

**Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie /
Andrzej Białas. – Wyd. 2, 1 dodr. – Warszawa, 2017**

Spis treści

Od Autora	15
1. Wstęp	27
1.1. Bezpieczeństwo informacji i usług a bezpieczeństwo teleinformatyczne	27
1.2. Interdyscyplinarny charakter zagadnień i szczególna rola informatyki	29
1.3. Podstawowe problemy bezpieczeństwa teleinformatycznego	30
1.4. Dwa podejścia do zagadnień bezpieczeństwa	30
1.5. Potrzeba tworzenia komputerowych narzędzi wspomagających	31
2. Wprowadzenie do zarządzania bezpieczeństwem informacji i usług	33
2.1. Bezpieczeństwo i jego atrybuty	33
2.2. Wrażliwość informacji i krytyczność usług - istota ochrony	35
2.3. Elementy bezpieczeństwa	36
3. Normy, standardy i zalecenia	45
3.1. Działalność połączonego komitetu technicznego ISO/IEC	47
3.2. Raporty techniczne ISO/IEC TR 13335	48
3.3. Rozwój i znaczenie rodziny standardów BS 7799	51
3.4. Szczegółne znaczenie standardu COBIT	56
3.5. Kryteria oceny zabezpieczeń	67
3.6. Standardy dotyczące rozwiązań technicznych	68
3.7. Przygotowanie organizacji do działań audytorskich	68
3.8. Zalecenia i inne wytyczne szczegółowe	69
3.9. Aktualny stan rozwoju standardów i sposób ich wykorzystania	70
4. Ryzyko w sensie ogólnym i technicznym	74
4.1. Podstawy analizy ryzyka w sensie ogólnym	75
4.2. Bezpieczeństwo funkcjonalne w świetle IEC 61508	79
4.3. Metody jakościowe oceny ryzyka	82
4.3.1. Metoda wstępnej analizy ryzyka i hazardu	82
4.3.2. Metoda HAZOP	82
4.3.3. Metody analizy defektów	83
4.4. Metody wykorzystujące struktury drzewiaste	84
4.4.1. Metoda drzewa błędów	84
4.4.2. Metoda drzewa zdarzeń	85

4.4.3. Analiza przyczynowo-skutkowa	87
4.4.4. Metoda inspekcji drzewa ryzyka	87
4.4.5. Technika przeglądu organizacji zarządzania bezpieczeństwem	88
4.5. Metody analizy dynamicznej	89
4.5.1. Metoda GO	89
4.5.2. Metody grafów	89
4.5.3. Zastosowanie modeli Markowa	90
4.5.4. Metoda DYLAM	91
4.5.5. Metoda DETAM	92
4.6. Podsumowanie przeglądu metod oceny ryzyka	92
5. Analiza ryzyka i strategie zarządzania nim w teleinformatyce	94
5.1. Podstawowe strategie zarządzania ryzykiem	94
5.2. Ogólny schemat analizy ryzyka	96
5.3. Metody kumulowania wielkości ryzyka	97
5.3.1. Macierz predefiniowanych wartości	97
5.3.2. Lista rankingowa zagrożeń	97
5.3.3. Częstość zagrożeń	98
5.3.4. Skala uproszczona wyrażająca tolerowanie ryzyka	99
5.4. Podstawowe metody redukcji ryzyka	100
5.4.1. Redukcja ryzyka przez stosowanie typowych zabezpieczeń - ochrona podstawowa	101
5.4.2. Redukcja ryzyka wspierana nieformalną jego analizą	102
5.4.3. Redukcja ryzyka wspierana jego szczegółową i formalną analizą	104
5.4.4. Metoda mieszana (kombinowana) redukcji ryzyka	104
6. Wybrane metody i komputerowe narzędzia wspomagające	106
6.1. Komputerowe wspomaganie analizy i zarządzania ryzykiem	106
6.2. Metodyka zarządzania ryzykiem opracowana w instytucie NIST	108
6.2.1. Analiza ryzyka	110
6.2.2. Ograniczanie ryzyka	117
6.3. Metodyka szacowania zagrożeń i ryzyka (TRA) opracowana w CSE	126
6.4. Metodyka CORA i komputerowe narzędzia wspomagające	130
6.4.1. Zasady budowy modelu ryzyka	134
6.4.2. Analiza modelu i wypracowanie optymalnej strategii ograniczania ryzyka	136
6.5. Metodyka i oprogramowanie CRAMM	142
6.5.1. CRAMM-Expert - faza przygotowawcza	144
6.5.2. CRAMM-Expert - etap analizy zasobów	144
6.5.3. CRAMM-Expert - etap analizy ryzyka	146
6.5.4. CRAMM-Expert - etap zarządzania ryzykiem	147
6.5.5. CRAMM-Expert - implementacja ISMS	148
6.6. Oprogramowanie COBRA	151
6.7. Metoda IRIS	152
6.8. Oprogramowanie RiskPAC	154

