

Spis treści

1. Wstęp	9
2. Rola GSM-R w systemie ERTMS	15
2.1. Interoperacyjność transportu kolejowego	15
2.2. Uwarunkowania techniczne wdrażania systemu ERTMS	15
2.3. Poziomy zaawansowania systemu	17
2.4. Uwarunkowania prawne wdrażania systemu ERTMS	20
3. Charakterystyka systemu GSM-R	23
3.1. Ogólna charakterystyka systemu GSM-R	23
3.2. Architektura systemu GSM-R	24
3.2.1. Podsystem stacji bazowych	30
3.2.2. Część komutacyjno-sieciowa NSS	31
3.2.3. Centrala MSC (<i>Mobile Switching Centre</i>)	32
3.2.4. Centrala GMSC (<i>Gateway Mobile Switching Centre</i>)	33
3.2.5. Rejestr abonentów własnych HLR (<i>Home Location Register</i>)	34
3.2.6. Centrum identyfikacji AuC (<i>Authentication Centre</i>)	34
3.2.7. Rejestr identyfikacji stacji ruchomych EIR (<i>Equipment Identification Register</i>)	34
3.3. Podstawowe parametry transmisji radiowej systemu GSM	35
3.4. Usługi i funkcje realizowane przez system GSM-R	37
4. Analiza ruchu telekomunikacyjnego w GSM-R	41
4.1. Źródła ruchu telekomunikacyjnego w sieci GSM-R	41
4.2. Połączenia głosowe	43
4.3. Transmisja danych	44
4.4. Usługi dodane	45
5. Identyfikacja zagrożeń transmisji informacji w systemie GSM-R	47
5.1. Ogólna klasyfikacja zagrożeń informacji	47
5.2. Analiza obszarów zagrożeń informacji w systemie GSM-R	49
5.2.1. Czynniki techniczne	49
5.2.2. Czynniki ludzkie	50
5.2.3. Czynniki organizacyjne	52
6. Analiza i szacowanie ryzyka w systemie zarządzania bezpieczeństwem informacji	53
6.1. Rola szacowania ryzyka w systemie zarządzania bezpieczeństwem informacji	53
6.2. Etapy procesu szacowania ryzyka	57
6.3. Identyfikacja zagrożeń i podatności w systemie cyfrowej radiołączności kolejowej	63

6.4. Sztuczne sieci neuronowe jako narzędzie do szacowania ryzyka w systemie zarządzania bezpieczeństwem informacji	69
7. Mechanizmy zapewnienia bezpieczeństwa transmisji informacji w sieciach komórkowych	73
7.1. Zabezpieczenie dostępu do sieci	73
7.1.1. Identyfikacja użytkownika	73
7.1.2. Uwierzytelnienie użytkownika	74
7.1.3. Poufność tożsamości i lokalizacji abonenta	75
7.1.4. Poufność i integralność transmisji	76
7.1.5. Weryfikacja urządzenia	77
7.1.6. Ochrona kryptograficzna procedury dostępu	78
7.2. Metody zabezpieczenia sieci szkieletowej	80
7.2.1. Redundancja sprzętowa	80
7.2.2. Automatyczne systemy dozoru	80
7.3. Metody zabezpieczenia domeny aplikacji	80
7.3.1. Protokoły szyfrujące	80
7.3.2. Ochrona sieci sygnalizacji SS7	82
7.3.3. Inne rozwiązania sprzętowe	83
7.4. Metody zabezpieczenia interfejsu radiowego	85
7.4.1. Interfejs radiowy a model OSI	85
7.4.2. Szyfrowanie interfejsu radiowego	86
7.4.3. Identyfikacja użytkownika	87
7.4.4. Identyfikacja modułu użytkownika	88
8. Metody zapewnienia bezpieczeństwa transmisji informacji w sieci GSM-R	91
8.1. Wprowadzenie	91
8.2. Metody zapewnienia pokrycia radiowego	91
8.2.1. Podstawowe zasady planowania sieci radiowej	91
8.2.2. Kontrola pokrycia radiowego	96
8.2.3. Ocena jakości sieci radiowej	105
8.2.4. Dostępność usług (<i>Accessability</i>)	108
8.2.5. Monitorowanie ciągłości usługi (<i>Retainability</i>)	111
8.2.6. Dostępność zasobów sieci radiowej	115
8.2.7. Jakość transmisji pakietowej	117
8.3. Metody zapewnienia ciągłości działania systemu GSM-R	118
8.3.1. Analiza metod zapewnienia dostępności	118
8.3.2. Metoda szacowania dostępności sieci GSM-R	124

9. Analiza i ocena dostępności systemu GSM-R na przykładzie ERTMS	137
9.1. Analiza wymagań dotyczących bezpieczeństwa działania systemu	137
9.2. Ocena dostępności systemu GSM-R na przykładzie ERTMS	139
10. Wybrane aspekty bezpieczeństwa fizycznego i środowiskowego systemu GSM-R	145
10.1. Bezpieczeństwo fizyczne systemu cyfrowej radiołączności kolejowej	145
10.2. Zagadnienia kompatybilności elektromagnetycznej w systemach cyfrowej radiołączności kolejowej	153
10.3. Analiza zakłóceń odbiorników sieci GSM-R	168
11. Metody administracyjno-organizacyjne zapewnienia bezpieczeństwa transmisji informacji w sieci GSM-R	175
12. Zakończenie	181
Literatura	185
Wykaz ważniejszych symboli i skrótów	195