

Franciszek Wołowski
Janusz Zawila-Niedźwiecki

Bezpieczeństwo systemów informacyjnych

Praktyczny przewodnik
zgodny z normami polskimi
i międzynarodowymi



Poradnik jest skierowany w pierwszej kolejności do administratorów bezpieczeństwa systemów informacyjnych, ale nie tylko. Także do szeroko rozumianej kadry kierowniczej organizacji różnych branż, charakteru i wielkości oraz do specjalistów różnych profesji, którzy mogą się przyczyniać do zapewniania bezpieczeństwa w organizacjach. Rzecz bowiem w tym, że stan bezpieczeństwa budują wszyscy, a zburzyć go może nawet tylko jedna osoba.

edu-Libri

© edu-Libri s.c. 2012

Redakcja merytoryczna i korekta: edu-Libri

Projekt okładki i stron tytułowych: GRAFOS

Wydawnictwo edu-Libri
ul. Zalesie 15, 30-384 Kraków
e-mail: edu-libri@edu-libri.pl

Skład i łamanie: GRAFOS
Druk i oprawa: Sowa Sp. z o.o.
Warszawa

ISBN 978-83-63804-00-8
ISBN e-book 978-83-63804-01-5 (PDF)
ISBN e-book 978-83-63804-02-2 (epub)

Spis treści

Wstęp	13
1. Wprowadzenie	15
1.1. Co to jest bezpieczeństwo informacji?	17
1.2. Dlaczego zapewnianie bezpieczeństwa informacji jest potrzebne?	18
1.3. Cele, strategie i polityki w zakresie bezpieczeństwa informacji	19
1.4. Czynniki decydujące o bezpieczeństwie systemów informacyjnych	21
1.5. Jak określać wymagania bezpieczeństwa?	22
1.6. Zarządzanie bezpieczeństwem informacji	24
1.7. Standardy związane z zarządzaniem bezpieczeństwem systemów informacyjnych	30
1.8. Zarządzanie ryzykiem a zarządzanie bezpieczeństwem informacji	38
1.9. Punkt wyjścia zapewniania bezpieczeństwa informacji	41
1.10. Krytyczne czynniki sukcesu	42
2. Zarządzanie ryzykiem systemów informacyjnych	43
2.1. Nazewnictwo związane z zarządzaniem ryzykiem	45
2.1.1. Pojęcia podstawowe	45
2.1.2. Nazewnictwo modelu zarządzania ryzykiem	46
2.2. Struktura ryzyka	47
2.2.1. Ryzyko polityczne	47
2.2.2. Ryzyko organizacyjne	48
2.2.3. Ryzyko operacyjne	49
2.3. Czynniki ryzyka systemów informacyjnych	55
2.3.1. Ludzie	55
2.3.2. Procesy i systemy	56
2.3.2.1. Systemy teleinformatyczne	57
2.3.2.2. Dokumentacja wewnętrzna i zewnętrzna	58
2.3.2.3. Lokalizacja	58
2.3.3. Zdarzenia zewnętrzne	59
2.3.3.1. Zdarzenia przewidywalne i nieprzewidywalne	59
2.3.3.2. Zlecenie czynności na zewnątrz (outsourcing)	60
2.4. Procesy zarządzania ryzykiem systemów informacyjnych	61
2.5. Ustalenie oczekiwań wobec zarządzania ryzykiem	64
2.5.1. Podstawowe kryteria oceny ryzyka systemów informacyjnych	65

