

Spis treści

Wykaz skrótów i symboli	8
Wstęp	11
1. Metodologiczne podstawy monografii	13
1.1. Analiza stanu wiedzy	13
1.2. Uzasadnienie wyboru problemu naukowego	14
1.3. Problemy badawcze	15
1.4. Przedmiot badań	16
1.5. Cele badawcze	17
1.6. Hipotezy robocze	18
1.7. Metodyka i metody badawcze	19
1.8. Przyjęte założenia i ograniczenia	21
1.9. Zakres monografii	22
2. Wprowadzenie do zarządzania bezpieczeństwem informacji organizacji	25
2.1. Określenie informacji i bezpieczeństwa informacji organizacji	25
2.2. Określenie i znaczenie zarządzania bezpieczeństwem informacji	29
2.3. Określenie i znaczenie systemu zarządzania bezpieczeństwem informacji	31
3. Polityka bezpieczeństwa informacji w procesie zarządzania bezpieczeństwem informacji organizacji	33
3.1. Uwarunkowania modelowania polityki bezpieczeństwa informacji	34
3.1.1. Zagrożenia informacji i systemów teleinformatycznych organizacji	35
3.1.2. Wymagania dotyczące bezpieczeństwa informacji i systemy teleinformatyczne organizacji	51
3.1.3. Metody i sposoby ochrony informacji i systemów teleinformatycznych organizacji	59
3.1.4. Zasoby bezpieczeństwa informacji i systemów teleinformatycznych organizacji	79
3.2. Proces i metodyka modelowania polityki bezpieczeństwa informacji	88
3.2.1. Określenie potrzeb w zakresie bezpieczeństwa informacji	90
3.2.2. Określenie uwarunkowań i otoczenia bezpieczeństwa informacji	91
3.2.3. Określenie funkcjonalności bezpieczeństwa informacji	97
3.2.4. Poszukiwanie i wybór właściwego rozwiązania bezpieczeństwa informacji	98

3.2.5.	Opracowanie rozwiązania bezpieczeństwa informacji	100
3.2.6.	Wdrożenie rozwiązania bezpieczeństwa informacji	102
3.3.	Modele i organizacja polityki bezpieczeństwa informacji w zarządzaniu bezpieczeństwem organizacji	103
3.3.1.	Polityka bezpieczeństwa informacji	103
3.3.2.	Polityka ochrony danych osobowych	111
3.4.	Funkcjonowanie polityki bezpieczeństwa informacji w procesie zarządza- nia bezpieczeństwem informacji organizacji	113
4.	Elementy i procesy zarządzania bezpieczeństwem informacji organizacji	115
4.1.	Zasoby organizacji związane z przetwarzaniem i bezpieczeństwem infor- macji	116
4.2.	Zagrożenia i incydenty związane z bezpieczeństwem informacji	119
4.3.	Podatność zasobów i następstwa niepożądanych incydentów	121
4.4.	Kontrola dostępu	122
4.5.	Zabezpieczenia przed zagrożeniami	124
4.6.	Ograniczenia i zgodność w bezpieczeństwie informacji	126
4.7.	Ryzyko i ryzyko szczytkowe	127
4.8.	Konfiguracja i zmiany	129
4.9.	Monitorowanie i audytowanie	130
4.10.	Bezpieczna eksploatacja	132
4.11.	Bezpieczeństwo komunikacji	134
4.12.	Relacje z dostawcami	135
4.13.	Ciągłość działania	138
4.14.	Rozwój systemów bezpieczeństwa	139
5.	Proces zarządzanie ryzykiem w bezpieczeństwie informacji organizacji	140
5.1.	Zarządzanie ryzykiem w bezpieczeństwie organizacji	140
5.1.1.	Proces zarządzania ryzykiem w organizacji	140
5.1.2.	Ocena ryzyka	147
5.1.3.	Techniki oceny ryzyka w organizacji	156
5.2.	Proces zarządzania ryzykiem w bezpieczeństwie informacji	159
5.2.1.	Ustanowienie kontekstu szacowania ryzyka bezpieczeństwa infor- macji	162
5.2.2.	Szacowanie ryzyka w bezpieczeństwie informacji	168
5.2.3.	Postępowanie z ryzykiem w bezpieczeństwie informacji	182
5.3.	Akceptowanie ryzyka w bezpieczeństwie informacji	185
5.4.	Informowanie o ryzyku w bezpieczeństwie informacji	187
5.5.	Monitorowanie i przegląd ryzyka w bezpieczeństwie informacji	188
5.6.	Szacowanie ryzyka bezpieczeństwa informacji w praktyce	189
5.6.1.	Szacowanie ryzyka w bezpieczeństwie informacji według rozwią- zań normalizacyjnych	190
5.6.2.	Szacowanie ryzyka bezpieczeństwa informacji w środowisku na- ukowym	198
6.	Audyt bezpieczeństwa informacji organizacji	207
6.1.	Proces audytu bezpieczeństwa informacji organizacji	209
6.2.	Metodyki i standardy prowadzenia audytu bezpieczeństwa informacji organizacji	213

