Лекція 4. Аутентифікація, ідентифікація, передача обслуговування, роумінг та інші функції мобільного звязку

1. Аутентифікація і ідентифікація

Розглянемо процедури **аутентифікації і ідентифікації**, які виконуються при кожному встановленні зв'язку.

Аутентифікація – це процедура підтвердження автентичності абонента РС. Слово ***аутентифікація*** **(англ. *authentication)*** походить від грецького ***authentikos*** – справжній, який витікає з першоджерела (для порівняння: ***автентичні тексти – це*** тексти договору на декількох мовах, що мають однакову силу).

Ідентифікація – це процедура ототожнення РС (абонентного радіотелефонного апарату), яка використовується для виявлення загублених, вкрадених або несправних апаратів. Слово ***ідентифікація*** **(англ. *identification)*** походить від ***лат.*** identificare – ототожнювати.

Ідея процедури аутентифікації в цифровій системі стільникового зв'язку полягає в шифруванні деяких паролів-ідентифікаторів з використанням квазівипадкових чисел, що періодично передаються на РС з центру комутації, і індивідуального для кожної РС алгоритму шифрування.

В стандарті GSM процедура аутентифікації пов'язана з використанням модуля ідентифікації абонента (Subscriber Identity Module – SIM), який називають також SIM-картою (SIM-card) або смарт-картою (smart-card). Модуль SIM – це змінний модуль, вигляд якого нагадує пластикову кредитну картку, що вставляється у відповідне гніздо абонентного апарату. Він містить персональний ідентифікаційний номер абонента (Personal Identification Number – PIN), міжнародний ідентифікатор абонента PC (International Mobile Subscriber Identity – IMSI), індивідуальний ключ аутентифікації абонента Ki, індивідуальний алгоритм аутентифікації абонента A3, алгоритм обчислення ключа шифрування A8.

Для аутентифікації використовується зашифрований відгук (signed response) S, який є результатом застосування алгоритму A3 до ключа Ki і квазівипадкового числа R, який PC отримує від центру аутентифікації через ЦК. Алгоритм A8 використовується для обчислення ключа шифрування трафіку. Унікальний ідентифікатор IMSI для поточної роботи замінюється тимчасовим ідентифікатором TMSI (Temporary Mobile Subscriber Identity – тимчасовий ідентифікатор абонента рухомого зв'язку), який присвоюється апарату при його першій реєстрації в конкретному регіоні, що визначається ідентифікатором LAI (Location Area Identity – ідентифікатор області місцеположення), і скидається при виході апарату за межі цього регіону.

Ідентифікатор PIN – код, відомий тільки абоненту, який повинен служити захистом від несанкціонованого використання SIM-карти, наприклад, у разі її втрати. Після трьох невдалих спроб набору PIN-коду SIM-карта блокується, і блокування може бути знято або набором додаткового коду – персонального коду розблокування (Personal unblocking key – PUK), або за командою з ЦК.

Процедура аутентифікації стандарту GSM схематично показана на рис**. 1,** де пунктиром позначені елементи, що не відносяться безпосередньо до процедури аутентифікації, проте використовуються для обчислення ключа шифрування Кс. Обчислення проводиться кожного разу при проведенні аутентифікації.

Процедура ідентифікації полягає в порівнянні ідентифікатора абонентного апарату з номерами, що містяться у відповідних "чорних списках" регістра апаратури, з метою вилучення вкрадених і зіпсованих апаратів.

