ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО
ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження безпеки телефонних розмов стандарту GSM»

на здобуття освітнього ступеня магістра
зі спеціальності __125_____
Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____Микита КРУГЛЯК

Виконав: здобувач вищої освіти групи СЗДМ-61

_____КРУГЛЯК Микита

Керівник: _____ПЕПА Юрій_____
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Систем інформаційного та кібернетичного захисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

КРУГЛЯКУ Микиті Олексійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Дослідження безпеки телефонних розмов стандарту GSM».
Керівник кваліфікаційної роботи: ПЕПА Юрій, к.т.н., доцент.
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

Затверджена наказом Державного університету інформаційно-комунікаційних технологій від «____» 2023 р. №_____.

2. Строк подання кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
__Загрози витоку інформації через радіоканал та мережу Інтернет.
__Стандарт стільникового зв'язку GSM.
__Оцінка методів шифрування, способів ідентифікації терміналів та рух між стільниками.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1.__Дослідження стандарту GSM та способів здійснення телефонних розмов.
2.__Аналіз методів шифрування та способів вибору частотного каналу для зв'язку з базовою станцією.
3.__Пропозиції щодо покращення захищеності каналу зв'язку та конфіденційних розмов між двома абонентами стільникової мережі.

5. Перелік графічного матеріалу: _____Презентаційний матеріал на слайдах_____
_____

6. Дата видачі завдання _____15.10.2023 р._____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз літературних джерел		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання четвертого розділу роботи		
6	Написання п’ятого розділу роботи		
7	Написання висновків по роботі		
8	Підготовка демонстраційних матеріалів		
9	Підготовка доповіді		

Здобувач вищої освіти _____ Микита КРУГЛЯК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій ПЕПА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи містить: 97 стор., 22 рис., 8 табл. та 16 джерел.

Об'єкт дослідження – стільникова мережа.

Предмет дослідження – методи та способи шифрування телефонних розмов в мережі GSM.

Мета роботи – проаналізувати сучасний стан системи стільникового зв'язку стандарту GSM та оцінити можливість здійснення конфіденційних телефонних розмов між двома абонентами в цій мережі.

Методи дослідження: аналітичні методи, методи порівнянь, метод ієрархій.

В роботі дослідженні питання організації телефонних розмов із застосуванням телефонів чи смартфонів рухомого стільникового зв'язку стандарту GSM, також приділено увагу методам захисту і шифрування, проаналізовано їх вразливості.

Розроблено рекомендації щодо підвищення рівня безпеки телефонних розмов з використанням криптографічних методів та крипто-телефонів, а також запропоновано оператору задіяти всі можливі способи шифрування, що передбачені у стандарті GSM, але не застосовуються в Україні.

Галузь використання – захист мовної інформації в мобільній мережі.

Ключові слова: КРИПТОАЛГОРИТМ, ЗЛАМ КЛЮЧІВ, ШИФРУВАННЯ, ІДЕНТИФІКАЦІЯ, АБОНЕНТ, ВИТІК ІНФОРМАЦІЇ.

ABSTRACT

The text part of the master's qualification work contains: 97 pages, 22 figures, 8 tables and 16 sources.

The object of research – cellular network.

Subject of research – methods and ways of encrypting telephone conversations in the GSM network.

Purpose – to analyze the current state of the GSM cellular communication system and to assess the possibility of confidential telephone conversations between two subscribers in this network.

Research methods: analytical methods, comparison methods, hierarchy method.

The paper investigates the organization of telephone conversations using GSM mobile cellular phones or smartphones, also pays attention to security and encryption methods, and analyzes their vulnerabilities.

Recommendations are developed to increase the level of security of telephone conversations using cryptographic methods and crypto-phones, and it is proposed that the operator use all possible encryption methods provided for in the GSM standard, but not used in Ukraine.

The field of application is the protection of speech information in a mobile network.

Keywords: CRYPTOALGORITHM, KEY CRACKING, ENCRYPTION, IDENTIFICATION, SUBSCRIBER, INFORMATION LEAKAGE.

ЗМІСТ

ВСТУП

GSM - це сама широко використовувана система стільникового телефонного зв'язку у світі й має більше 100 мільйонів користувачів. GSM була однією з перших систем цифрового мобільного зв'язку, що з'явилися після ери аналогових систем. Загальновідомі проблеми аналогових систем, конкурента GSM: можливість шахрайства шляхом клонування телефону, що дає можливість дзвонити за чужий рахунок, перехоплювати телефонні розмови в ефірі й прослуховувати їх. Система GSM повинна була вирішити ці проблеми за рахунок строгої аутентифікації між мобільним телефоном і Мобільним Центром комутації, а також здійснювати стійке шифрування даних для трансляції в ефірі по каналі передачі між мобільним телефоном і базовою станцією.

Технічні вимоги GSM таємно розроблялися Консорціумом GSM і надавалися виробникам устаткування й програмного забезпечення й операторам зв'язку GSM тільки в міру необхідності. Технічні вимоги ніколи не були надбанням громадськості, щоб учені світового співтовариства не могли вивчити закладені усередині її алгоритми аутентифікації й шифрування, а також модель безпеки GSM у цілому. Консорціум GSM покладався на Безпеку через невідомість, тобто алгоритми складніше зламати, якщо вони не доступні привселюдно. У світовому вченому співтоваристві вважається, що одна з основних вимог по безпеці криптографічних алгоритмів - це безпека криптосистеми, що залежить тільки від ключа. Це відомо, як "припущення Керкхоффа". Алгоритм повинен бути відомий, щоб його можна було досліджувати. Вважається, що ніяка організація не може найняти достатню кількість експертів, які зможуть змагатися зі світовим співтовариством учених у розшифровці алгоритму. Таким чином, алгоритми, розроблені й реалізовані потай, будуть, імовірно, криптографічно слабкими й будуть із помилки в дизайні. Імовірно,

алгоритми GSM стали відомі, і з тих пір їх всебічно вивчають, у ході криптоаналізу алгоритмів A3, A5 і A8 було виявлено багато цікавих фактів.

У цій роботі буде розглянута модель безпеки GSM і вивчені всі вразливі місця цієї моделі для того, щоб показати, що всі ці місця можуть бути атаковані ворогом, зловмисником, оператором або користувачем. Також буде показано, що перехоплення GSM і прослуховування телефонної розмови можливо в існуючих у цей час системах GSM, незалежно від заяви Консорціуму GSM. При дослідженні різних ділянок атак у системі GSM будуть показані можливі способи перехоплення розмов по мобільному телефону, які можна здійснити для прослуховування дзвінка по мобільному телефону.

1 РАДІОКАНАЛ ВИТОКУ ІНФОРМАЦІЇ

1.1 Структура радіоканалів витоку інформації

У сучасних умовах насиченості нашого життя найрізноманітнішими технічними, особливо електронними, засобами виробничої й трудової діяльності, різними засобами зв'язку, різного роду допоміжними системами (телебачення, радіомовлення) конче потрібно розуміти небезпеку виникнення каналу витоку інформації з обмеженим доступом саме через технічні засоби її обробки. Більше того, технічні засоби чи відносяться не до найнебезпечнішим і широко розповсюджених каналів витоку інформації.

Аналіз фізичної природи численних перетворювачів і випромінювачів показує, що:

- джерелами небезпечного сигналу є елементи, вузли й провідники технічних засобів забезпечення виробничої й трудової діяльності, а також радіо- і електронна апаратура;
- кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;
- кожна електронна система, що містить у собі сукупність елементів, вузлів і провідників, має деяку множину технічних каналів витоку інформації.

З певним ступенем узагальнення множину радіоканалів витоку інформації можна представити у вигляді наступної структури (Рис. 1.1).

Кожний із цих каналів, залежно від конкретної реалізації елементів, вузлів і виробів у цілому, буде мати певний прояв, специфічні характеристики й особливості утворення, пов'язані з умовами розташування й виконання.

Наявність і конкретні характеристики кожного джерела утворення каналу витоку інформації вивчаються, досліджуються й визначаються конкретно для кожного зразка технічних засобів на спеціально обладнані для цього іспитових стендах і в спеціальних лабораторіях.

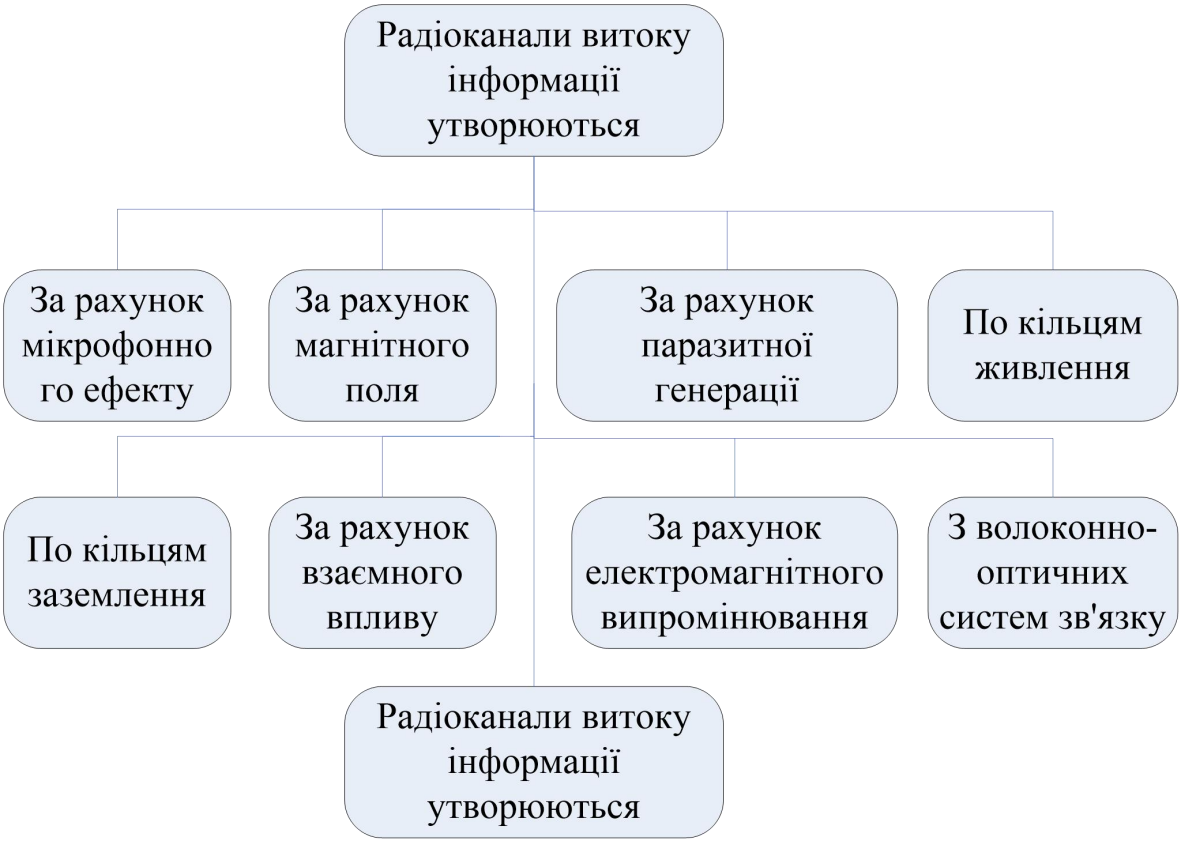

Рисунок 1.1 — Структура радіоканалів витоку інформації

Класифікація радіоканалів витоку інформації по природі утворення, діапазону випромінювання й середовищу поширення представлена на рис. 1.2.

Оцінка електромагнітних полів корисних і сигналів, що заважають, у місці прийому або оцінка властиво радіосигналів на вході приймача (після перетворення електромагнітного поля в радіосигнали антеною приймального пристрою) становить сутність електромагнітної обстановки, що відображається статичною моделлю (рис. 1.3).

Рисунок 1.2 — Класифікація радіоканалів витоку інформації

Модель містить блоки каналу передачі інформації й ланки опису станів інформації. Блоки моделі відповідають матеріальним елементам, що забезпечують формування, передачу, поширення й, частково, прийом радіосигналів. Відповідно до цього містить у собі наступні блоки: джерело корисних сигналів; джерела сигналів, що заважають (ненавмисних перешкод); середовище поширення електромагнітних коливань.

Інформаційний опис процесів формування ЕМО з урахуванням наявності ненавмисних перешкод здійснюється в ланках (просторах): просторі повідомлень Λ, просторі корисних сигналів S, просторі сигналів, що заважають, V і просторі вхідних сигналів U.

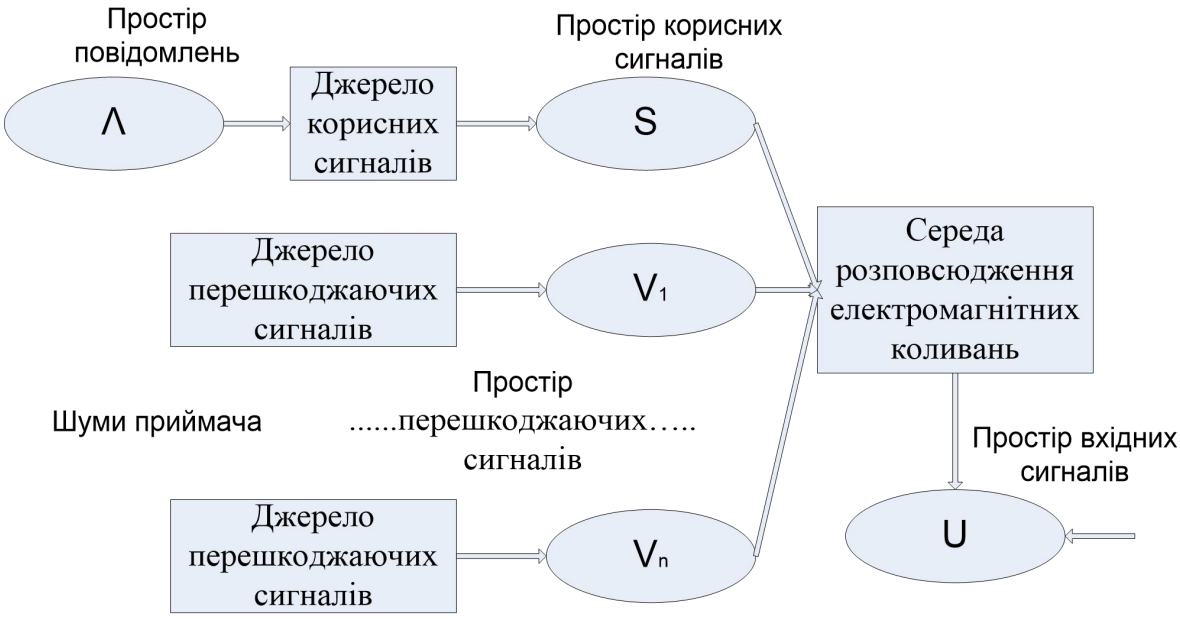

Рисунок 1.3 — Статична модель формування електромагнітної обстановки

При цьому вхідні сигнали можуть розглядатися у двох варіантах:

- на вході приймального пристрою у формі електромагнітних полів;
- на вході приймача у формі радіосигналу.

Початковим у моделі є ланка, що становить простір повідомлень. Простір повідомлень поєднує множину всіх можливих класів (різновидів) повідомлень. Кожне з повідомлень є строго детермінованим, але поява того або іншого повідомлення на приймальному кінці каналу передачі інформації для одержання повідомлення є випадковою подією. З обліком цього повідомлення буде розглядатися як випадкову подію кінцевої множини можливих повідомлень.

Зміст повідомлення й кількість класів повідомлень залежать від функціональних завдань, виконуваних радіоелектронними засобами.

1.2 Випромінювачі електромагнітних коливань

Джерелами небезпечного сигналу є елементи, вузли й провідні ланцюги технічних засобів із струмами й напругами небезпечних сигналів, а

також голосовий апарат людини й елементи технічних засобів, що створюють акустичні поля небезпечних сигналів.

До основних технічних систем і засобів ставляться засоби, призначені для передачі, прийому, обробки й зберігання інформації з обмеженим доступом ЗІОД:

- електронно-обчислювальні машини (ЕОМ), у тому числі персональні (ПЕВМ);
- апаратура звукозапису, звуковідтворення й звукопідсилення;
- системи оперативно-командного й гучномовного зв'язка;
- системи внутрішнього телебачення;
- засоби виготовлення й розмноження документів.

Допоміжні технічні системи й засоби не призначені для обробки ЗІОД, але при спільній установці з основними технічними системами й засобами або при установці в службових приміщеннях, де ведуться переговори або роботи, пов'язані з ЗІОД, вони можуть сприяти витоку інформації або утворювати “самостійні” системи витоку.

До допоміжних технічних систем і засобів відносяться:

- системи відкритого телефонного зв'язку;
- системи радіотрансляції;
- системи електроживлення;
- системи охоронної й пожежної сигналізації.

Допоміжні технічні засоби, а також різного роду ланцюга, розташовані в безпосередній близькості від основних технічних систем і засобів, можуть мати антенний ефект. Цей ефект полягає в перетворенні енергії прихожої від основних технічних систем і засобів електромагнітної хвилі в енергію електричних струмів. Вторинні технічні системи й засоби, а також утворювані ними ланцюга, називаються також випадковими прийомними антенами. До зосередженого випадковими прийомним антенам ставляться телефонні апарати, електричні дзвінки, датчики охоронної й пожежної сигналізації й т.п.

До розподілених випадкових антен ставляться різного роду кабелі, проведення систем сигналізації, ретрансляційні мережі, труби, металеві конструкції й т.п.

При проходженні небезпечних сигналів по елементах і ланцюгам технічних засобів, сполучним лініям, у навколишньому просторі виникає електромагнітне поле. Тому такі засоби й лінії можна вважати випромінювачами. Всі джерела небезпечного сигналу прийнято розглядати як випромінювачі, підрозділяються умовно на три типи: крапкові, лінійні (розподілені) і майданні.

Крапкові випромінювачі - це технічні засоби або випромінюючі елементи їхніх електричних схем, розміри яких значно менше довжини хвилі небезпечного сигналу, оброблюваного технічною системою й засобом, і відстані до границі контрольованої зони.

До розподілених випромінювачів відносять кабельні й сполучні провідні лінії.

Майданні випромінювачі - це сукупність технічних засобів, рівномірно розподілених на деякій площі й обтічних тим самим струмом.

Технічні засоби, для яких характерна більша амплітуда напруги небезпечного сигналу й мала амплітуда струму, ставляться до електричних випромінювачів. Технічні засоби з великою амплітудою струму й малою амплітудою напруги розглядаються, як магнітні випромінювачі.

Крім того, електромагнітні випромінювання радіоелектронного обладнання (РЕО) можна розділити на основні й небажані.

Основні радіовипромінювання характеризуються:

- несучою частотою;
- потужністю (напруженістю) поля;
- широкою смугою випромінюваних частот;
- параметрами модуляції.

Небажані випромінювання підрозділяються на побічні, позаполосні й шумові. Найнебезпечнішими, з погляду утворення каналів витоку інформації, є побічні випромінювання.

Побічні випромінювання - це радіовипромінювання, що виникають у результаті будь-яких нелінійних процесів у радіоелектронному пристрої, крім процесів модуляції. Побічні випромінювання виникають як на основній частоті, так і на гармоніках, а також у вигляді їхньої взаємодії. Радіовипромінювання на гармоніці - це випромінювання на частоті (частотах), у ціле число раз більшої частоти основного випромінювання. Радіовипромінювання на суб-гармоніках - це випромінювання на частотах, у ціле число раз менші частоти основного випромінювання. Комбінаційне випромінювання - це випромінювання, що виникає в результаті взаємодії на лінійних елементах радіоелектронних пристроїв коливань несучої (основної) частоти і їхніх гармонійних складових.

Відзначаючи різноманіття форм електромагнітних випромінювань, варто підкреслити, що є й так зване інтермодуляційне випромінювання, що виникає в результаті впливу на нелінійний елемент високочастотного (ВЧ) тракту радіоелектронної системи (РЕС) згенерованих коливань і зовнішнього електромагнітного поля.

Кожний електронний пристрій є джерелом магнітних і електромагнітних полів широкого частотного спектра, характер яких визначається призначенням і схемними рішеннями, потужністю пристрою, матеріалами, з яких воно виготовлено, і його конструкцією.

Відомо, що характер поля змінюється залежно від відстані до прийомного пристрою. Якщо ця відстань значно менше довжини хвилі електромагнітного сигналу ($r << \lambda$), поле має яскраво виражений магнітний (або електричний) характер, а в далекій зоні ($r >> \lambda$) поле носить явний електромагнітний характер і поширюється у вигляді плоскої хвилі, енергія якої ділиться нарівно між електричним і магнітним компонентами.

Чим швидше довжина хвилі визначає відстань і тим більше призначення, устрій, принцип роботи й інші характеристики правомірно підрозділяти випромінювачі електромагнітних сигналів на низькочастотні, високочастотні й оптичні.

