

Spis treści

Wykaz skrótów 9

Wstęp 13

1. **Znaczenie informacji w funkcjonowaniu organizacji 17**
2. **Zagrożenia bezpieczeństwa informacji i systemów teleinformatycznych organizacji 25**
 - 2.1. Identyfikacja i klasyfikacja zagrożeń bezpieczeństwa informacji oraz systemów teleinformatycznych organizacji 27
 - 2.2. Charakterystyka i analiza zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych organizacji 30
 - 2.2.1. Siły wyższe 31
 - 2.2.2. Uchybienia organizacyjne 36
 - 2.2.3. Błędy ludzkie 43
 - 2.2.4. Błędy techniczne 46
 - 2.2.5. Działania rozmyślne 48
 - 2.3. Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa informacji i systemów teleinformatycznych organizacji 50
 - 2.3.1. Określenia i istota cyberterroryzmu 50
 - 2.3.2. Kategorie i rodzaje przestępstw oraz zagrożeń w cyberprzestrzeni 52
 - 2.3.3. Obszary zainteresowania i ataku cyberterroryzmu 57
 - 2.4. Wnioski i uogólnienia dotyczące zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych organizacji 59
3. **Bezpieczeństwo informacji niejawnych i danych wrażliwych organizacji 63**
 - 3.1. Bezpieczeństwo informacji niejawnych 65
 - 3.2. Bezpieczeństwo danych wrażliwych 71
4. **Metody zapewnienia bezpieczeństwa informacji organizacji 81**
 - 4.1. Metody administracyjno-organizacyjne zapewnienia bezpieczeństwa informacji organizacji 84
 - 4.1.1. Określenie potrzeb w zakresie bezpieczeństwa informacji organizacji 87
 - 4.1.2. Określanie uwarunkowań i otoczenia systemu bezpieczeństwa informacji organizacji 89

4.1.3.	Określanie funkcjonalności systemu bezpieczeństwa informacji organizacji	95
4.1.4.	Poszukiwanie i wybór właściwego rozwiązania bezpieczeństwa informacji organizacji	96
4.1.5.	Opracowanie rozwiązania bezpieczeństwa informacji organizacji	98
4.1.6.	Wdrożenie rozwiązania bezpieczeństwa informacji organizacji	100
4.2.	Podstawy prawne i normalizacyjne bezpieczeństwa informacji organizacji	101
4.2.1	Podstawy prawne bezpieczeństwa informacji	101
4.2.2.	Normalizacja i standaryzacja w bezpieczeństwie informacji organizacji	105
4.3	Metody techniczne przeciwdziałania zagrożeniom informacji i systemów teleinformatycznych organizacji	112
4.3.1.	Metody kryptograficzne	112
4.3.2.	Metody programowo-sprzętowe	120
4.3.3.	Metody ochrony elektromagnetycznej	135
4.3.4.	Elektroniczne systemy ochrony fizycznej obiektów i zasobów teleinformatycznych organizacji	138
4.4.	Metody fizyczne zapewnienia bezpieczeństwa informacji organizacji	139
4.4.1.	Systemy sygnalizacji włamania i napadu	141
4.4.2.	Systemy sygnalizacji pożarów	150
4.4.3.	Systemy telewizji użytkowej	151
4.4.4.	Systemy kontroli dostępu	152
4.4.5.	Systemy inteligentnych budynków	153
4.4.6.	Podstawy prawne i normalizacyjne	155
5.	Ryzyko, zarządzanie ryzykiem bezpieczeństwa informacji organizacji	157
5.1.	Proces zarządzania ryzykiem bezpieczeństwa informacji organizacji	159
5.1.1.	Ustanowienie zakresu procesu szacowania ryzyka (kontekst)	163
5.1.2.	Szacowanie ryzyka bezpieczeństwa informacji organizacji	165
5.1.3.	Opracowanie planu postępowania z ryzykiem	179
5.1.4.	Akceptowanie ryzyka bezpieczeństwa informacji organizacji	183
5.1.5.	Informowanie o ryzyku i konsultowanie ryzyka bezpieczeństwa informacji organizacji	183
5.1.6.	Monitorowanie i przegląd ryzyka bezpieczeństwa informacji organizacji	184
5.2.	Metody analiz i zarządzania ryzykiem bezpieczeństwa informacji organizacji	185

