

CYBERBEZPIECZEŃSTWO

Zarys wykładu

redakcja naukowa Cezary Banasiński

Cezary Banasiński, Cezary Błaszczuk, Jacek M. Chmielewski
Władysław Hydzik, Dariusz Jagiełło, Filip Krzyżankiewicz
Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak
Adam Szafrński, Ryszard Szpyra, Kazimierz Waćkowski
Paweł Widawski, Joanna Worona, Zofia Zawadzka

SERIA AKADEMICKA

CYBERBEZPIECZEŃSTWO

Zarys wykładu

CYBERBEZPIECZEŃSTWO

Zarys wykładu

redakcja naukowa Cezary Banasiński

Cezary Banasiński, Cezary Błaszczyk, Jacek M. Chmielewski
Władysław Hydzik, Dariusz Jagiełło, Filip Krzyżankiewicz
Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak
Adam Szafranski, Ryszard Szpyra, Kazimierz Waćkowski
Paweł Widawski, Joanna Worona, Zofia Zawadzka

SERIA AKADEMICKA

Stan prawny na 15 października 2018 r.

Recenzent

Prof. dr hab. Hanna Gronkiewicz-Waltz

Wydawca

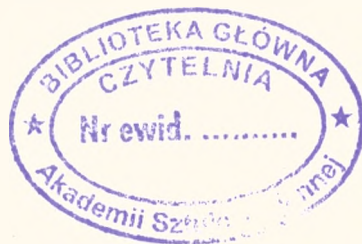
Agata Jędrasik

Redaktor prowadzący

Joanna Olówek

Opracowanie redakcyjne i łamanie

Violet Design Wioletta Kowalska



Poszczególne rozdziały napisali:

Cezary Banasiński – rozdz. I

Cezary Banasiński, Włodzimierz Nowak – rozdz. III

Cezary Błaszczuk – rozdz. VII

Jacek M. Chmielewski, Kazimierz Waćkowski – rozdz. II

Władysław Hydzik – rozdz. IX

Dariusz Jagiełło – rozdz. XIV, XV

Filip Krzyżankiewicz, Arwid Mednis – rozdz. XII

Włodzimierz Nowak – rozdz. IV

Marcin Rojszczak – rozdz. V, VIII

Adam Szafrński – rozdz. XIII

Ryszard Szpyra – rozdz. VI

Paweł Widawski – rozdz. X

Joanna Worona, Zofia Zawadzka – rozdz. XI

© Copyright by

Wolters Kluwer Polska Sp. z o.o., 2018

ISBN 978-83-8160-139-9

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. 22 535 82 19

e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW	11
WSTĘP	15

CZĘŚĆ I

WPROWADZENIE DO PROBLEMATYKI CYBERBEZPIECZEŃSTWA

ROZDZIAŁ I

PODSTAWOWE POJĘCIA I PODSTAWY PRAWNE BEZPIECZEŃSTWA

W CYBERPRZESTRZENI	21
1. Pojęcia cyberbezpieczeństwa i cyberprzestrzeni	21
1.1. Wprowadzenie	21
1.2. Pojęcie cyberprzestrzeni	23
1.3. Pojęcie cyberbezpieczeństwa	27
2. Cyberbezpieczeństwo jako przedmiot badań	33
3. Podstawy prawne cyberbezpieczeństwa	38
3.1. Regulacje cyberbezpieczeństwa w działalności ONZ	38
3.2. Inicjatywy legislacyjne Rady Europy	43
3.3. Dorobek prawny Unii Europejskiej	45