6.9. Oprogramowanie ASSET	156
6.10. Inne wybrane metody i narzędzia	158
6.10.1. Pakiet MARION	158
6.10.2. Metoda VIR'94	158
6.10.3. Metoda MAGERIT	159
6.10.4. Metoda MASSIA	159
6.10.5. Metoda TISM	159
6.10.6. Metoda SIM	160
6.11. Przykłady analizatorów bezpieczeństwa i innych narzędzi wspomagających jego utrzymywanie na bieżąco	161
6.11.1. Pakiet SARA	161
6.11.2. Security Analyzer firmy NetIQ	162
6.11.3. Security Manager firmy NetIQ	162
6.11.4. Pakiet OmniGuard ESM firmy Axent	163
6.11.5. Symantec Enterprise Security Manager	163
6.11.6. Inne narzędzia wspomagające utrzymywanie bezpieczeństwa	164
7. Trójpoziomowy model odniesienia	165
7.1. Trójpoziomowy model hierarchii celów, strategii i polityki	165
7.2. Hierarchiczna struktura dokumentacji bezpieczeństwa według modelu odniesienia	169
7.3. Hierarchiczna struktura zarządzająca według modelu odniesienia	171
7.3.1. Zaangażowanie zarządu instytucji	173
7.3.2. Struktura organizacyjna zespołów odpowiedzialnych	174
7.3.3. Skład i kompetencje rady ds. bezpieczeństwa teleinformatyki	176
7.3.4. Inspektor bezpieczeństwa teleinformatycznego	178
7.3.5. Oddziałowy inspektor bezpieczeństwa teleinformatycznego	178
7.3.6. Inspektor bezpieczeństwa teleinformatycznego systemu lub realizowanego projektu	179
7.4. Trójpoziomowy model odniesienia w praktyce	179
7.5. Polityka a zarządzanie bezpieczeństwem	181
8. System bezpieczeństwa instytucji	182
8.1. Wprowadzenie	182
8.2. Fazy realizacji i ogólny schemat funkcjonowania systemu bezpieczeństwa instytucji	185
8.3. Zapis sformalizowany modelu trójpoziomowego	191
8.4. Zapis sformalizowany procesów związanych z utrzymaniem bezpieczeństwa	194
9. Bezpieczeństwo w instytucji	199
9.1. Architektura systemu bezpieczeństwa instytucji	200
9.2. Analiza procesów biznesowych ze względu na stopień zaangażowania systemów teleinformatycznych w ich realizację	201
9.3. Ogólne potrzeby bezpieczeństwa systemów teleinformatycznych	