Низькочастотними (НЧ) випромінювачами електромагнітних коливань в основному є звукопідсилювальні пристрої різного функціонального призначення й конструктивного виконання. У ближній зоні таких пристроїв найбільш потужним виступає магнітне поле небезпечного сигналу. Таке поле підсилювальних систем досить легко виявляється й приймається за допомогою магнітної антени й селективного підсилювача звукових частот (рис. 1.4)

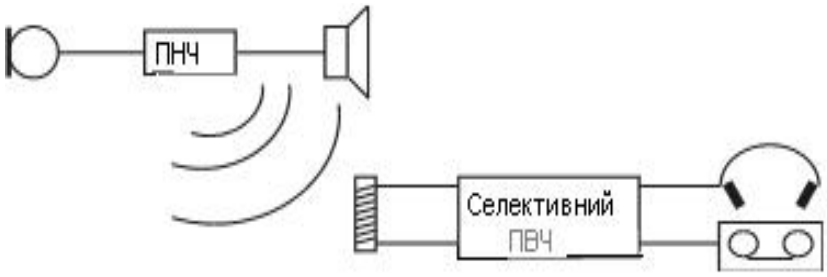

Рисунок 1.4 — Приймання НЧ сигналів

До групи високочастотних (ВЧ) випромінювачів ставляться ВЧ автогенератори, модулятори ВЧ коливань і пристрою, що генерують паразитні ВЧ коливання по різних причинах і умовам (рис. 1.5)

Джерелами небезпечного сигналу є ВЧ генератори радіоприймачів, телевізорів, вимірювальних генераторів, монітори ЕОМ.

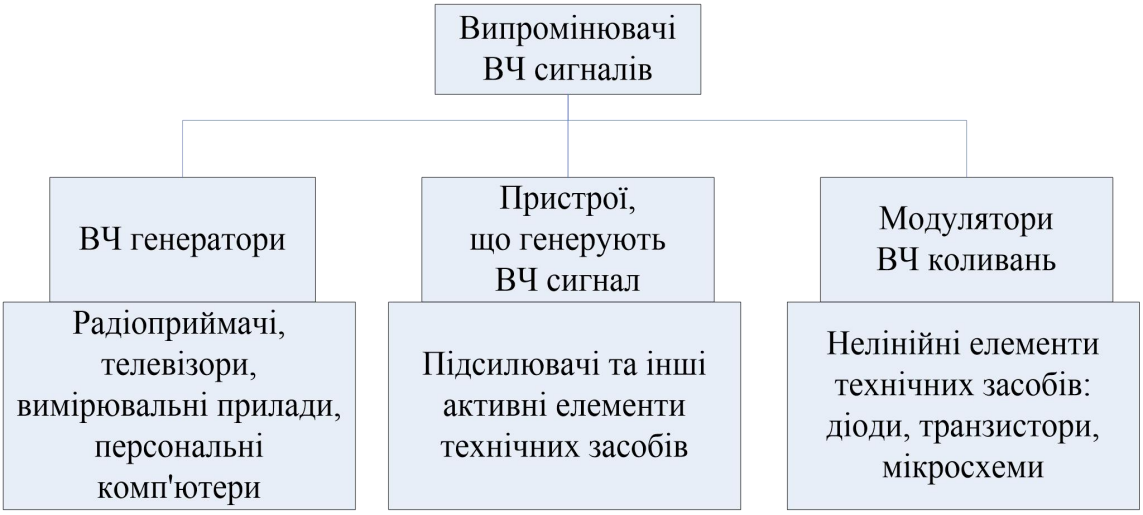

Рисунок 1.5 — Класифікація випромінювачів ВЧ сигналів

Модулятори ВЧ коливань як елементи, що володіють нелінійними характеристиками (діоди, транзистори, мікросхеми), утворять небажані складові ВЧ характеру.

Досить небезпечними джерелами ВЧ коливань можуть бути підсилювачі й інші активні елементи технічних засобів, що працюють у режимі паразитної генерації за рахунок небажаного позитивного зворотного зв'язка.

Джерелами випромінювання ВЧ коливань у різній апаратурі є вбудовані в них генератори, частота яких по тим або інших причинах може бути промодульованою мовним сигналом.

У радіоприймачах, телевізорах, магнітофонах і в ряді електровимірювальних приладів завжди є вбудовані генератори (гетеродини). До них примикають різні підсилювальні системи - підсилювачі НЧ, системи звукопідсилення, здатні по тим або інших причинах увійти в режим самозбудження (тобто по суті стати неконтрольованим гетеродином).

Основним елементом гетеродина є коливальний контур з конденсатором змінної ємності. Під впливом акустичного тиску буде змінюватися відстань між пластинами перемінного повітряного конденсатора гетеродина. Зміна відстані приведе до зміни ємності, а останнє — до зміни

значення частоти гетеродина ($\omega_o = 1/\sqrt{LC}$) за законом акустичного тиску, тобто до частотної модуляції гетеродина акустичним сигналом.

Крім конденсаторів, акустичному впливу піддаються котушки індуктивності з підстроювальними осердями, монтажні проведення значної довжини.

Практика показала, що акустична реакція гетеродина можлива на відстані до декількох метрів, особливо в приміщеннях з гарною акустикою. Залежно від типу приймача, прийом такого сигналу можливий на значній відстані, що іноді досягає порядку 1-2 км.. Джерелом випромінювання ВЧ коливань в апаратурі звукозапису є генератор стирання-підмагнічування, частота якого може бути промодульованою мовним сигналом за рахунок нелінійних елементів у підсилювачі запису, головки запису й ін. через наявність загальних ланцюгів електроживлення взаємного проникнення в тракти посилення.

У ланцюгах технічних засобів, що перебувають у зоні впливу потужних ВЧ випромінювань, напруга наведених сигналів може становити від декількох до десятків вольтів. Якщо в зазначених ланцюгах є елементи, параметри яких (індуктивність, ємність або опір) змінюються під дією НЧ сигналів, то в навколишньому просторі буде створюватися вторинне поле ВЧ випромінювання, модульоване НЧ сигналом (рис. 1.6).

Рисунок 1.6 — Класифікація випромінювачів ВЧ сигналів

Роль нелінійного елемента можуть грати:

- телефони, різні датчики (ВЧ нав'язування по проводам);
- приймачі, магнітофони (ВЧ нав'язування по ефіру).

Як правило, причиною випромінювання кабелів є поганий стан:

- з'єднувачів;
- спрямованих відгалужень і т.п.

Теоретично, якщо немає дефектів у екрануючій поверхні (екрані) кабелю, його екран послабляє випромінювання більш ніж в 100 дБ. Цього цілком достатньо для запобігання будь-якого випромінювання кабелю, яке можна зареєструвати. Для того щоб сигнал був зареєстрований приймачем, його максимальний рівень у кабелі не перевищує 100 мкВ, а мінімальний на поверхні кабелю - не більше 1 мкВ.

Тепловий шум на вході приймача обмежує прийом сигналу. Це підтверджується розрахунковими значеннями рівня шуму у широкосмуговому кабелі (табл. 1.1).

Таблиця 1.1 — Рівні шуму у широкосмуговому кабелі

Швидкість передачі даних, Мбіт/с	Необхідна смуга пропущення, МГц	Середньоквадратичне значення шуму в смузі приймача, мкВ
5	6	2,68
0,1	0,3	0,6
0,01	0,03	0,2

З табл. 1.1 видно, що середньоквадратичне значення теплового шуму на поверхні кабелю вище 1 мкВ для кабелю з високою швидкістю передачі даних (відношення сигнал/шум більше 1). При таких значеннях цілком можливе перехоплення даних по випромінюванню кабелю. Зі збільшенням відстані між кабелем і приймачем ця можливість зменшується.

Таким чином, при справному кабелі перехопити інформацію з випромінювання дуже важко. Однак на практиці кабелі не завжди екрановані. Це приводить до того, що несправні або покриті корозією з'єднувачі можуть бути причиною значних випромінювань. Сигнал в 1 мкВ може бути виявлений на відстані 3 м від кабелю, а в 1 мВ - на відстані 300 м.

1.3 Радіоканали й радіорелейні лінії

Канал витоку інформації існує не сам по собі, а завдяки наявності певних об'єктів і технічних засобів, взаємодіючих між собою. Сукупність призначених для передачі інформації на відстань технічних засобів і передавального середовища називається каналом зв'язку. Передавальні середовища називаються лініями зв'язку (провідна, радіо й т.д.).

По призначенню канали зв'язки розділяються на телефонні, телеграфні, телевізійні й ін.; по характеру експлуатації - на виділені й що комутируються. Виділеними каналами зв'язку називаються канали, які постійно включені між двома пунктами. Канали, що комутируються, виділяються тільки по виклику й розпадаються автоматично після завершення сеансу зв'язку.

Залежно від характеру коливань, що використовуються для передачі інформації, канали називаються електричними, електромагнітними, оптичними, акустичними, пневматичними й т.д.

Найпоширеніші телеграфні, телефонні й телевізійні канали мають типову смугу пропущення, нормований вхідний і вихідний рівень сигналів, нормовані рівні перешкод і інші нормовані показники. Телевізійний канал має смугу пропущення 6 МГц. Телефонний канал має смугу пропущення від 300 до 2200-3200 Гц. Такий канал може бути додатково ущільнений по частоті каналами тонального телеграфування (телеграфними каналами) зі смугою пропущення 120-200 Гц кожний.

Лінії зв'язку діляться на:

- основні (використаються для передачі секретних відомостей);
- допоміжні (використаються для передачі інформації, що не є секретною).

Крім того, лінії зв'язку позначаються номерами, що відповідають режиму переданої інформації:

- лінії №1 (лінії передачі секретної інформації);
- лінії №2 (внутрішня телефонна мережа);
- лінії №3 (зовнішня телефонна мережа).

Лінії зв'язку по характеристиках передавального середовища можна розділити на провідні лінії, високочастотні лінії, повітряні лінії електропередачі високої напруги, лінії радіозв'язку й радіорелейні лінії, лінії розподільних силових мереж.

Провідні лінії (повітряні і кабельні) характеризуються первинними (погонні активний послідовний опір, ємність, індуктивність і провідність) і вторинними (загасання, хвильовий опір і пропускна здатність) параметрами. Пропускна здатність лінії визначається її смугою пропущення, рівнем перешкод і максимальним припустимим рівнем сигналу в лінії.

Загасання й провідність (витік) повітряної лінії в значній мірі залежать від кліматичних умов (дощ, іній, ожеледь), а також від якості технічного обслуговування лінії зв'язку.

Параметри кабельних ліній залежать в основному від температури ґрунту й майже не залежать від інших зовнішніх умов, тому вони значно більше стабільні, чим у повітряних ліній. В Україні та країнах СНД зараз використовуються такі кабельні провідні лінії, як лінії телефонної мережі, що комутуються, загального користування, лінії мережі передачі даних ПД-200 (швидкість передачі становить 200 біт/с) і лінії мережі абонентського телеграфу АТ-50. До цього різновиду ліній зв'язку відносяться й волоконно-оптичні лінії, що вводяться останнім часом.

Високочастотні лінії зв'язку застосовуються у високочастотних каналах. Останні являють собою сукупність спеціальної передавальної, ретрансляційної й прийомної апаратури й ліній зв'язку, призначених для незалежної від інших каналів передачі повідомлень на відстань струмами високої частоти. Частотне ущільнення струмами високої частоти дозволяє утворити на основі однієї провідної лінії кілька додаткових каналів зв'язку. Такі канали широко застосовуються при передачі інформації телефонного, телеграфного й іншого зв'язку по повітряних сталевих, мідних і біметалічних ланцюгах або по симетричних і коаксіальних кабелях зв'язку.

Повітряні лінії електропередачі високої напруги широко застосовуються як для зв'язку, так і для передачі телеметричних повідомлень. В останні роки вони починають застосовуватися для телеконтролю й телекерування місцевими електростанціями, підстанціями й іншими установками в сільському господарстві, а також як резервні лінії зв'язку загальнодержавного значення.

Лінії електропередачі 35, 110, 220 і 400 кВ мають високу електричну й механічну міцність, тому утворені на їхній основі канали зв'язку характеризуються високою надійністю (за умови, звичайно, що каналоутворювальна апаратура також має високу надійність).

Передача сигналів по цих лініях здійснюється струмами високої частоти в діапазоні від 300 до 500 кГц, а на деяких повітряних лініях і до 1000 кГц. У кабельних силових мережах використаються значно більше низькі частоти (до звукових).

Ці канали мають порівняно високий рівень перешкод, тому для одержання достатнього для нормальної роботи відносини сигнал/перешкода застосовується спеціальна апаратура каналів з порівняно високою вихідною потужністю сигналу, а також якісні фільтри для поділу сигналів і зменшення перехресних перешкод.

Характерною рисою ліній радіозв'язку є можливість значного впливу перешкод від сусідніх радіостанцій і промислових джерел радіоперешкод у порівнянні із провідними лініями.

До цього виду ліній належать космічна, радіорелейна, КВ, УКХ, мобільний і стільниковий зв'язки.

Лінії розподільних силових мереж широко використовуються для створення каналів циркулярної передачі команд масовим об'єктам як у ряді європейських країн (Франція, Австрія й ін.), так і в Україні. За допомогою таких каналів здійснюється централізоване включення вуличного освітлення, передача пожежної тривоги, команд цивільної оборони й т.п. Команди (сигнали) передаються тільки в одному напрямку із центрального пункту, а відповідна, сповіщувальна сигналізація відсутня.

Передача інформації з каналів здійснюється в діапазоні звукових частот або в діапазоні 10-200 кГц. Відповідно розвиваються два напрямки.

- Перший напрямок пов'язаний з передачею циркулярних команд масовим об'єктам без сповіщувальної сигналізації. При цьому звичайно використовується одна або кілька частот у діапазоні 175-3000 кГц.
- Для другого напрямку характерне використання діапазону частот від 10-15 до 200 кГц. Рівень перешкод у цьому діапазоні значно менше, внаслідок чого відкривається можливість двосторонньої передачі сигналів.

Різновидом розподільних силових мереж є контактні мережі для електричного транспорту. Вони використовуються як канали телефонного зв'язку з рухомих об’єктів і для передачі повідомлень телекерування, телесигналізації й телевимірювання.

Із всіх перерахованих ліній зв'язку можна зняти інформацію, використовуючи для цього:

- гальванічне підключення до лінії;
- електромагнітний метод;
- індукційне знімання за допомогою кліщів.

У наш час все більшого значення набуває якісний і безперебійний зв'язок. Крім того, постійно зростають об'єми й вимоги до швидкості передачі інформації. Радіорелейні лінії (РРЛ) використовуються для передачі сигналів багатоканальної телефонії, телевізійних сигналів, сигналів віщання, телеграфних сигналів, включаючи передачу бінарної інформації, фототелеграфних сигналів, передачу газетних текстів, і забезпечують цю передачу з високою якістю й великою надійністю зв'язку. У цей час тривають розробки апаратури нових радіорелейних систем, які приведуть до збільшення пропускної здатності й надійності РРЛ.

Існують магістральні, тобто призначені для передачі сигналів на більші відстані й зональні (як правило обласні) радіорелейні лінії.

У нових радіорелейних системах все обладнання уніфіковане, високочастотні стовбури є універсальними, тобто придатними для передачі

сигналів як багатоканальної телефонії й віщання, так і телебачення з каналами звукового супроводу.

Для організації службових каналів, по яких передаються сигнали службових телефонних переговорів, системи телеобслуговування й контролю за роботою встаткування призначений службовий зв'язок у радіорелейній системі. Система службового зв'язку охоплює всі станції РРЛ, а також забезпечує з'єднання РРЛ із вузлами зв'язку, міжміськими телефонними станціями й телецентрами. Наявність надійного службового зв'язку дозволяє обслуговуючому персоналу РРЛ постійно стежити за технічним станом апаратури всіх станцій радіорелейної лінії, а службам по експлуатації РРЛ постійно підтримувати високі експлуатаційні показники РРЛ.

Для забезпечення високої надійності роботи радіорелейної магістралі призначене резервування (заміна несправного обладнання справним). Крім того, резервування дозволяє утворювати ланцюг для профілактичних вимірів електронних характеристик стовбурів в експлуатації без порушення зв'язку. Для РРЛ застосовуються різні способи резервування. Найбільше поширення одержала постанційна й зональна система резервування, а також різної їхньої комбінації.

Апаратура сучасних РРЛ в основному розрахована на живлення напругою постійного струму напругою 24В або 48В. Основним джерелом електропостачання радіорелейних станцій є лінії електропередач (зовнішні джерела) із застосуванням перетворювачів змінної напруги 220В в постійне 24В або 48В, а також у важкодоступних районах альтернативні джерела напруги (сонячні й вітрові). Для підвищення надійності як додаткове джерело електроживлення використовуються акумуляторні батареї й автоматизовані дизель-генераторні установки.

Все більше застосування знаходять системи цифрової передачі інформації, що забезпечують все кращу якість передач. Ці нові лінії зв'язку вимагають до себе особливої уваги для забезпечення їхніх якісних показників.

Радіорелейний зв'язок спочатку застосовувався для організації багатоканальних ліній телефонного зв'язку, ліній, у яких повідомлення передавалися за допомогою аналогового електричного сигналу. Перша така лінія з 5 телефонними каналами з'явилася в США в 1935 році. Вона з'єднувала міста Нью-Йорк і Філадельфію й мала довжина 200 км.

Завдяки науковим досягненням стало можливим створення в 50-х роках комплексів уніфікованої приймально-передавальної апаратури, що використовують діапазон надвисоких частот і методи частотного й/або тимчасового поділу каналів – багатоканальні радіорелейні станції (РРС). До початку 70-х років у всіх розвинених країнах була створена густа мережа багатоканальних ліній радіорелейного зв'язку з декількома тисячами типових каналів у кожній лінії. З'являються РРС на автомобільній платформі (в основному військового призначення), що забезпечують оперативне розгортання мережі радіорелейного зв'язку в районах бойових дій або в районах стихійних лих.

Досвід застосування радіорелейних ліній виявив ряд переваг цього роду зв'язку, які значно розширювали можливості зв'язку взагалі. Це:

• швидкість і економічність розгортання (у порівнянні із проводовим зв'язком) ліній зв'язку;

• економічно вигідна, а в ряді випадків і єдино можлива організація багатоканального зв'язку на територіях, що мають складний рельєф (ліс, гори, болота та ін.), а також у тих місцях, де прокладка кабелю недоцільна;

• можливість аварійного відновлення зв'язку магістралей провідного зв'язку шляхом заміни її ушкоджених ділянок;

• якість зв'язку, що не уступає проводовому зв'язку.

Необхідність передавати дані – інформацію, представлену в дискретному цифровому виді, підштовхнула до створення цифрових систем передачі, прискорила розробку сучасних методів перетворення дискретної інформації в аналогову й назад (методи модуляції й демодуляції), а також

методів її кодування. З'явилися системи, здатні обмінюватися цифровою інформацією – системи передачі даних (СПД). З'явилися цифрові РРС.

Будь-яка радіорелейна лінія розділена на секції. Секція являє собою комбінацію елементів, що утворюють комутуючу секцію (рис. 1.7). Це радіорелейна секція з кінцевими станціями (ретрансляторами з введенням/виводом) на обох кінцях і без ретрансляторів між ними, або ж із проміжними ретрансляторами. За допомогою секції можна виконувати функції перемикання на резерв. Секція використовується для передачі трафіку даних. Секції можуть бути з'єднані разом для утворення мережі більших розмірів. У секції також є канал передачі службової інформації, призначений для виконання операцій контролю й керування. Розподіл на секції необхідно для зонального резервування й забезпечення більше надійної роботи лінії зв'язку.

Рисунок 1.7 — Схема радіорелейної секції

Устаткування, застосовуване на станціях, ставиться до одному із трьох типів, названих кінцевими станціями (терміналами), ретрансляторами з уведенням/виводом (дубль-терміналами) і просто ретрансляторами (репітерами). Термінал - кінцева станція, дубль-термінал - проміжна станція, на якій відбувається резервування. Репітер - це проміжна станція без можливості резервування. Для передачі сигналів використовується система N+1 (N основних і один резервний стовбур) або N+0 (немає стовбура для резервування). Магістральні радіорелейні лінії зв'язку повинні обов'язково мати резервування, тоді як зонові можуть обійтися без нього. Резервування

відбувається автоматично, критерієм резервування є поява шумів або помилок у приймальному сигналі. Сигнал резервується тільки між двома терміналами, при цьому використовується резервний стовбур цілої секції.

Резервування необхідно у випадках несправностей устаткування основного стовбура або при селективних (тобто частотозалежних) завмираннях.

2 СТРУКТУРА СТАНДАРТУ GSM

Global Mobile Communications (GSM) - глобальна система рухомого зв'язку; європейський цифровий стандарт; діапазон частот 890 - 960 МГц і 1710-1880 МГц.

Перша система, що складається з одного шестиканального передавача, була створена в північноамериканському місті Сент-Луїсі ще в 1946 році. Активне ж впровадження стільникового зв'язку почалася значно пізніше - перші комерційні системи з'явилися в Америці в 1979 році, а придбали національний масштаб тільки в 1983 році. У Європі в 1981 році з'явилася перша міжнародна система, що об'єднала Норвегію, Данію, Швецію й Фінляндію.

Сьогодні абревіатуру GSM розшифровують як Global System for Mobile Communications, а стандарт GSM і його версії прийняті до використання приблизно в 80 країнах світу і налічує більш ніж 1 000 000 000 абонентів.