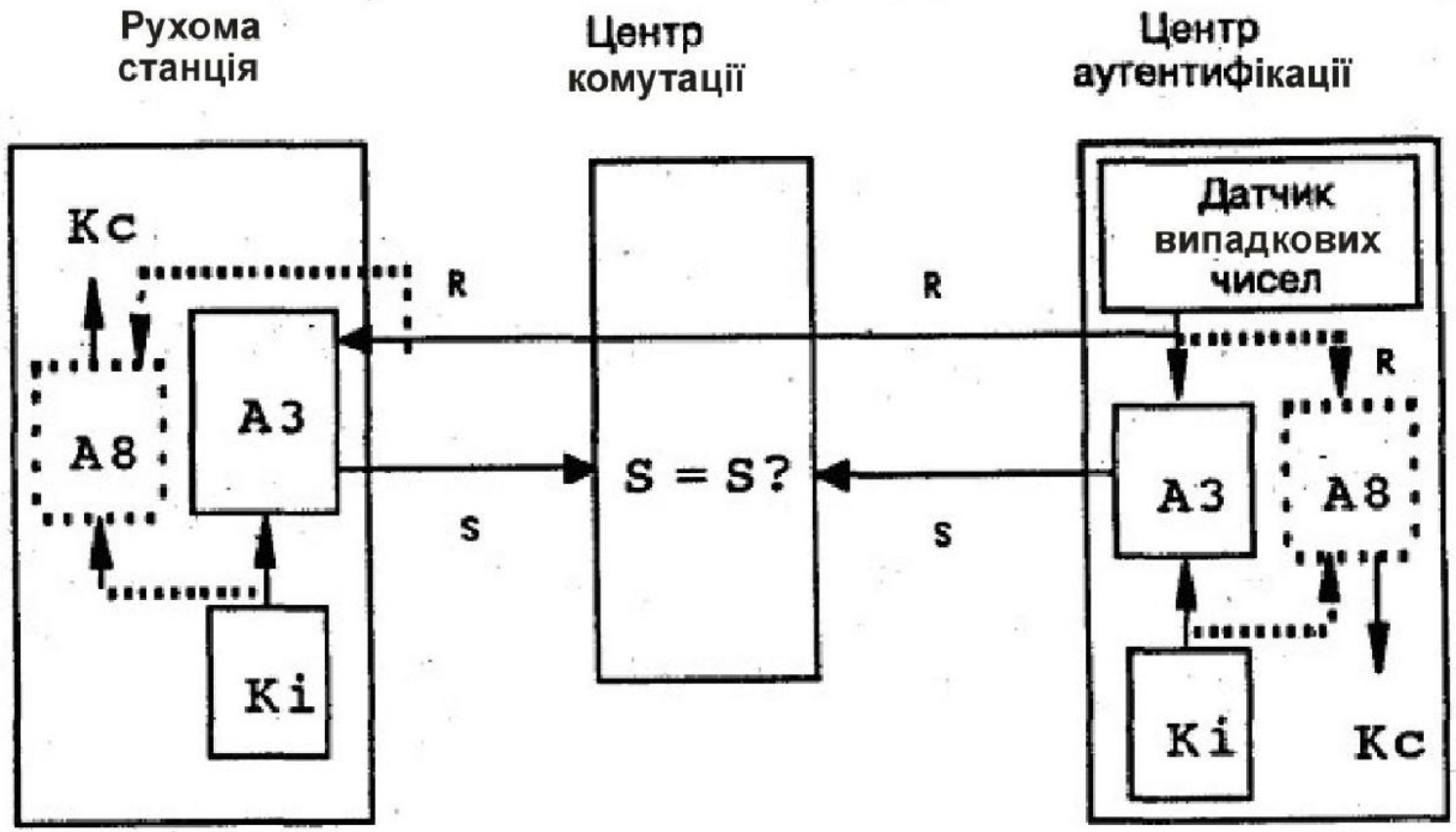