instytucji	211
9.4. Formułowanie dokumentu polityki bezpieczeństwa instytucji	214
9.5. Zarządzanie bezpieczeństwem na poziomie instytucji	217
10. Ogólne zasady bezpieczeństwa teleinformatycznego w instytucji	218
10.1. Architektura systemu bezpieczeństwa teleinformatycznego instytucji	218
10.2. Cele bezpieczeństwa systemów teleinformatycznych instytucji	221
10.3. Otoczenie prawne	224
10.4. Wybór strategii redukcji ryzyka	226
11. Wysokopoziomowa (ogólna) analiza ryzyka i wyznaczenie obszarów wymagających ochrony	228
11.1. Wymagania ochronne	229
11.2. Domeny bezpieczeństwa	232
11.3. Przebieg wysokopoziomowej analizy ryzyka	233
12. Koncepcja hierarchii zasobów	236
12.1. Wprowadzenie	236
12.2. Interpretacja praktyczna modelu	238
12.3. Przekroje modelu	241
12.4. Zbiór dostępnych typów zasobów	241
12.5. Zbiór eksploatowanych zasobów	244
12.6. Specjalne znaczenie klasy zasobów reprezentującej personel	247
12.7. Znaczenie przekrojów modelu zasobów dla zarządzania bezpieczeństwem	248
13. Przebieg szczegółowej analizy ryzyka w systemach teleinformatycznych	249
13.1. Wprowadzenie	249
13.2. Granice obszarów zajmowanych przez zasoby instytucji	252
13.3. Analiza zasobów - identyfikacja i wycena	252
13.3.1. Przygotowanie zbioru dostępnych zasobów	253
13.3.2. Przygotowanie zbioru eksploatowanych zasobów	253
13.3.3. Atrybuty przekroju zarządzania zasobami	254
13.3.4. Wycena zasobów	254
13.4. Ocena podatności	259
13.5. Środowisko zagrożeń	264
13.6. Identyfikacja istniejących lub planowanych zabezpieczeń	267
13.7. Podsumowanie wyników analizy ryzyka	269
14. Wzorce wymagań dotyczących zabezpieczeń	276
14.1. Wzorcowa lista wymagań według PN-ISO/IEC 17799 (PN-I-07799-2)	276

14.2. Tworzenie list wymagań na podstawie katalogu zabezpieczeń zapewniających ochronę podstawową	282
14.3. Rekomendacje bankowe, normy branżowe, akty prawne	284
15. Wypracowanie strategii wyboru zabezpieczeń	287
15.1. Ustalanie listy wymagań, przyjmując cele bezpieczeństwa jako podstawowe ich źródło	289
15.2. Ustalanie listy wymagań na podstawie listy wzorcowej	291
15.3. Ustalanie listy wymagań na podstawie wyników analizy ryzyka	292
16. Ogólne zasady tworzenia architektury bezpieczeństwa na poziomie II i III	293
16.1. Podstawy tworzenia odrębnych wersji polityki bezpieczeństwa dla oddziałów instytucji (poziom IIa)	293
16.1.1. Architektura systemu bezpieczeństwa teleinformatycznego na poziomie oddziałów instytucji	294
16.1.2. Zarządzanie bezpieczeństwem na poziomie oddziałów instytucji	295
16.2. Wpływ jednorodności wymagań na architekturę bezpieczeństwa	296
16.3. Architektura systemu bezpieczeństwa na poziomie systemów teleinformatycznych	297
17. Dobór zabezpieczeń na podstawie zdefiniowanych wymagań	300
17.1. Wprowadzenie	300
17.2. Identyfikacja ograniczeń	303
17.3. Ogólna koncepcja ochrony podstawowej	307
17.4. Dobór zabezpieczeń podstawowych według rodzaju systemu	307
17.5. Dobór zabezpieczeń podstawowych według potrzeb bezpieczeństwa i zagrożeń	312
17.6. Przykład metodyki ochrony podstawowej - IT Grundschutz	316
17.6.1. Identyfikacja składników systemów teleinformatycznych	319
17.6.2. Identyfikacja aplikacji oraz przetwarzanych informacji	325
17.6.3. Określenie wymagań ochronnych dla elementów systemu	327
17.6.4. Dobór zabezpieczeń zapewniających ochronę podstawową	330
17.7. Dobór zabezpieczeń wynikających z analizy ryzyka	339
17.7.1. System zarządzania bezpieczeństwem informacji ISMS i zawarte w nim podejście do redukcji ryzyka	343
17.8. Uwzględnienie architektury systemów w architekturze bezpieczeństwa na poziomie systemów teleinformatycznych	356
17.9. Akceptacja ryzyka	357
18. Polityka bezpieczeństwa teleinformatycznego - ogółu systemów teleinformatycznych w instytucji (poziom II)	360
18.1. Zasady konstruowania	360
18.2. Zawartość i przykłady	362
18.3. Zarządzanie bezpieczeństwem na poziomie systemów	

