

Cyberbezpieczeństwo : zarys wykładu / redakcja naukowa Cezary Banasiński ; poszczególne rozdziały napisali: Cezary Banasiński, Cezary Błaszczuk, Jacek M. Chmielewski, Władysław Hydzik, Dariusz Jagiełło, Zuzanna Krauzowicz, Filip Krzyżankiewicz, Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak, Adam Szafranski, Ryszard Szpyra, Kazimierz Waćkowski, Paweł Widawski, Joanna Worona-Vlugt, Zofia Zawadzka. – Wydanie 2, stan prawny na 14 sierpnia 2023 r. – Warszawa, 2023

Spis treści

WYKAZ SKRÓTÓW	13
WSTĘP	19
CZĘŚĆ I	
WPROWADZENIE DO PROBLEMATYKI CYBERBEZPIECZEŃSTWA	
ROZDZIAŁ I	
PODSTAWOWE POJĘCIA I PODSTAWY PRAWNE BEZPIECZEŃSTWA W CYBERPRZESTRZENI	25
1. Pojęcia cyberbezpieczeństwa i cyberprzestrzeni	25
1.1. Wprowadzenie	25
1.2. Pojęcie cyberprzestrzeni	27
1.3. Pojęcie cyberbezpieczeństwa	31
2. Cyberbezpieczeństwo jako przedmiot badań	37
3. Podstawy prawne cyberbezpieczeństwa	42
3.1. Regulacje cyberbezpieczeństwa w działalności ONZ	42
3.2. Inicjatywy legislacyjne Rady Europy	47
3.3. Dorobek prawny Unii Europejskiej	49
ROZDZIAŁ II	
TECHNOLOGIE TELEINFORMATYCZNE - PODSTAWY, ROZWÓJ I BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH	74
1. Wprowadzenie	74
2. Podejście usługowe w metodykach COBIT' i ITIL"	76
3. Kilka słów o bezpieczeństwie operacyjnym organizacji	78
4. Modele sieciowe	84
4.1. Model ISO OSI	84
4.2. Porównanie modelu ISO/OSI z modelem TCP/IP	88
5. Klasyfikacja ataków sieciowych według modelu ISO/OSI	90
5.1. Ataki w 2. warstwie łącza danych	90
5.2. Ataki w 3. warstwie sieciowej	94
5.3. Ataki w 4. warstwie transportowej	97
5.4. Ataki w 7. warstwie aplikacji	98
5.5. Podsumowanie klasyfikacji ataków wg warstw ISO/OSI	102
6. Firewall podstawowym elementem chroniącym sieć komputerową	103
7. Historia eskalacji zagrożeń w cyberprzestrzeni	109
8. Dedykowany atak APT/TPT	111

9. Ataki APT na infrastrukturę krytyczną, szczególnie energetyczną państw	116
9.1. Czynniki wpływające na podatność infrastruktury energetycznej na cyberataki	117
9.2. Przykłady ataków APT na sektory energetyczne państw	119
9.2.1. Ataki na elektrownie w USA, Turcji i Szwajcarii w 2017 r.	119
9.2.2. Infrastruktura krytyczna wschodniej flanki NATO i Ukrainy w latach 2021/2022	120
9.3. Sytuacja w polskiej cyberprzestrzeni po 14.02.2022 r.	123
9.4. Ataki na instytucje rządowe, dezinformacja społeczeństw i ingerencje w wybory	125
9.4.1. Wzrost liczby ataków na sektory rządowe państw	125
9.4.2. Dezinformacja w sieci	127
9.4.3. Atak grupy prorosyjskich hakerów Killnet na Włochy	127
9.4.4. Atak grupy hakywistów Anonymous	128
9.4.5. Przykład ataku phishingowego w Polsce na Krajową Radę Komorniczą	128
10. Stopnie alarmowe CRP obowiązujące na terytorium Polski	132
11. Architektura zerowego zaufania	134
12. Planowanie architektury korporacyjnej (organizacji) z cyberbezpieczeństwem	134
13. Ontologia „Siatka Zachmana”	143
14. Geneza powstania siatki SABSA	160
15. Podsumowanie	167

CZĘŚĆ II

CYBERBEZPIECZEŃSTWO PAŃSTWA

ROZDZIAŁ III

EUROPEJSKI I KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA 175

1. Podstawy ustrojowe europejskiego cyberbezpieczeństwa	175
2. Dyrektywa NIS	179
3. Dyrektywa NIS 2	185
4. Organizacja krajowego systemu cyberbezpieczeństwa	191