2.5.2. Zakres i granice procesu zarządzania ryzykiem systemów informacyjnych	66
2.5.3. Organizacja zarządzania ryzykiem systemów informacyjnych	67
2.6. Zarządzanie zasobami i aktywami systemów informacyjnych.....	67
2.6.1. Zapewnianie zasobów i aktywów oraz odpowiedzialność za nie	69
2.6.1.1. Inwentaryzacja zasobów i aktywów.....	71
2.6.1.2. Własność zasobów	73
2.6.1.3. Akceptowalne użycie zasobów.....	73
2.6.2. Klasyfikacja informacji	74
2.6.2.1. Zalecenia do klasyfikacji.....	74
2.6.2.2. Oznaczanie informacji i postępowanie z informacjami	75
2.6.3. Wartość biznesowa aktywów, zwłaszcza informacji	76
2.7. Szacowanie ryzyka systemów informacyjnych	79
2.7.1. Analiza ryzyka systemów informacyjnych.....	80
2.7.1.1. Identyfikacja ryzyka	80
2.7.1.2. Oszacowanie (wycena) ryzyka.....	91
2.7.2. Ocena ryzyka systemów informacyjnych.....	97
2.8. Postępowanie z ryzykiem systemów informacyjnych	98
2.8.1. Unikanie ryzyka	103
2.8.2. Przeniesienie ryzyka.....	104
2.8.3. Utrzymanie/akceptowanie ryzyka.....	105
2.8.4. Redukcja ryzyka	105
2.8.5. Środki sterowania bezpieczeństwem.....	106
2.8.6. Środki łagodzenia ryzyka (przeciwdziałanie).....	108
2.8.7. Strategia łagodzenia ryzyka	115
2.9. Akceptacja ryzyka przez kierownictwo	116
2.10. Informowanie o ryzyku	117
2.11. Monitorowanie i przegląd ryzyka.....	118
2.12. Kluczowe role w procesie zarządzania ryzykiem.....	120
3. Zarządzanie ryzykiem w projektach systemów informacyjnych.....	124
3.1. Wprowadzenie	124
3.2. Kryteria sukcesu projektu.....	125
3.3. Procesy zarządzania ryzykiem projektowym.....	126
3.4. Planowanie zarządzania ryzykiem projektowym.....	128
3.5. Identyfikacja zagrożeń	130
3.6. Analiza ryzyka	131
3.7. Szacowanie prawdopodobieństwa i skutku ryzyka	131
3.8. Planowanie reakcji na ryzyko.....	134
3.9. Sterowanie ryzykiem.....	135
3.10. Monitorowanie ryzyka	136
4. Zarządzanie reakcją na incydenty związane z naruszeniem bezpieczeństwa informacji	137
4.1. Podstawowe zagadnienia i korzyści związane z zarządzaniem incydentami...	138
4.2. Przykłady incydentów związanych z naruszeniem bezpieczeństwa informacji .	140
4.3. Procedury w zarządzaniu incydentami	142
4.3.1. Planowanie i przygotowanie	142
4.3.2. „Stosowanie” – wdrożenie i eksploatacja.....	153
4.3.3. Przegląd	170
4.3.4. Doskonalenie	172