teleinformatycznych instytucji	366
19. Polityka dotycząca bezpieczeństwa poszczególnych systemów (poziomu III) i plany zabezpieczeń	368
19.1. Zasady konstruowania	368
19.2. Zawartość dokumentu	369
19.3. Plany zabezpieczeń poszczególnych systemów	371
19.4. Zarządzanie bezpieczeństwem na poziomie systemów	373
20. Procesy wdrożeniowe	374
20.1. Wdrożenie zabezpieczeń	375
20.1.1. Opracowanie dokumentacji wdrażanych zabezpieczeń	376
20.1.2. Realizacja planu zabezpieczeń i weryfikacja jego skuteczności	378
20.2. Działania uświadamiające i ich nadzorowanie	380
20.3. Szkolenia	384
20.4. Akredytacja systemów	387
21. Czynności powdrożeniowe	391
21.1. Wykrywanie zmian i zarządzanie zmianami	392
21.2. Monitorowanie elementów systemu bezpieczeństwa	394
21.3. Zarządzanie zabezpieczeniami i utrzymywanie ich skuteczności	398
21.4. Kontrola zgodności	399
21.5. Zarządzanie incydentami i doskonalenie systemu bezpieczeństwa	404
22. Wnioski i uwagi końcowe	412
Wykaz niektórych skrótów angielskich i polskich	424
oraz oznaczeń	416
Literatura	424
Dodatki	
I. Przykład polityki dotyczącej bezpieczeństwa instytucji (poziom I)	437
I.1. Deklaracja o ustanowieniu Polityki Bezpieczeństwa Firmy e-GADGET sp. z o.o.	437
I.2. Cel opracowania i zawartość dokumentu	438
I.3. Podstawy normatywne	439
I.4. Podstawy prawne	439
I.5. Zakres oddziaływania polityki	439
I.6. Bezpieczeństwo w Firmie e-GADGET	440
I.7. Role i odpowiedzialność	441
I.8. Rozpowszechnianie i zarządzanie dokumentem polityki	442
I.9. Załączniki	442
I.9.1. Regulaminy, instrukcje, procedury	442
I.9.2. Role dotyczące bezpieczeństwa teleinformatycznego	442

I.10. Odwołanie do Polityki Bezpieczeństwa Teleinformatycznego Firmy e-GADGET sp. z o.o.	442
--	-----

II. Przykład polityki dotyczącej bezpieczeństwa teleinformatycznego instytucji (poziom II)	444
II.1. Umocowanie prawne	444
II.2. Cel opracowania i zawartość dokumentu	444
II.3. Podstawy normatywne i terminologia	445
II.4. Podstawy prawne	445
II.5. Zakres oddziaływania	446
II.6. Bezpieczeństwo informacji i usług elektronicznych w Firmie e-GADGET	446
II.6.1. Procesy biznesowe wspierane przez technologie teleinformatyczne	446
II.6.2. Postanowienia ogólne	449
II.6.3. Postępowanie wobec ryzyka	451
II.6.4. Otoczenie prawne i identyfikacja zasobów	452
II.6.5. Ogólne potrzeby bezpieczeństwa wynikające z procesów biznesowych, wspomaganych w realizacji technologiami teleinformatycznymi	460
II.6.6. Wnioski ogólne z analizy ryzyka	460
II.6.7. Metoda postępowania przy tworzeniu systemu bezpieczeństwa	461
II.6.8. Cele zabezpieczeń i ogólne strategie	462
II.6.9. Szczegółowe zasady i wymagania dotyczące zabezpieczeń	465
II.6.9.1. Wymagania dotyczące dokumentu polityki bezpieczeństwa	465
II.6.9.2. Wymagania dotyczące organizacji systemu bezpieczeństwa	465
II.6.9.3. Klasyfikacja i nadzór nad zasobami	467
II.6.9.4. Bezpieczeństwo osobowe	467
II.6.9.5. Bezpieczeństwo fizyczne i środowiskowe	468
II.6.9.6. Zarządzanie systemem	469
II.6.9.7. Kontrola dostępu	471
II.6.9.8. Rozwój i utrzymanie systemów	472
II.6.9.9. Ciągłość procesów biznesowych	474
II.6.9.10. Zgodność	474
II.7. Role i odpowiedzialność	475
II.7.1. Ogólna organizacja służb odpowiedzialnych i ich role	475
II.7.2. Komitet Bezpieczeństwa Teleinformatycznego (KBTI)	476
II.7.3. Zespół Bezpieczeństwa Teleinformatycznego (ZBTI)	477
II.7.4. Pion Eksploatacji (PE)	478
II.7.5. Użytkownicy i inni pracownicy	478
II.7.6. Postanowienia dodatkowe	480
II.7.7. Odpowiedzialność za naruszenia polityki	480
II.8. Rozpowszechnianie i zarządzanie dokumentem polityki	481
II.9. Załączniki	481
II.9.1. Normy i zalecenia wykorzystywane do tworzenia polityki	481