До України технологія дійшла з традиційним запізненням: перша система цифрового мобільного зв’язку з’явилась десь тільки в 1992 році. Незважаючи на це, темпи розвитку стільникового зв'язку на пострадянському просторі настільки високі, що всього за кілька років цей сервіс перетворився з "привілею обраних" у нагальну потребу для людей із середніми доходами. На сьогоднішній день проникнення мобільного зв’язку на ринку України перевищує 100%, а це означає мобільних абонентів стало більше ніж мешканців в країні. Замість символу статку стільниковий зв'язок стає тим, чим він й повинен бути - засобом зв'язку, конкуруючи вже в окремих областях із провідними мережами.

Принцип побудови стільникових систем полягає в наступному: у межах території дії мережі встановлюється деяка кількість щодо малопотужних стаціонарних приймально-передавальних станцій (базових станцій), кожна з яких має невелику зону дії (звичайно кілька кілометрів). При цьому зони дії сусідніх станцій трохи перекривають одна одну, щоб забезпечити можливість

переміщення абонента з однієї зони в іншу без втрати зв'язку. Щоб таке перекриття було можливим, сусідні станції повинні використовувати різні робочі частоти. Для повного покриття певної території потрібно як мінімум три різні частоти, щоб розташовані у вигляді трикутника станції могли мати перекриття зон обслуговування. Четверта ж станція може знову використати одну із цих трьох частот, тому що вона граничить тільки із двома зонами. При такому підході форма зони дії кожної базової станції являє собою шестикутник, а розташування цих зон у точності повторює структуру бджолиних стільник, що й дало назву системам зв'язку з подібним принципом побудови.

Стандарт GSM відноситься до другого покоління стандартів для стільникового зв'язку, заснованому на цифровій технології. Реалізоване в системах GSM повно-швидкісне кодування мови дозволяє зробити її якість наближеною до якості стаціонарних телефонних мереж. Радіотелефон стандарту GSM можна умовно розділити на дві частини: абонентський модуль SIM (SIM-карта) і безпосередньо сам телефон, що містить апаратне й програмне забезпечення. SIM-карта служить підтвердженням дійсності абонента й містить у своїй пам'яті всі необхідні дані, пов'язані з можливостями конкретного абонента. Щоб викрадач не зміг нею скористатися, у неї вводять спеціальний ідентифікаційний номер (PIN-код). Використання SIM-карти також зручно тим, що при зміні апарата абонентові не потрібно міняти свій мобільний номер, він просто переставляє карту, і всі збережені на ній дані, включаючи записну книжку, стають доступними в новому апараті. Коли SIM-карти немає в апараті, доступ до абсолютної більшості послуг закритий, за винятком екстрених викликів (якщо дозволяє мережа). Виготовити дублікат SIM-карти дуже складно й у сукупності з функціями захисту, вона дає високий рівень захисту користувачів і мереж від несанкціонованого доступу.

У стандарті GSM уведено кілька функцій захисту. У першу чергу це кодування радіоканалу, що виключає прослуховування третьою стороною, а

також захист номера абонента (для запобігання розкриття його місцезнаходження). Крім стандартних можливостей, надаваних операторами стільникового зв'язку - місцевий, міжміський й міжнародний зв'язок, переадресація виклику й т.д.. Телефони стандарту GSM дають своїм власникам ряд додаткових функцій: збереження мовних повідомлень, що надійшли в період, коли абонент був недоступний (голосова пошта), прийом повідомлення про факс, що прийшла (факс-пошта), визначення номера що дзвонить. Передбачено можливість передачі коротких повідомлень "із крапки в крапку" (пейджинга), тобто абоненти при бажанні можуть обмінюватися простими короткими (кілька десятків символів) повідомленнями (тарифи на цю послугу трохи нижче, ніж на звичайні переговори). Функція мобільного модему/факсу поряд з повсюдним поширенням портативних комп'ютерів дає можливість доступу до Інтернету й електронної пошти через мережі GSM. Ці послуги значно збільшують привабливість використання телефонів GSM для користувачів. Так, приміром, факс-пошта може бути дуже корисна діловій людині, тому що дозволяє не пропустити інформацію про факс у будь-який час, незалежно від місцезнаходження абонента. Мобільний телефон сповістить свого власника, а той може одержати факс коли завгодно й де завгодно, тому що факс автоматично надходить у його електронну поштову скриньку.

До особливостей та переваг стандарту GSM можна віднести:

- Менші в порівнянні з аналоговими стандартами розміри й вага телефонних апаратів при більшому часі роботи без підзарядки акумулятора. В основному це досягається за рахунок апаратури базової станції, що постійно аналізує рівень сигналу, прийнятого від апарата абонента. У тих випадках, коли він вище необхідного, автоматично знижується випромінювана потужність.

- Відносно висока ємність мережі.

- Низький рівень промислових перешкод у даному частотному діапазоні.

- Трохи неприродне звучання мови, але немає шипіння й тріску.

- Максимальний захист від підслуховування й нелегального використання, що досягається шляхом застосування алгоритмів шифрування з відкритим ключем. EFR-технологія виявляє собою вдосконалену систему кодування мови. Ця система була розроблена фірмою Nokia і згодом стала промисловим стандартом кодування / декодування для технології GSM.

- Зв'язок на відстані не більше 35 км від найближчої базової станції навіть при використанні підсилювачів і спрямованих антен (для стандарту GSM-900).

- Максимальна випромінювана потужність мобільних телефонів стандарту GSM-1800: 1Вт; GSM-900: 2Вт.

- Високий захист від підслуховування й нелегального використання номера.

- Висока ємність мережі - важливо для великих міст.

- Максимальне видалення абонента від базової станції в стандарті 1800: 5...6 км.

2.1 Структура й склад устаткування мереж зв'язку

Функціональна побудова й інтерфейси, прийняті в стандарті GSM: MSC (Mobile Switching Centre) - центр комутації рухомого зв'язку; BSS (Base Station System) - устаткування базової станції; OMC (Operations and Maintenance Centre) - центр керування й обслуговування; MS (Mobile Stations) - рухливі станції.

Функціональне спряження елементів системи здійснюється рядом інтерфейсів. Всі мережні функціональні компоненти в стандарті GSM взаємодіють відповідно до системи сигналізації МККТТ SS N 7 (CCITT SS. N 7).

Центр комутації рухомого зв'язку обслуговує групу стільник і забезпечує всі види з'єднань, у яких має потребу в процесі роботи рухлива станція. MSC аналогічний ISDN комутаційної станції і являє собою

інтерфейс між фіксованими мережами (PSTN, PDN, ISDN і т.д.) і мережею рухомого зв'язку. Він забезпечує маршрутизацію викликів і функції керування викликами. Крім виконання функцій звичайної ISDN комутаційної станції, на MSC покладають функції комутації радіоканалів. До них ставляться "естафетна передача", у процесі якої досягається безперервність зв'язку при переміщенні рухливої станції зі стільники в стільнику, і перемикання робочих каналів в базовій станції з появою перешкод або несправностях.

Кожний MSC забезпечує обслуговування рухливих абонентів, розташованих у межах певної географічної зони (наприклад, Київ й область). MSC управляє процедурами встановлення виклику й маршрутизації. Для телефонної мережі загального користування (PSTN) MSC забезпечує функції сигналізації по протоколу SS. N 7, передачі виклику або інші види інтерфейсів відповідно до вимог конкретного проекту.

MSC формує дані, необхідні для виписки рахунків за надані мережею послуги зв'язку, накопичує дані по розмовах, що відбулися, і передає їх у центр розрахунків (білінг-центр). MSC становить також статистичні дані, необхідні для контролю роботи й оптимізації мережі.

MSC підтримує також процедури безпеки, застосовувані для керування доступами до радіоканалів.

MSC не тільки бере участь у керуванні викликами, але також управляє процедурами реєстрації місця розташування й передачі керування, крім передачі керування в підсистемі базових станцій (BSS). Реєстрація місця розташування рухливих станцій необхідна для забезпечення доставки виклику рухливим абонентам, що переміщаються, від абонентів телефонної мережі загального користування або інших рухливих абонентів. Процедура передачі виклику дозволяє зберігати з'єднання й забезпечувати ведення розмови, коли рухлива станція переміщається з однієї зони обслуговування в іншу. Передача викликів у стільниках, керованих одним контролером базових станцій (BSC), здійснюється цим BSC (рис. 2.1). Коли передача

викликів здійснюється між двома мережами, керованими різними BSC, те первинне керування здійснюється в MSC. У стандарті GSM також передбачені процедури передачі виклику між мережами (контролерами), що ставляться до різних MSC. Центр комутації здійснює постійне спостереження за рухливими станціями, використовуючи регістри положення (HLR) і переміщення (VLR). В HLR зберігається та частина інформації про місце розташування якої-небудь рухливої станції, що дозволяє центру комутації доставити виклик станції. Регістр HLR містить міжнародний ідентифікаційний номер рухомого абонента (IMSI). Він використається для впізнавання рухливої станції в центрі аутентифікації (AUC).

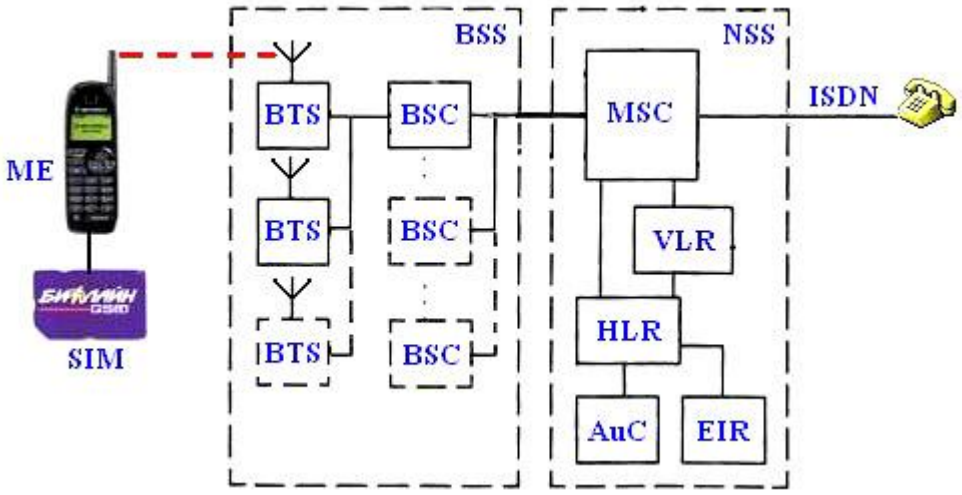

Рисунок 2.1 — Структурна схема мережі GSM

Практично HLR являє собою довідкову базу даних про постійно прописані в мережі абонентах. У ній утримуються розпізнавальні номери й адреси, а також параметри дійсності абонентів, состав послуг зв'язку, спеціальна інформація про маршрутизацію. Ведеться реєстрація даних про роумінг (блуканні) абонента, включаючи дані про тимчасовий ідентифікаційний номер рухомого абонента (TMSI) і відповідному VLR.

До даних, що втримується в HLR, мають дистанційний доступ всі MSC і VLR мережі й, якщо в мережі є трохи HLR, у базі даних утримується тільки один запис про абонента, тому кожний HLR являє собою певну частину

загальної бази дані мережі про абонентів. Доступ до бази даних про абонентів здійснюється за номером IMSI або MSISDN (номеру рухомого абонента в мережі ISDN). До бази даних можуть одержати доступ MSC або VLR, що ставляться до інших мереж, у рамках забезпечення міжмережевого роумінгу абонентів.

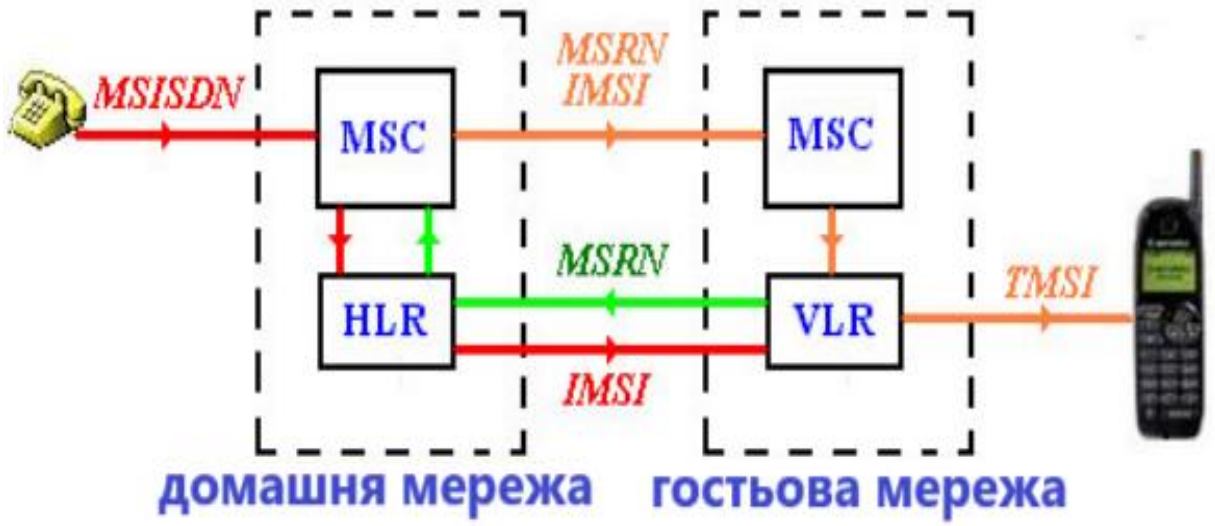

Рисунок 2.2 — Взаємодія MSC, HLR таVLR під час забезпечення виклику

Склад тимчасових даних, що зберігаються в HLR і VLR.

Практично HLR являє собою довідкову базу даних про постійно прописаних в мережі абонентів. У ній утримуються розпізнавальні номери й адреси, а також параметри дійсності абонентів, склад послуг зв'язку, спеціальна інформація про маршрутизацію. Ведеться реєстрація даних про роумінг (блукання) абонента, включаючи дані про тимчасовий ідентифікаційний номер рухомого абонента (TMSI) і відповідному VLR.

До даних, що втримується в HLR, мають дистанційний доступ всі MSC і VLR мережі й, якщо в мережі є декілька HLR, у базі даних утримується тільки один запис про абонента, тому кожний HLR являє собою певну частину загальної бази дані мережі про абонентів. Доступ до бази даних про абонентів здійснюється за номером IMSI або MSISDN (номеру рухомого абонента в мережі ISDN). До бази даних можуть одержати доступ MSC або

VLR, що ставляться до інших мереж, у рамках забезпечення між мережевого роумінгу абонентів.

Другий основний пристрій, що забезпечує контроль за пересуванням рухливої станції із зони в зону, - регістр переміщення VLR. З його допомогою досягається функціонування рухливої станції за межами зони, контрольованої HLR. Коли в процесі переміщення рухлива станція переходить із зони дії одного контролера базової станції BSC, що поєднує групу базових станцій, у зону дії іншого BSC, вона реєструється новим BSC, і в VLR заноситься інформація про номер області зв'язку, що забезпечить доставку викликів рухливої станції. Для збереження даних, що перебувають в HLR і VLR, у випадку збоїв передбачений захист пристроїв пам'яті цих регістрів.

VLR містить такі ж дані, як і HLR, однак ці дані втримуються в VLR тільки доти, поки абонент перебуває в зоні, контрольованої VLR.

У мережі рухомого зв'язку GSM стільники групуються в географічні зони (LA), яким привласнюється свій ідентифікаційний номер (LAC). Кожний VLR містить дані про абонентів у декількох LA. Коли рухомий абонент переміщається з однієї LA в іншу, дані про його місце розташування автоматично обновляються в VLR. Якщо стар і нова LA перебувають під керуванням різних VLR, то дані на старому VLR стираються після їхнього копіювання в новий VLR. Поточна адреса VLR абонента, що втримується в HLR, також обновляється.

VLR забезпечує також присвоєння номера "блукаючої" рухливої станції (MSRN). Коли рухлива станція приймає вхідний виклик, VLR вибирає його MSRN і передає його на MSC, що здійснює маршрутизацію цього виклику до базових станцій, що перебуває рядом з рухливим абонентом.

VLR також розподіляє номера передачі керування при передачі з'єднань від одного MSC до іншого. Крім того, VLR управляє розподілом нових TMSI і передає їх в HLR. Він також управляє процедурами встановлення дійсності під час обробки виклику. За рішенням оператора

TMSI може періодично змінюватися для ускладнення процедури ідентифікації абонентів. Доступ до бази даних VLR може забезпечуватися через IMSI, TMSI або MSRN. У цілому VLR являє собою локальну базу даних про рухомого абонента для тої зони, де перебуває абонент, що дозволяє виключити постійні запити в HLR і скоротити час на обслуговування викликів.

Для виключення несанкціонованого використання ресурсів системи зв'язки вводяться механізми аутентифікації - посвідчення дійсності абонента. Центр аутентифікації складається з декількох блоків і формує ключі й алгоритми аутентифікації. З його допомогою перевіряються повноваження абонента й здійснюється його доступ до мережі зв'язку. AUC ухвалює рішення щодо параметрів процесу аутентифікації й визначає ключі шифрування абонентських станцій на основі бази даних, зосередженої в регістрі ідентифікації встаткування (EIR - Equipment Identification Register).

Кожний рухомий абонент на час користування системою зв'язку одержує стандартний модуль дійсності абонента (SIM), що містить: міжнародний ідентифікаційний номер (IMSI), свій індивідуальний ключ аутентифікації (Ki), алгоритм аутентифікації (A3).

За допомогою записаної в SIM інформації в результаті взаємного обміну даними між рухливою станцією й мережею здійснюється повний цикл аутентифікації й дозволяється доступ абонента до мережі.

Процедура перевірки мережею дійсності абонента реалізується в такий спосіб. Мережа передає випадковий номер (RAND) на рухливу станцію. На ній за допомогою Ki і алгоритму аутентифікації A3 визначається значення відгуку (SRES), тобто SRES = Ki x [RAND]

Рухлива станція посилає обчислене значення SRES у мережу, що звіряє значення прийнятого SRES зі значенням SRES, обчисленим мережею. Якщо обоє значення збігаються, рухлива станція приступає до передачі повідомлень. У противному випадку зв'язок переривається, і індикатор рухливої станції показує, що впізнавання не відбулося. Для забезпечення

таємності обчислення SRES відбувається в рамках SIM. Несекретна інформація (наприклад, Ki) не піддається обробці в модулі SIM.

EIR - регістр ідентифікації встаткування.

Містить централізовану базу даних для підтвердження дійсності міжнародного ідентифікаційного номера встаткування рухливої станції (IMEI). Ця база даних відноситься винятково до встаткування рухливої станції. База даних EIR складається зі списків номерів IMEI, організованих у такий спосіб:

БІЛИЙ СПИСОК - містить номера IMEI, про які є відомості, що вони закріплені за санкціонованими рухливими станціями.

ЧОРНИЙ СПИСОК - містить номера IMEI рухливих станцій, які украдені або котрим відмовлене в обслуговуванні з іншої причини.

СІРИЙ СПИСОК - містить номера IMEI рухливих станцій, у яких існують проблеми, виявлені за даними програмного забезпечення, що не є підставою для внесення в "чорний список".

До бази даних EIR одержують дистанційний доступ MSC даної мережі, а також MSC інших рухливих мереж.

Як і у випадку з HLR, мережа може мати більше одного EIR, при цьому кожний EIR управляє певними групами IMEI. До складу MSC входить транслятор, що при одержанні номера IMEI повертає адресу EIR, що управляє відповідною частиною бази даних про встаткування.

IWF - між мережевий функціональний стик, є однієї зі складових частин MSC. Він забезпечує абонентам доступ до засобів перетворення протоколу й швидкості передачі даних так, щоб можна було передавати їх між його термінальним устаткуванням (DIE) мережі GSM і звичайним термінальним устаткуванням фіксованої мережі. Між мережевий функціональний стик також "виділяє" модем зі свого банку встаткування для сполучення з відповідним модемом фіксованої мережі. IWF також забезпечує інтерфейси типу прямого з'єднання для встаткування, що поставляється клієнтам, наприклад, для пакетної передачі даних PAD по протоколу X.25.

До бази даних EIR одержують дистанційний доступ MSC даної мережі, а також MSC інших рухливих мереж.

ЄС – луно-понижувач , використається в MSC з боку PSTN для всіх телефонних каналів (незалежно від їхньої довжини) через фізичні затримки в трактах поширення, включаючи радіоканал, мереж GSM. Типовий луно-понижувач може забезпечувати придушення в інтервалі 68 мілісекунд на ділянці між виходом ЄС і телефоном фіксованої телефонної мережі. Загальна затримка в каналі GSM при поширенні в прямому й зворотному напрямках, викликана обробкою сигналу, кодуванням/декодуванням мови, канальним кодуванням і т.д., становить близько 180 мс. Ця затримка була б непомітна рухомому абонентові, якби в телефонний канал не був включений гібридний трансформатор з перетворенням тракту з двопровідного на чотирипровідний режим, установка якого необхідна в MSC, тому що стандартне з'єднання з PSTN є двопровідним. При з'єднанні двох абонентів фіксованої мережі луни-сигнали відсутні. Без включення ЄС затримка від поширення сигналів у тракті GSM буде викликати роздратування в абонентів, переривати мову й відволікати увагу.

