SPIS TREŚCI

O autorach 11

Od autorów 13

Bezpieczeństwo systemów informatycznych 15

Wprowadzenie do bezpieczeństwa systemów informatycznych 15

Jakie są elementy bezpieczeństwa? 17

Jakie są trzy najważniejsze atrybuty bezpieczeństwa informacji? 23

Dlaczego uważa się, że zagadnienia związane z bezpieczeństwem systemów informatycznym mają charakter interdyscyplinarny? 23

Jaka jest klasyczna definicja Siebera przestępczości komputerowej bądź przestępstwa komputerowego? 24

Co oznacza pojęcie „ciemnej liczby" w odniesieniu do statystyki związanej z przestępczością komputerową? 25

Co oznaczają terminy haker, kraker, friker, lamer? 25

Co to jest sabotaż komputerowy w świetle regulacji prawnych polskiego kodeksu karnego? 26

Co się rozumie pod pojęciem socjotechnika bądź inżynieria społeczna (social engineering)? 27

Rodzaje, charakterystyka i ocena zagrożeń 30

Jak można ogólnie sklasyfikować zagrożenia systemu informatycznego? 32

Jakie są najczęściej występujące zagrożenia według CERT Polska? 33

Jakie są najważniejsze trendy cyberprzestępczości? 34

Kto najczęściej ulega atakom, a kto atakuje? 35

Co atakujący może zrobić z naszą informacją? 35

Co to jest atak typu DoS, DDoS i DRDoS? 36

Jakie są typowe sposoby działań intruzów w systemach informatycznych? 37
Jakie rozróżniamy programy destrukcyjne (złośliwe)? 38
Jak przedstawia się opracowany przez CSI diagram częstości występowania zagrożeń w sieciach komputerowych? 41
Co to jest emisja ujawniająca (emanacja elektromagnetyczna)? 42
Polityka bezpieczeństwa 45
Co rozumiemy pod pojęciem polityki bezpieczeństwa instytucji? 46
Jakie elementy są niezbędne w dokumencie zwanym polityką bezpieczeństwa, a jakie elementy są niepożądane? 50
Rodzaje zabezpieczeń systemów informatycznych 53
Jak klasyfikujemy metody obrony przed zagrożeniami systemów informatycznych? 55
Jakie przykładowo elementy składają się na zabezpieczenia fizyczne? 56
Jakie przykładowo elementy składają się na zabezpieczenia techniczne? 58
Jakie przykładowo elementy składają się na zabezpieczenia organizacyjno-administracyjne? 59
Jakie przykładowo elementy składają się na zabezpieczenia prawne? 61
Kryptografia i podpis elektroniczny 63
Czym się zajmuje kryptologia i z jakich dziedzin się składa? 66
Czym się różni kryptosystem z kluczem prywatnym od kryptosystemu z kluczem publicznym? 66
Czym różni się prosty szyfr podstawieniowy od prostego szyfru przestawieniowego? 68
Jakie są popularne systemy szyfrujące na świecie? 69
Co to jest podpis cyfrowy i czym się różni od podpisu zwykłego? 72
Jaki jest schemat tworzenia i weryfikacji podpisu cyfrowego? 72
Co to jest Infrastruktura Klucza Publicznego? 74
Co to jest certyfikat klucza publicznego i jaka jest procedura jego wydawania? 75
Od kiedy i w jaki sposób funkcjonuje podpis elektroniczny w Polsce? 76
Co to jest bezpieczny podpis elektroniczny i co to jest kwalifikowany certyfikat? 77

Karty elektroniczne 80
Jak klasyfikujemy karty elektroniczne? 80
Dlaczego karty elektroniczne są bezpieczniejsze niż magnetyczne? 83
Jakie są typowe zastosowania kart elektronicznych? 83
W jakim celu stosuje się karty elektroniczne w systemie PKI? 85
Kontrola dostępu do systemu informatycznego 87
Co to jest kontrola dostępu do systemu informatycznego? 87
Jakie wyróżniamy sposoby uwierzytelniania w systemie? 88
Jakie warunki powinno spełniać bezpieczne hasło? 90
Jakie są przykłady stosowania złych haseł? 90
Jakie są zalecenia stosowania dobrych haseł? 91
Co to są metody kontroli dostępu typu challenge-response, przekształcenia zegarowego, dialogowe, haseł jednorazowych? 92
Archiwizowanie informacji 96
Jakie są zasady poprawnego archiwizowania informacji w dużych systemach informatycznych? 97
Jakie są różnice pomiędzy archiwizacją prostą, różnicową i przyrostową? 98
O czym należy pamiętać podczas archiwizacji informacji? 99
Co to jest koncepcja systemów FTS, czyli systemów tolerujących błędy? 100
Co to są macierze dyskowe RAID należące do klasy systemów FTS? 100