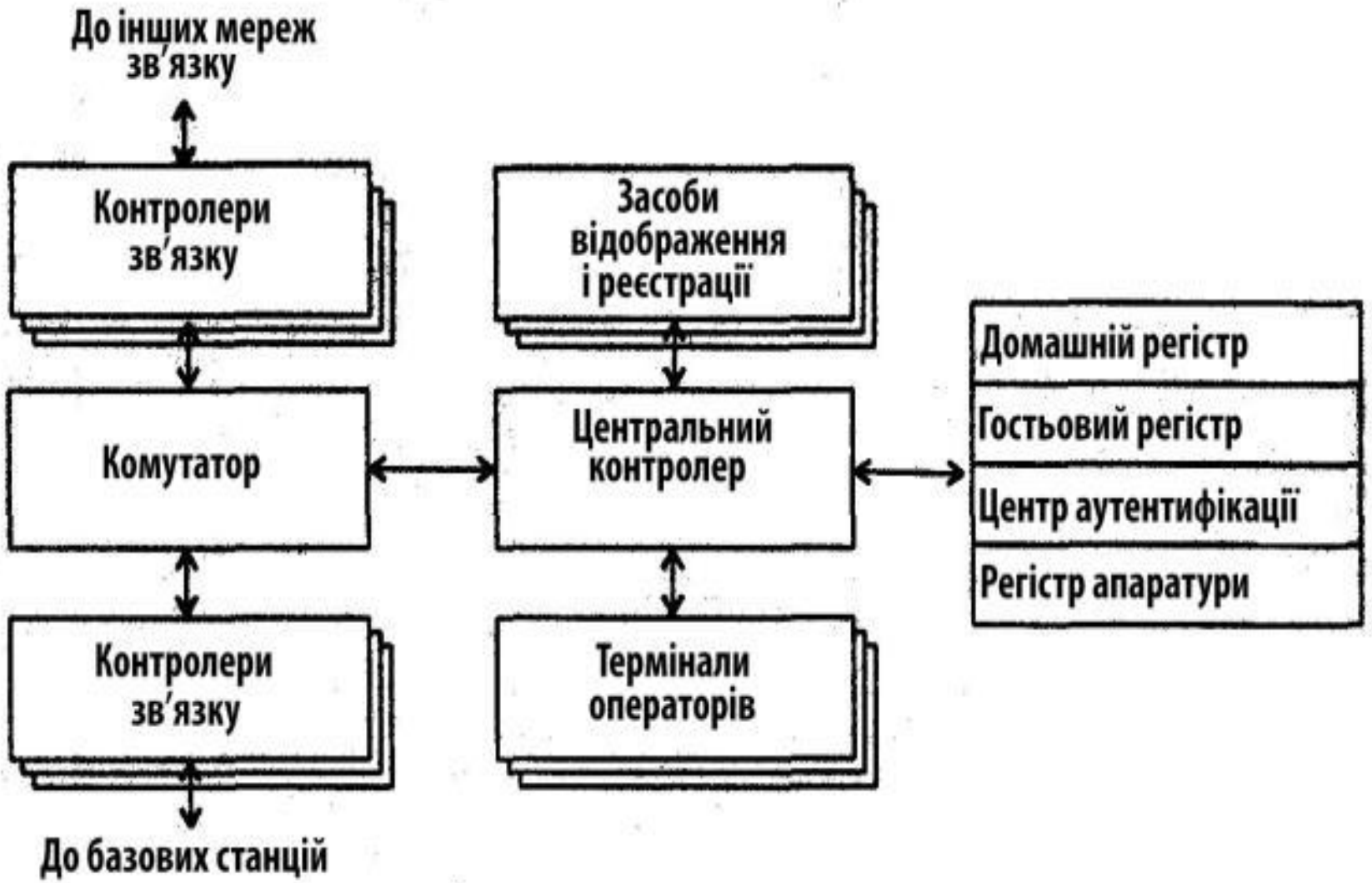