ОМС - центр експлуатації й технічного обслуговування, є центральним елементом мережі GSM, що забезпечує контроль і керування іншими компонентами мережі й контроль якості її роботи. ОМС з'єднується з іншими компонентами мережі GSM по каналах пакетної передачі протоколу X.25. ОМС забезпечує функції обробки аварійних сигналів, призначених для оповіщення обслуговуючого персоналу, і реєструє відомості про аварійні ситуації в інших компонентах мережі. Залежно від характеру несправності ОМС дозволяє забезпечити її усунення автоматично або при активному втручанні персоналу. ОМС може забезпечити перевірку стану встаткування мережі й проходження виклику рухливої станції. ОМС дозволяє робити керування навантаженням у мережі. Функція ефективного керування включає збір статистичних даних про навантаження від компонентів мережі GSM, запису їх у дискові файли й вивід на дисплей для візуального аналізу.

OMC забезпечує керування змінами програмного забезпечення й базами даних про конфігурацію елементів мережі. Завантаження програмного забезпечення на згадку можуть вироблятися з OMC в інші елементи мережі або з них в OMC.

NMC - центр керування мережею, дозволяє забезпечувати раціональне ієрархічне керування мережею GSM. Він забезпечує експлуатацію й технічне обслуговування на рівні всієї мережі, підтримуваної центрами OMC, які відповідають за керування регіональними мережами. NMC забезпечує керування трафіком у всій мережі й забезпечує диспетчерське керування мережею при складних аварійних ситуаціях, як наприклад, вихід з ладу або перевантаження вузлів. Крім того, він контролює стан пристроїв автоматичного керування, задіяних в устаткуванні мережі, і відбиває на дисплеї стан мережі для операторів NMC. Це дозволяє операторам контролювати регіональні проблеми й, при необхідності, надавати допомогу OMC, відповідальному за конкретний регіон. Таким чином, персонал NMC знає стан всієї мережі й може дати вказівка персоналу OMC змінити стратегію рішення регіональної проблеми.

NMC зосереджує увагу на маршрутах сигналізації й з'єднаннях між вузлами для того, щоб не допускати умов для виникнення перевантаження в мережі. Контролюються також маршрути з'єднань між мережею GSM і PSTN щоб уникнути поширень умов перевантаження між мережами. При цьому персонал NMC координує питання керування мережею з персоналом інших NMC. NMC забезпечує також можливість керування трафіком для мережного встаткування підсистеми базових станцій (BSS). Оператори NMC в екстремальних ситуаціях можуть задіяти такі процедури керування, як "пріоритетний доступ", коли тільки абоненти з високим пріоритетом (екстрені служби) можуть одержати доступ до системи.

NMC може брати на себе відповідальність у якому-небудь регіоні, коли місцевий OMC такий, що не обслуговується, при цьому OMC діє як

транзитний пункт між NMC і встаткуванням мережі. NMC забезпечує операторів функціями, аналогічними функціям OMC.

NMC є також важливим інструментом планування мережі, тому що NMC контролює мережу і її роботу на мережному рівні, а, отже, забезпечує планувальників мережі даними, визначальними її оптимальний розвиток.

BSS - устаткування базової станції, складається з контролера базової станції (BSC) і приймально-передавальних базових станцій (BTS). Контролер базової станції може управляти декількома приймально-передавальними блоками. BSS управляє розподілом радіоканалів, контролює з'єднання, регулює їхня черговість, забезпечує режим роботи зі стрибучою частотою, модуляцію й демодуляцію сигналів, кодування й декодування повідомлень, кодування мови, адаптацію швидкості передачі для мови, даних і виклику, визначає черговість передачі повідомлень персонального виклику.

BSS разом з MSC, HLR, VLR виконує деякі функції, наприклад: звільнення каналу, головним чином, під контролем MSC, але MSC може запросити базову станцію забезпечити звільнення каналу, якщо виклик не проходить через радіоперешкоди. BSS і MSC спільно здійснюють пріоритетну передачу інформації для деяких категорій рухливих станцій.

TCE- транскодер, забезпечує перетворення вихідних сигналів каналу передачі мови й даних MSC (64 кбіт/с ІКМ) до виду, що відповідає рекомендаціям GSM по радіо-інтерфейсу (Рік. GSM 04.08). Відповідно до цих вимог швидкість передачі мови, представленої в цифровій формі, становить 13 кбіт/с. Цей канал передачі цифрових мовних сигналів називається "повношвидкісним". Стандартом передбачається в перспективі використання напівшвидкісного мовного каналу (швидкість передачі 6,5 кбіт/с).

Зниження швидкості передачі забезпечується застосуванням спеціального мово-перетворювального пристрою, що використає лінійне предикативне кодування (LPC), довгострокове пророкування (LTP), залишкове імпульсне порушення (RPE - іноді називається RELP).

Транскодер звичайно розташовується разом з MSC, тоді передача цифрових повідомлень у напрямку до контролера базових станцій - BSC ведеться з додаванням до потоку зі швидкістю передачі 13 кбіт/с, додаткових бітів до швидкості передачі даних 16 кбіт/с. Потім здійснюється ущільнення із кратністю 4 у стандартний канал 64 кбіт/с. Так формується певна Рекомендаціями GSM 30-канальна ІКМ лінія, що забезпечує передачу 120 мовних каналів. Шістнадцятий канал (64 кбіт/с), "тимчасове вікно", виділяється окремо для передачі інформації сигналізації й часто містить трафік SS N7 або LAPD. В іншому каналі (64 кбіт/с) можуть передаватися також пакети даних, що погодяться із протоколом X.25 МККТТ.

Таким чином, що результирует швидкість передачі по зазначеному інтерфейсі становить 30х64 кбіт/с + 64 кбі/с + 64 кбіт/с = 2048 кбіт/с.

MS - рухлива станція, складається з устаткування, що служить для організації доступу абонентів мереж GSM до існуючих фіксованих мереж електрозв'язку. У рамках стандарту GSM прийняті п'ять класів рухливих станцій від моделі 1-го класу з вихідною потужністю 20 Вт, установлюваної на транспортному засобі, до портативної моделі 5-го класу, максимальною потужністю 0,8 Вт. При передачі повідомлень передбачається адаптивне регулювання потужності передавача, що забезпечує необхідну якість зв'язку.

Рухомий абонент і станція незалежні один від одного. Як вже відзначалось, кожний абонент має свій міжнародний ідентифікаційний номер (IMSI), записаний на його інтелектуальну картку. Такий підхід дозволяє встановлювати радіотелефони, наприклад, у таксі й автомобілях, здаваних на прокат. Кожної рухливої станції також привласнюється свій міжнародний ідентифікаційний номер (1ME1). Цей номер використається для запобігання доступу до мереж GSM викраденій станції або станції без повноважень.

2.2 Основні характеристики стандарту GSM

Відповідно до рекомендації CEPT 1980 р., що стосується використання спектра частот рухомого зв'язку в діапазоні частот 862-960 МГц, стандарт

GSM на цифрову загальноєвропейську (глобальну) стільникову систему наземного рухомого зв'язку передбачає роботу передавачів у двох діапазонах частот: 890-915 Мгц (для передавачів рухливих станцій - MS), 935-960 МГц (для передавачів базових станцій - BTS).

У стандарті GSM використовується вузько-смуговий багато-станційний доступ з тимчасовим поділом каналів (NB TDMA). У структурі TDMA кадру втримується 8 тимчасових позицій на кожній з 124 несучих.

Для захисту від помилок у радіоканалах при передачі інформаційних повідомлень застосовується блокове й загортальне кодування з перерозподілом. Підвищення ефективності кодування й перерозподілу при малій швидкості переміщення рухливих станцій досягається повільним перемиканням робочих частот (SFH) у процесі сеансу зв'язку зі швидкістю 217 стрибків у секунду.

Для боротьби з інтерференційними завмираннями прийнятих сигналів, викликаними багатопроменевим поширенням радіохвиль в умовах міста, в апаратурі зв'язку використаються еквалайзери, що забезпечують вирівнювання імпульсних сигналів із середньоквадратичним відхиленням часу затримки до 16 мкс.

Система синхронізації розрахована на компенсацію абсолютного часу затримки сигналів до 233 мкс, що відповідає максимальній дальності зв'язку або максимальному радіусу осередку (стільники) 35 км.

У стандарті GSM обрана гаусівська частотна модуляція з мінімальним частотним зрушенням (GMSK). Обробка мови здійснюється в рамках прийнятої системи переривчастої передачі мови (DTX), що забезпечує включення передавача тільки при наявності мовного сигналу й відключення передавача в паузах і наприкінці розмови. У якості пристрою перетворювання голосу обраний мовний кодек з регулярним імпульсним порушенням, довгостроковим передбачуванням і лінійним предикативним кодуванням із передбачуванням (RPE/LTR-LTP-кодек). Загальна швидкість перетворення мовного сигналу - 13 кбіт/с.

У стандарті GSM досягається високий ступінь безпеки передачі повідомлень; здійснюється шифрування повідомлень по алгоритму шифрування з відкритим ключем (RSA).

У цілому система зв'язку, що діє в стандарті GSM, розрахована на її використання в різних сферах. Вона надає користувачам широкий діапазон послуг і можливість застосовувати різноманітне встаткування для передачі мовних повідомлень і даних, викличних і аварійних сигналів; підключатися до телефонних мереж загального користування (PSTN), мережам передачі даних (PDN) і цифровим мережам з інтеграцією служб (ISDN). У таблиці №1 наведені основні характеристики стандарту GSM.

Таблиця 2.1 — Основні характеристики стандарту GSM

Частоти передачі рухливої станції (прийому базової станції)	МГц 890...915
Частоти прийому рухливої станції й передачі базової станції	МГц 935...960
Дуплексний рознос частот прийому й передачі	МГц 45
Швидкість передачі повідомлень у радіоканалі	кбіт/с 270, 833
Швидкість перетворення мовного кодека	кбіт/с 13
Ширина смуги каналу зв'язку, кГц 200	
Максимальна кількість каналів зв'язку	124
Максимальна кількість каналів, організованих у базовій станції	16...20
Вид модуляції	GMSK
Індекс модуляції	BT 0,3
Ширина смуги передмодуляційного гаусівського фільтру	кГц 81,2
Кількість стрибків по частоті в секунду	217
Тимчасове рознесення в інтервалах TDMA кадру (передача/прийом) для рухливої станції	2
Вид мовного кодека	RPE/LTP
Максимальний радіус стільники, км	до 35
Схема організації каналів	TDMA/FDMA

2.3 Інтерфейси та протоколи передачі інформації

Мережні й радіоінтерфейси.

При проектуванні цифрових стільникових систем рухомого зв'язку стандарту GSM розглядаються інтерфейси трьох видів: для з'єднання із зовнішніми мережами; між різним устаткуванням мереж GSM; між мережею GSM і зовнішнім устаткуванням. Всі існуючі внутрішні інтерфейси мереж GSM повністю відповідають вимогам Рекомендацій ETSI/GSM 03.02.

Інтерфейси із зовнішніми мережами.

З'єднання з PSTN.

З'єднання з телефонною мережею загального користування здійснюється MSC по лінії зв'язку 2 Мбіт/с відповідно до системи сигналізації SS N 7. Електричні характеристики 2 Мбит/з інтерфейсу відповідають Рекомендаціям МККТТ G.732.

З'єднання з ISDN.

Для з'єднання зі створюваними мережами ISDN передбачаються чотири лінії зв'язку 2 Мбіт/с, підтримувані системою сигналізації SS N 7,що відповідають Рекомендаціям Блакитної книги МККТТ Q.701-Q.710, Q.711-Q.714, Q.716, Q.781, 0.782, 0.791, 0.795, 0.761-0.764, 0.766.

З'єднання з існуючою мережею NMT-450.

Центр комутації рухомого зв'язку з'єднується з мережею NMT-450 через чотири стандартні лінії зв'язку 2 Мбіт/с і системи сигналізації SS N7. При цьому повинні забезпечуватися вимоги Рекомендацій МККТТ по підсистемі користувачів телефонною мережею (TUP - Telephone User Part) і підсистемі передачі повідомлень (MTP - Message Transfer Part) Жовтої книги. Електричні характеристики лінії 2 Мбіт/с відповідають Рекомендаціям МККТТ G.732.

З'єднання з міжнародними мережами GSM.

У цей час забезпечується підключення мережі GSM у Києві до загальноєвропейських мереж GSM. Ці з'єднання здійснюються на основі протоколів систем сигналізації (SCCP) і міжмережевою комутацією рухомого зв'язку (GMSC).

Внутрішні GSM - інтерфейси.

Інтерфейс між MSC і BSS (А-інтерфейс) забезпечує передачу повідомлень для керування BSS, передачі виклику, керування пересуванням. А-інтерфейс поєднує канали зв'язку й лінії сигналізації. Останні використають протокол SS N7 МККТТ. Повна специфікація А-інтерфейс відповідає вимогам серії 08 Рекомендацій ETSI/GSM.

Інтерфейс між MSC і HLR сполучений з VLR (У-інтерфейс). Коли MSC необхідно визначити місце розташування рухливої станції, він звертається до VLR. Якщо рухлива станція ініціює процедуру місце-виявлення з MSC, він інформує свій VLR, що заносить всю інформацію, що змінюється, у свої регістри. Ця процедура відбувається завжди, коли MS переходить із однієї області місце-виявлення в іншу. У випадку, якщо абонент запитує спеціальні додаткові послуги або змінює деякі свої дані, MSC також інформує VLR, що реєструє зміни й при необхідності повідомляє про них HLR.

Інтерфейс між MSC і HLR (З-інтерфейс) використається для забезпечення взаємодії між MSC і HLR. MSC може послати вказівку (повідомлення) HLR наприкінці сеансу зв'язку для того, щоб абонент міг оплатити розмову. Коли мережа фіксованого телефонного зв'язку не здатна виконати процедуру встановлення виклику рухомого абонента, MSC може запросити HLR з метою визначення місця розташування абонента для того, щоб послати виклик MS.

Інтерфейс між HLR і VLR (D-інтерфейс) використається для розширення обміну даними про положення рухливої станції, керування процесом зв'язку. Основні послуги, надавані рухомому абонентові, полягають у можливості передавати або приймати повідомлення незалежно від місця розташування. Для цього HLR повинен поповнювати свої дані. VLR повідомляє HLR про положення MS, управляючи нею й привласнюючи їй номера в процесі блукання, посилає всі необхідні дані для забезпечення обслуговування рухливої станції.

Інтерфейс між MSC (E-інтерфейс) забезпечує взаємодія між різними MSC при здійсненні процедури HANDOVER - "передачі" абонента із зони в зону при його русі в процесі сеансу зв'язку без її перерви.

Інтерфейс між BSC і BTS(A-bis інтерфейс) служить для зв'язку BSC з BTS і визначений Рекомендаціями ETSI/GSM для процесів установлення з'єднань і керування встаткуванням, передача здійснюється цифровими потоками зі швидкістю 2,048 Мбіт/с. Можливе використання фізичного інтерфейсу 64 кбіт/с.

Інтерфейс між BSC і OMC (Про-інтерфейс) призначений для зв'язку BSC з OMC, використається в мережах з пакетною комутацією МККТТ X.25.

Внутрішній BSC-інтерфейс контролера базової станції забезпечує зв'язок між різним устаткуванням BSC і встаткуванням транскодування (TCE); використає стандарт ІКМ передачі 2,048 Мбіт/з і дозволяє організувати із чотирьох каналів зі швидкістю 16 кбіт/з один канал на швидкості 64 кбіт/с.

Інтерфейс між MS і BTS (Um-радиоинтерфейс) визначений у серіях 04 і 05 Рекомендацій ETSI/GSM.

Мережний інтерфейс між OMC і мережею, так званий керуючий інтерфейс між OMC і елементами мережі, визначений ETSI/GSM Рекомендаціями 12.01 і є аналогом інтерфейсу Q.3, що визначений у багаторівневій моделі відкритих мереж ISO OSI.

З'єднання мережі з OMC можуть забезпечуватися системою сигналізації МККТТ SS N7 або мережним протоколом X.25. Мережа X.25 може з'єднуватися з об'єднаними мережами або з PSDN у відкритому або замкнутому режимах.

GSM-протокол керування мережею й обслуговуванням також повинен задовольняти вимогам Q.3 інтерфейси, що визначений в ETSI/GSM Рекомендаціях 12.01.

Інтерфейси між мережею GSM і зовнішнім устаткуванням.

Інтерфейс між MSC і сервісом-центром (SC) необхідний для реалізації служби коротких повідомлень. Він визначений в ETSI/GSM Рекомендаціях 03.40.

Інтерфейс до іншим OMC. Кожний центр керування й обслуговування мережі повинен з'єднуватися з іншими OMC, що управляють мережами в інших регіонах або інших мережах. Ці з'єднання забезпечуються X - інтерфейсами відповідно до Рекомендацій МККТТ М.ЗО. Для взаємодії OMC із мережами вищих рівнів використається Q.З - інтерфейс.

Структура служб і передача даних у стандарті GSM.

Стандарт GSM містить два класи служб: основні служби й телеслужби. Основні служби забезпечують: передачу даних (асинхронно) у дуплексному режимі зі швидкостями 300, 600, 1200, 2400, 4800 і 9600 біт/із через телефонні мережі загального користування; передачу даних (синхронно) у дуплексному режимі зі швидкостями 1200, 2400, 4800 і 9600 біт/із через телефонні мережі загального користування, що комутуються мережі передачі даних загального користування (CSPDN) і ISDN; доступ за допомогою адаптера до пакетної асинхронної передачі даних зі стандартними швидкостями 300-9600 біт/із через комутуються мережі, що, пакетної передачі даних загального користування (PSPDN), наприклад, Datex-P; синхронний дуплексний доступ до мережі пакетної передачі даних зі стандартними швидкостями 2400-9600 біт/с.

При передачі даних зі швидкістю 9,6 кбіт/с завжди використається канал зв'язку з повною швидкістю передачі. У випадку передачі на швидкостях нижче 9,6 кбіт/с можуть використатися напівшвидкісні канали зв'язку.

Перераховані функції каналів передачі даних передбачені для термінального встаткування, у якому використаються інтерфейси МККТТ зі специфікаціями V.24 або X.21 серій. Ці специфікації визначають питання передачі даних по звичайних каналах телефонного зв'язку. Телекомунікаційні служби надають наступні послуги:

- телефонний зв'язок (сполучається зі службою сигналізації: охорона квартир, сигнали небезпеки та ін.);

- передача коротких повідомлень;

- доступ до служб "Відеотекс", "Телетекс";

- служба "Телефакс"

Додатково стандартизований широкий спектр особливих послуг (передача виклику, оповіщення про тарифні витрати, включення в закриту групу користувачів).

Тому що очікується, що більшість абонентів буде використати послуги GSM у ділових цілях, особлива увага приділяється аспектам безпеки і якості надаваних послуг.

Структура служб зв'язку.

- GSM PLMN - GSM Public Land Mobile Network - мережа зв'язку з наземними рухливими об'єктами;

- TI (Terminal Equipment) -термінальне встаткування;

- MT (Mobile Terminal) - рухомий термінал;

- IWF (Interworking Function) - межсетевой функціональний стик).

До передачі даних ставиться й новий вид служби, використовуваний в GSM, - передача коротких повідомлень (передача службових буквено-цифрових повідомлень для окремих груп користувачів).

При передачі коротких повідомлень використається пропускна здатність каналів сигналізації. Повідомлення можуть передаватися й прийматися рухливою станцією. Для передачі коротких повідомлень можуть використатися загальні канали керування. Обсяг повідомлень обмежений 160-ю символами, які можуть прийматися протягом поточного виклику або в неробочому циклі. У керування радіоканалами, захист від помилок у радіоканалі, кодування-декодування мови, що тече контроль і розподіл даних користувача й викликів, адаптацію по швидкості передачі між радіоканалом і даними, забезпечення паралельної роботи навантажень (терміналів), забезпечення безперервної роботи в процесі руху.

Використається три типи кінцевого встаткування рухливої станції: МТО (Mobile Termination 0) - багатофункціональна рухлива станція, до складу якої входить термінал даних з можливістю передачі й прийому даних і мови; МТ1 (Mobile Termination 1) - рухлива станція з можливістю зв'язку через термінал з ISDN; МТ2 (Mobile Termination 2) - рухлива станція з можливістю підключення термінала для зв'язку по протоколі МККТТ V або X серій.

Термінальне встаткування може складатися з устаткування одного або декількох типів, такого як слухавка з номеронабирачем, апаратури передачі даних (DTE), телекс і т.д.

Розрізняють наступні типи терміналів: ТІ1 (Terminal Equipment 1) - термінальне встаткування, що забезпечує зв'язок з ISDN; ТІ2 (Terminal Equipment 2) - термінальне встаткування, що забезпечує зв'язок з будь-яким устаткуванням через протоколи МККТТ V або X серій (зв'язок з ISDN не забезпечує). Термінал ТІ2 може бути підключений як навантаження до МТ1 (рухливої станції з можливістю зв'язку з ISDN) через адаптер ТА.

