

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	3
ВСТУП	5
РОЗДІЛ 1. КОРОТКИЙ ОГЛЯД СУЧАСНИХ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ	7
1.1. Стандарт GSM (Global System for Mobile Communications)	7
1.2. Стандарт UMTS (Universal Mobile Telecommunications System)	9
1.3. Стандарт Wi-Fi (Wireless Fidelity)	12
1.4. Стандарт WIMAX (Worldwide Interoperability for Microwave Access)	15
1.5. Технологія LTE (Long Term Evolution)	18
РОЗДІЛ 2. КОРОТКИЙ ОГЛЯД ТА ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ТЕХНОЛОГІЇ LTE	20
2.1. Архітектура технології LTE	21
2.2. Частотні діапазони для FDD і TDD та вимоги до технології LTE	22
2.3. Діапазони частот, які підтримуються для технології LTE	23
2.4. Ортогонально-частотне мультиплексування OFDM та багаторазова технологія доступу OFDMA	24
2.4.1. Технологія доступу для низхідного каналу	24
2.4.2. Технологія передачі даних у висхідному каналі	27
2.5. Інформаційні потоки	31
2.6. Механізм диспетчеризації та повторні передачі	32
2.7. Багатоантенні системи	33
РОЗДІЛ 3. АВТЕНТИФІКАЦІЯ ТА ШИФРУВАННЯ В МЕРЕЖАХ GSM/GPRS	35
3.1. Архітектура GPRS	35
3.2. Модель безпеки GPRS	37
3.3. Автентифікація GPRS	38
3.4. Шифрування GPRS	41
РОЗДІЛ 4. БЕЗПЕКА UMTS	43
4.1. Огляд архітектури безпеки	46
4.1.1. Захист доступу до мережі	47
4.1.2. Безпека домену мережі	48
4.1.3. Безпека домену користувача	49
4.1.4. Захист домену додатків	51
4.1.5. Видимість і конфігурація безпеки	52
4.2. Ідентичність користувача	52
4.3. Автентифікація та забезпечення ключів сесії	54
4.4. Захист каналу зв'язку	57
4.5. Автентифікація та узгодження ключів	58
4.5.1. Двоступеневий підхід	58
4.5.2. Одноразова взаємна автентифікація та узгодження ключа	58
4.5.3. Специфічні функції оператора і набір алгоритмів MILENAGE	62

4.6. Конфіденційність і захист цілісності	64
4.6.1. Криптографічне ядро KASUMI	64
4.6.2. Забезпечення конфіденційності	65
4.6.3. Забезпечення цілісності	66
4.7. Обговорення та короткий аналіз UMTS АКА	68
4.7.1. Забезпечення конфіденційності	69
4.7.2. Забезпечення цілісності	72
4.7.3. Альтернативні алгоритми для F8 і F9	75
4.7.4. Передача ключа	75
4.8. Висновок про безпеку UMTS	75
РОЗДІЛ 5. БЕЗПЕКА НА РІВНІ LTE	77
5.1. Концепція безпеки LTE	77
5.2. Процедура безпеки в LTE	78
5.3. Автентифікація EPS і узгодження ключів	81
5.3.1. Запит автентифікації UE	83
5.3.2. Автентифікація обміну даними між MME і HSS	84
5.3.3. Взаємна автентифікація UE і MME	85
5.4. NAS і безпека AS	87
5.4.1. Безпека NAS	88
5.4.1.1. Налаштування безпеки NAS	88
5.4.1.2. Після налаштування безпеки NAS	97
5.4.2. AS Security	98
5.4.2.1. Налаштування безпеки AS	98
5.5. Після налаштування безпеки AS	103
5.6. Контекст безпеки та ієрархія ключів у LTE / E-UTRAN	105
5.7. LTE Security	106
5.8. Порівняння безпеки в стандартах 4G, 3G, 2G	108
РОЗДІЛ 6. АНАЛІЗ ТЕХНОЛОГІЇ 5G ТА ПОКАЗНИКІВ БЕЗПЕКИ В МЕРЕЖІ	110
6.1. Загальні відомості про 5G мережі	110
6.2. Поняття безпеки в 5G	115
6.3. Архітектура безпеки в 5G	118
6.3.1. Аналіз системи та впровадження архітектури безпеки	122
6.3.2. Показники ефективності архітектури безпеки 5G-мережі	123
РОЗДІЛ 7. АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ В 5G МЕРЕЖАХ	126
7.1. Загрози 5G пов'язані з Інтернетом речей	126
7.2. Загрози пов'язані з Massive IoT	128
7.3. Загрози опорної мережі	130
7.4. Загрози мережевого доступу	136
7.5. Загрози граничних обчислень мультисервісного доступу	138
7.6. Загрози віртуалізації	138
7.7. Загрози фізичної інфраструктури	139
7.8. Загрози загального характеру	140
7.9. Аналіз загроз в непублічній мережі	143
7.9.1. Вразливості SIM-карт	144

7.9.2. Вразливості мережі	145
7.9.3. Вразливості ідентифікації	146
РОЗДІЛ 8. ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ	148
8.1. Вдосконалена модель безпеки 5G	148
8.2. Моніторинг безпеки	151
8.3. Безпека фізичної інфраструктури 5G мереж	152
8.4. Потенційні рішення проблем з безпекою	154
8.4.1. Рішення проблем безпеки в мобільних хмарах	154
8.4.2. Рішення проблем безпеки в SDN та NFV	155
8.4.3. Рішення проблем безпеки в каналах зв'язку	156
8.4.4. Рішення проблем конфіденційності в 5G	156
8.4.5. Рішення проблем безпеки граничних обчислень	157
8.4.6. Виявлення загроз	158
8.4.7. Безпека Інтернету речей	159
8.4.8 Безпека МіоТ	161
8.4.9. Забезпечення безпеки в непублічній мережі	162
8.5. Рекомендації по забезпеченню безпеки	163
ЛАБОРАТОРНИЙ ПРАКТИКУМ	167
РЕКОМЕНДОВАНА ЛІТЕРАТУРА	177