Рис.1. Схема процедури аутентифікації (стандарт GSM):
R – випадкове число; A3 – алгоритм аутентифікації; A8 – алгоритм обчислення ключа шифрування; Ki – ключ аутентифікації; Кс – ключ шифрування; S – зашифрований відгук (Signed Response – SRES)

Рис.8. Блок-схема центра комутації



Шифрование

Как только подлинность абонента была проверена, таким образом защищая и абонента и сетевого оператора от влияния мошеннического доступа, пользователь должен быть защищен от подслушивания.

Это достигается путем шифрования данных, передаваемых по радио-интерфейсу, с использованием второго ключа Kc и изначально секретного алгоритма A5. Kc генерируется в ходе проверки подлинности, используя Ki, RAND и секретный алгоритм A8, который также хранится в SIM-карте. Подобно алгоритму A3, A8 не уникален, и он может также быть выбран оператором. Ключи Kc для каждого пользователя вычисляются в AuC домашней сети и передаются в VLR в составе набора триплетов, где каждому триплету и, соответственно — ключу Kc, присваивается номер ключа — CKSN (Cipher Key Sequence Number). В некоторых реализациях алгоритмы A3 и A8 объединены в единственный алгоритм A38, который использует RAND и Ki, чтобы сгенерировать Kc и SRES.

В отличие от A3 и A8, которые, возможно, различны для каждого индивидуального оператора, A5 выбирается из списка из 7 возможных вариантов.

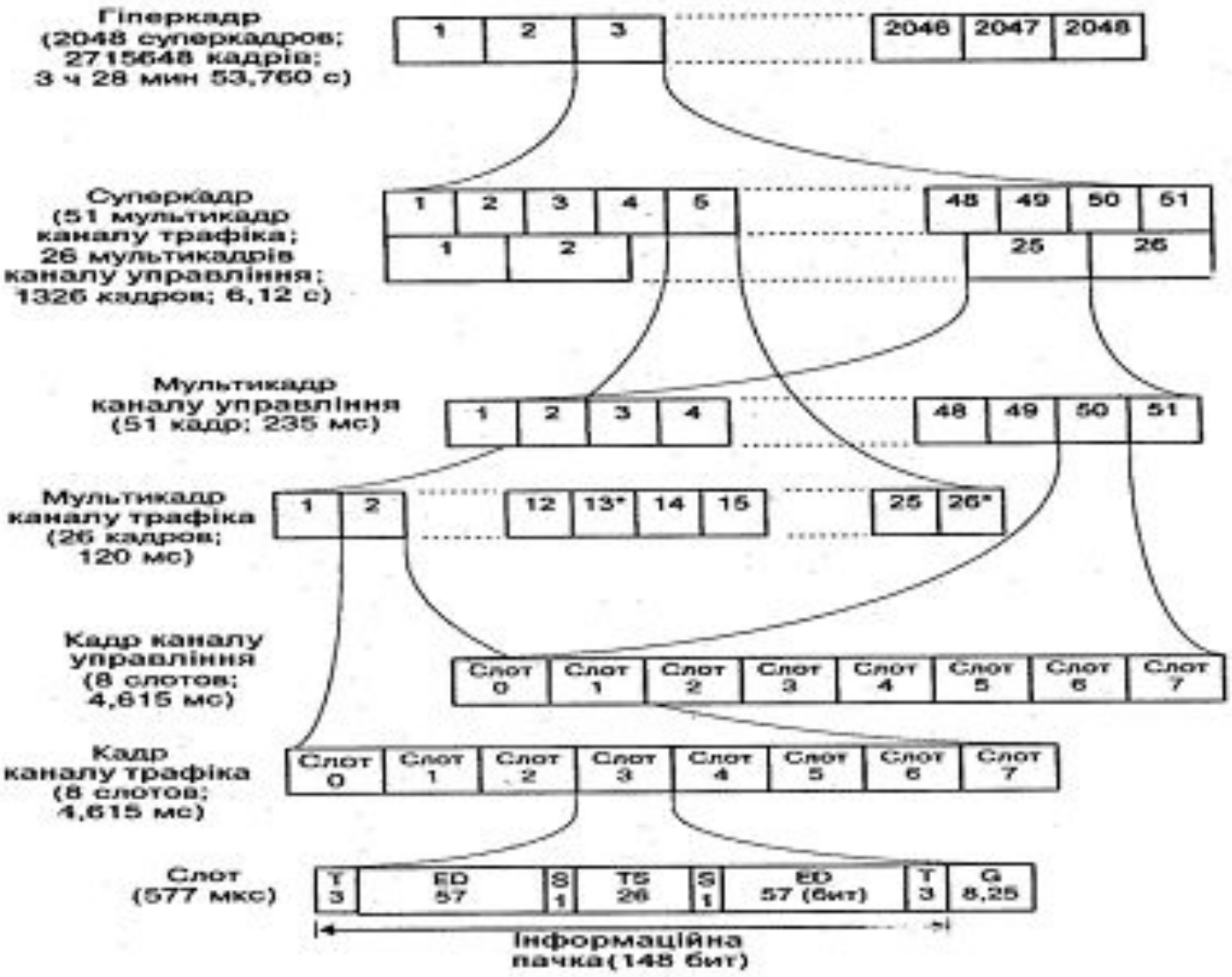
Перед шифрованием происходит фаза переговоров в ходе которой определяется, какая версия A5 будет использована. Если сеть и мобильная станция не имеют общих версий A5, связь должна продолжиться в открытом режиме или соединение должно быть разорвано.