ROZDZIAŁ IV

OCHRONA INFRASTRUKTURY KRYTYCZNEJ W CYBERPRZESTRZENI 208

1. Zagrożenia i ryzyka	208
2. Cztery kroki analizy i oceny sytuacji	218
2.1. Hiperboliczna mapa internetu	218
2.2. Model OSI	220
2.3. Matryca cyberbezpieczeństwa	222
2.4. Kompetencje	225
2.5. Cykl życia systemów	228
3. Technologie kwantowe a nowe spojrzenie na problematykę cyberbezpieczeństwa	228
3.1. Komputer kwantowy - zagrożenie dla cyberbezpieczeństwa	230
3.2. Algorytm asymetryczny	231
3.3. Algorytmy symetryczne	232
3.4. Algorytmy hybrydowe	233

3.5. Kryptografia postkwantowa i kwantowa	235
4. Podsumowanie	239

ROZDZIAŁ V

CYBERBEZPIECZEŃSTWO W ŁĄCZNOŚCI ELEKTRONICZNEJ 241

1. Uwagi wprowadzające	241
2. Wielopłaszczyznowość problematyki ochrony łączności elektronicznej	244
3. Ochrona łączności elektronicznej w prawie Unii Europejskiej	246
3.1. Podstawowe regulacje	246
3.2. Zagadnienia węzłowe prawa łączności elektronicznej	254
3.2.1. Poufność transmisji	254
3.2.2. Bezpieczeństwo sieci i usług	257
3.2.3. Ochrona przed niezamówionymi informacjami handlowymi i spamem	259
4. Płaszczyzna przepisów krajowych	261
5. Oczekiwane kierunki zmian w prawodawstwie	266

ROZDZIAŁ VI

CYBERBEZPIECZEŃSTWO I CYBERAKTYWNOŚĆ MILITARNA 268

1. Geneza i istota zjawiska	268
2. Współczesne rozumienie cyberbezpieczeństwa w naukach społecznych	270
3. Ewolucja wojskowego myślenia o cyberbezpieczeństwie i cyberoperacjach militarnych	275
3.1. Stany Zjednoczone	275
3.2. NATO	282
4. Współczesne koncepcje doktrynalne cyberwalki - wybrane przykłady	284
4.1. Militarne operacje w cyberprzestrzeni i poprzez cyberprzestrzeń	287
4.2. Bezpieczeństwo sieci informacyjnych nienależących do Departamentu Obrony	289
5. Kognitywna sfera cyberzagrożeń	290
5.1. Rosyjskie poglądy na wojnę informacyjną	290
5.2. Chińskie poglądy na walkę informacyjną	293
5.3. Walka w sferze poznawczej (Cognitive Warfare)	297
6. Przyszłość	299

CZĘŚĆ III

CYBERBEZPIECZEŃSTWO W PRAWIE GOSPODARCZYM

ROZDZIAŁ VII

PROWADZENIE DZIAŁALNOŚCI GOSPODARCZEJ

W CYBERPRZESTRZENI 305

1. Wstęp	305
1.1. Pojęcie prawa gospodarczego	305
1.2. Zasady i źródła prawa gospodarczego	307
1.3. Prawo gospodarcze a cyberprzestrzeń i cyberbezpieczeństwo	308
2. Prawo gospodarcze a prawo autorskie	309
2.1. Podstawowe informacje	309
2.2. Prawo autorskie w internecie	311
2.3. Odpowiedzialność cywilna za naruszenie praw autorskich	314
2.4. Uwagi końcowe	316

3. Zawieranie umów a cyberprzestrzeń	317
3.1. Zagadnienia ogólne	317
3.2. Oświadczenia woli	319
3.3. Formy czynności prawnych	322
3.4. Sposób i okoliczności zawarcia umowy	328
4. Wybrane umowy związane z cyberprzestrzenią i cyberbezpieczeństwem	333
4.1. Wprowadzenie	333
4.2. Umowa licencyjna	334
4.3. Umowa o świadczenie usług drogą elektroniczną	341
4.4. Umowa o rejestrację domeny internetowej	345
4.5. Umowa sprzedaży przez internet	349
4.6. Umowa o świadczenie usług telekomunikacyjnych	352