Система характеристик стандарту GSM, прийнята функціональна схема мереж зв'язку й сукупність інтерфейсів забезпечують високі параметри передачі повідомлень, сумісність із існуючими й перспективними інформаційними мережами, надають абонентам широкий спектр послуг цифрового зв'язку.

2.4 Формування сигналів у стандарті GSM

Структура TDMA кадрів і формування сигналів у стандарті GSM.

У результаті аналізу різних варіантів побудови цифрових стільникових систем рухомого зв'язку (ССПС) у стандарті GSM прийнятий багато станційний доступ з тимчасовим поділом каналів (TDMA). Довжина періоду послідовності в цій структурі, що називається гіперкадром, дорівнює Тг = 3 ч 28 хв 53 с 760 мс (12533,76 с). Гіперкадр ділиться на 2048 суперкадрів, кожний з яких має тривалість Ті = 12533,76/2048 = 6,12 с.

Суперкадр складається з мультикадрів. Для організації різних каналів зв'язку й керування в стандарті GSM використаються два види мультикадрів:

1) 26-позиційні TDMA кадри мультикадру;

2) 51-позиційні TDMA кадри мультикадру.

Суперкадр може містити в собі 51 мультикадр першого типу або 26 мультикадрів другого типу. Тривалості мультикадрів відповідно:

1) Тм= 6120/51 = 120 мс;

2) Тм = 6120/26 = 235,385 мс (3060/13 мс). Тривалість кожного TDMA кадру Тк = 120/26 = 235,385/51 = 4,615 мс (60/13 мс).

У періоді послідовності кожний TDMA кадр має свій порядковий номер (NF) від Про до NFmax, де NFmax = (26x51x2048) -1 = 2715647.

Таким чином, гіперкадр складається з 2715647 TDMA кадрів. Необхідність такого великого періоду гіперкадру пояснюється вимогами застосовуваного процесу криптографічного захисту, у якому номер кадру NF використається як вхідний параметр. TDMA кадр ділиться на вісім тимчасових позицій з періодом Те = 60/13:8 = 576,9 мкс (15/26 мс).

Кожна тимчасова позиція позначається TN з номером від 0 до 7. Фізичний зміст тимчасових позицій, які інакше називаються вікнами – це час, протягом якого здійснюється модуляція несучим цифровим інформаційним потоком, що відповідає мовному повідомленню або даним. Цифровий інформаційний потік являє собою послідовність пакетів, розташовуваних у цих тимчасових інтервалах (вікнах). Пакети формуються небагато коротше, ніж інтервали, їхня тривалість становить 0,546 мс, що необхідно для прийому повідомлення при наявності тимчасової дисперсії в каналі поширення.

Інформаційне повідомлення передається по радіоканалі зі швидкістю 270,833 кбіт/с.

2.5 Частотний план стандарту GSM

Стандарт GSM розроблений для створення стільникових систем рухомого зв'язку (ССПС) у наступних смугах частот: 890-915 МГц - для

передачі рухливими станціями (лінія "нагору"); 935-960 МГц - для передачі базовими станціями (лінія "униз").

Мережі GSM функціонують паралельно з існуючими європейськими національними мережами аналогових ССПС стандартів NMT-900, TAGS, ETACS.

Кожна зі смуг, виділених для мереж GSM, розділяється на частотні канали. Рознос каналів становить 200 кГц, що дозволяє організувати в мережах GSM 124 частотних каналу. Частоти, виділені для передачі повідомлень рухливою станцією на базову й у зворотному напрямку, групуються парами, організувати дуплексний канал з розносом 45 МГц. Ці пари частот зберігаються й при перескоках частоти. Кожна стільника характеризується фіксованим присвоєнням певної кількості пара частот.

Якщо позначити FI (п) - номер несучої частоти в смузі 890-915 МГц, Fu (п) - номер несучої частоти в смузі 935-960 МГц, то частоти каналів визначаються по наступних формулах:

$$FI(п) = 890{,}2 + 0{,}2(п-1), \text{ МГц};$$

$$Fu(п) = FI(п) + 45, \text{ Мгц}; \quad 1 < п < 124.$$

Номінали частот каналів для прийому (RX) і передачі (TX) базовими станціями, і відповідні їм номера каналів наведені в таблиці №2.

Кожна частотна несуча містить 8 фізичних каналів, розміщених в 8 тимчасових вікнах у межах TDMA кадру й у послідовності кадрів. Кожний фізичний канал використає те саме тимчасове вікно в кожному тимчасовому TDMA кадрі.

До формування фізичного каналу повідомлення й дані, представлені в цифровій формі, групуються й поєднуються в логічні канали двох типів: канали зв'язку - для передачі кодованої мови або даних (ТСН); канали керування - для передачі сигналів керування й синхронізації (ССН).

Більш ніж один тип логічного каналу може бути розміщений на тому самому фізичному каналі, але тільки при їхній відповідній комбінації.

Структура логічних каналів зв'язку.

У стандарті GSM розрізняють логічні канали зв'язку двох основних видів:

TCH/F (Full Rate Traffic Channel) - канал передачі повідомлень із повною швидкістю 22,8 кбит/з (інше позначення Вт);

TCH/H (Half Rate Traffic Channel) - канал передачі повідомлень із половинною швидкістю 11,4 кбит/з (інше позначення Lm).

Один фізичний канал (табл. 2.2) може являти собою канал передачі повідомлень із повною швидкістю або два канали з половинною швидкістю передачі. У першому випадку канал зв'язку займає одне тимчасове вікно; у другому - два канали зв'язку займають те ж саме тимчасове вікно, але з переміщуванням у сусідніх кадрах (тобто кожний канал - через кадр).

Таблиця 2.2 — Частотний план

Канал		Частота прийому	Частота передачі	Канал		Частота прийому	Частота передачі
Dec	Hex	МГц	МГц	Dec	Hex	МГц	МГц
1	2	3	4	5	6	7	8
1	1	890.20	935.20	63	3F	902.60	947.60
2	2	890.40	935.40	64	40	902.80	947.80
3	3	890.60	935.60	65	41	903.00	948.00
4	4	890.80	935.80	66	42	903.20	948.20
5	5	891.00	936.00	67	43	903.40	948.40
6	6	891.20	936.20	68	44	903.60	948.60
7	7	891.40	936.40	69	45	903.80	948.80
8	8	891.60	936.60	70	46	904	949.00
9	9	891.80	936.80	71	47	904.20	949.20
10	OA	892.00	937.00	72	48	904.40	949.40
11	OB	892.20	937.20	73	49	904.60	949.60
12	OC	892.40	937.40	74	4A	904.80	949.80
13	OD	892.60	937.60	75	4B	905.00	950.00

Частотний план (продовження)

14	OE	892.80	937.80	76	4C	905.20	950.20
15	OF	893.00	938.00	77	4D	905.40	950.40
16	10	893.20	938.20	78	4E	905.60	950.60
17	11	893.40	938.40	79	4F	905.80	950.80
18	12	893.60	938.60	80	50	906.00	951.00
19	13	893.80	938.80	81	51	906.20	951.20
20	14	894.00	939.00	82	52	906.40	951.40
21	15	894.20	939.20	83	53	906.60	951.60
22	16	894.40	939.40	84	54	906.80	951.80
23	17	894.60	939.60	85	55	907.00	952.00
24	18	894.80	939.80	86	56	907.20	952.20
25	19	895.00	940.00	87	57	907.40	952.40
26	1A	895.20	940.20	88	58	907.60	952.60
27	1B	895.40	940.40	89	59	907.80	952.80
28	1C	895.60	940.60	90	5A	908.00	953.00
29	ID	895.80	940.80	91	5B	908.20	953.20
30	IE	896.00	941.00	92	5C	908.40	953.40
31	IF	896.20	941.20	93	5D	908.60	953.60
32	20	896.40	941.40	94	5E	908.80	953.80
33	21	896.60	941.60	95	5F	909.00	954.00
34	22	896.80	941.80	96	60	909.20	954.20
35	23	897.00	942.00	97	61	909.40	954.40
36	24	897.20	942.20	98	62	909.60	954.60
37	25	897.40	942.40	99	63	909.80	954.80
38	26	897.60	942.60	100	64	910.00	955.00
39	27	897.80	942.80	101	65	910.20	955.20
40	28	898.00	943.00	102	66	910.40	955.40
41	29	898.20	943.20	103	67	910.60	955.60
42	2A	898.40	943.40	104	68	910.80	955.80

Частотний план (продовження)

43	2B	898.60	943.60	105	69	911.00	956.00
44	2C	898.80	943.80	106	6A	911.20	956.20
45	2D	899.00	944.00	107	6B	911.40	956.40
46	2E	899.20	944.20	108	6C	911.60	956.60
47	2F	899.40	944.40	109	6D	911.80	956.80
48	30	899.60	944.60	110	6E	912.00	957.00
49	31	899.80	944.80	111	6F	912.20	957.20
50	32	900.00	945.00	112	70	912.40	957.40
51	33	900.20	945.20	113	71	912.60	957.60
52	34	900.40	945.40	114	72	912.80	957.80
53	35	900.60	945.60	115	73	913.00	958.00
54	36	900.80	945.80	116	74	913,2	958.20
55	37	901.00	946.00	117	75	913.40	958.40
56	38	901.20	946.20	118	76	913.60	958.60
57	39	901.40	946.40	119	77	913.80	958.80
58	3A	901.60	946.60	120	78	914.00	959.00
59	3У	901.80	946.80	121	79	914.20	959.20
60	3C	902.00	947.00	122	7A	914.40	959.40
61	3D	902.20	947.20	123	7У	914.60	959.60
62	3E	902.40	947.40	124	7C	914.80	959.80

Для передачі кодованої мови й даних призначені канали зв'язку наступних типів:

- TCH/FS (Full Rate Traffic Channel for Speech).

- канал для передачі мови з повною швидкістю; TCH/HS (Half Rate Traffic Channel for Speech).

- канал для передачі мови з половинною швидкістю; TCH/F 9,6 (Full Rate Traffic Channel for 9,6 kbit/s User Data).

- канал передачі даних з повною швидкістю 9,6 кбит/з: TCH/F 4,8 (Full Rate Traffic Channel for 4,8 kbit/s User Data).

- канал передачі даних з повною швидкістю 4,8 кбит/з; TCH/F 2,4 (Full Rate Traffic Channel for 2,4 kbit/s User Data).

- канал передачі даних з повною швидкістю 2,4 кбит/з; TCH/H 4,8 (Half Rate Traffic Channel for 9,6 kbit/s User Data).

- канал передачі даних з половинною швидкістю 4,8 кбит/з; CH/H 2,4 (Half Rate Traffic Channel for 9,6 kbit/s User Data) - канал передачі даних з половинною швидкістю 2,4 кбіт/с.

Швидкість передачі цифрового мовного сигналу в каналі TCH/FS дорівнює 13 кбіт/с (за рахунок кодування збільшується до 22,8 кбіт/с у каналі TCH/F). Передача мови в каналі з половинною швидкістю TCH/HS ще не використається. Цей канал розглядається як перспективний при подальшому розвитку GSM, його застосування дозволить практично подвоїти ємність трафіку.

Канали зв'язку можуть передавати широкий набір інформаційних повідомлень, але вони не використаються для передачі сигналів керування. Крім того, для передачі даних по каналах зв'язку можуть використатися різні протоколи, наприклад, МККТТ X.25.

Структура логічних каналів керування.

Канали керування (CCH) забезпечують передачу сигналів керування й синхронізації. Розрізняють чотири види каналів керування:

BCCH (Broadcast Control Channels) - канали передачі сигналів керування; CCCH (Common Control Channels) - загальні канали керування;

SDCCH (Stand-alone Dedicated Control Channels) - індивідуальні канали керування; ACCH (Associated Control Channels) - сполучені канали керування. Канали передачі сигналів керування використаються тільки в напрямку з базової станції на всі рухливі станції. Вони несуть інформацію, що необхідна рухливим станціям для роботи в системі.

Розрізняють три види каналів передачі сигналів керування BCCH:
FCCH (Frequency Correction Channel) - канал підстроювання частоти, що використається для синхронізації несучої в рухливій станції. По цьому каналі

передається немодульована несуча з фіксованим частотним зрушенням щодо номінального значення частоти каналу зв'язку;

SCH (Synchronization Channel) - канал синхронізації, по якому передається інформація на рухливу станцію про кадрову (тимчасовий) синхронізації;

BCCH (Broadcast Control Channel) - канал керування передачею, забезпечує передачу основних команд по керуванню передачею (номер загальних каналів керування тих з них, які поєднуються з іншими каналами, у тому числі й з фізичними й т.д.).

Використовуються три типи загальних каналів керування CCCH:

PCH (Paging Channel) - канал виклику, використовується тільки в напрямку від базової станції до рухомого для її виклику;

RACH (Random Access Channel) - канал паралельного доступу, використовується тільки в напрямку від рухливої станції до базового для запиту про призначення індивідуального каналу керування;

AGCH (Access Grant Channel) - канал дозволеного доступу, використається тільки для передачі з базової станції на рухливу (для виділення спеціального каналу керування, що забезпечує прямий доступ до каналу зв'язку).

Виділені індивідуальні канали керування використаються у двох напрямках для зв'язку між базовою й рухливою станціями. Розрізняють два види таких каналів:

SDCCH/4 (Stand-alone Dedicated Control Channel) - індивідуальний канал керування, складається із чотирьох подканалов;

SDCCH/8 (Stand-alone Dedicated Control Channel) - індивідуальний канал керування, складається з восьми підканалів.

Ці канали призначені для установки необхідного користувачем виду обслуговування. По них забезпечується запит рухливої станції про необхідний вид обслуговування, контроль правильної відповіді базової станції й виділення вільного каналу зв'язку, якщо це можливо.

Сполучені канали керування також використовуються у двох напрямках між базовою й рухливою станціями. По напрямку "униз" вони передають команду керування з базової станції, а по напрямку "нагору" - інформацію про статус рухливої станції.

Розрізняють два види АССН:

FACCH (Fast Associated Control Channel) - швидкий сполучений канал керування, служить для передачі команд при переході рухливої станції зі стільники в стільнику, тобто при "естафетній передачі" рухливої станції; SACCH (Slow Assocaited Control Channel) - повільний сполучений канал керування, по напрямку "униз" передає команди для установки вихідного рівня потужності передавача рухливої станції. По напрямку "нагору" рухлива станція посилає дані, що стосуються рівня встановленої вихідної потужності, обмірюваного приймачем рівня радіосигналу і його якості.

У сполученому каналі керування завжди втримується один із двох каналів: канал зв'язку або індивідуальний канал керування.

Сполучені канали керування завжди поєднуються разом з каналами зв'язку або з індивідуальними каналами керування. При цьому розрізняють шість видів об'єднаних каналів керування:

FACCH/F, об'єднаний з TCH/F; FACCH/H, об'єднаний із TCH/H;

SACCH/TF, об'єднаний з TCH/F; SACCH/TH, об'єднаний із TCH/H;

SACCH/C4, об'єднаний з SDCCH/4; SACCH/C8, об'єднаний з SDCCH/8.

Організація фізичних каналів.

Для передачі каналів зв'язку TCH і сполучених каналів керування FACCH і SACCH використається 26-кадровий мультикадр. У повно швидкісному каналі зв'язку в кожному 13-му TDMA кадрі мультикадру передається пакет інформації каналу SACCH; кожний 26-й TDMA кадр мультикадру вільний. У напівшвидкісному каналі зв'язку пакет інформації каналу SACCH передається в кожному 13-м і 26-м TDMA кадрах мультикадру.

Для одного фізичного каналу в кожному TDMA кадрі використається 114 біт. Тому що в мультикадрі для передачі каналу зв'язку TCH використається 24 TDMA кадру з 26 і тривалість мультикадра становить 120 мс, загальна швидкість передачі інформаційних повідомлень по TCH каналі становить 22,8 кбіт/с. Канал SACCH займає в повно швидкісному каналі зв'язку тільки один TDMA кадр, тобто 114 біт, коли швидкість передачі по SACCH каналі складе 950 біт/с. Повна швидкість передачі в об'єднаному TCH/SACCH каналі з обліком порожнього (вільного) 26-го TDMA кадру складе 22,8 + 0,950 +0,950 - 24,7 кбіт/с.

За час 26-кадрового мультикадру (в одному фізичному каналі) може передаватися два напівшвидкісних TCH канали, кожний по 12 TDMA кадрів (T и t). Порожній 26-й TDMA кадр у повно швидкісному каналі TCH приділяється для каналу SACCH у другому напівшвидкісному каналі TCH. Для кожного напівшвидкісного каналу TCH швидкість передачі становить 11,4 кбіт/с; повна швидкість передачі в об'єднаному напівшвидкісному каналі TCH/SACCH залишається колишньої - 24,7 кбіт/с.

Швидкий сполучений канал керування FACCH передається половиною інформаційних біт тимчасового інтервалу TDMA кадру в каналі TCH, з яким він сполучається у вісьмох послідовних T або t кадрах.

Для передачі каналів керування (за винятком FACCH і SACCH) використається 51-кадровий мультикадр.

Об'єднання BCCH/CCCH каналів.

На відміну від структури об'єднаного каналу TCH/SACCH, де фізичний канал виділяється для одного або двох абонентів, об'єднаний канал BCCH/CCCH призначений для всіх рухливих станцій, які в те саме час перебувають в одній соте. Більше того, всі підканали, передані в цій структурі, є симплексними.

У каналі передачі сигналів керування (BCCH, "мережа - рухлива станція") передається загальна інформація про мережу (соте), у якій рухлива станція перебуває в цей момент, і про суміжні стільники.

У каналі синхронізації (SCH, "мережа - рухлива станція") передається інформація про часовий (цикловий) синхронізації й упізнаванні приймача-передавача базової станції.

У каналі підстроювання частоти (FCCH, "мережа - рухлива станція") передається інформація для синхронізації несучої.

Канал паралельного доступу (RACH, "рухлива станція - мережа") використається рухливою станцією в режимі пакетної передачі ALOHA для доступу до мережі у випадку, якщо треба пройти реєстрацію при включенні або зробити виклик.

Канал дозволеного доступу (AGCH, "мережа - рухлива станція") використається для заняття спеціальних видів обслуговування (SDCCH або TCH) рухливою станцією, що раніше запитувала їх через канал RACH.

Канал виклику (PCH, "мережа - рухлива станція") використається для виклику рухливої станції у випадку, коли ініціатором виклику є мережа (абонент мережі).

Лінія "нагору" BCCH/CCCH каналів використається тільки для передачі каналу паралельного доступу RACH, що є єдиним каналом керування від рухливої станції до мережі. Рухлива станція може використати нульовий часовий інтервал у кожному з кадрів для здійснення доступу до мережі.

На лінії "униз" 51 кадр групується в 5 груп по 10 кадрів, при цьому один кадр залишається вільним, кожна із цих груп починається з каналу FCCH, за яким треба канал SCH. Інші 8 кадрів у кожній групі утворять два блоки із чотирьох кадрів. Перший блок першої групи призначений для каналу CCH, тоді як інші 9 блоків (вони називаються блоками передачі сигналу виклику) використаються для передачі каналів PCH і AGCH загального каналу керування CCCH. Таким чином, у розглянутому випадку: 4 кадри використаються для каналу BCCH, 5 - для FCCH, 5 - для SCH і 36 або для AGCH, або для PCH (9 блоків виклику).

Кожна рухлива станція може займати один з дев'яти блоків виклику, але кожний викличний блок може використатися для виклику більше однієї станції.

Повна швидкість передачі для каналу BCCH, а також для каналу AGCH/PCH становить 1,94 кбіт/с (4х114 біт за 235 мс).

Існують і інші змінні структури, які можуть використатися в 51-кадровому мультикадрі. "Змінними" їх називають тому, що їхня структура змінюється залежно від навантаження в соті. В одному випадку може розглядатися індивідуальний канал керування 8SDCCH/8 в одному фізичному каналі. Однак, якщо навантаження в соте мала, засоби BCCH/CCCH можна об'єднати з індивідуальним каналом керування SDCCH/4 в одному фізичному каналі. Якщо стільника випробовує більше навантаження, одного фізичного каналу може бути недостатньо для всього трафіку BCCH/CCCH. У цьому випадку тимчасові інтервали 2, 4 і 6 у структурі BCCH також використають для цієї мети, однак у цьому випадку передаються порожні інтервали замість SCH і FCCH.

Відображення логічних каналів на фізичні канали здійснюється через процеси кодування й шифрування переданих повідомлень.

Для захисту логічних каналів від помилок, які мають місце в процесі передачі, використають 1ри виду кодування: блокове - для швидкого виявлення помилок при прийманні; найбільш точне - для виправлення одиночних помилок; переміщення - для перетворення пакетів помилок в одиночні.

Для захисту каналів від підслуховування в каналах зв'язку й керування застосовується шифрування.

Дня передачі повідомлень по фізичних каналах використається гаусівська частотна модуляція з мінімальним частотним зрушенням (GMSK).

Модуляція радіосигналу.

У стандарті GSM застосовується спектрально-ефективна гаусівська частотна маніпуляція п мінімальним частотним зрушенням (GMSK).