Алгоритм A5 использует 64-битный ключ Kc и 22-битный номер фрейма TDMA для вычисления двух 114-битных слов шифрования — BLOCK1 и BLOCK2, использующихся при передаче и приёме соответственно.

Поскольку зашифрованные данные вычислены, используя номер фрейма TDMA, то слова изменяются от посылки к посылке и не повторяются на протяжении гиперфрейма (приблизительно 3,5 часа).

Перед тем, как начать шифрование, мобильная станция (MS) отправляет в VLR номер ключа шифрования CKSN, который хранится в её памяти с момента последней процедуры аутентификации. CKSN не содержит секретных данных, а служит лишь для того, чтобы MS могла сообщить сети, какой ключ Kc она «помнит». После этого VLR отправляет в MS команду на включение шифрования и передаёт в базовую станцию (BTS) ключ Kc из того триплета, который соответствует номеру CKSN, полученному от MS. Таким образом между MS и VLR достигается договорённость о выборе ключа шифрования без передачи самого ключа по радиоинтерфейсу.

Рис.2.3. Структура ефірного інтерфейсу (канал трафіку) системи GSM



2. Передача обслуговування

Передача обслуговування (амер. термін handoff, англ. – handover) при переміщенні РС здійснюється від БС першої комірки до БС другої комірки (рис. 2). Передача обслуговування має місце тільки тоді, коли РС перетинає межу комірок під час сеансу зв'язку, і зв'язок (телефонна розмова) при цьому не переривається. Якщо ж РС переміщується з однієї комірки до іншої, знаходячись в режимі очікування, вона просто відстежує ці переміщення за інформацією системи, яка передається по каналах управління, і в потрібний момент перебудовується на більш сильний сигнал іншої БС.