ROZDZIAŁ VIII

CYBERBEZPIECZEŃSTWO Z PERSPEKTYWY PRZEDSIĘBIORCY 356

1. Uwagi wprowadzające	356
2. Źródła wymagań w obszarze cyberbezpieczeństwa	359
3. Model zarządzania bezpieczeństwem IT według normy ISO/IEC 27001	362
3.1. Historia standaryzacji w obszarze systemów zarządzania bezpieczeństwem informacji	362
3.2. Rodzina norm ISO/IEC 27000	363
3.3. Ramowy model SZBI	364
3.4. Procesowe zarządzanie bezpieczeństwem (PDCA)	366
3.5. Katalog zabezpieczeń	368
4. Model zarządzania cyberbezpieczeństwem według normy ISO/IEC 27032	369
5. Inne schematy zarządzania cyberbezpieczeństwem	372
5.1. Wytyczne i rekomendacje instytucji Unii Europejskiej (ENISA)	373
5.2. Wytyczne i rekomendacje publikowane w Stanach Zjednoczonych	375
6. Podsumowanie	378

ROZDZIAŁ IX

ZARZĄDZANIE RYZYKIEM W CELU ZAGWARANTOWANIA CYBERBEZPIECZEŃSTWA

379

1. Wprowadzenie	379
2. Terminologia i spektrum zarządzania ryzykiem IT	380
3. Modelowanie zarządzania ryzykiem IT	383
3.1. Ramowa struktura zarządzania ryzykiem IT	383
3.2. Rejestr ryzyka	386
3.3. Kontekst	386
3.4. Opis modelu Bow-Tie	387
3.5. Koncepcja oceny ryzyka	387
3.6. Zdarzenia ryzyka i krajobraz zagrożeń	390
3.7. Konsekwencje	391
3.8. Środki kontroli	392
3.9. Ocena ryzyka wrodzonego i rezydualnego	392
3.10. Plany postępowania z ryzykiem	393
4. Podsumowanie	393

ROZDZIAŁ X

CYBERBEZPIECZEŃSTWO W USŁUGACH PŁATNICZYCH 394

1. Wstęp - znaczenie bezpieczeństwa w świadczeniu usług płatniczych	394
2. Model odpowiedzialności dostawcy usług płatniczych i użytkownika za nieautoryzowane transakcje płatnicze	400
3. Zarządzanie ryzykami operacyjnymi i ryzykami dla bezpieczeństwa w wytycznych Europejskiego Urzędu Nadzoru Bankowego i rekomendacji Komisji Nadzoru Finansowego	402
4. Bezpieczeństwo świadczenia usług płatniczych w ustawie o usługach płatniczych	404
5. Model zgłaszania incydentów	404
6. Silne uwierzytelnienie klienta	405
6.1. Wyłączenia względem stosowania silnego uwierzytelnienia klienta	408
6.2. Analiza ryzyka transakcji	409
6.3. Płatności zbliżeniowe	410
6.4. Opłaty za transport i parking	410
6.5. Zaufani odbiorcy płatności i transakcje powtarzające się	410
6.6. Transakcje o niskiej wartości	411
6.7. Wyłączenia dla usługi dostępu do informacji na rachunku płatniczym	411
6.8. Monitoring transakcji	411
7. Poufność i integralność indywidualnych danych uwierzytelniających użytkowników usług płatniczych	412
8. Wymogi dotyczące powszechnej i bezpiecznej komunikacji	414
9. Rozporządzenie DORA - nowe, horyzontalne podejście do cyberbezpieczeństwa w sektorze finansowym	417
9.1. Wstęp	417
9.2. Zakres przedmiotowy i podmiotowy rozporządzenia DORA	419
9.3. Zarządzanie ryzykiem związanym z ICT	420
9.4. Strategia operacyjnej odporności cyfrowej	425
9.5. Zarządzanie incydentami związanymi z ICT, ich klasyfikacja i zgłaszanie	426
9.5.1. Klasyfikacja incydentów	428
9.5.2. Zgłaszanie incydentów	428
9.6. Testowanie operacyjnej odporności cyfrowej	429
9.7. Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT	431

ROZDZIAŁ XI

CYBERBEZPIECZEŃSTWO W PRAWIE WŁASNOŚCI INTELEKTUALNEJ 433

1. Wprowadzenie	433
2. Pojęcie własności intelektualnej	433
3. Prawo autorskie i prawa pokrewne	435
3.1. Prawo autorskie	435
3.1.1. Programy komputerowe	437
3.2. Prawa pokrewne	438
4. Prawo własności przemysłowej	438
4.1. Prawo patentowe	438
4.2. Prawo wzorów użytkowych	439
4.3. Prawo wzorów przemysłowych	439
4.4. Prawo znaków towarowych	439

