Techniczne, organizacyjne i prawne aspekty bezpieczenstwa systemów teleinformatycznych

Wstęp …… 5

Rozdział 1.
Cel i zakres pracy…… 7

Rozdział 2.
Wprowadzenie do problematyki bezpieczenstwa systemów teleinformatycznych
2.1. Podstawowe pojęcia……9
2.2. Zarządzanie bezpieczenstwem……10
2.3. Rola polityki bezpieczenstwa ……11
2.3.1. Co powinna zawierac polityka bezpieczenstwa……12
2.3.2. Czego nie powinna zawierac polityka bezpieczenstwa ……12
2.3.3. Polityka bezpieczenstwa ……13
2.4. Elementy bezpieczenstwa ……21
2.4.1. Zasoby……21
2.4.2. Zagrozenia ……21
2.4.3. Podatnosc ……22
2.4.4. Nastepstwa ……22
2.4.5. Ryzyko ……23
2.4.6. Zabezpieczenia……23
2.4.7. Ryzyko szczatkowe……24
2.4.8. Ograniczenia ……25
2.5. Rola uswiadamiania problemów bezpieczenstwa……25

Rozdział 3.
Rodzaje i charakterystyka zagrozen
3.1. Rodzaje zagrozen……27

3.2. Zagrozenia pasywne ……29
3.2.1. Podsluch……29
3.2.2. Przegladanie……29
3.2.3. Analiza ruchu……30
3.3. Zagrozenia aktywne……31
3.3.1. Podszywanie ……31
3.3.2. Modyfikacja ……32
3.3.3. Podrobienie ……32
3.3.4. Odmowa usługi ……32
3.4. Zlosliwe programy……33
3.4.1. Programy wymagajace programu-gospodarza……33
3.4.2. Programy niezalezne……35
3.5. Intruzi……36
3.6. Motywy ataków ……38
3.7. Zagrozenia dla hasel ……40

Rozdział 4.
Analiza ryzyka
4.1. Etapy analizy……45
4.1.1. Identyfikacja zasobów ……45
4.1.2. Identyfikacja zagrozen……46
4.1.3. Identyfikacja podatnosci ……46
4.2. Szacowanie ryzyka ……47
4.2.1. Skutki naruszenia integralnosci ……48
4.2.2. Skutki naruszenia poufnosci ……49
4.2.3. Skutki naruszenia dostepnosci ……49
4.2.4. Identyfikacja zagrozen……50
4.2.5. Szacowanie podatnosci ……50
4.2.6. Okreslenie ryzyka ……50
4.3. Zarządzanie ryzykiem……52
4.4. Ryzyko szczatkowe……53

Rozdział 5.
Środki ochrony
5.1. Podstawowe usługi chroniace przed zagrozeniami ……58

5.2. Przeglad metod ochrony ……61
5.2.1. Ochrona fizyczna ……61
5.2.2. Ochrona techniczna……62
5.2.3. Ochrona organizacyjno-administracyjna ……63
5.3. Strefy bezpieczenstwa……64
5.3.1. Systemy kontroli dostepu……65
5.3.2. Systemy alarmowe……66
5.4. Ochrona elektromagnetyczna ……67
5.5. Ochrona zasilania……69
5.5.1. Przeglad zasilaczy UPS ……70
5.5.2 Dobór zasilacza UPS ……72
5.6. Archiwizacja informacji ……75
5.6.1. Macierze RAID……77
5.6.2. Kopie awaryjne ……79
5.6.3. Oprogramowanie do kopiowania……81
5.6.4. Strategia tworzenia kopii ……82
5.6.5. Harmonogram tworzenia kopii ……84
5.6.6. Rotacja nosników……85
5.6.7. Przechowywanie kopii……85
5.6.8. Praktyczne wskazówki……86
5.7. Kontrola dostepu do systemu i jego obiektów……87
5.7.1. Kontrola dostepu do systemu……87
5.7.2. Kontrola dostepu do obiektów systemu……89
5.7.3. Macierz dostepu……90
5.8. Ochrona hasel ……92
5.8.1. Strategie wyboru bezpiecznych hasel ……92
5.8.2. Zarządzanie haslami ……95
5.9. Kontrola dostepu do sieci ……99
5.9.1. Rodzaje i zasady działania zapór sieciowych……99
5.9.2. Strategia wyboru zapory sieciowej ……101
5.10. Wykrywanie wlaman ……103
5.10.1. Narzedzia do wykrywania wlaman……103
5.10.2. Strategie postępowania po wykryciu wlamania……107
5.11. Ochrona antywirusowa ……109
5.11.1. Programy antywirusowe ……109
5.11.2. Praktyczne wskazówki……112

Rozdział 6.
Ochrona kryptograficzna

6.1. Szyfry podstawieniowe……114
6.1.1. Szyfrowanie jednoalfabetowe……115
6.1.2. Szyfry homofoniczne……117
6.1.3. Szyfrowanie wieloliterowe ……119
6.1.4. Szyfry wieloalfabetowe ……120
6.2. Szyfry przestawieniowe……123
6.3. Szyfrowanie symetryczne ……123
6.3.1. Dystrybucja kluczy ……126
6.3.2. DES……127
6.3.3. IDEA……130
6.4. Szyfrowanie asymetryczne ……131
6.4.1. Dystrybucja kluczy jawnych……135
6.4.2. Algorytm RSA ……138
6.4.3. Algorytm ElGamala……142
6.4.4. Algorytm LUC……143

Rozdział 7.
Prawne aspekty przetwarzania informacji w systemach teleinformatycznych

7.1. Podstawowe akty prawne……145
7.2. Podstawowe zasady bezpieczenstwa ……147
7.3. Administrowanie systemem……150
7.4. Bezpieczeństwo przetwarzania ……151
7.4.1. Ochrona fizyczna ……154
7.4.2. Ochrona elektromagnetyczna ……155
7.4.3. Ochrona kryptograficzna ……156
7.4.4. Ochrona przed zagrozeniami ze strony sieci Internet ……157
7.5. Inne uwagi dotyczace bezpieczenstwa ……158
7.5.1. Ochrona antywirusowa ……158
7.5.2. Zapewnienie dostepnosci informacji ……159
7.5.3. Incydenty naruszenia bezpieczenstwa ……160
7.5.4. Bezpieczeństwo nosników informacji ……161
7.5.5. Ochronie informacji niejawnych a ochrona danych

osobowych ……162
7.6. Przestepstwa przeciwko ochronie informacji ……162

Podsumowanie ……170
Bibliografia……172