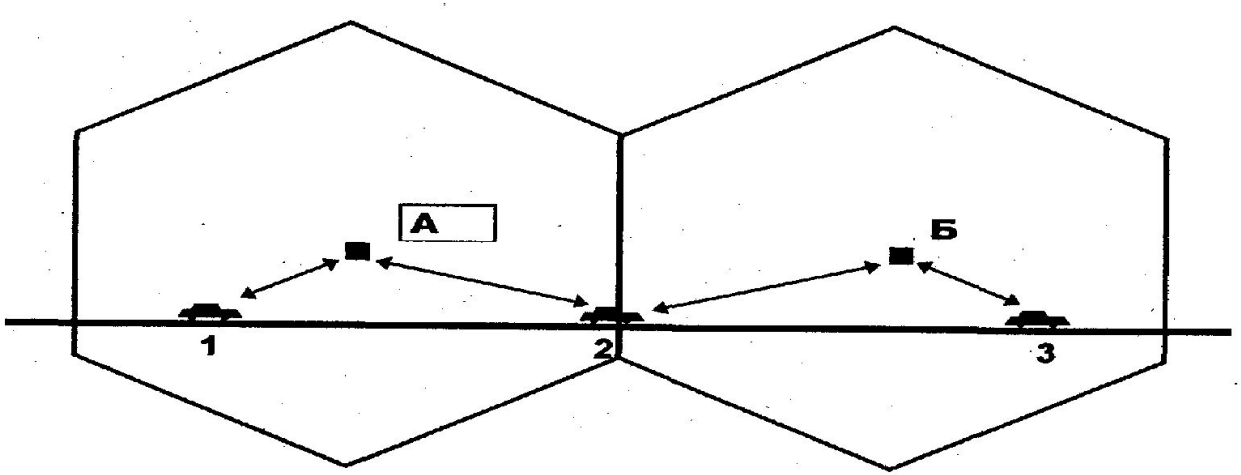


Рис.2. Передача обслуговування з комірки А в комірку Б при перетині РС межі комірок

Необхідність в передачі обслуговування виникає тоді, коли якість каналу зв'язку, яка оцінюється за рівнем сигналу, падає нижче за допустиму межу.

В стандарті GSM вказані параметри постійно вимірюються РС як для своєї комірки, так і для суміжних (до 16 комірок), і результати вимірювань передаються на БС.

В стандарті D-AMPS ці характеристики РС вимірює лише для робочої комірки, проте у разі погіршення якості зв'язку РС про це повідомляє ЦК через БС, і по команді ЦК аналогічні вимірювання здійснюють рухомі станції сусідніх комірок і за їх результатами ЦК вибирає комірку з більш високою якістю каналу зв'язку, в яку має бути передано обслуговування. ЦК, прийнявши рішення про передачу обслуговування і вибравши нову комірку, повідомляє про це БС нової комірки, а РС старої комірки через БС видає необхідні команди, в яких вказуються:

новий частотний канал,

номера робочого слота та інше.

РС за частки секунди, які залишаються непомітними для абонента, перебудовується на новий канал і налаштовується на спільну роботу з новою БС.

3. Роумінг

Роумінг (від англ. ***roam*** – бродити, мандрувати; абонент, що використовує послуги роумінга, – ***ромер*** **(англ. *roamer*)) – це функція, або процедура надання послуг стільникового зв'язку абоненту одного оператора в системі іншого оператора.**

Роумінг з'являвся у міру розвитку стільникових систем і використовував різні технічні і організаційні рішення в різних стандартах, країнах і регіонах.

Для реалізації роумінгу необхідно мати в обох системах однаковий стандарт стільникового зв'язку. З розвитком мобільного зв'язку поняття роумінгу помітно розширяється: з'явилась можливість роумінгу між системами стільникового і мобільного супутникового зв'язку.

Схема організації роумінгу наступна. Абонент стільникового зв'язку, що потрапив на територію "чужої системи", яка допускає реалізацію роумінгу, ініціює виклик звичайним способом (ніби він перебуває на території "своєї системи"). ЦК, переконавшись, що в його домашньому регістрі цей абонент не значиться, сприймає його як ромера і заносить його в **гостьовий регістр. Це занесення здійснюється на основі** запрошених в домашньому регістрі "рідної системи" ромера і отриманих від цієї системи відомостей, необхідних для організації обслуговування ромера (види послуг, паролі, шифри тощо). При цьому ЦК нової системи повідомляє "рідну систему" ромера про те, в якій саме системі ромер перебуває в даний час; остання інформація фіксується в домашньому регістрі "рідної системи" ромера.