5. System Zarządzania Bezpieczeństwem Informacji (SZBI)	174
5.1. Ustanowienie SZBI	176
5.1.1. Zakres i granice SZBI	176
5.1.2. Polityka bezpieczeństwa i jej akceptacja przez kierownictwo	177
5.1.3. Polityka bezpieczeństwa informacji	178
5.1.4. Dokument polityki bezpieczeństwa informacji	179
5.1.5. Przegląd polityki bezpieczeństwa informacji	180
5.1.6. Strategia zarządzania ryzykiem	181
5.2. Wdrożenie i eksploatacja SZBI	182
5.3. Monitorowanie i przegląd SZBI	182
5.4. Utrzymanie i doskonalenie SZBI	182
5.5. Organizacja zapewniania bezpieczeństwa informacji	183
5.5.1. Organizacja wewnętrzna	183
5.5.1.1. Zaangażowanie kierownictwa w zapewnianie bezpieczeństwa informacji	184
5.5.1.2. Koordynacja zarządzania zapewnianiem bezpieczeństwa informacji	184
5.5.1.3. Przepisanie odpowiedzialności w zakresie zapewniania bezpieczeństwa informacji	185
5.5.1.4. Proces autoryzacji środków przetwarzania informacji	186
5.5.1.5. Umowy o zachowaniu poufności	186
5.5.1.6. Kontakty z organami władzy	187
5.5.1.7. Kontakty z grupami zaangażowanymi w zapewnianie bezpieczeństwa	187
5.5.1.8. Niezależne przeglądy bezpieczeństwa informacji	188
5.5.2. Strony zewnętrzne	188
5.5.2.1. Ryzyko związane ze stronami zewnętrznymi	189
5.5.2.2. Bezpieczeństwo w kontaktach z klientami	190
5.5.2.3. Bezpieczeństwo w umowach ze stroną trzecią	191
5.6. Bezpieczeństwo zasobów ludzkich	194
5.6.1. Przed zatrudnieniem	195
5.6.1.1. Role i zakresy odpowiedzialności	196
5.6.1.2. Postępowanie sprawdzające	196
5.6.1.3. Zasady zatrudnienia	197
5.6.2. Podczas zatrudnienia	198
5.6.2.1. Odpowiedzialność kierownictwa	199
5.6.2.2. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	200
5.6.2.3. Postępowanie dyscyplinarne	200
5.6.3. Zakończenie lub zmiana zatrudnienia	201
5.6.3.1. Odpowiedzialność związana z zakończeniem zatrudnienia	201
5.6.3.2. Zwrot zasobów	202
5.6.3.3. Odebranie praw dostępu	202
5.7. Bezpieczeństwo fizyczne i środowiskowe	203
5.7.1. Obszary bezpieczne	205
5.7.1.1. Fizyczna granica obszaru bezpiecznego	206
5.7.1.2. Środki ochrony fizycznego wejścia	207
5.7.1.3. Zabezpieczanie biur, pomieszczeń i urządzeń	207
5.7.1.4. Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	208
5.7.1.5. Praca w obszarach bezpiecznych	208
5.7.1.6. Obszary publicznie dostępne dla dostaw i załadunku	209

5.7.2. Bezpieczeństwo wyposażenia.....	209
5.7.2.1. Rozmieszczenie i ochrona wyposażenia.....	210
5.7.2.2. Systemy wspomagające przetwarzanie informacji.....	210
5.7.2.3. Bezpieczeństwo okablowania.....	211
5.7.2.4. Bezpieczna konserwacja sprzętu.....	212
5.7.2.5. Bezpieczeństwo wyposażenia znajdującego się poza siedzibą organizacji.....	212
5.7.2.6. Bezpieczne usuwanie lub ponowne wykorzystanie wyposażenia.....	213
5.7.2.7. Wynoszenie mienia.....	213
5.8. Zarządzanie eksploatacją i komunikacją SZBI.....	214
5.8.1. Procedury eksploatacyjne i odpowiedzialność.....	214
5.8.1.1. Dokumentowanie procedur eksploatacyjnych.....	214
5.8.1.2. Zarządzanie zmianami.....	215
5.8.1.3. Rozdzielanie obowiązków.....	216
5.8.1.4. Oddzielanie środowisk rozwojowych, testowych i eksploatacyjnych.....	216
5.8.2. Zarządzanie usługami dostarczonymi przez strony trzecie.....	217
5.8.2.1. Bezpieczne dostarczanie usług.....	218
5.8.2.2. Monitorowanie i przegląd usług strony trzeciej.....	218
5.8.2.3. Bezpieczne zarządzanie zmianami usług strony trzeciej.....	219
5.8.3. Planowanie i odbiór systemów.....	219
5.8.3.1. Zarządzanie pojemnością systemów.....	220
5.8.3.2. Akceptacja systemu.....	220
5.8.4. Ochrona przed kodem złośliwym i nadzór nad kodem mobilnym.....	221
5.8.4.1. Środki ochrony przed kodem złośliwym.....	222
5.8.4.2. Środki nadzoru nad kodem mobilnym.....	224
5.8.5. Kopie zapasowe.....	224
5.8.6. Zarządzanie bezpieczeństwem sieci.....	226
5.8.6.1. Systemy ochrony sieci.....	227
5.8.6.2. Bezpieczeństwo usług sieciowych.....	227
5.8.7. Obsługa nośników danych i dokumentacji.....	228
5.8.7.1. Zarządzanie nośnikami wymiennymi.....	229
5.8.7.2. Usuwanie nośników.....	229
5.8.7.3. Procedury postępowania z informacjami.....	230
5.8.7.4. Bezpieczeństwo dokumentacji systemowej.....	230
5.8.8. Wymiana informacji.....	231
5.8.8.1. Polityka i procedury wymiany informacji.....	231
5.8.8.2. Umowy o wymianie informacji.....	233
5.8.8.3. Transportowanie fizycznych nośników informacji.....	234
5.8.8.4. Wiadomości elektroniczne.....	234
5.8.8.5. Systemy informacyjne organizacji.....	235
5.8.9. Usługi handlu elektronicznego.....	236
5.8.9.1. Handel elektroniczny.....	236
5.8.9.2. Transakcje on-line.....	238
5.8.9.3. Informacje dostępne publicznie.....	238
5.9. Kontrola dostępu.....	239
5.9.1. Wymagania biznesowe i polityka kontroli dostępu.....	241
5.9.2. Zarządzanie dostępem użytkowników.....	243
5.9.2.1. Rejestracja użytkowników.....	244