Zarządzanie bezpieczeństwem systemów informatycznych 105
Procesy zarządzania bezpieczeństwem systemów informatycznych 105
Co to jest zarządzanie konfiguracją? 107
Na czym polega zarządzanie zmianami? 109
Jak przebiega proces zarządzania ryzykiem? 110
System zarządzania bezpieczeństwem informacji 125
Jakie są etapy ustanawiania bezpieczeństwa informacji? 127
Jak przebiega prawidłowe wdrożenie i eksploatacja ISMS? 128
Na czym polega monitorowanie i przegląd ISMS? 129

Jakie są zasady skutecznego utrzymania i doskonalenia ISMS? 130
Jakie wymagania powinna spełniać dokumentacja ISMS? 130
Jakie są zasady przeglądu ISMS realizowanego przez kierownictwo? 131
Na czym polega model PDCA? 134
Na czym polega faza planowania? 136
Jakie działania podejmowane są w ramach fazy wykonania? 137
Jakie działania wykonywane są w ramach fazy sprawdzania? 137
Na czym polega faza działania? 139

Audyt systemów informatycznych 143
Wprowadzenie do audytowania 143
Co to jest audyt systemów informatycznych? 145
Czym zajmuje się ISACA? 146
Co to jest CISA? 147
Jakie są rodzaje audytów? 147
Na czym polega audyt bezpieczeństwa informacji? 149
Jak przebiega audyt zarządzania licencjami? 151
Co to jest audyt projektów informatycznych? 154
Na czym polega audyt aplikacji? 156
Na czym polega audyt outsourcingu? 157
Co to jest audyt zgodności z ustawą o ochronie danych osobowych? 159
Jakie relacje występują między różnymi rodzajami przeglądów? 161
Czym różnią się kontrola, audyt i controlling? 162
Metodyki prowadzenia audytu systemów informatycznych 168
Do czego służy metodyka COBIT? 170
Jaka jest struktura metodyki COBIT? 174
Jakie są kluczowe koncepcje COBIT? 174
Jaka jest ogólna procedura audytu według Audit Guidelines (COBIT 3.0)? 180
Jaka jest procedura audytu według IT Assurance Guide (COBIT 4.1)? 186

Jakie są główne założenia metodyki LP-A? 190
Jak przebiega proces audytowania według metodyki MARION 192
Na czym polega metodyka OSSTM? 192
Do jakich działań można wykorzystać metodykę TISM? 195
Wykonanie audytu 200
Jak zdefiniować obiekty, cele i zakres audytu? 202
Jakie fazy wchodzą w skład audytu? 205
Co powinna zawierać dokumentacja audytu? 206
Jak pozyskać odpowiednie dowody audytowe? 208
Na czy polega próbkowanie audytowe? 210
Jak przebiega proces audytowy? 212
Jak przebiega planowanie procesu audytowego? 212
Jak przebiega faza badania w procesie audytowym? 218
Na czy polega faza raportowania w procesie audytowym? 220
Na czym polega monitorowanie wykonania rekomendacji audytu? 223
Planowanie ciągłości działania 228
Jak wygląda model planowania ciągłości działania według DRII? 230
Jak audyt wpływa na proces planowania ciągłości działania? 231
Jak przebiega audyt planu ciągłości działania? 232
Komputerowe wspomaganie audytu 239
Jak wykorzystać CAATs w procesie audytu? 240
Co to są uniwersalne programy audytowe? 242
Jakie są najpopularniejsze programy wspomagające audyt? 243

Literatura 247
Źródła internetowe 251