

Spis treści

<b>Przedmowa</b>	<b>9</b>
<b>Notacja</b>	<b>21</b>
<b>O autorach</b>	<b>23</b>
<b>CZĘŚĆ III PROBLEMY ZARZĄDZANIA</b>	
<b>Rozdział 14. Zarządzanie bezpieczeństwem IT i ocena ryzyka</b>	<b>25</b>
14.1. Zarządzanie bezpieczeństwem IT	27
14.2. Kontekst organizacyjny i polityka bezpieczeństwa	30
14.3. Ocena ryzyka bezpieczeństwa	34
14.4. Szczegółowa analiza ryzyka bezpieczeństwa	38
14.5. Studium przypadku: Silver Star Mines	52
14.6. Podstawowe pojęcia, pytania sprawdzające i zadania	58
<b>Rozdział 15. Środki, plany i procedury bezpieczeństwa IT</b>	<b>61</b>
15.1. Wdrażanie mechanizmów zarządzania bezpieczeństwem IT	62
15.2. Środki bezpieczeństwa lub zabezpieczenia	63
15.3. Plan bezpieczeństwa IT	72
15.4. Wdrażanie zabezpieczeń	74
15.5. Monitorowanie zagrożeń	75
15.6. Studium przypadku: Silver Star Mines	78
15.7. Podstawowe pojęcia, pytania sprawdzające i zadania	81
<b>Rozdział 16. Bezpieczeństwo fizyczne i środowiskowe</b>	<b>83</b>
16.1. Przegląd	85
16.2. Zagrożenia dla bezpieczeństwa fizycznego	85
16.3. Zapobieganie zagrożeniom fizycznym i środki łagodzące	94
16.4. Odtwarzanie po naruszeniach bezpieczeństwa fizycznego	98
16.5. Przykład: korporacyjna polityka bezpieczeństwa fizycznego	99
16.6. Integracja bezpieczeństwa fizycznego i logicznego	99
16.7. Podstawowe pojęcia, pytania sprawdzające i zadania	107
<b>Rozdział 17. Bezpieczeństwo zasobów ludzkich</b>	<b>109</b>
17.1. Świadomość bezpieczeństwa, szkolenie i edukacja	110
17.2. Praktyki i zasady zatrudniania	117
17.3. Zasady korzystania z poczty e-mail i internetu	121
17.4. Zespoły reagowania na incydenty bezpieczeństwa komputerowego	124

17.5. Podstawowe pojęcia, pytania sprawdzające i zadania	132
<b>Rozdział 18. Audyt bezpieczeństwa</b>	<b>135</b>
18.1. Architektura audytu bezpieczeństwa	137
18.2. Ślad audytu bezpieczeństwa	143
18.3. Implementacja funkcji logowania	148
18.4. Analiza śladu audytu bezpieczeństwa	162
18.5. Zarządzanie informacjami o bezpieczeństwie i zdarzeniach	167
18.6. Podstawowe pojęcia, pytania sprawdzające i zadania	169
<b>Rozdział 19. Aspekty prawne i etyczne</b>	<b>173</b>
19.1. Cyberprzestępczość i przestępczość komputerowa	174
19.2. Własność intelektualna	178
19.3. Prywatność	186
19.4. Kwestie etyczne	194
19.5. Podstawowe pojęcia, pytania sprawdzające i zadania	201
<b>CZĘŚĆ IV ALGORYTMY KRYPTOGRAFICZNE</b>	
<b>Rozdział 20. Szyfrowanie symetryczne i poufność wiadomości</b>	<b>207</b>
20.1. Zasady szyfrów symetrycznych	208
20.2. Standard DES	214
20.3. Standard AES	216
20.4. Szyfry strumieniowe i RC4	223
20.5. Tryby działania szyfrów blokowych	228
20.6. Dystrybucja kluczy	234
20.7. Podstawowe pojęcia, pytania sprawdzające i zadania	236
<b>Rozdział 21. Kryptografia klucza publicznego i uwierzytelnianie komunikatów</b>	<b>243</b>
21.1. Bezpieczne funkcje haszowania	244
21.2. HMAC	251
21.3. Szyfrowanie uwierzytelnione	255
21.4. Algorytm szyfrowania RSA z kluczem publicznym	258
21.5. Algorytm Diffiego-Hellmana i inne algorytmy asymetryczne	265
21.6. Podstawowe pojęcia, pytania sprawdzające i zadania	270
<b>CZĘŚĆ V BEZPIECZEŃSTWO SIECI</b>	
<b>Rozdział 22. Protokoły i standardy bezpieczeństwa internetu</b>	<b>275</b>
22.1. Bezpieczne wiadomości e-mail i S/MIME	276
22.2. Poczta DKIM	280
22.3. Zabezpieczenia SSL i TLS	283
22.4. HTTPS	293
22.5. Bezpieczeństwo IPv4 i IPv6	294
22.6. Podstawowe pojęcia, pytania sprawdzające i zadania	301