5.9.2.2. Zarządzanie przywilejami.....	245
5.9.2.3. Zarządzanie hasłami użytkowników.....	246
5.9.2.4. Przeglądy praw dostępu użytkowników.....	246
5.9.3. Odpowiedzialność użytkowników.....	247
5.9.3.1. Używanie haseł.....	247
5.9.3.2. Pozostawianie sprzętu użytkownika bez opieki.....	251
5.9.3.3. Polityka czystego biurka i czystego ekranu.....	251
5.9.4. Kontrola dostępu do sieci.....	252
5.9.4.1. Zasady korzystania z usług sieciowych.....	252
5.9.4.2. Uwierzytelnianie użytkowników przy połączeniach zewnętrznych.....	253
5.9.4.3. Identyfikacja urządzeń w sieciach.....	254
5.9.4.4. Ochrona zdalnych portów diagnostycznych i konfiguracyjnych.....	254
5.9.4.5. Rozdzielanie sieci.....	255
5.9.4.6. Kontrola połączeń sieciowych.....	256
5.9.4.7. Kontrola routingu w sieciach.....	256
5.9.5. Kontrola dostępu do systemów operacyjnych.....	256
5.9.5.1. Procedury bezpiecznego logowania się.....	257
5.9.5.2. Identyfikacja i uwierzytelnianie użytkowników.....	258
5.9.5.3. System zarządzania hasłami.....	259
5.9.5.4. Użycie systemowych programów narzędziowych.....	259
5.9.5.5. Zamykanie sesji po określonym czasie.....	260
5.9.5.6. Ograniczanie czasu trwania połączenia.....	260
5.9.6. Kontrola dostępu do informacji i aplikacji.....	261
5.9.6.1. Ograniczanie dostępu do informacji.....	261
5.9.6.2. Izolowanie systemów wrażliwych.....	261
5.9.7. Przetwarzanie mobilne i praca na odległość.....	262
5.9.7.1. Przetwarzanie i komunikacja mobilna.....	262
5.9.7.2. Praca zdalna.....	263
5.10. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.....	265
5.10.1. Wymagania bezpieczeństwa systemów informacyjnych.....	265
5.10.2. Poprawne przetwarzanie w aplikacjach.....	266
5.10.2.1. Potwierdzanie poprawności danych wejściowych.....	266
5.10.2.2. Kontrola przetwarzania wewnętrznego.....	267
5.10.2.3. Integralność wiadomości.....	268
5.10.2.4. Potwierdzanie poprawności danych wyjściowych.....	268
5.10.3. Zabezpieczenia kryptograficzne.....	268
5.10.3.1. Zasady korzystania z zabezpieczeń kryptograficznych.....	269
5.10.3.2. Zarządzanie kluczami.....	270
5.10.4. Bezpieczeństwo plików systemowych.....	271
5.10.4.1. Zabezpieczanie eksploatowanego oprogramowania.....	271
5.10.4.2. Ochrona systemowych danych testowych.....	273
5.10.4.3. Kontrola dostępu do kodów źródłowych programów.....	273
5.10.5. Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej..	274
5.10.5.1. Procedury kontroli zmian.....	274
5.10.5.2. Techniczny przegląd aplikacji po zmianach w systemie operacyjnym.....	275