Модуляція називається "гаусівською" тому, що послідовність інформаційних біт до модулятора проходить через фільтр нижніх частот (ФНЧ) з характеристикою Гауса, що дає значне зменшення смуги частот випромінюваного радіосигналу. формування GMSK радіосигналу здійснюється таким чином, що на інтервалі одного інформаційного біта фаза несучої змінюється на 90°. Це найменша можлива зміна фази, розпізнавана при даному типі модуляції. Безперервна зміна фази синусоїдального сигналу дає в результаті частотну модуляцію з дискретною зміною частоти. Застосування фільтра Гауса дозволяє при дискретній зміні частоти одержати "гладкі переходи". У стандарті GSM застосовується GMSK-модуляція з величиною нормованої смуги BT = 0,3, де B - ширина смуги фільтра за рівнем мінус 3 дБ, T - тривалість одного біта цифрового повідомлення.

2.6 Обробка сигналів мовного діапазону

Загальний опис процесів обробки мови.

Процеси обробки мови в стандарті GSM спрямовані на забезпечення високої якості переданих повідомлень, реалізацію додаткових сервісних можливостей і підвищення споживчих якостей абонентських терміналів.

Обробка мови здійснюється в рамках прийнятої системи переривчастої передачі мови. Система переривчастої передачі мови (DTX) забезпечує включення передавача тільки тоді, коли користувач починає розмову й відключає його в паузах і наприкінці розмови. DTX управляється детектором активності мови (VAD), що забезпечує виявлення й виділення інтервалів передачі мови із шумом і шуму без мови навіть у тих випадках, коли рівень шуму досягає рівня мови. До складу системи переривчастої передачі мови входить також пристрій формування комфортного шуму, що включається й прослуховується в паузах мови, коли передавач відключений. Експериментально показане, що відключення фонового шуму на виході приймача в паузах при відключенні передавача дратує абонента й знижує розбірливість мови, тому застосування комфортного шуму в паузах

вважається необхідним. DTX процес з приймачі включає також інтерполяцію фрагментів мови, загублених через помилки в каналі.

Головним пристроєм у схемі обробки мови є мовний кодек.

Вибір мовного кодека для стандарту GSM.

Робочою групою по розробці стандарту GSM були пред'явлені наступні основні вимоги до мовного кодеку:

- висока якість мови, що не уступає якості передачі мови в кращих існуючих аналогових стільникових системах зв'язку;

- низька швидкість передачі мови, що забезпечує можливість ефективного канального кодування й результуючу швидкість передачі в каналі зв'язку не вище 16 кбіт/с;

- мала затримка повідомлення в процесі перетворення мови;

- стійкість до помилок у каналі передачі;

- можливість роботи в широкому динамічному діапазоні вхідних впливів як сигналу, так і шуму;

- великий динамічний діапазон вихідних сигналів;

- незначне зниження якості мови при каскадному з'єднанні кодеков;

- прозорість для сигналів даних;

- пряме сполучення із суміжними пристроями терміналів;

- простота реалізації;

- мале споживання;

- низька вартість.

Для вибору мовного кодека GSM був організований конкурс проектів.

Спочатку для розгляду було запропоновано 20 різних кодеков від 9 європейських країн. Після міжнародного формального тестування ця кількість була скорочена до 6 з 6 країн. На наступному етапі два із чотирьох смугових (SBC) кодеків (норвезький і італійський) були зняті з розгляду, до останнього етапу конкурсу залишилося два SBC кодека й два кодека в предикативним кодуванням:

RPE-LPC - Regular-Pulse Excitation/Linear Predicative Coding (Німеччина, Philips) -кодек з регулярним імпульсним порушенням і лінійним кодуванням із пророкуванням;

MPE-LTP - Multi-Pulse Excitation/Long-Term Prediction (Франція, IBM) - кодек із багатоімпульсним порушенням і довгостроковим передбачуванням.

На другому етапі відбувається подальше зниження динамічного діапазону за рахунок довгострокового пророкування, у процесі якого кожний сегмент вирівнюється до рівня наступних один за одним сегментів мови. У принципі, LTP фільтр віднімає попередній період сигналу з поточного періоду.

Цей фільтр характеризується параметром затримки N і коефіцієнтом підсилення b. Період обчислення цих параметрів дорівнює 5 мс.

Вісім коефіцієнтів r (i) LPC фільтра, що аналізує, і параметри фільтра LTP аналізу кодуються й передаються зі швидкістю 3,6 кбіт/с.

Для формування послідовності порушення залишковий сигнал пропускають через фільтр нижніх частот із частотою зрізу 3-4 кГц.

Остаточно періодична послідовність фрагментів передається зі швидкістю 9,4 кбіт/с. Загальна швидкість передачі становить 3,6+9,4 = 13 кбіт/с.

У декодері мовний сигнал відновлюється по відгуках послідовності регулярного імпульсного порушення (RPE) двоступінчастим синтезуючим фільтром.

При цьому якість мови відповідає якості мови, переданої по ISDN, і перевершує якість мови в аналогових радіотелефонних системах.

Теоретично час затримки мовного сигналу в кодекс дорівнює тривалості сегмента й становить 20 мс. Реальний час затримки, з урахуванням операцій канального кодування й переміщування, а також фізичного виконання розглянутих операцій, становить 70-80 мс.

Детектор активності мови.

Детектор активності мови (VAD) відіграє вирішальну роль у зниженні споживання енергії від акумуляторної батареї в портативних абонентських терміналах. Він також знижує інтерференційні перешкоди за рахунок перемикання вільних каналів у пасивний режим. Реалізація VAD залежить від типу застосовуваного мовного кодека. Головне завдання при проектуванні VAD - забезпечити надійну відмінність між умовами активного й пасивного каналів. Якщо канал на мить вільний, його можна заблокувати, оскільки середня активність мови мовця нижче 50%, то це може привести до істотної економії енергії акумуляторної батареї. До пристроїв VAD пред'являються наступні основні вимоги:

- мінімізація ймовірності фіктивної тривоги при впливі тільки шуму з високим рівнем;

- висока ймовірність правильного виявлення мови низького рівня;

- висока швидкодія розпізнавання мови, для виключення затримок включення;

- мінімальний час затримки вимикання.

У стандарті GSM прийнята схема VAD з обробкою в частотній області. Її робота заснована на розходженні спектральних характеристик мови й шуму. Уважається, що фоновий шум є стаціонарним протягом щодо великого періоду часу, його спектр також повільно змінюється в часі. VAD визначає спектральні відхилення вхідного впливу від спектра фонового шуму. Ця операція здійснюється інверсним фільтром, коефіцієнти якого встановлюються стосовно до впливу на вході тільки фонового шуму. При наявності на вході мови й шуму інверсний фільтр здійснює придушення компонентів шуму й, у цілому, знижує його інтенсивність. Енергія суміші «сигнал+шум» на виході інверсного фільтра рівняється з порогом, що встановлюється в період впливу на вході тільки шуму. Цей поріг перебуває вище рівня енергії шумового сигналу. Перевищення граничного рівня приймається за наявність на вході реалізації (сигнал+шум). Коефіцієнти інверсного фільтра й рівень порога змінюються в часі залежно від поточного

значення рівня шуму при впливі на вході тільки шуму. Оскільки ці параметри (коефіцієнти й поріг) використаються детектором VAD для виявлення мови, сам VAD не може на цій же основі приймати рішення, коли їх змінювати. Це рішення приймається вторинним VAD на основі порівняння спектрів, що обгинають, у послідовні моменти часу. Якщо вони аналогічні для відносно тривалого періоду часу, передбачається, що має місце шум, і коефіцієнти фільтра й шумовий поріг можна змінювати, тобто адаптувати під поточний рівень і спектральні характеристики вхідного шуму.

VAD з обробкою в спектральній області вдало сполучається з мовним RPE/LTP-LPC кодеком, тому що в процесі LPC аналізу вже визначається окружна спектра вхідного впливу, необхідна для роботи вторинного VAD.

Формування комфортного шуму.

Формування комфортного шуму здійснюється в паузах активної мови й управляється мовним декодером. Коли детектор активності мови (VAD) у передавачі виявить, що мовець припиняє розмову, передавач залишається ще включеним протягом наступних п'яти мовних кадрів. Під час перших чотирьох з них характеристики фонового шуму оцінюються шляхом усереднення коефіцієнта підсилення й коефіцієнтів фільтра LPC аналізу. Ці усереднені значення передаються в наступному п'ятому кадрі, у якому містять інформацію про комфортний шум (SID кадр).

У мовному декодері комфортний шум генерується на основі LPC аналізу SID кадру. Щоб виключити дратівний вплив модуляції шуму, комфортний шум повинен відповідати по амплітуді й спектру реальному фоновому шуму в місці передачі. В умовах рухомого зв'язку фоновий шум може постійно змінюватися. Це значить, що характеристики шуму повинні передаватися з передавальної сторони на прийомну сторону не тільки наприкінці кожного мовного сплеску, але й у мовних паузах так, щоб між комфортним і реальним шумом не було б різких неузгодженостей у наступних мовних кадрах. Із цієї причини SID кадри посилають кожні 480 мс протягом мовних пауз.

Динамічна зміна характеристик комфортного шуму забезпечує натуральність відтворення мовного повідомлення при використанні системи переривчастої передачі мови.

Екстраполяція загубленого мовного кадру.

В умовах завмирань сигналів у рухомому зв'язку мовні фрагменти можуть піддаватися значним перекручуванням. При цьому для виключення дратівного ефекту при відтворенні необхідно здійснювати екстраполяцію мовного кадру.

Було встановлено, що втрата одного мовного кадру може бути значно компенсована шляхом повторення попереднього фрагмента. При значних по тривалості перервах у зв'язку попередній фрагмент більше не повторюється, і сигнал на виході мовного декодера поступово заглушається, щоб указати користувачеві на руйнування каналу.

Те ж саме відбувається й з SID кадром. Якщо SID кадр загублений під час мовної паузи, то формується комфортний шум з параметрами попереднього SID кадру. Якщо загублено ще один SID кадр, то комфортний шум поступово заглушається.

Застосування екстраполяції мови при цифровій передачі, формування плавних акустичних переходів при завмираннях сигналу в каналах у сукупності з повним DTX процесом значно поліпшує споживчі якості зв'язку з GSM PLMN у порівнянні з існуючими аналоговими стільниковими системами зв'язку.

3 БЕЗПЕКА ЦИФРОВОГО СТІЛЬНИКОВОГО СТАНДАРТУ GSM

Криптозахист GSM мереж ґрунтується на поділюваній між SI і HLR секретної інформації. Цією секретною інформацією є Ki - секретний 128-бітний ключ, що зберігатися в SI і HLR, і використається для генерації 32-бітного відкликання (SRES) на випадковий пароль (RAND) у процедурі аутентифікації, а також для вироблення 64-бітного сесійного ключа (Kc), що використається для шифрування даних у радіоканалі. З першою появою MS у мережі HLR надає MSC п'ять трійок, які містять випадковий пароль (RAND), відкликання на цей пароль (SRES), згенерований за допомогою секретного ключа (Ki), а так само сесійний ключ (Kc) , отриманий з Ki. Кожна із трійок використається тільки для однієї сесії зв'язку з MS і MSC. Після 5 сесій MSC запитує в HLR новий набір з 5 трійок.

Коли MS уперше з'являється в області даного MSC, MSC посилає RAND з однієї із трійок, що ставляться до даного MS. MS виробляє SRES за допомогою A3 алгоритми, використовуючи отриманий RAND і Ki, що зберігається в SI. MS відсилає SRES, і, якщо він збігається з тим SRES, що втримується в даній трійці, то процедура аутентифікації вважається пройденої успішно.

Після цього MS посилає MSC SRES, що може підтвердити, що SRES дійсно відповідає Запиту, посланому відповідної SRES від MS і SRES у трійці від HLR. Таким чином, MS засвідчує в MSC (рис. 3.1).

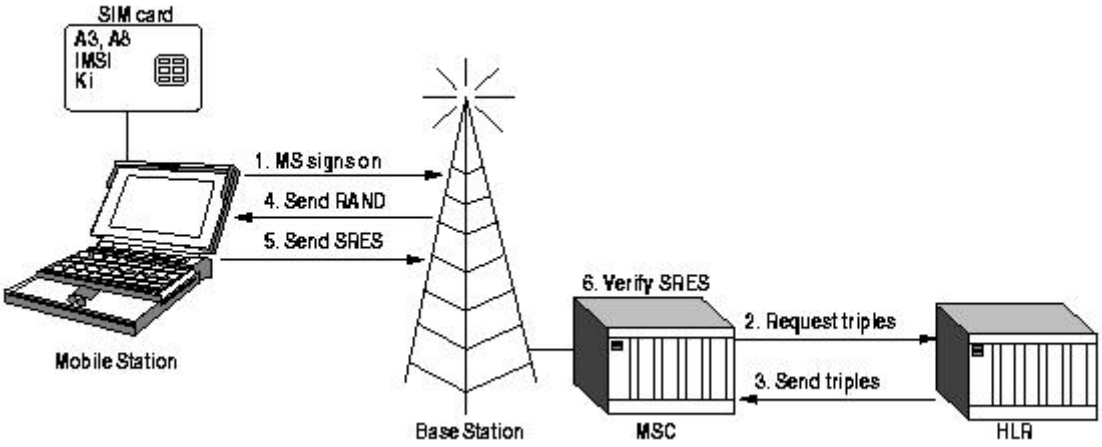

Рисунок 3.1 — Аутентифікація мобільної станції

Далі MS генерує сесійний ключ Kc, за допомогою алгоритму A8, використовуючи вже отриманий RAND і наявний Ki. Базова станція (BTS), використовувана для зв'язку з даної MS, одержує необхідний Kc в MSC. Із цього моменту радіоканал стає шифрованим.

Кожний кадр переданого по радіоканалі трафика кодується своєю 114-бітною ключовою послідовністю. Ця послідовність генерується за допомогою алгоритму A5.

3.1 Шифр A5

Шифр A5 – це потоковий шифр, який використовується для шифрування зв’язку GSM (мобільний груповий спеціальний зв’язок). Це європейський стандарт для мобільних цифрових стільникових телефонів. Він використовується для шифрування каналу „телефон/базова станція”. Частина каналу яка залишилася не шифрується, тому телефонна компанія може легко підслуховувати всі розмови.

Навколо цього протоколу ведуться дивні політичні ігри. Спочатку передбачалося, що з-за криптографії у стандарті GSM експорт телефонів в деякі держави був би заборонений. Зараз ряд чиновників обмірковують, чи не пошкодить шифр A5 експортним продажам, не дивлячись на те, що шифр такий слабий, що навряд чи являється великою перепоною. По слухам в

середині вісімдесятих років різні секретні служби НАТО посперечались по питанню, повинно бути шифрування GSM сильним чи слабим. Німцям потрібна була сильна криптографія, бо поряд з ними находився Радянський Союз. Однак перемогла друга точка зору, і шифр А5 представляє собою французьку розробку.

Більшість деталей шифру нам відома. Британська телефонна компанія передала всю документацію Бредфордському університету, забув примусити його підпис погодження про непоширення. Інформація десь просочилася і, в кінці кінців була опублікована в Інтернеті.

Генератор А5 складається з трьох РЗЛЗЗ довжиною 19, 22 і 23, всі багаточлени зворотного зв'язку у нього проріджені. Виходом являється операція XOR над трьома РЗЛЗЗ. В А5 використовується управління тактуванням яке змінюється. Кожний регістр тактується в залежності від свого середнього біту, а потім над регістром виконується операція XOR з зворотною пороговою функцією середніх бітів усіх трьох регістрів. Звичайно на кожному етапі тактується два РЗЛЗЗ.

Існує тривіальне розкриття А5, яке потребує 2^{40} шифрувань: припустимо утримання перших двох РЗЛЗЗ і спробуємо визначити третій РЗЛЗЗ по гамі. (Чи можливий в дійсності такий спосіб розкриття, остається від питанням, який скоро буде дозволено за допомогою спеціально розробленої машини для апаратного пошуку ключів).

Не дивлячись на це, становиться ясно, що ідеї, які лежать в основі А5, непогані. Алгоритм дуже ефективний. Він задовольняє усім відомим статистичним тестам, єдиною його слабістю являється те, що його регістри дуже короткі, щоб запобігти пошук ключа перебором. Варіанти А5 з більш довгими регістрами зсуву і більш щільними багаточленами зворотного зв'язку повинні бути безпечні.

З виправлень Шнайєра: „Додаткові відомості про алгоритм GSM. А3 – алгоритм аутентифікації на старт-картці. А8 – всього лише перетасовка бітів виходу А3, яка перетворюється в сеансів ключ для А5. А5 – алгоритм для

захисту розмов. Існує дві модифікації, які використовуються в GSM: A5/1 та A5/2. A5/1 може бути використано тільки в окремих державах; A5/2 – у всіх". На сьогоднішній день алгоритм A5 (в обох варіантах) повністю розкрито. Атака потребує 2^{48} попередніх розрахунків, а потім потребує декілька секунд на персональному комп'ютері.

Алгоритм A5 ініціалізується сеансовым ключем і номером переданого кадру, таким чином, для кожного кадру виходить власна послідовність. Це означає, що дешифрування одного дзвінка можливо, тільки якщо аналітик знає Кс і номер кадру. Той самий Кс використається, поки MSC не ініціює процедуру аутентифікації заново, при цьому буде згенеровано новий Кс. На практиці той самий Кс може використатися кілька днів, тому що аутентифікація не є обов'язковою процедурою на початку дзвінка й виробляється нечасто (рис. 3.2).

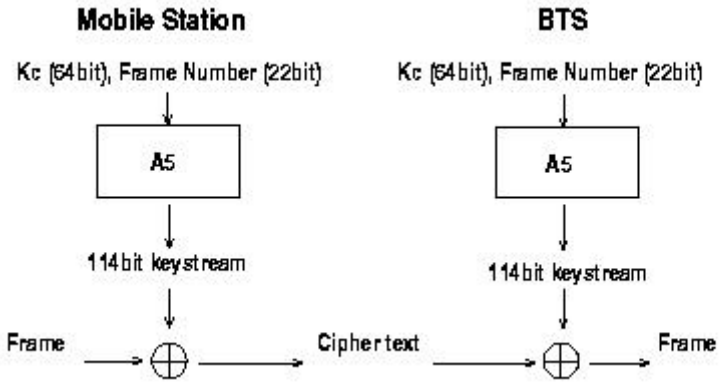

Рисунок 3.2 — Кадрове шифрування й розшифровка

У мережі GSM шифрується тільки ефірний трафик. Як тільки BTS бере кадр, він розшифровує його й посилає відкритим текстом операторові мережі.

3.2 Алгоритм аутентифікації A3 для MS

Алгоритм аутентифікації A3 використається для генерації відкликання SRES на випадковий пароль RAND, одержуваний від MSC. На вході A3 передаються RAND (128 біт) і Ki (128 біт), на виході одержують SRES (32 біта), як на рис. 3.3.

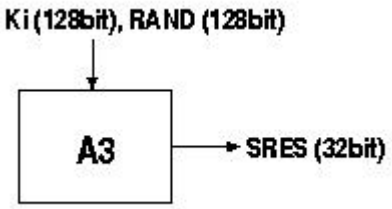

Рисунок 3.3 — Розрахунок підтвердженого результату (SRES)

Практично всі оператори GSM у світі використають алгоритм COMP128 у якості A3 і A8 алгоритмів. COPM128 був затверджений Консорціумом GSM як опорний для A3 і A8. Є пари операторів, які використають інші, але теж відомі, алгоритми.

Насправді , COMP128 на виході генерує 128-бітний рядок, але як SRES використаються тільки перші 32 біта.

3.3 Алгоритм A8 генерації ключа секретної розмови

Алгоритм A8 - це алгоритм генерації ключа в моделі безпеки GSM. A8 генерує сеансовый ключ, Kc, з випадкового числа, RAND, отриманого від MSC і секретного ключа Ki. Алгоритм A8 берет два вступних 128-битий і генерує з них 64-бітний висновок. Цей висновок є вивідним 64-бітним сеансовым ключем Kc [6]. Див. Малюнок 4. BTS одержав такий же ключ Kc від MSC. HLR зміг генерувати Kc, тому що HLR відомо й RAND (його згенерував HLR) і секретний ключ Ki, що він має для всіх абонентів даного оператора GSM мережі. Один сеансовый ключ Kc (рис. 3.4), використовується доти, поки MSC не прийме рішення знову аутентифіціювати MS. Це може відбутися через кілька днів.

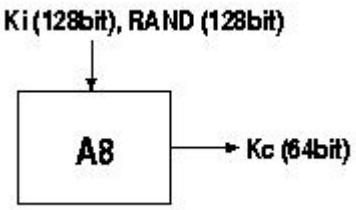

Рисунок 3.4 — Розрахунок Сеансового ключа (Kc)

Як зазначено в п. 3.1, COMP128 використається для алгоритмів A3 і A8 у більшості GSM мереж. COMP128 генерує одночасно й SRES, і сеансовый ключ, Kc. Останні 54 бітів висновку COMP128 формують сеансовый ключ, Kc, доти , поки знову не виробляється аутентифікація MS. Див Малюнок 5. Зверніть увагу, що довжина ключа в цьому місці становить 54 біта замість 64 бітів, що є довжиною ключа даного як уведення алгоритму A5. Десять нульових бітів додаються до ключа, згенерованому алгоритмом COMP128 (рис. 3.5). Таким чином, у нас є 64 бітний ключ із обнуленими останніми десятьма бітами. Це ефективно скорочує простір ключа з 64 бітів до 54 бітів. Це робиться у всіх реалізаціях l A8, включаючи ті, які не використають COMP128 для генерації ключа, імовірно, ця навмисна властивість реалізацій алгоритму A8.