ROZDZIAŁ II

TECHNOLOGIE TELEINFORMATYCZNE – PODSTAWY, ROZWÓJ

I BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH	66
1. Wprowadzenie	66
2. Zarządzanie usługami IT i bezpieczeństwem teleinformatycznym w organizacjach	68
2.1. Metodyka ITIL®	69
2.2. Standard COBIT®	71
2.3. Podejście usługowe w COBIT i ITIL	74
3. Kilka słów o bezpieczeństwie operacyjnym organizacji	75
4. Model ISO OSI	81
5. Klasyfikacja ataków sieciowych według modelu ISO OSI	85
5.1. Ataki w 2. warstwie łącza danych	85
5.2. Ataki w 3. warstwie sieciowej	89
5.3. Ataki w 4. warstwie transportowej	92
5.4. Ataki w 7. warstwie aplikacji	93
5.5. Podsumowanie modelu OSI	95

6. Firewall podstawowym elementem chroniącym sieć komputerową	95
7. Historia eskalacji zagrożeń w cyberprzestrzeni	101
8. Dedykowany atak APT/TPT	103
9. Ataki APT na sektory energetyczne państw	108
9.1. Czynniki wpływające na podatność infrastruktury energetycznej na cyberataki	108
9.2. Przykłady ataków APT na sektory energetyczne państw	110
10. Planowanie architektury korporacyjnej (organizacji)	116
11. Ontologia – „Siatka Zachmana”	125
12. Podsumowanie	142

CZĘŚĆ II

CYBERBEZPIECZEŃSTWO PAŃSTWA

ROZDZIAŁ III

EUROPEJSKI I KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA	149
1. Podstawy ustrojowe europejskiego cyberbezpieczeństwa	149
2. Dyrektywa NIS	154
3. Organizacja krajowego systemu cyberbezpieczeństwa	160

ROZDZIAŁ IV

OCHRONA INFRASTRUKTURY KRYTYCZNEJ W CYBERPRZESTRZENI	173
1. Zagrożenia i ryzyka	173
2. Cztery kroki analizy i oceny sytuacji	183
2.1. Hiperboliczna mapa internetu	183
2.2. Model OSI	185
2.3. Matryca cyberbezpieczeństwa	187
2.4. Kompetencje	190
2.5. Cykl życia systemów	192
3. Podsumowanie	193

ROZDZIAŁ V

CYBERBEZPIECZEŃSTWO W ŁĄCZNOŚCI ELEKTRONICZNEJ	195
1. Uwagi wprowadzające	195
2. Wielopłaszczyznowość problematyki ochrony łączności elektronicznej	198
3. Ochrona łączności elektronicznej w prawie Unii Europejskiej	200
3.1. Podstawowe regulacje	200
3.2. Zagadnienia węzłowe prawa łączności elektronicznej	207
3.2.1. Poufność transmisji	207
3.2.2. Bezpieczeństwo sieci i usług	210
3.2.3. Ochrona przed niezamówionymi informacjami handlowymi i spamem	212
4. Płaszczyzna przepisów krajowych	214
5. Oczekiwane kierunki zmian w prawodawstwie	218

ROZDZIAŁ VI

CYBERBEZPIECZEŃSTWO I CYBERAKTYWNOŚĆ MILITARNA	220
1. Geneza i istota zjawiska	220
2. Ewolucja wojskowego myślenia o cyberbezpieczeństwie i cyberoperacjach militarnych	223

2.1. Stany Zjednoczone	223
2.2. NATO	229
3. Współczesne koncepcje teoretyczne – model bazujący na teorii bezpieczeństwa	232
3.1. Kierowanie procesem zapewniania cyberbezpieczeństwa – moduł kierowania	235
3.2. Uzyskiwanie świadomości sytuacyjnej cyberbezpieczeństwa – moduł informacyjny ...	236
3.3. Przeciwdziałanie cyberzagrożeniom – moduł operacyjny	238
4. Współczesne koncepcje doktrynalne – wybrane przykłady	241
4.1. Militarne operacje w cyberprzestrzeni i poprzez cyberprzestrzeń	244
4.2. Bezpieczeństwo sieci informacyjnych nienależących do Departamentu Obrony	246
5. Przyszłość	246