5.10.5.3. Ograniczenia dotyczące zmian w pakietach oprogramowania	276
5.10.5.4. Wyciek informacji	276
5.10.5.5. Prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej	277
5.11. Wymagania dotyczące dokumentacji	277
5.11.1. Nadzór nad dokumentami	278
5.11.2. Nadzór nad zapisami	279
6. Zarządzanie zapewnianiem ciągłości działania	280
6.1. Osadzenie zapewniania ciągłości działania w kulturze organizacji	280
6.2. Zrozumienie istoty działania organizacji	292
6.2.1. Wprowadzenie procesu systematycznego zarządzania zapewnianiem ciągłości działania	292
6.2.2. Generalna analiza wpływu zakłóceń na działalność	297
6.2.3. Identyfikacja, analiza i ocena ryzyka ogólnego	299
6.2.4. Bezpieczeństwo informacji i ciągłość działania systemów informatycznych a zapewnianie ciągłości działania organizacji	302
6.3. Określanie strategii zarządzania zapewnianiem ciągłości działania	303
6.4. Opracowywanie i wdrażanie rozwiązań zapewniania ciągłości działania	305
6.4.1. Analiza ryzyka operacyjnego i mapa zakłóceń	305
6.4.2. Opracowywanie regulaminów, procedur, instrukcji	307
6.4.3. Projektowanie scenariuszy awaryjnych	309
6.4.4. Wdrażanie przyjętego postępowania z zakłóceniami	310
6.5. Testowanie, utrzymywanie i audyt rozwiązań zapewniania ciągłości działania	312
6.5.1. Testowanie	312
6.5.2. Utrzymywanie	312
6.5.3. Audyt	314
7. Odpowiedzialność kierownictwa organizacji	315
7.1. Zaangażowanie kierownictwa	315
7.2. Szkolenie, uświadamianie i kompetencje pracowników	317
8. Monitorowanie bezpieczeństwa	319
8.1. Monitorowanie i przeglądy SZBI	320
8.1.1. Niezależne przeglądy bezpieczeństwa informacji	321
8.1.2. Dzienniki zdarzeń	322
8.1.3. Monitorowanie wykorzystywania systemu	322
8.1.4. Ochrona informacji zawartych w dziennikach zdarzeń	323
8.1.5. Dzienniki zdarzeń administratora i operatora	324
8.1.6. Rejestrowanie błędów	324
8.1.7. Synchronizacja zegarów	325
8.1.8. Monitorowanie i przegląd usług strony trzeciej	325
8.1.9. Zgodność przeglądów z politykami bezpieczeństwa i standardami oraz zgodność techniczna	326
8.2. Przeglądy realizowane przez kierownictwo	327
8.2.1. Dane wejściowe do przeglądu	327
8.2.2. Wyniki przeglądu	327
9. Audyty SZBI	329
9.1. Audyty systemów informacyjnych	330