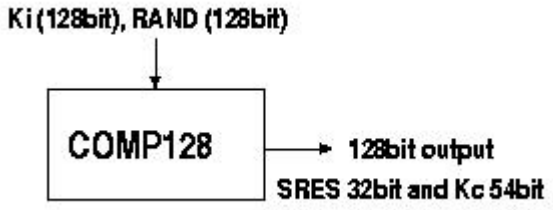

Рисунок 3.5 — Розрахунок COMP128

Обидва алгоритми, A3 і A8. утримуються в SI для запобігання стороннього втручання. Це означає, що сам оператор може вирішувати, який з алгоритмів використати незалежно від виробників устаткування й інших операторів мереж. Аутентифікація працює й в інших країнах теж, тому що місцева мережа запитує в HLR п'ять трійок домашньої мережі абонента. Таким чином, домашня мережа не повинна знати нічого про використовувані алгоритми A3 та A8.

3.4 Стійкий алгоритм A5/1 секретної розмови в ефірі

Алгоритм A5 - це потоковий шифр, використовуваний для шифрування передач в ефірі. Потоковий шифр инициализируется щораз для кожного кадру, що відсилає. Потоковий шифр инициализируется разом у сеансовым

ключем, Kc, а номер кадру шифрується/розшифровується. Цей же Kc використається протягом усього виклику, але 22-бітний номер кадру змінюється під час дзвінка, генеруючи в такий спосіб унікальну гаму шифру для кожного кадру (рис. 3.6).

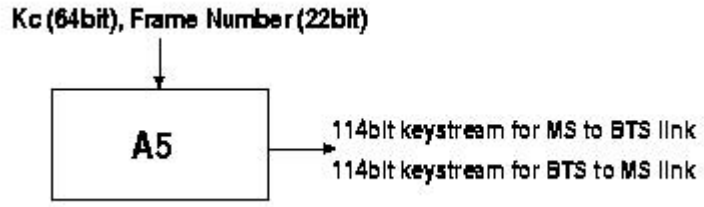

Рисунок 3.6 — Генерація Потокового шифру

Схема алгоритму A5 використовуваного в європейських країнах містить 3 LSFR (рис. 3.7) різні довжини (19, 22, 23 біта), сумарною довжиною в 64 біта. Для одержання чергового біта ключової послідовності, виходи всіх регістрів складаються по модулі 2. Всі 3 регістри мають керування зрушенням, тобто можна заборонити зрушення по черговому сигналі тактового генератора. Керування зрушенням відбувається по середньому біті. Зрушення відбувається, якщо значення середнього біта регістра збігається з переважним значенням середніх бітів всіх 3 регістрів. Приміром, якщо значення середніх бітів 0 0 1, то зрушення буде зроблений тільки в 1 і 2 регістрів, а якщо 1 0 1, то в 1 і 3. Таким чином, принаймні 2 з 3 регістрів зрушуються на кожному кроці (рис. 3.8).

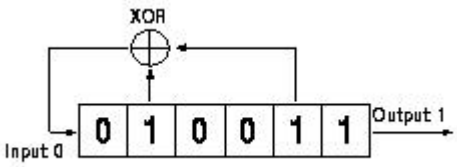

Рисунок 3.7 — Приклад LSFR з багаточленом зворотного зв'язка x6 + x4 + x

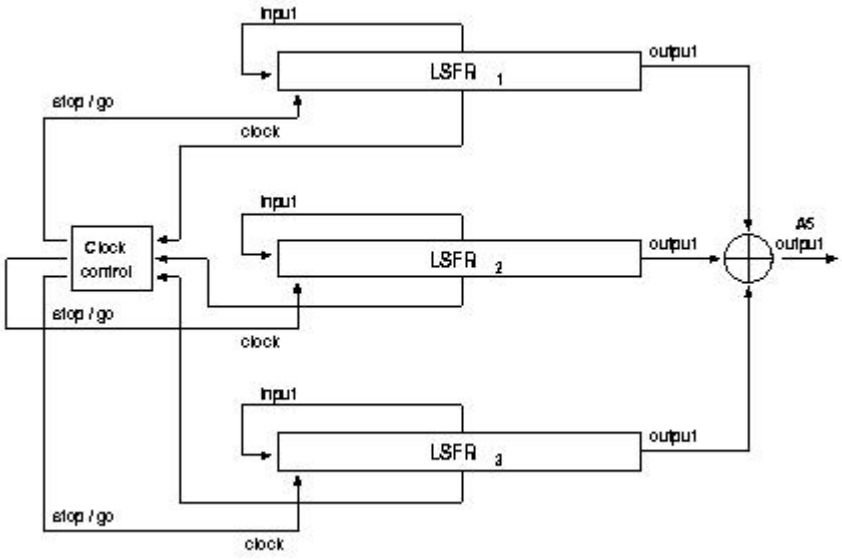

Рисунок 3.8 — Структура A5 LSFR

Три LSFR-а инициализируются сеансовым ключі, Kc, і номером кадру. 64-бітовий сеансовый ключ Kc спочатку завантажується в регістр біт за бітом. LSB ключа - це результат XOR у кожному регістрі LSFR. Потім всі регістри синхронізуються (правило синхронізації більшості відключене). Всі 64 біта ключа завантажуються в регістр однаково. 22-бітний номер кадру також завантажується в регістр у такий же спосіб, але із цього моменту застосовується правило синхронізації більшості. Після того, як регістри були в такий спосіб ініціалізовані, роблять 100 кроків і отриману послідовність відкидають. Наступний 228 біт становлять вихідну ключову послідовність перші 114 біт якої використають для шифрування кадру від MS до BTS, а інші 114 назад від BTS до MS. Для шифрування наступного кадру, схема инициализируется заново, і процес повторюється.

З тих пір як з'явилися перші GSM системи, були розроблені й реалізовані й інші алгоритми A5. Основним мотивуванням було те, що оригінальний алгоритм шифрування A5 - занадто стійкий для експорту на Близький Схід. Тому перший оригінальний алгоритм A5 був перейменований на A5/1. Інші алгоритми включають A5/0, що означає, відсутність шифрування, і більше слабкий алгоритм A5/2. Загалом , алгоритми A5 після

A5/1 називалися A5/x. Більшість із них значно слабкіше, ніж A5/1, (має стійкість 254). Стійкість A5/2 216. Це шифрування використається в США. Про інші варіанти A5 достовірних відомостей ні, як, втім, і підтвердження того, що вони успішно застосовуються.

4 ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ GSM

Як і в будь-якій системі шифрування, у системі безпеки GSM найбільший інтерес представляє її стійкість до дешифрування, особливо, якщо, принаймні , один з алгоритмів уже зламаний.

Учені в усьому світі одностайні в думці, що прослуховування, перехоплення й розшифровка даних, переданих по радіоканалі в реальному часі на даний момент поки ще неможливо, незалежно від скорочення ключового простору. Але, імовірно, існують інші способи злому системи, які являють дійсну загрозу.

4.1 Лобова атака A5

Як було зазначено вище, лобова атака системи безпеки в реальному часі неможливий. Складність атаки становить 254 (264 якщо 10 битов не були 0). Буде потрібно занадто багато часу, щоб прослуховування GSM дзвінків у реальному часі стало можливим. Можна було б записати кадри між MS і BTS і після цього почати атаку.

Якщо ми маємо чип класу Pentium III, що містить приблизно 20 мільйонів чипів, а для реалізації одного набору LSFR схеми шифрування алгоритму A5 потрібно 2000, то в одному чипі можна організувати приблизно 10000 реалізацій A5/1. При тактовій частоті 600 МГЦ, і якщо кожна реалізація A5 видає 1 біт за такт, і необхідно згенерувати 100+114+114 біт, у реалізації A5/1 можна перевіряти 2 мільйони ключів у секунду. Простір ключів в 254 вимагає для перебору 900000 секунд або приблизно 250 годин при одному чипі. Атака може бути оптимізована відкиданням цілих класів ключів після першого "поганого" біта ключової послідовності. Це скоротить необхідний час на одну третину. Атаку можна розподілити між декількома чипами, і в такий спосіб значно скоротити час.

4.2 Атака A5 “Розділяй і Пануй”

Атака Розділяй і Пануй дозволяє зменшити стійкість алгоритму з 254 при лобовій атаці до 245, і це вже є відносно значною зміною (29 - це в 512 разів швидше). Атака Розділяй і Пануй заснована на відомій атаці відкритого тексту. Атакуючий намагається визначити початкові стани регістрів LSFR з відомої послідовності гами. Атакуючий повинен знати 64 послідовні біта гами, які можна витягти, якщо атакуючий знає який-небудь текст шифру й відповідний відкритий текст. Це у великому ступені залежить від формату GSM кадрів, що посилають туди й назад. Кадри GSM містять велика кількість постійної інформації, наприклад, заголовки кадрів. Необхідні 64 битка не завжди можуть бути отримані, але 32 або 48 біт, іноді й більше, звичайно відомі. Атакуючий необхідний тільки сегмент із 64 битов відкритого тексту.

Одним словом, атака Розділяй і пануй реалізується шляхом угадування змісту двох більше коротких LSFR, а потім обчислення третього LSFR з відомої гами. Це була б атака 240 , якби синхронізація перших двох регістрів не залежала від третього регістра. Внаслідок того, що центральний біт третього регістра використається для синхронізації, нам необхідно також угадати майже половину бітів третього регістра між бітом синхронізації й LSB. Цей факт збільшує складність атаки з 240 до 245.

Однак Дж. Голик запропонував іншу атаку Розділяй і Пануй, засновану на цих же з, приблизна складність атаки 240 . Він описує, як одержати лінійну рівність, вгадуючи n біти в регістрах LSFR. Вирішивши ці лінійні рівняння, можна відновити початкові із трьох LSFR. Складність рішення лінійних рівнянь становить 240. Існує тільки 50-процентна ймовірність рішення.

У цій же роботі Голик запропонував атаку, з на Парадоксі днів народжень. Метою цієї атаки було відновлення початкових станів трьох LSFR у відомий проміжок часу для відомої гами, що відповідає відомому номеру кадру, і, таким чином, відновлення сеансового ключа, Kc.

4.3 Доступ до сигнальної мережі

Два приклади, наведені вище, чітко доводять, що криптографічний алгоритм A5 ненадійний, з огляду на можливість здійснити не тільки Лобову атаку, але й інші атаки. У цей час почати лобову атаку не складно, беручи до уваги доступне зараз устаткування. Однак, алгоритм досить стійкий для запобігання перехоплення в ефірі й злому шифрування в реальному часі. На жаль, у системі GSM уразливою ділянкою з не тільки радіохвилі між MS і BTS.

Як вказувалося вище, передачі шифруються тільки між MS і BTS. За межами BTS у мережі оператора трафік передається відкритим текстом. Це відкриває нові можливості.

Якщо зловмисник може одержати доступ до сигнальної мережі оператора, він зможе слухати всі передачі, включаючи самі телефонні дзвінки, а також RAND, SRES і Kc. Сигнальна мережа SS7, використовувана операторами GSM мережі, абсолютно незахищена, якщо зловмисник одержує до неї прямий доступ. При іншому сценарії зловмисник може атакувати HLR певної мережі. Якщо зловмисник зможе одержати доступ до HLR, він зможе витягти всі Ki абонентів даної мережі. На щастя, HLR звичайно більше безпечна, чим вся інша мережа, таким чином, вона є менш очевидною ділянкою для проникнення.

Одержати доступ до мережі не представляє особливих труднощів. Хоча всі BTS звичайно з'єднані кабелем, у деяких з них зв'язок мікрохвильова або супутникова. Одержати доступ до цього зв'язку відносно просто при наявності відповідного встаткування. Очевидно, саме ця уразливість використається при прослуховуванні мобільного телефону за допомогою наявного в продажі встаткування. На жаль, я не можу підтвердити це, тому що специфікації на це встаткування є тільки в співробітників правоохоронних установ. Однак, мікрохвильова лінія може бути зашифрована, тому прослуховувати її небагато складніше. Важливо те, чи хоче зловмисник зламати шифрування A5, що забезпечує захищу сеансу

зв'язку окремої MS, або шифрування між BTS і BSC для одержання доступу до основної мережі. Також не треба виключати й можливість доступу до кабелю, що йде від BTS. Це може бути реальною погрозою, і атаку можна реалізувати непомітно довгий час, якщо робити це акуратно. Прослуховування інформації, переданої між BTS і BSC, надасть можливість зловмисникові або прослуховувати дзвінок, прослуховуючи канал, або він зможе витягти сеансовый ключ, Kc, прослуховуючи канал, перехоплюючи дзвінок в ефірі, відразу розшифровуючи його. Тепер, коли йому відомий Kc, шифрування в реальному часі не представляє проблеми.

Не варто виключати й інший підхід. Зловмисник може видати себе за ремонтника, проникнути в потрібний будинок і встановити прослуховування. Він також може підкупити інженера, і той видасть йому всі Ki всіх абонентів даного оператора зв'язку. Таких можливостей безліч, і вони існують.

4.4 Витягування ключа з SI

Вся модель безпеки GSM заснована на секретному ключі Ki. Якщо цей ключ скомпрометований, буде скомпрометований і весь рахунок. Як тільки зловмисник витяг Ki, він не тільки зможе прослуховувати дзвінки абонентів, але й переадресовувати рахунку за дзвінки на рахунок абонентів, тому що тепер він може визначити й легального абонента. У мережі GSM є для цього пастка. Якщо два телефони з тим самим ID включаються одночасно, мережа GSM зауважує це, робить запит про місцезнаходження цих телефонів, зауважує, що той самий телефон перебуває у двох місцях одночасно, і закриває рахунок, не даючи можливість дзвонити ні зловмисникові, ні законному абонентові. Але це не відбувається, якщо зловмисник зацікавлений тільки в прослуховуванні дзвінків абонента. У цьому випадку, зловмисник може залишатися пасивним і просто прослуховувати дзвінок, залишаючись невидимим для мережі GSM.

Асоціація Розроблювачів Смарткарт і дослідницька група ISAAC винайшли діру в алгоритмі COMP128 algorithm, що дозволяла витягати

секретний ключ, Ki, з SI. Атака вживала на SI, до якої в них був фізичний доступ, однак, така ж атака застосовна й в ефірі.

Атака ґрунтувалася на атаці обраний виклик, що здійсненний, тому що алгоритм COMP128 зламаний таким чином, що за допомогою атаки витягає інформація про Ki, коли відповідним RAND задаються як аргументи алгоритму A8. Доступ до SI був отриманий через Smartcard reader, з'єднаної з PC. PC робив близько 150.000 викликів SI, SI генерувала SRES і сеансовый ключ, Kc, заснований на виклику й секретному ключі. Секретний ключ можна було відняти з відгуку SRES шляхом диференціального криптоаналізу. Smartcard reader, використовувана для реалізації атаки, могла зробити 6.25 запитів SI card у секунду. Для реалізації атаки було потрібно 8 годин. Її результати необхідно було ретельно перевірити, але проте це було відносно швидко в порівнянні з дійсною атакою. Таким чином, зловмисникові потрібен доступ до SI хоча б протягом 8 годин. Ця уразливість також має соціальний сценарій (залучення інженера). Можна припустити, що корумпований GSM дилер клонує SI карти в такий спосіб і продасть клоновані карти третім особам, які хочуть залишитися невідомими й не бажають купувати справжні SI карти. Клонована SI карта може також бути продана кому-небудь із метою прослуховування згодом його розмов. Корумпований співробітник також може надати зловмисникові SI жертви, щоб клонувати SI і згодом прослуховувати розмови власника карти. Все це дуже реалістичні сценарії. модель безпеки системи GSM повністю Уразливість, виявлена в алгоритмі COMP128, компрометує всю модель безпеки системи GSM і залишає абонентів без захисту.

4.5 Витягування ключа з SI карти в ефірі

Дослідники SDA ISAAC упевнені, що така ж атака із клонуванням SI карти може бути реалізована й ефірі. На жаль, вони не можуть підтвердити своє припущення, тому що встаткування, необхідне для цього, незаконно в США. Атака в ефірі заснована на наступному. Потрібно, щоб MS

відгукувалася на кожний виклик мережі GSM. Якщо потужність законного сигналу BTS перевищена нестандартної BTS зловмисника, зловмисник може бомбардувати викликами цільову MS і реконструювати секретний ключ по відгуках. MS повинна бути доступна зловмисникові в ефірі увесь час, необхідне для атаки. Невідомо, скільки часу протриває атака в ефірі. Приблизно від 8 до 13 годин.

Атака може бути почата в метро, коли недоступний сигнал законної BTS, але телефон включений. Абонент не помітить атаку, хоча той факт, що батарейка розрядиться швидше звичайного, може спантеличити його. Атаку також можна реалізувати вроздріб : замість того, щоб атакувати протягом 8 годин, зловмисник може впливати на телефон щодня протягом 20 хвилин, поки жертва йде на роботу. Коли SI карта буде клонована, SiM-клон можна використати тільки доти, поки абонент не скористається нової SI картою, що на практиці це трапляється рідко.

При іншому сценарії абонент може перебувати в робочому відрядженні за кордоном. Зловмисник якимось образом змусив місцевого оператора GSM почати атаку на мобільний телефон абонента. Зловмисник знову зможе реконструювати Ki на підставі SRES відповідей мобільної станції, і атака, імовірно, не буде замічена, тому що виклики приходили із законної мережі. Помнете, локальної мережі нічого не відомо про Ki, тому що трійки виходять від HLR домашньої мережі абонента. Таким чином, локальна мережа повинна відняти Ki з відгуків A3.

4.6 Витягування ключа з Au

Така ж атака по витягу Ki з SI карти може бути використана для витягу Ki з Au. Au не одержує відповідь на запити, зроблені мережею GSM і повертає дійсні трійки для аутентифікації MS. Процедура в основному схожа на процедуру одержання доступу SI карти в MS. Розходження полягає в тому, що Au набагато швидше обробляє запити, чим SI карта, тому що йому потрібно обробити набагато більше запитів, чим однієї SI карті. Безпека Au

відіграє більшу роль для запобігання можливості атаки, але це не є темою даної роботи.

4.7 Злам алгоритму A8

Також існує ймовірність, що хто-небудь може без особливих зусиль зламати алгоритм генерації ключа A8 і витягти секретний ключ, Ki, заснований на випадковому виклику, RAND, сеансовому ключі, Kc, і відгуку SRES (передбачається, що той самий алгоритм використається в A3 і A8, як у випадку з COMP128). Наприклад, з може знайти RAND, що робить у результаті Ki (найлегший приклад). Всі три змінні відносно просто знайти. RAND і SRES відсилаються по ефірі відкритим текстом. Сеансовий ключ Kc можна відносно легко при наявності достатньої кількості часу відняти із зашифрованих кадрів і відомого відкритого тексту. Уразливість такого роду в алгоритмі генерації ключа, звичайно, зруйнує всю систему безпеки GSM і дасть Консорціуму GSM привід для міркування, коли вони будуть винаходити свої наступні алгоритми безпеки.

4.8 Безпека GPRS проти GSM безпеки

У системі GPRS кадри транслюються з MS в SGSN у вигляді шифрованого тексту, тому що система GPRS використає безліч таймслотів паралельно в мережі, збільшуючи в такий спосіб швидкість передачі MS. Кадри можуть відсилатися паралельними таймслотами в ту саму BTS або у дві різні BTS, якщо MS передається від однієї BTS іншої.

BTS бачить передачу одного таймслота у вигляді окремого дзвінка. Таким чином, BTS не в змозі скласти воєдино всі кадри з різних таймслотів. Це значить, що в мережі повинен бути компонент, що міг би одержувати кадри від однієї MS, дефрагментувати їх і відсилати їх далі по призначенню. BTS не в змозі розшифровувати кадри, тому що послідовні кадри в одному каналі не мають послідовних номерів кадрів. Див Малюнок 9. Для того, щоб полегшити виконання завдання, кадри розшифровуються в SGSN, де

закінчуються всі кадри й де дійсно просто відстежити номера кадрів. Рішення засноване на простоті виконання, воно не виконувалося, щоб підсилити систему безпеки. Як побічний ефект, система GPRS ефективно запобігає прослуховуванню між BTS і SGSN, тому що на цій ділянці кадри усе ще зашифровані. В GPRS трійки від HLR передаються в SGSN, але не в MSC. Таким чином, безпека GPRS залежить великою мірою від розміщення й безпеки вузлів забезпечення GPRS (рис. 4.1).