CZĘŚĆ III

CYBERBEZPIECZEŃSTWO W PRAWIE GOSPODARCZYM

ROZDZIAŁ VII

PROWADZENIE DZIAŁALNOŚCI GOSPODARCZEJ W CYBERPRZESTRZENI	253
1. Wstęp	253
1.1. Pojęcie prawa gospodarczego	253
1.2. Zasady i źródła prawa gospodarczego	255
1.3. Prawo gospodarcze a cyberprzestrzeń i cyberbezpieczeństwo	256
2. Prawo gospodarcze a prawo autorskie	257
2.1. Podstawowe informacje	257
2.2. Prawo autorskie w internecie	259
2.3. Odpowiedzialność cywilna za naruszenie praw autorskich	261
3. Zawieranie umów a cyberprzestrzeń	264
3.1. Zagadnienia ogólne	264
3.2. Oświadczenia woli	266
3.3. Formy czynności prawnych	268
3.4. Sposób i okoliczności zawarcia umowy	275
4. Wybrane umowy związane z cyberprzestrzenią i cyberbezpieczeństwem	280
4.1. Wprowadzenie	280
4.2. Umowa licencyjna	281
4.3. Umowa o świadczenie usług drogą elektroniczną	288
4.4. Umowa o rejestrację domeny internetowej	292
4.5. Umowa sprzedaży przez internet	296
4.6. Umowa o świadczenie usług telekomunikacyjnych	298

ROZDZIAŁ VIII

CYBERBEZPIECZEŃSTWO Z PERSPEKTYWY PRZEDSIĘBIORCY	303
1. Uwagi wprowadzające	303
2. Źródła wymagań w obszarze cyberbezpieczeństwa	306
3. Model zarządzania bezpieczeństwem IT według normy ISO/IEC 27001	309
3.1. Historia standaryzacji w obszarze systemów zarządzania bezpieczeństwem informacji ...	309
3.2. Rodzina norm ISO/IEC 27000	310
3.3. Ramowy model SZBI	311
3.4. Procesowe zarządzanie bezpieczeństwem (PDCA)	314
3.5. Katalog zabezpieczeń	315

4. Model zarządzania cyberbezpieczeństwem według normy ISO/IEC 27032	316
5. Inne schematy zarządzania cyberbezpieczeństwem	319
5.1. Wytyczne i rekomendacje instytucji Unii Europejskiej (ENISA)	320
5.2. Wytyczne i rekomendacje publikowane w Stanach Zjednoczonych	323
6. Podsumowanie	325

ROZDZIAŁ IX

ZARZĄDZANIE RYZYKIEM W CELU ZAGWARANTOWANIA

CYBERBEZPIECZEŃSTWA	327
1. Wprowadzenie	327
2. Kluczowe terminy	327
3. Ramowy proces zarządzania ryzykiem w świetle wymogów prawnych oraz norm polskich i międzynarodowych	332
4. Przykład wdrożenia zarządzania ryzykiem w cyberbezpieczeństwie	334
5. Podsumowanie	338

ROZDZIAŁ X

CYBERBEZPIECZEŃSTWO W USŁUGACH PŁATNICZYCH

1. Wstęp – znaczenie bezpieczeństwa w świadczeniu usług płatniczych	339
2. Model odpowiedzialności dostawcy usług płatniczych i użytkownika za nieautoryzowane transakcje płatnicze	345
3. Zarządzanie ryzykami operacyjnymi i ryzykami dla bezpieczeństwa w wytycznych Europejskiego Urzędu Nadzoru Bankowego i rekomendacji Komisji Nadzoru Finansowego	347
4. Bezpieczeństwo świadczenia usług płatniczych w ustawie o usługach płatniczych	349
5. Model zgłaszania incydentów	349
6. Silne uwierzytelnienie klienta	350
6.1. Wyłączenia względem stosowania silnego uwierzytelnienia klienta	353
6.2. Analiza ryzyka transakcji	354
6.3. Płatności zbliżeniowe	355
6.4. Opłaty za transport i parking	355
6.5. Zaufani odbiorcy płatności i transakcje powtarzające się	355
6.6. Transakcje o niskiej wartości	356
6.7. Wyłączenia dla usługi dostępu do informacji na rachunku płatniczym	356
6.8. Monitoring transakcji	356
7. Poufność i integralność indywidualnych danych uwierzytelniających użytkowników usług płatniczych	357
8. Wymogi dotyczące powszechnej i bezpiecznej komunikacji	359