Після цього ромер користується стільниковим зв'язком, як вдома: виклики від нього обслуговуються звичайним способом (з тією лише різницею, що це фіксується не в домашньому, а в гостьовому регістрі); якщо викликається ромер, то виклики переадресовуються "домашньою системою" на ту систему, де в даний час перебуває ромер. Після повернення ромера додому в домашньому регістрі "рідної системи"
стирається адреса тієї системи, де перебував ромер, а в гостьовому регістрі тієї системи, у свою чергу, стираються відомості про ромера. Послуги роумінгу оплачуються абонентом через "домашню систему", яка, в свою чергу, відшкодовує згідно з умовами роумінгової угоди витрати за послуги роумінга компанії-оператору.

В стандарті GSM процедура роумінгу закладена як обов'язковий елемент.

4. Функції стільникового зв'язку

Функції (послуги) стільникового зв'язку досить різноманітні, а саме: звичайний двосторонній радіотелефонний зв'язок (передача мови) з рухомими та нерухомими абонентами; передача факсимільних повідомлень і комп'ютерних даних; переадресація виклику і автодозвон; автоматична реєстрація тривалості телефонних розмов; голосова пошта тощо.

В стандарті GSM існують такі функції стільникового зв'язку: функції передачі і телефункції.

Функції передачі включають чотири категорії:

1. Асинхронний обмін даними з комутованими телефонними мережами загального користування з швидкостями 300...9600 бит/с.
2. Синхронний обмін даними з комутованими телефонними мережами загального користування, комутованими мережами передачі даних загального користування і цифровими мережами з інтеграцією функцій з швидкостями 300...9600 бит/с
3. Асинхронний пакетний обмін даними з мережею передачі даних загального користування з пакетною комутацією (доступ через ассемблер/дизассемблер) з швидкостями 300...9600 бит/с.
4. Синхронний пакетний обмін даними з мережею передачі даних загального користування з пакетною комутацією з швидкостями 2400...9600 бит/с.

Функції передачі можуть бути прозорими, коли захист від помилок забезпечується лише за рахунок поточної корекції помилок, та непрозорими, коли передбачається додатковий захист у вигляді автоматичного перезапитання.

Телефункції включають в себе такі категорії:

1. Передача інформації мови і тональної сигналізації в смузі мови.
2. Передача коротких повідомлень (буквено-цифрових – до 180 символів – у бік рухомого абонента).
3. Доступ до системи обробки повідомлень (наприклад, передача повідомлення від системи персонального радіовиклику на РС стільниковому зв'язку).
4. Передача факсимільних повідомлень.

Додаткові функції включають такі категорії:

1. Ідентифікація і відображення номера, що викликається чи підключається, обмеження ідентифікації і відображення номера, що викликається чи підключається (стороні, яка викликає, надається право обмежити можливість ідентифікації її номера).
2. Переадресування виклику на інший номер (коли абонент зайнятий або не відповідає) і передача виклику (перемикання встановленої лінії зв'язку на іншого абонента).

3. Очікування виклику (при зайнятому терміналі абонент отримує звістку про виклик, що поступив, і може відповісти на нього, відмовитися від прийому виклику або проігнорувати його надходження) і збереження виклику (абонент може перервати сеанс зв'язку, що проводиться, відповівши на інший виклик або зробивши інший виклик, а потім повернутися до продовження перерваної розмови).
4. Конференц-зв'язок – одночасна розмова трьох або більшої кількості абонентів.
5. Закрита група користувачів – ця функція дозволяє групі користувачів спілкуватися лише між собою; у разі необхідності один або декілька членів групи можуть мати доступ по входу/виходу до абонентів, що не входять до групи.
6. Оперативна інформація про вартість послуг, що надаються або наданих.
7. Заборона певних функцій (наприклад, заборона на вхідні виклики, на міжнародні виклики тощо).
8. Надання відкритої лінії зв'язку мережа /користувач для реалізації функцій, які визначає оператор.