

Spis treści

Przedmowa	7
Wprowadzenie - transformacja cyfrowa	9
1. CHARAKTERYSTYKA SYSTEMÓW IoT	11
1.1. Definicja Internetu Rzeczy (IoT)	11
1.2. Kontekst chmury obliczeniowej	13
1.3. Infrastruktura informatyczna	16
1.4. Aplikacje IoT	19
2. ARCHITEKTURA ODNIESIENIA IoT	21
2.1. Zasady ogólne	21
2.2. Cechy systemów IoT	22
2.2.1. Wiarygodność systemu IoT	22
2.2.2. Architektura systemu IoT	26
2.2.3. Funkcjonalność systemu IoT	32
2.3. Model konceptualny	39
2.3.1. Zasady ogólne	39
2.3.2. Koncepcje	40
2.4. Model referencyjny	46
2.4.1. Kontekst	46
2.4.2. Rodzaje modeli referencyjnych	46
2.5. Model interoperacyjności	50
3. KOMUNIKACJA W SYSTEMACH IoT	53
3.1. Zarządzanie danymi	53
3.1.1. Informacje a dane	53
3.1.2. Eksploracja danych	54
3.1.3. Wymiana danych	55
3.1.4. Operacje przetwarzania danych w chmurze obliczeniowej	55
3.2. Standardy komunikacji	56
3.2.1. Zasady ogólne	56
3.2.2. Struktura protokołu komunikacyjnego	57
3.2.3. Implementacja protokołu IP	59
3.2.4. Topologia sieci	60
3.2.5. Standardy komunikacji bezprzewodowej	61
3.2.6. Technologie oparte na paśmie ISM	61
3.2.7. Inne technologie mobilne oparte na paśmie	66
3.3. Kryteria wyboru sposobu komunikacji	68
4. MODEL BEZPIECZEŃSTWA IoT	71
4.1. Podatność systemu	71
4.2. Ogólne wymagania cyberbezpieczeństwa	74
4.3. Moduł cyberbezpieczeństwa	78

4.4. Identyfikacja komponentów systemu IoT	79
4.4.1. Zasady ogólne	79
4.4.2. Jednoznaczne opakowanie	80
4.4.3. Schematy URN	81
4.4.4. Stosowanie URI w systemach IoT	82
4.4.5. Zastosowania niepowtarzalnej identyfikacji	82
5. ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM W SYSTEMACH IoT	83
5.1. Zasady ogólne	83
5.2. Kontrola dostępu	84
5.2.1. Prawa dostępu	84
5.2.2. Dostęp do usług sieciowych	85
5.2.3. Dostęp do aplikacji	87
5.2.4. Komunikacja mobilna	87
5.2.5. System kontroli dostępu	88
5.3. Zabezpieczenia kryptograficzne	91
5.3.1. Wprowadzenie	91
5.3.2. Zasady stosowania	93
5.4. Wdrażanie i serwis systemów informatycznych	94
5.4.1. Projektowanie zabezpieczeń - wymagania	94
5.4.2. Jakość i bezpieczeństwo oprogramowania	95
5.4.3. Testowanie oprogramowania	96
5.4.4. Wybór zabezpieczeń	97
5.4.5. Serwisowanie	98
5.5. Zarządzanie bezpieczeństwem sieci	99
5.5.1. Zabezpieczenia sieci	99
5.5.2. Wymagania bezpieczeństwa w stosunku do usług sieciowych	99
5.5.3. Aspekty bezpieczeństwa komunikacji	100
5.5.4. Separacja sieci	102
5.5.5. Techniki wykrywania włamań	103
5.6. Bezpieczeństwo eksploatacji	105
5.6.1. Zasady ogólne	105
5.6.2. Zapewnienie integralności oprogramowania	106
5.6.3. Kopie zapasowe	108
5.6.4. Ochrona przed wyciekiem danych	108
5.6.5. Testy bezpieczeństwa systemu	109
5.6.6. Monitorowanie zdarzeń	109
5.6.7. Zarządzanie podatnościami technicznymi	111
5.7. Zarządzanie incydentami bezpieczeństwa	111
5.7.1. Zasady ogólne	111
5.7.2. Analiza incydentów bezpieczeństwa	112
6. PODSUMOWANIE - WNIOSKI	113
Bibliografia	116
Załącznik. Wykaz akronimów i ich objaśnienia	121