ROZDZIAŁ XI

CYBERBEZPIECZEŃSTWO W PRAWIE WŁASNOŚCI INTELEKTUALNEJ

1. Wprowadzenie	362
2. Pojęcie własności intelektualnej	362
3. Prawo autorskie i prawa pokrewne	364
3.1. Prawo autorskie	364
3.1.1. Programy komputerowe	366
3.2. Prawa pokrewne	366

4. Prawo własności przemysłowej	367
4.1. Prawo patentowe	367
4.2. Prawo wzorów użytkowych	367
4.3. Prawo wzorów przemysłowych	368
4.4. Prawo znaków towarowych	368
4.5. Ochrona oznaczeń geograficznych	369
4.6. Ochrona topografii układów scalonych	369
4.7. Ochrona baz danych	369
5. Prawo ochrony konkurencji	369
6. Kwestia cyberbezpieczeństwa w odniesieniu do praw własności intelektualnej	370
6.1. Cyberbezpieczeństwo na poziomie krajowym	370
6.2. Cyberbezpieczeństwo w sektorze prywatnym	372
6.3. Cyberbezpieczeństwo a użytkownik końcowy	373
7. Wybrane problemy własności intelektualnej w aspekcie cyberbezpieczeństwa	374
7.1. Cyberbezpieczeństwo programów komputerowych	374
7.2. Internet rzeczy	375
7.3. Uczenie maszynowe	377
7.4. Chmura obliczeniowa	377

CZĘŚĆ IV CYBERBEZPIECZEŃSTWO A OBYWATEL

ROZDZIAŁ XII

OCHRONA DANYCH OSOBOWYCH	381
1. Wprowadzenie	381
2. Rys historyczny	381
3. Rozporządzenie ogólne o ochronie danych osobowych (RODO)	383
4. Zakres przedmiotowy i podmiotowy RODO	384
5. Zasady dotyczące przetwarzania danych osobowych	392
6. Podstawy prawne przetwarzania	397
7. Bezpieczeństwo danych osobowych	403
8. Przejrzyste informowanie osób, których dane dotyczą	406
9. Prawa osób, których dane dotyczą	410
10. Organ nadzorczy	418
11. Administracyjne kary pieniężne	419
12. Pozostałe kwestie	420
13. Przepisy krajowe o ochronie danych osobowych	421
14. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 (tzw. dyrektywa policyjna)	427

ROZDZIAŁ XIII

PRAWNA OCHRONA DZIECI I MŁODZIEŻY W CYBERPRZESTRZENI ZE SZCZEGÓLNYM UWZGLĘDNIENIEM OCHRONY

PRZED TREŚCIAMI PORNOGRAFICZNYMI	433
1. Wstęp	433
2. Podstawowe zagrożenia	434
3. Zagrożenie dzieci i młodzieży dostępem do pornografii w cyberprzestrzeni	436

4. Stan prawny dotyczący zagrożeń dzieci w cyberprzestrzeni w odniesieniu do innych zagrożeń niż dostęp do treści pornograficznych	437
5. Prawna ochrona dzieci przed dostępem do pornografii	441
6. Podsumowanie	445