4.5. Ochrona oznaczeń geograficznych	440
4.6. Ochrona topografii układów scalonych	440
4.7. Ochrona baz danych	440
5. Prawo ochrony konkurencji	441
6. Kwestia cyberbezpieczeństwa w odniesieniu do praw własności intelektualnej	441
6.1. Cyberbezpieczeństwo na poziomie krajowym	441
6.2. Cyberbezpieczeństwo w sektorze prywatnym	443
6.3. Cyberbezpieczeństwo a użytkownik końcowy	445
7. Wybrane problemy własności intelektualnej w aspekcie cyberbezpieczeństwa	446
7.1. Cyberbezpieczeństwo programów komputerowych	446
7.2. Internet rzeczy	447
7.3. Uczenie maszynowe	449
7.4. Chmura obliczeniowa	451

CZĘŚĆ IV

CYBERBEZPIECZEŃSTWO A OBYWATEL

ROZDZIAŁ XII

OCHRONA DANYCH OSOBOWYCH 455

1. Wprowadzenie	455
2. Rys historyczny	455
3. Rozporządzenie ogólne o ochronie danych osobowych (RODO)	457
4. Zakres przedmiotowy i podmiotowy RODO	458
5. Zasady dotyczące przetwarzania danych osobowych	466
6. Podstawy prawne przetwarzania	470
7. Bezpieczeństwo danych osobowych	477
8. Przejrzyste informowanie osób, których dane dotyczą	480
9. Prawa osób, których dane dotyczą	484
10. Organ nadzorczy	492
11. Administracyjne kary pieniężne	493
12. Pozostałe kwestie	494
13. Przepisy krajowe o ochronie danych osobowych	495
14. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 (tzw. dyrektywa policyjna)	501

ROZDZIAŁ XIII

PRAWNA OCHRONA DZIECI I MŁODZIEŻY W CYBERPRZESTRZENI ZE SZCZEGÓLNYM UWZGLĘDNIENIEM OCHRONY PRZED TREŚCIAMI PORNOGRAFICZNYMI 502

1. Wstęp	502
2. Podstawowe zagrożenia	503
3. Zagrożenie dzieci i młodzieży dostępem do pornografii w cyberprzestrzeni	505
4. Stan prawny dotyczący zagrożeń dzieci w cyberprzestrzeni w odniesieniu do innych zagrożeń niż dostęp do treści pornograficznych	507
5. Prawna ochrona dzieci przed dostępem do pornografii	511
6. Podsumowanie	515

CZĘŚĆ V CYBERPRZESTĘPCZOŚĆ

ROZDZIAŁ XIV

KARNOPRAWNE RAMY ODPOWIEDZIALNOŚCI ZA PRZESTĘPSTWA POPEŁNIANE W CYBERPRZESTRZENI	519
1. Uwagi wprowadzające	519
2. Przestępstwa stricte komputerowe	521
2.1. Nieautoryzowany dostęp do systemu komputerowego (hacking)	521
2.2. Nielegalny podsłuch komputerowy (naruszenie tajemnicy komunikacji)	524
2.3. Naruszenie integralności danych komputerowych	525
2.4. Naruszenie integralności systemu komputerowego	527
3. Przestępstwa związane z wykorzystaniem sieci i systemów teleinformatycznych oraz nowych technologii	529
4. Przestępstwa popełnione z wykorzystaniem komputera i sieci teleinformatycznych	532
5. Przestępstwa z wykorzystaniem komputerów skierowane przeciwko wolności seksualnej popełnione na szkodę małoletniego	535
6. Przestępstwa przeciwko czci	537

ROZDZIAŁ XV

PRZESTĘPSTWA W CYBERPRZESTRZENI – PROBLEMATYKA KARNA I ŚLEDCTWA	540
1. Uwagi wprowadzające	540
2. Dowód cyfrowy - pojęcie i klasyfikacja	541
3. Dowód cyfrowy a prawo dowodowe	544
4. Miejsce popełnienia przestępstwa w świecie wirtualnym	548
5. Karnoprocesowa problematyka dowodzenia znamion przestępstw komputerowych	552
6. Kryminalistyka cyfrowa - płaszczyzny i problemy	555
7. Dowody z urządzeń mobilnych	556
8. Kryptowaluty - ocena wpływu na płaszczyzny przestępczej działalności	561

BIBLIOGRAFIA	563
---------------------	------------

AUTORZY	581
----------------	------------