7. System Zarządzania Bezpieczeństwem Informacji organizacji	224
7.1. Określenie i znaczenie Systemu Zarządzania Bezpieczeństwem Infor- macji	224
7.2. Model Systemu Zarządzania Bezpieczeństwem Informacji	226
7.3. Organizacja i funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji	231
7.3.1. Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji	232
7.3.2. Wdrożenie i eksploatacja Systemu Zarządzania Bezpieczeństwem Informacji	233
7.3.3. Monitorowanie i przegląd System Zarządzania Bezpieczeństwem Informacji	233
7.3.4. Utrzymanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji	234
8. Podstawy prawne i normalizacyjne zarządzania bezpieczeństwem infor- macji	236
8.1. Programy i akta prawne Unii Europejskiej	237
8.2. Programy i akta prawne Rzeczypospolitej Polskiej	246
8.3. Dokumenty normalizacyjne dotyczące bezpieczeństwa i zarządzania bez- pieczeństwem informacji	265
9. Praktyczne uwagi w zarządzaniu bezpieczeństwem informacji organizacji	267
Zakończenie	284
Bibliografia	286
Załączniki	292
Spis tabel i rysunków	314

W okresie cywilizacji informacyjnej oraz społeczeństwa informacyjnego w sposób masowy przetwarza się informację. Współcześnie znaczne ilości informacji przetwarzają różnorodne organizacje i stowarzyszenia zarówno w wymiarze międzynarodowym, jak i krajowym. Przetwarzane są także przez zwykłych obywateli. Informacja to wiedza o otaczającym nas świecie, występujących zjawiskach i istniejących procesach, które stymulują rozwój współczesnej rzeczywistości.

Prowadzone badania oraz praktyka wskazują, że informacja w cywilizacji informacyjnej (poza dobrem, jakie sobą niesie) stwarza również zagrożenia. Środowisko cyberprzestrzeni, w jakim jest głównie przetwarzana, sprzyja zagrożeniom informacji. Przykładem takiego stanu są rezultaty powszechnie stosowanego Internetu oraz różnorodnych sieci teleinformatycznych, które przetwarzają informacje w publicznych chmurach obliczeniowych. By przeciwdziałać temu niekorzystnemu zjawisku w przetwarzaniu informacji, w sieciach i systemach teleinformatycznych, stosuje się szereg różnorodnych metod i sposobów ochrony informacji, rozwiązań standaryzacyjnych i normalizacyjnych po uregulowania prawne włącznie.

Współcześnie występujące i dynamicznie rozwijające się zagrożenia informacji w cyberprzestrzeni, a także stosowane różnorodne rozwiązania ochrony przetwarzanej informacji wymagają działania uporządkowanego i sprzyjającego bezpieczeństwu informacji. Tego rodzaju działania realizowane są przez organizacje w ramach zarządzania bezpieczeństwem informacji. Zarządzanie bezpieczeństwem informacji jest szczególnym sposobem kierowania zasobami osobowymi i materialnymi organizacji, których treścią jest zapewnienie ochrony przetwarzanej informacji w imię osiągnięcia celów biznesowych tej organizacji. W swej istocie dotyczy modelowania i organizowania oraz wdrażania rozwiązań

z zakresu bezpieczeństwa informacji, kierowania i zarządzania procesami bezpieczeństwa informacji w celu przeciwdziałania zagrożeniom i zapewnienia jej poufności, integralności oraz dostępności.

Niniejsza monografia kierowana jest do osób zajmujących się zarządzaniem bezpieczeństwem informacji w różnych organizacjach, zajmujących się modelowaniem bezpieczeństwa informacji oraz tych osób, które zajmujących się ochroną informacji. Monografia kierowana jest do środowiska naukowego związanego z bezpieczeństwem informacji oraz studentów poznających i studiujących problemy z tym związane.