CZĘŚĆ V CYBERPRZESTĘPCZOŚĆ

ROZDZIAŁ XIV

KARNOPRAWNE RAMY ODPOWIEDZIALNOŚCI ZA PRZESTĘPSTWA

POPEŁNIANE W CYBERPRZESTRZENI	449
1. Uwagi wprowadzające	449
2. Przestępstwa <i>stricte</i> komputerowe	451
2.1. Nieautoryzowany dostęp do systemu komputerowego (hacking)	451
2.2. Nielegalny podsłuch komputerowy (naruszenie tajemnicy komunikacji)	453
2.3. Naruszenie integralności danych komputerowych	455
2.4. Naruszenie integralności systemu komputerowego	457
3. Przestępstwa związane z wykorzystaniem sieci i systemów teleinformatycznych oraz nowych technologii	459
4. Przestępstwa popełnione z wykorzystaniem komputera i sieci teleinformatycznych	461
5. Przestępstwa z wykorzystaniem komputerów skierowane przeciwko wolności seksualnej popełnione na szkodę małoletniego	465
6. Przestępstwa przeciwko czci	466

ROZDZIAŁ XV

PRZESTĘPSTWA W CYBERPRZESTRZENI

– PROBLEMATYKA KARNA I ŚLEDCTWA	469
1. Uwagi wprowadzające	469
2. Dowód cyfrowy – pojęcie i klasyfikacja	470
3. Dowód cyfrowy a prawo dowodowe	473
4. Miejsce popełnienia przestępstwa w świecie wirtualnym	477
5. Karnoprocesowa problematyka dowodzenia znamion przestępstw komputerowych	481
6. Kryminalistyka cyfrowa – płaszczyzny i problemy	484
7. Dowody z urządzeń mobilnych	485
8. Kryptowaluty – ocena wpływu na płaszczyzny przestępczej działalności	490

BIBLIOGRAFIA	493
---------------------------	------------

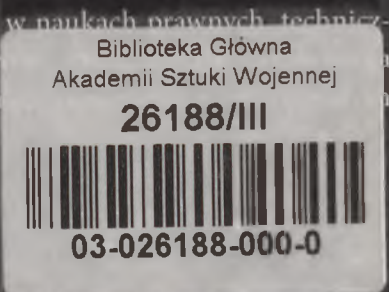
Cyberbezpieczeństwo jest przedmiotem analiz zarówno nych, jak i stosunkach międzynarodowych czy wojskow jako interdyscyplinarny podręcznik akademicki, zawiera obszarów cyberbezpieczeństwa, m.in.:

- bezpieczeństwa państwa,
- bezpieczeństwa cyfrowego obrotu gospodarczego,
- cyberbezpieczeństwa przedsiębiorcy oraz obywatela.

W publikacji odniesiono się do aktualnych regulacji prawnych – 2016/679 (RODO) oraz ustawa o krajowym systemie cyberbezpieczeństwa, także omówienie uznawanych międzynarodowo standardów z w obszarze zarządzania ryzykiem oraz budowy systemów zarządzania informacją. Dokonano także analizy aktualnych przepisów prawnych z obszarem przestępstw komputerowych oraz zaleceń związanych z procesem zabezpieczania dowodów elektronicznych.

Autorami są zarówno pracownicy naukowcy reprezentujący różne środowiska naukowe, m.in.: Uniwersytet Warszawski, Uniwersytet SWPS, Politechnika Warszawska czy Akademia Obrony Narodowej, jak i praktycy zajmujący się problematyką cyberbezpieczeństwa w pracy zawodowej.

Publikacja jest przeznaczona dla studentów prawa oraz informatyki, a także słuchaczy studiów podyplomowych z zakresu cyberbezpieczeństwa. Będzie także cennym źródłem wiedzy dla szerokiego grona praktyków, specjalistów zajmujących się na co dzień zagadnieniami z obszaru bezpieczeństwa IT.



Czyt. 3
004.056

LEXOTEKA
więcej niż podręcznik

Poszukaj pozostałych podręczników
dostępnych online

www.lexoteka.pl

9788381601399 W01P01

ISBN 978-83-8160-139-9

9 788381 601399

ZAMÓWIENIA:

INFOLINIA 801 04 45 45, FAX 22 535 80 01
ZAMOWIENIA@WOLTERSKLUWER.PL
WWW.PROFINFO.PL