9.1.1. Bezpieczne prowadzenie audytu.....	330
9.1.2. Ochrona narzędzi audytu.....	330
9.2. Audyty wewnętrzne SZBI.....	331
9.3. Procesy audytowe	332
9.3.1. Etap przygotowawczy audytu	332
9.3.1.1. Spotkanie wstępne.....	332
9.3.1.2. Seminarium dla gremiów kierowniczych organizacji.....	333
9.3.2. Etap wykonawczy audytu	333
9.3.2.1. Ścieżka formalna audytu	333
9.3.2.2. Ścieżka techniczna audytu.....	334
9.3.3. Etap sprawozdawczy audytu.....	335
9.3.3.1. Opracowanie dokumentu końcowego.....	335
9.3.3.2. Przekazanie zleceniodawcy zbioru dokumentów audytowych.....	335
10. Doskonalenie SZBI.....	336
10.1. Ciągłe doskonalenie.....	336
10.2. Działania korygujące.....	336
10.3. Działania zapobiegawcze.....	336
11. Zgodność z przepisami prawa.....	338
11.1. Ustalenie odpowiednich przepisów prawa.....	338
11.2. Prawo do własności intelektualnej.....	338
11.3. Ochrona zapisów w organizacji	339
11.4. Ochrona danych osobowych i prywatność informacji dotyczących osób fizycznych.....	341
11.5. Zapobieganie nadużywaniu środków przetwarzania informacji	341
11.6. Regulacje dotyczące zabezpieczeń kryptograficznych.....	342
11.7. Sprawdzanie zgodności technicznej.....	343
12. Terminologia	344
12.1. Pojęcia i definicje	345
12.2. Akronimy	373
Bibliografia	388

Franciszek Wołowski – absolwent Politechniki Śląskiej (1968) oraz Studium Podyplomowego Ekonometrii i Programowania Matematycznego Wyższej Szkoły Ekonomicznej w Katowicach.

Zajmuje się zarządzaniem bezpieczeństwem systemów informacyjnych, ryzykiem oraz zastosowaniami biometrii i kryptografii klucza publicznego (podpisu elektronicznego). Wykładowca na studiach podyplomowych w Politechnice Warszawskiej, Politechnice Lubelskiej oraz w Instytucie Orgmasz, jak również na szkoleniach organizowanych przez instytucje administracji publicznej. Prelegent na wielu konferencjach zawodowych poświęconych ryzyku i bezpieczeństwu oraz autor szeregu publikacji w specjalistycznych wydawnictwach, w tym współautor książki *Podpis elektroniczny w administracji i zarządzaniu* (2005).

Janusz Zawila-Niedźwiecki – od kilkunastu lat pracownik naukowy Wydziału Zarządzania Politechniki Warszawskiej, wykładowca Collegium Civitas, członek Polskiej Komisji Akredytacyjnej. Redaktor naukowy książek *Informatyka gospodarcza* (4 tomy, 2010) i *Zarządzanie ryzykiem operacyjnym* (2008). Autor książki *Ciągłość działania organizacji* (2008) oraz kilkudziesięciu artykułów i referatów konferencyjnych naukowych i zawodowych z zakresu zarządzania ryzykiem, bezpieczeństwem i ciągłością działania.

Równocześnie menedżer praktyk, w przeszłości m.in. w NBP, Pol-Mot, Giełdzie Papierów Wartościowych, Fund Services, Grupie PZU, Komisji Nadzoru Finansowego, Urzędzie Komunikacji Elektronicznej. Obecnie doradca biznesowy w firmie Casus Unicus.

W roku 1998 jako dyrektor IT Giełdy laureat nagrody „Lider Informatyki” przyznawanej przez Computerworld. Członek założyciel polskiego oddziału stowarzyszenia ISACA, przewodniczący Rady Fundacji im. Prof. Kazimierza Bartla.

www.edu-libri.pl

Wydawnictwo edu-Libri jest nowoczesną oficyną wydawniczą e-publikacji naukowych i edukacyjnych.

Współpracujemy z doświadczonymi redaktorami merytorycznymi oraz technicznymi specjalizującymi się w przygotowywaniu publikacji naukowych i edukacyjnych. Stawiamy na jakość i profesjonalizm łączone z nowoczesnością, a najważniejsze dla nas są przyjemność współtworzenia i satysfakcja z dobrze wykonanego zadania.

Nasze publikacje są dostępne w księgarniach internetowych związanych z platformą cyfrową iFormat oraz w czytelniku on-line ibuk.pl (dystrybucja realizowana przez – działający w obrębie grupy PWN – OSDW Azymut).

Na życzenie drukujemy dowolną liczbę egzemplarzy papierowych książek.