<b>Rozdział 23. Aplikacje do uwierzytelniania w internecie</b>	<b>305</b>
23.1. Kerberos	306
23.2. X.509	313
23.3. Infrastruktura klucza publicznego	317
23.4. Podstawowe pojęcia, pytania sprawdzające i zadania	320
<b>Rozdział 24. Bezpieczeństwo sieci bezprzewodowych</b>	<b>323</b>
24.1. Bezpieczeństwo sieci bezprzewodowych	324
24.2. Bezpieczeństwo urządzeń mobilnych	328
24.3. Przegląd sieci bezprzewodowych IEEE 802.11	333
24.4. Bezpieczeństwo sieci bezprzewodowych IEEE 802.11i	341
24.5. Podstawowe pojęcia, pytania sprawdzające i zadania	357
<b>Rozdział 25. Bezpieczeństwo Linuksa</b>	<b>361</b>
25.1. Wprowadzenie	362
25.2. Model bezpieczeństwa Linuksa	362
25.3. DAC w szczegółach: bezpieczeństwo systemu plików	364
25.4. Luki w systemie Linux	372
25.5. Wzmacnianie systemu Linux	375
25.6. Bezpieczeństwo aplikacji	384
25.7. Obligatoryjne mechanizmy kontroli dostępu	387
25.8. Literatura	394
<b>Rozdział 26. Bezpieczeństwo systemu Windows</b>	<b>395</b>
26.1. Podstawowa architektura bezpieczeństwa systemu Windows	396
26.2. Luki w systemie Windows	408
26.3. Mechanizmy obronne systemu Windows	409
26.4. Zabezpieczenia przeglądarki	420
26.5. Usługi kryptograficzne	422
26.6. Specyfikacja Common Criteria	424
26.7. Literatura	424
26.8. Podstawowe pojęcia i projekty	425
<b>Rozdział 27. Środowiska zaufane i zabezpieczenia wielopoziomowe</b>	<b>427</b>
27.1. Model bezpieczeństwa komputerowego Bell-Lapadula	429
27.2. Inne formalne modele bezpieczeństwa komputerowego	440
27.3. Koncepcja systemów zaufanych	447
27.4. Zastosowania zabezpieczeń wielopoziomowych	451
27.5. Środowiska zaufane i moduł TPM	458
27.6. Specyfikacja Common Criteria oceny bezpieczeństwa informatycznego	463
27.7. Gwarancje i ocena	470
27.8. Literatura	476
27.9. Podstawowe pojęcia, pytania sprawdzające i zadania	477

## **DODATKI**

<b>Spis treści tomu 1</b>	<b>483</b>
<b>Dodatek A Projekty i inne ćwiczenia dla studentów uczących się bezpieczeństwa komputerów</b>	<b>487</b>
<b>Dodatek B Wybrane elementy teorii liczb</b>	<b>495</b>
<b>Dodatek C Standardy i organizacje standaryzacyjne</b>	<b>505</b>
<b>Dodatek D Generowanie liczb losowych i pseudolosowych</b>	<b>519</b>
<b>Dodatek E Kody uwierzytelniania komunikatów bazujące na szyfrach blokowych</b>	<b>531</b>
<b>Dodatek F Architektura protokołów TCP/IP</b>	<b>537</b>
<b>Dodatek G Konwersja Radix-64</b>	<b>545</b>
<b>Dodatek H System DNS</b>	<b>549</b>
<b>Dodatek I Zaniedbywanie miarodajności</b>	<b>561</b>
<b>Dodatek J SHA-3</b>	<b>567</b>
<b>Słowniczek</b>	<b>585</b>
<b>Akronimy</b>	<b>595</b>
<b>Lista dokumentów NIST i ISO</b>	<b>597</b>
<b>Literatura</b>	<b>599</b>
<b>Skorowidz</b>	<b>613</b>