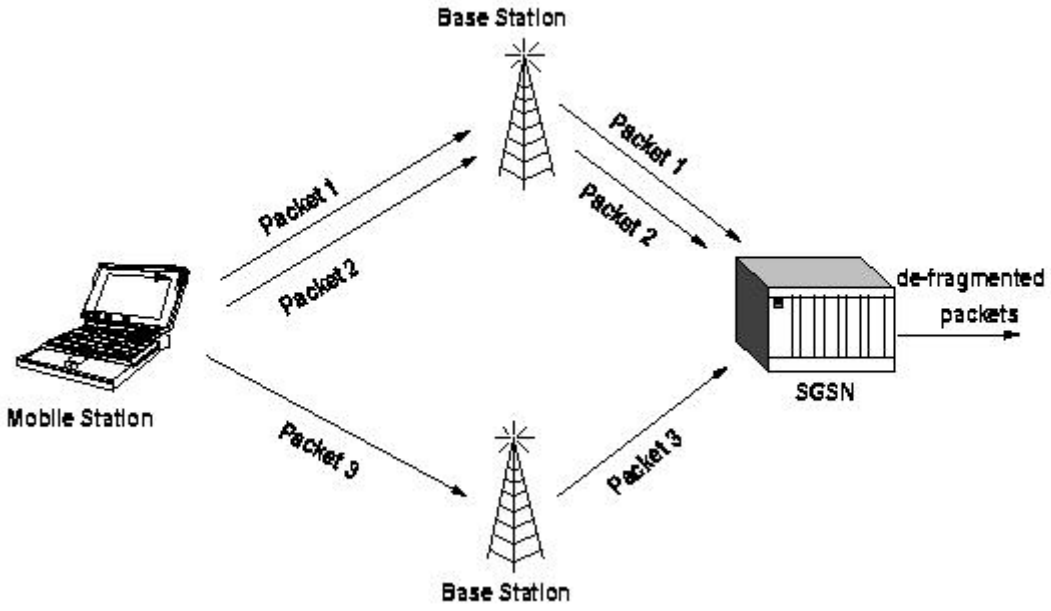

Рисунок 4.1 — Архітектура GPRS

Система GPRS використає також і нову реалізацію A5, у вільному доступі її немає. Цей факт і той факт, що кадри розшифровуються не в BTS, а в SGSN, перешкоджає декільком атакам. По-перше, дуже важко атакувати реалізацію A5, коли вона невідома. По-друге, Kc не транслюється в BTS, канал передачі між BTS і SGSN зашифрований, що робить марним прослуховування між BTS і SGSN. Це не означає, що модель безпеки GPRS сильніше моделі безпеки тільки GSM. Це означає, що однакові атаки не працюють на GPRS, але спрацьовують просто в мережі GSM. Як тільки стане відомо про реалізації A5, використовуваної в in GPRS, модель безпеки GPRS буде піддана новим атакам. А реалізація обов'язково стане відома, або дизайн

буде успішно інвертований. Як було зазначено вище, безпека крипто системи буде заснована тільки на ключі. Однак, більшість атак проти винятково системи GSM можна застосувати й проти GPRS. Приміром , атака клонування SI. Крім того, модель GPRS демонструє ще одну погрозу безпеки через використання SGSN, яким від HLR відомі трійки. Це означає, безпека мережі GPRS у великому ступені залежить від розташування SGSN в архітектурі мережі й від їхньої безпеки. Якщо SGSN уразливі для атаки, трійки теж уразливі.

5 ПІДВИЩЕННЯ БЕЗПЕКИ GSM

Значно підвищити рівень безпеки розмов у мережі стандарту GSM можна за допомогою абонентського шифрування. Воно може здійснюватися як програмними методами, так і апаратними. Апаратні методи шифрування можуть здійснюватися за допомогою додаткового чіпу всередині апарату GSM, або за допомогою додаткового пристрою, який виконує функцію шифрування і під'єднується до мобільного терміналу.

Австралійська компанія SecureGSM анонсувала нове програмне забезпечення для смартфонів і комунікаторів, що дозволить домогтися 256-бітного кодування розмови. Використаються надійні шифрувальні алгоритми AES, Twofish і Serpent. Весь процес криптоперетворень відбувається "на лету". Програмі потрібні ОС Windows Mobile і процесор з тактовою частотою не менше 200 МГц.

Криптосмартфон розробки компанії АНКОРТ (рис. 5.1) з самого початку планувався для криптографічного захисту. У телефоні є спеціалізований крипто-чип, спеціальні фільтри й металевий екран, які запобігають небезпечні випромінювання.

Рисунок 5.1 — Захищений GSM смартфон

У складі криптосмартфона відсутні такі високо випромінюючі елементи як відеокамера, Bluetooth, інфрачервоний порт, знімна додаткова пам'ять, Wi-Fi. Крім того, розроблена унікальна система контролю правильності роботи шифратора.

Реалізація особливої системи синхронізації забезпечує надійну роботу криптосмартфона в роумінгу. Особливо, тоді коли роумінг доводиться здійснювати на значно вилучені відстані й де при передачі використаються аналогові засоби передачі даних. У цьому випадку в криптосмартфоні розроблена унікальна система відновлення криптосинхронізації, що забезпечує високу надійність з'єднання.

Розроблений криптосмартфон компанією АНКОРТ має найвищі криптографічні, інженерно криптографічні характеристики, що забезпечують надійний криптографічний захист (табл. 5.1).

Таблиця 5.1 — Криптографічні характеристики

Криптопроцесор	TMS 320 VC 5416
Крипто дзвінок	Так
Крипто SMS	Так
Крипто E-mail	Так (шифруються текст и вкладення)
Кнопка Крипто дзвінка	Окрема кнопка
Ключова стійкість	10^{77}
Криптоалгоритм	ГОСТ 28147-89
Метод розподілу ключів	Відкритий ключ, довжиною 256 біт, заснований на розрахунку параметрів еліптичних кривих.
Шифрування даних в криптосмартфоні	Так
Складова розбірливість	87%

5.1 Талісман-GSM

Базовий варіант із інтегрованим криптомодулем ТАЛІСМАН GSM - пристрій криптографічного захисту мовної інформації, переданої з використанням мобільних мереж зв'язку GSM (900/1800 МГЦ).

На базі пристроїв ТАЛІСМАН GSM може бути побудована Закриту користувальницька група з необмеженим числом абонентів. З'єднання може бути встановлене як у мережі одного, так і різних операторів зв'язку, включаючи роумінг.

Для побудови системи захищеного зв'язку необхідний як мінімум два ТАЛІСМАНИ GSM.

Криптомодуль інтегрований у стандартний мобільний телефон без зміни конструктивних параметрів корпусних деталей.

Ведення відкритих (звичайних) переговорів можливо з усіма абонентами, включаючи абонентів закритої користувальницької групи.

При конфіденційному зв'язку здійснюється вокодерне перетворення мовного сигналу й шифрування по алгоритму ДСТУ 28147-89 з високою стійкістю до розкриття. Захист здійснюється на всьому тракті абонент.

Для режиму конфіденційного зв'язку використається канал передачі дані мережі GSM. Швидкість передачі даних становить 9600 біт/с.

Спеціальне програмне забезпечення ТАЛІСМАН GSM дозволяє створювати закриті групи користувачів. Шифроване з'єднання можливо тільки тоді, коли телефони обох абонентів належати однієї й тойже закритій користувальницькій групі.

Обов'язковою умовою роботи ТАЛІСМАН GSM у захищеному режимі, є наявність підключеної послуги "передача даних". Дана послуга надається оператором стільникового зв'язка при висновку контракту, або по запиті користувача.

Таблиця 5.2 — Криптографічні характеристики ТАЛІСМАН GSM

Основні характеристики	
Стиснення мови (визначається користувачем)	2000/4800/6300 біт/с
Режим передачі даних	асинхронний, непрозорий
Тип з’єднання	повний дуплекс
Затримка сигналу в лінії	не більше 500 мс
Час встановлення з’єднання	V.110 - 2 сек., V.32 - 15 сек.

5.2 CriptoCell

Криптоселл - це термінал "включив і працюй", що забезпечує надійну передачу закодованих цифровим образом повідомлень. Криптоселл приєднується безпосередньо до мобільного телефону стандарту GSM. Завдяки використанню міжкінцевої і багатоточкової системи захисту, Криптоселл (рис. 5.2) є першим і поки єдиним пристроєм, що забезпечує захист зв'язку GSM за доступною ціною (версії багатоточкового зв'язку), навіть за умови установки термінала Криптоселл тільки в одного з абонентів, що розмовляють.

Рисунок 5.2 — CriptoCell модуль

Криптоселл, на відміну від інших присутніх на ринку подібних пристроїв для мережі GSM, що вимагають придбання спеціального й дуже дорогого мобільного телефону, є пристосуванням, що може використатися разом із загальнодоступними й розповсюдженими моделями мобільних телефонів Ericsson і Sony-Ericsson. Досить приєднати Криптоселл до мобільного телефону для установки телефонного зв'язку з Військовим рівнем таємності й найвищою якістю голосу. Криптоселл може також кодувати дані (опція) на каналі V110 GSM за допомогою міні-USB конектора. Криптоселл сполучимо з іншими пристроями, наприклад, із Криптотел і може передавати на них дані.

Основні характеристики пристрою Криптоселл:

- Надійний міжабонентський й багатоточковий телефонний зв'язок по мережі GSM.
- Можливість проведення безпечних телефонних переговорів будь-яким абонентом по будь-якому номері.
- Абсолютний захист змісту телефонної розмови, номера абонента, що дзвонить, і набраного номера.
- Простота у використанні.
- Сумісність із різними моделями наявних у продажі мобільних телефонів стандарту GSM.
- Знімний пристрій з використанням за принципом "включив і працюй".
- Звукова й світлова сигналізація досягнутого рівня захисту для кожного дзвінка.
- Звукова сигналізація для незахищених дзвінків.
- Інформація виводиться на екран мобільного телефону.
- Відмінна якість голосу.
- Високий рівень кодування з витягом нового ключа для кожного сеансу й використанням алгоритмів асиметричного кодування із ключем (Diffie Hellman) для обміну ключем і симетричним кодуванням (AES) для сеансів.
- Економічність.

- Мінімальний вплив на автономію батареї внаслідок мінімального споживання електроенергії.

Наведені характеристики КриптоСелл в табл. 5.3.

Таблиця 5.3 — Технічні характеристики КриптоСелл

Алгоритми шифрування асиметричний ключ - Diffie Hellman 1024 біт і симетричний ключ - AES 128/192/256 біт Вокодер G.723.1 сумісний V110 Відповідає стандарту PRI ISDN Максимальна швидкість передачі 14,400 біт/с Час синхронізації 7 сек. Швидкість обміну (с/на мобільний) 88 кбіт/с Швидкість передачі Залежить від мережі даних GSM Режим мережі GSM Непрозорий	Конектор USB Стандартний міні-USB Споживання потужності 17,5 мвт у режимі очікування, максимум 280 мВт 5 мВт off Вага 11 м Габарити 40мм х 22мм х 7мм Температури Робота: від 0° до +60° С Зберігання: від -20° до +70° С Підтримувані моделі мобільних телефонів Ericsson: T39, T65, T68, R520 Sony Ericsson: T68i, T200, T300

Cancort - це новий спеціалізований криптографічний мобільний телефон стандарту GSM 900/1800 (рис. 5.3), що забезпечує зв'язок у мережах GSM, призначений для одержання й передачі голосових повідомлень і даних по мережі GSM у криптографічному режимі (пряме з'єднання) з використанням спеціальних засобів криптографічного захисту.

Рисунок 5.3 — Смарт телефон "Cancort"

Характеристики:

- Стійкий алгоритм забезпечує надійне шифрування голосу й даних в одному GSM телефоні.
- Повна взаємодія всіх типів телефонного зв'язку з алгоритмом шифруванням даних.
- Підключений до комп'ютера, дозволяє відправляти зашифровані повідомлення електронної пошти по мережі Інтернет.
- По зовнішньому вигляді не відрізняється від звичайних мобільних телефонів бізнес класу.
- Сполучимо із уже існуючим рядом крипто телефонів - Telephone Coder-GSM, Coder-iSDN, телефон Voice-Coder 9600, призначених для аналогових телефонних ліній, IP телефон, супутникового телефону.
- Забезпечує створення корпоративної захищеної мережі, тому що всі ці телефони криптографічно сумісні й можуть створити, таким чином, надійно захищену лінію зв'язку.

Cancort забезпечує роботу на лініях зв'язку стандарту GSM 900/1800 у двох режимах:

- Відкритий режим (звичайний режим GSM);
- Режим шифрування з гарантованим від злому шифруванням інформації.

Cancort виконує наступні функції:

- шифрування/розшифровка голосової інформації.
- шифрування/розшифровка коротких повідомлень (послуга SMS).
- шифрування/розшифровка даних (послуга BS26 і GPRS).
- шифрування/розшифровка електронної пошти.
- шифрування/розшифровка інформації всіх телефонних директорій (SI PB).
- шифрування/розшифровка інформації MMS.

Комплект поставки.

У комплект входить стандартний набір аксесуарів стільникового телефону. Крім того, є додатковий комплект, у який входить:

- станція генерації ключів для генерації унікальних ключів для Cancort.
- пристрій для уведення ключової інформації (користувач може самостійно генерувати ключі).
- Режими роботи і криптографічні характеристики Cancort наведені в табл. 5.4 і табл. 5.5.

Таблиця 5.4 — Режим роботи

Параметри	Коментар
Шифрування голосу	Повнодуплексний режим (4800, 9600 біт/сек)
Сумісність с Coder-ISDN	-
Радіомодем стандарту GSM 900/1800 МГц	
Модем	V.110
Швидкість модему	9600 біт/сек
Час синхронізації	1…2 сек
Запити оператора	Послуга передачі даних
	Фіксована швидкість 9,6 кбіт/с
	Асинхронний режим передачі даних
	"Прозора" трансляція

Таблиця 5.5 — Криптографічні характеристики

Параметри	Коментар
Алгоритм	Не розголошується, 256 біт
Метод розподілу ключів	Симетричний
	Сеансові ключі формуються автоматично для кожного сеансу зв’язку
Генератор ключів	Ключі формуються за допомогою апаратного генератора шуму
Ключова стійкість	10^{77}
Розподіл додаткових ключів	Формування й запис довгострокових групових ключів на зовнішньому носії
Контроль доступу	Наявність індивідуального довгострокового ключа
Функція очищення	По закінченні сеансу зв'язку сеансові ключі автоматично знищуються
	Відновлення сеансового ключа зв'язку неможливо навіть при доступі супротивника до телефону

Структурна схема будови мережі наведена на рис. 5.4.

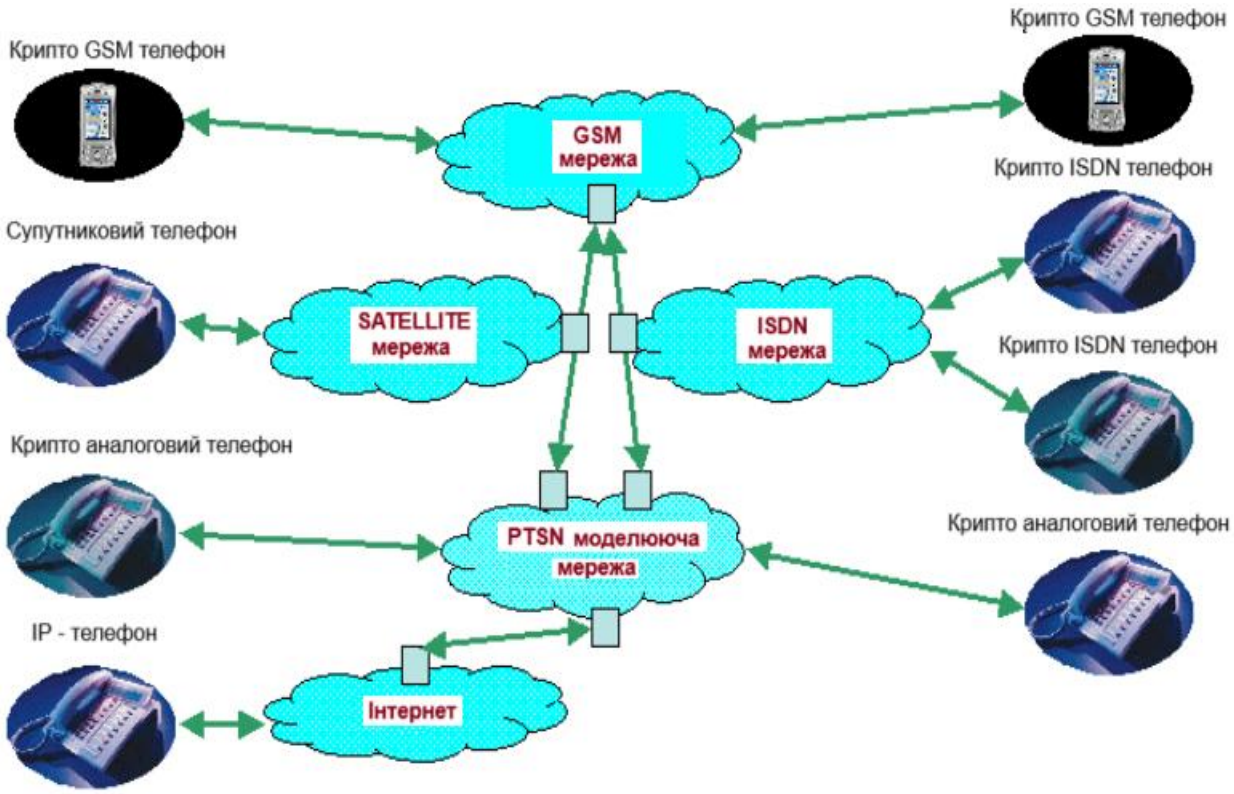

Рисунок 5.4 — Структурна схема комунікаційної стільникової мережі

ВИСНОВКИ

Модель безпеки GSM може бути зламана на багатьох рівнях, це робить її уразливої для безлічі атак, націлених на різні ділянки мережі.

Крім того, доведено, що секретно розроблені алгоритми безпеки, впроваджені в систему GSM, мають дефекти. Алгоритм A5, використовуваний для шифрування каналу передачі в ефірі уразливий щодо відомого відкритого тексту й атаки "розділяй і пануй", а навмисно скорочений простір ключа досить мало для виконання лобової атаки. Доведено, що алгоритм COMP128, використовуваний у більшості мереж GSM, як алгоритм A3/A8, має дефект, так що секретний ключ Ki може бути реконструйований в ефірі за допомогою атаки вибраний виклик приблизно за 10 годин.

Все це означає, що якщо хто-небудь має намір перехопити дзвінок GSM, він зможе це зробити. Не можна допускати, що модель безпеки GSM надає захист від будь-якого зловмисника. Ресурси, які необхідні для цього, залежать від вибраної атаки. Таким чином, при передачі конфіденційної інформації з мережі GSM не можна покладатися тільки на модель безпеки GSM.

Крім можливості перехоплення дзвінка, алгоритм COMP128, що має дефект, дозволяє клонувати SIM карту, надаючи зловмисникові можливість виконувати дзвінки за чужий рахунок. Дана тема виходить за рамки цієї роботи.

Сучасний стандарт GSM і його реалізація дозволяють і клонування абонента, і прослуховування дзвінка. Хоча реалізувати клонування й прослуховування дзвінка складніше з погляду використання цифрових технологій, у порівнянні з аналоговими, погроза дуже реальна, особливо в тих випадках, коли трансльовані дані являють цінність. В основному, ми й зараз виявляємося в тім же положенні, що стосується безпеки, як і з аналоговими стільниковими телефонами, хоча Консорціум GSM заперечує це.

Забезпечити конфіденційність переговорів в мережі GSM можна за допомогою додаткового або “абонентського” шифрування. Звісно використання лише технічних засобів не може дати 100% гарантії конфіденційності розмови, тому не слід уникати адміністративних мір поводження з конфіденційною інформацією. Так слід звести до мінімуму кількість конфіденційної інформації, що передається за допомогою стільникового зв’язку GSM, не використовувати мобільних терміналів з відеокамерами, засобами бездротової передачі інформації (Wi-Fi, Bluetooth, IrDA), смартфонів, тому що вони мають на порядок більше можливостей, а відповідно і способів перехоплення інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Хорошко В.А., Чекатков А.А. Методи та засоби захисту інформації / Под. ред. Ю.С.Ковтанюка – К.: «ЮНІОР», 2003. – 504 с.
2. Хореев А.А. Захист інформації від витоку технічними каналами. – К.: ДДК, 2008. – 316 с.
3. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. – К.: "ДіаСофт", 1999. - 480 с.
4. http://security.ukrnet.net/
5. Защита информации. Сборник научных трудов НАУ, 2003.
6. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».
7. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».
8. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі».
9. НД ТЗІ «Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації».
10. http://www.ixbt.com
11. Закон України «Про інформацію».
12. Закон України «Про державну таємницю»
13. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
14. Anderson Ross, A5 - The GSM Encryption Algorithm, 17.6.1994, [referred 30.9.1999] < http://chem.leeds.ac.uk/ICAMS/people/jon/a5.html >
15. Anon., Crack A5, [referred 29.9.1999] < http://jya.com/crack-a5.htm >
16. Anon., GSM Alliance Clarifies False & Misleading Reports of Digital Phone Cloning, [referred 29.9.1999] < http://jya.com/gsm042098.txt >