisko oszustw w handlu internetowym	129
1. Konstrukcja przestępstwa klasycznego oszustwa	129
1.1. Przedmiot ochrony	130
1.2. Strona przedmiotowa	135
1.2.1. Wprowadzenie w błąd, wyzyskanie błędu lub niezdolności do należytego pojmowania	135
1.2.2. Niekorzystne rozporządzenie mieniem	140
1.2.3. Rola pokrzywdzonego	148
1.2.3.1. Posiadacz konta	152
1.2.3.2. Wierzyciel (np. sprzedawca lub dostawcy usług)	155
1.2.3.3. Bank dłużnika	159
1.3. Podmiot i znamiona strony podmiotowej	162
1.4. Zbieg przepisów ustawy karnej i przestępstw	166
1.5. Sankcja karna	171
2. Konstrukcja przestępstwa oszustwa komputerowego	173
2.1. Przedmiot ochrony	174
2.2. Znamiona strony przedmiotowej czynu zabronionego	175
2.2.1. Znamiona określające czynność sprawczą	175
2.2.1.1. Wpływanie na proces automatycznego gromadzenia, przetwarzania i gromadzenia danych informatycznych	177
2.2.1.2. Zmianie, usuwanie i dodawanie nowych zapisów danych informatycznych	181
2.2.2. Klauzula normatywna „bez upoważnienia”	190
2.2.2.1. Wykładnia związana z klasycznym oszustwem	193
2.2.2.2. Wykładnia autonomiczna	197
2.2.2.3. Krytyka wykładni autonomicznej	199
2.3. Podmiot przestępstwa i strona podmiotowa	206
2.4. Skutek oszustwa komputerowego	208
2.5. Zbieg przepisów ustawy karnej i przestępstw	212
2.6. Sankcja karna i tryb ścigania	217
3. Wnioski	218

ROZDZIAŁ III

Karnoprawna reakcja na zjawisko oszustw i innych związanych z nimi przestępstw w bankowości elektronicznej	221
1. Karnoprawna reakcja na przypadek wykorzystania cudzej karty płatniczej oraz karty wirtualnej – uwagi wprowadzające	221
1.1. Wykorzystanie karty płatniczej przez nieupoważnionego trzeciego w celu wypłaty pieniędzy z bankomatu	228
1.1.1. Kradzież karty płatniczej	228
1.1.1.1. Kradzież karty uprawniającej do podjęcia gotówki z automatu bankowego	228
1.1.1.2. Kradzież karty płatniczej niebędącej kartą uprawniającą wyłącznie do podjęcia gotówki z automatu bankowego	237
1.1.2. Karnoprawna reakcja na wypłatę pieniędzy z bankomatu ...	242
1.1.2.1. Przesłępstwo kradzieży	242
1.1.2.2. Przesłępstwo przywłaszczenia	246
1.1.2.3. Nadużycie zaufania (przesłępstwo niegospodarności)	250
1.1.2.4. Oszustwo na szkodę właściciela konta	254
1.1.2.5. Fałszerstwo dokumentu	255
1.1.3. Wnioski	258
1.2. Wykorzystanie cudzej karty płatniczej do zapłaty w terminalach POS i w Internecie	259
1.2.1. Wykorzystanie karty przez osobę nieupoważnioną	260
1.2.2. Nadużycie karty przez osobę trzecią, która otrzymała ją w dobrej wierze	263
1.2.2.1. Wykorzystanie karty zgodnie z wolą posiadacza karty	263
1.2.2.2. Wykorzystanie karty wbrew woli posiadacza karty	264
1.2.3. Wnioski	269
2. Karnoprawna reakcja na przypadek nadużycia karty płatniczej przez jej posiadacza	271
2.1. Przesłępstwo kradzieży i przywłaszczenia	271
2.2. Przesłępstwo nadużycia zaufania	278
2.3. Oszustwo klasyczne	280
2.4. Oszustwo komputerowe	283
2.5. Zaniechanie powiadomienia	285
2.6. Wnioski	287
3. Podsumowanie	290

ROZDZIAŁ IV

Karalność przygotowania do oszustwa i innych związanych z nim przestępstw w handlu internetowym i bankowości elektronicznej	292
Uwagi wprowadzające	292
1. Poszczególne etapy zamachu na poufność i bezpieczeństwo informacji przetwarzanych w systemach komputerowych	294
1.1. Zbieranie informacji i nielegalny podsłuch komputerowy	294
1.1.1. Skanowanie portów i wyszukiwanie błędów lub podatności systemowych	295
1.1.2. Przechwytywanie komunikacji pomiędzy dwoma stronami	297
1.1.3. Phishing i pharming	298
1.1.4. Narzędzia wykorzystywane w celu zbierania informacji	303
1.2. Uzyskiwanie dostępu do systemu komputerowego	310
1.2.1. Łamanie haseł	310
1.2.2. Łamanie zabezpieczeń stron internetowych	311
1.2.3. Przechwycenie sesji użytkownika (Session Hijacking)	313
1.3. Ukrywanie śladów ataku	313
2. Kryminalizacja czynów będących <i>de facto</i> przygotowaniem do przestępstwa oszustwa jako osobne przestępstwo	315
2.1. Zbieranie informacji i uzyskiwanie dostępu do systemu komputerowego	316
2.1.1. Nielegalny dostęp do systemu komputerowego (267 § 1 k.k.)	317
2.1.1.1. Pojęcie informacji i danych komputerowych	320
2.1.1.2. Pojęcie sieci telekomunikacyjnej	323
2.1.1.3. Warunek zabezpieczenia informacji	324
2.1.1.4. Warunek naruszenia lub ominięcia zabezpieczeń chroniących informacje oraz „uzyskania dostępu do informacji”	331
2.1.2. Uzyskanie dostępu do systemu informatycznego (art. 267 § 2)	334
2.1.3. Nieuprawniona ingerencja w dane i system	336
2.2. Keylogging i nielegalny podsłuch komputerowy	338
2.2.1. Naruszenie tajemnicy komunikacji (art. 267 § 3)	338
2.2.2. Wytwarzanie, sprzedaż, oferowanie, posiadanie etc. „narzędzi hackerskich” (art. 269b)	341
2.3. Phishing i pharming	345
2.3.1. Phishing z wykorzystaniem formularza przesłanego mailem	346

2.3.1.1. Nielegalny dostęp do systemu komputerowego (267 § 1 k.k.)	347
2.3.1.2. Narzędzia hackerskie (art. 269b k.k.)	352
2.3.1.3. Fałszerstwo dokumentu	353
2.3.1.4. Niedozwolone przetwarzanie danych osobowych	358
2.3.2. Phishing z wykorzystaniem sfałszowanej strony internetowej	359
2.3.2.1. Fałszerstwo dokumentu	359
2.3.2.2. Nielegalny podsłuch komputerowy	361
2.3.2.3. Narzędzia hackerskie	363
2.3.2.4. Kradzież tożsamości	363
2.3.3. Pharming	364
2.3.3.1. Uszkodzenie i zamiana danych informatycznych	365
2.3.3.2. Nielegalny podsłuch komputerowy	366
2.3.3.2. Nielegalne uzyskanie dostępu do całości lub części systemu informatycznego	367
2.3.3.4. Fałszerstwo dokumentu	367
3. Karalność przygotowania do przestępstw związanych z kartami płatniczymi	369
3.1. Fałszerstwo karty płatniczej	369
3.2. Fałszerstwo wirtualnych pieniędzy i kart wirtualnych	371
4. Wnioski	375
Zakończenie	380
Bibliografia	385