5.3.	Standardy analiz i zarządzania ryzykiem bezpieczeństwa informacji organizacji	188
6.	Audyt bezpieczeństwa informacji organizacji	197
6.1.	Określenie audytu bezpieczeństwa informacji organizacji	199
6.2.	Proces audytu bezpieczeństwa informacji organizacji	201
6.3.	Metodyki prowadzenia audytu bezpieczeństwa informacji organizacji	203
6.3.1.	Metodyka COBIT	204
6.3.2.	Metodyka OSSTM	208
6.3.3.	Metodyka TISM	210
6.3.4.	Metodyka LP-A	211
6.4.	Standardy audytu i certyfikacji bezpieczeństwa informacji organizacji	212
6.4.1.	Polskie i międzynarodowe normy audytu i certyfikacji	213
6.4.2.	Standard ISACA	213
6.4.3.	Standardy IIA	215
7.	Modele i strategie bezpieczeństwa informacji organizacji	217
7.1.	Rodzaje modeli bezpieczeństwa informacji organizacji	222
7.2.	Modele organizacyjne bezpieczeństwa informacji organizacji	224
7.2.1.	Brak ochrony	224
7.2.2.	Bezpieczeństwo dzięki brakowi zainteresowania ze strony otoczenia	225
7.2.3.	Ochrona na poziomie poszczególnych komputerów	225
7.2.4.	Bezpieczna baza danych	226
7.2.5.	Ochrona w skali całego systemu bezpieczeństwa informacji i systemów teleinformatycznych	227
7.2.6.	Wojskowy model klasyfikacji	227
7.2.7.	Komercyjne modele bezpieczeństwa informacji	228
7.3.	Modele bezpieczeństwa informacji organizacji	228
7.3.1.	Model kratowy	232
7.3.2.	Model macierzowy	233
7.3.3.	Model Bella–LaPaduli	234
7.3.4.	Model Biby	235
7.3.5.	Model Grahama–Denninga	236
7.3.6.	Model Harrisona–Ruzzo–Ullmana	237
7.3.7.	Model „take–grant”	237
7.3.8.	Model Clarka–Wilsona	238

7.3.9.	Model Brewera–Nasha	239
7.3.10.	BMA	239
7.3.11.	Model Wooda	239
7.3.12.	Model Sea View	242
7.4.	Modele bezpieczeństwa systemu teleinformatycznego w dokumentach ETSI	244
7.5.	Aplikacje modeli bezpieczeństwa informacji organizacji	253
7.5.1.	Model administracji państwowej	253
7.5.2.	Wielopoziomowy model polityki bezpieczeństwa systemów teleinformatycznych	259
8.	Układ polityki bezpieczeństwa informacji organizacji	265
8.1.	Układ polityki bezpieczeństwa informacji jako rezultat działań normalizacyjnych i standaryzacyjnych	268
8.2.	Praktyczne uwagi na potrzeby układu polityki bezpieczeństwa informacji organizacji	273
9.	Metodyki opracowania polityki bezpieczeństwa informacji organizacji	277
9.1.	Metodyki COBIT i COBRA	279
9.2.	Metodyka TISM	281
9.3.	Praktyczne uwagi w metodycznym opracowywaniu polityki bezpieczeństwa informacji organizacji	288
10.	Zarządzanie bezpieczeństwem informacji organizacji	293
10.1.	Określenie i zakres zarządzania bezpieczeństwem informacji organizacji	295
10.2.	Elementy procesu zarządzania bezpieczeństwem informacji organizacji	298
10.3.	Procesy zarządzania bezpieczeństwem informacji organizacji	303
10.4.	System zarządzania bezpieczeństwem informacji organizacji	307
10.5.	Praktyczne uwagi w zarządzaniu bezpieczeństwem informacji organizacji	312
Zakończenie		329
Spis rysunków		331
Spis tablic		333
Bibliografia		335
Skorowidz		344