II.9.2. Definicje wykorzystywanych pojęć	482
II.9.3. Tajemnice prawnie chronione, występujące w Firmie e-GADGET jako element otoczenia prawnego, oznaczane jako EG-POUFNE	485
II.9.4. Tajemnice przedsiębiorstwa chronione na zasadach wzajemności, na podstawie wielostronnych umów zawartych przez Firmę e-GADGET, oznaczane EG-POUFNE	486
II.9.5. Tajemnice przedsiębiorstwa określone na podstawie zarządzeń wewnętrznych w Firmie e-GADGET, oznaczane EG-POUFNE	486
II.9.6. Działania zgodne z prawem, występujące w Firmie e-GADGET jako element otoczenia prawnego	487
II.9.7. Regulaminy, instrukcje, procedury, wzorce dokumentów	487
II.9.8. Role członków zarządu	488
II.9.9. Role w Pionie Bezpieczeństwa	488
II.9.10. Role dotyczące właścicieli zasobów	488
II.9.11. Role w Pionie Eksploatacji	489
II.9.12. Uregulowania specjalne dotyczące ról	489
II.9.13. Dokumentacja projektowa i plany	489
II.10. Odwołanie do polityki dotyczącej bezpieczeństwa poszczególnych systemów teleinformatycznych w Firmie e-GADGET sp. z o.o.	490
III. Przykład polityki dotyczącej bezpieczeństwa systemów informacyjnych instytucji w układzie ISMS	491
III.1. Wprowadzenie	491
III.2. Cel opracowania	491
III.3. Zakres oddziaływania	492
III.4. Zasady polityki	492
III.5. Zasady odpowiedzialności za bezpieczeństwo	494
III.5.1. Zasady ogólne	494
III.5.2. Odpowiedzialność kierownictwa firmy	494
III.5.3. Odpowiedzialność Inspektora Bezpieczeństwa Informacji	494
III.5.4. Odpowiedzialność Inspektora Bezpieczeństwa Technologii Informatycznych	495
III.5.5. Odpowiedzialność ogólna	496
III.6. Wskazania ogólne	496
III.7. Przegląd dokumentu polityki	496
III.8. Dokumenty związane	496
IV. Specyfikacja zagadnień bezpieczeństwa zawartych w normie PN-ISO/IEC 17799	497
V. Specyfikacja zagadnień bezpieczeństwa organizacyjnego i fizycznego zawartych w raporcie ISO/IEC TR 13335-4. Dobór zabezpieczeń podstawowych według specyficznych cech systemu	506

VI. Specyfikacja zagadnień bezpieczeństwa teleinformatycznego zawartych w raporcie ISO/IEC TR 13335-4. Dobór zabezpieczeń podstawowych według specyficznych cech systemu	515
VII. Specyfikacja zagadnień bezpieczeństwa w układzie według zagrożeń zawartych w raporcie ISO/IEC TR 13335-4. Dobór zabezpieczeń podstawowych według zagrożeń	521
Skorowidz	541

oprac. BPK