Лабораторна робота № 6

Структура логічних каналів управління і алгоритми функціонування систем GSM

1. Мета роботи

Вивчити структуру логічних каналів управління і алгоритми функціонування систем GSM по встановленню вихідного і вхідного з'єднань.

2. Завдання

1. Вивчити структуру логічних каналів управління.
2. Вивчити алгоритм встановлення вихідного з'єднання (MS→BTS, МС→БС).
3. Вивчити алгоритм встановлення вхідного з'єднання (BTS→MS, БС→МС).
4. Вивчити механізми безпеки.
5. Скласти звіт.

3. Теоретичні відомості

Фізичний канал в стандарті GSM є комбінацією тимчасового і частотного розділення сигналів і визначається як послідовність радіочастотних каналів і тимчасових вікон TDMA кадрів. Фізичний канал управління (ФКУ) призначений для забезпечення встановлення з'єднання і утворення логічних каналів управління (ЛКУ). ФКУ передають службові повідомлення і дані, представлені в цифровій формі. Залежно від функціонального призначення службової інформації і даних, службові повідомлення в певному порядку об'єднуються в ЛКУ. Призначенням ЛКУ є забезпечення передачі МС і БС сигналів управління службових повідомлень і сигналів синхронізації. Залежно від виконуючих функцій розрізняють чотири види ЛКУ (рис. 4.1):

КПСУ – канали передачі сигналів управління (BCCH);

ЗКУ – загальні канали управління (CCCH);

ІКУ – індивідуальні канали управління (SDCCH);

СКУ – суміщені канали управління (ACCH).

КПСУ використовуються тільки у напрямку БС → *М*С і містять інформацію про підстроювання частоти, кадрову синхронізацію та забезпечують передачу основних команд по управлінню передачею. До зазначених каналів належать:

КПЧ – канал підстроювання частоти (FCCH);

КУС – канал управління синхронізацією (SCH);

КУП – канал управління передачею (BCCH).

ЗКУ призначені для виклику МС, для запиту МС про призначення ІКУ, для виділення спеціального каналу управління (КУ), що забезпечує прямий доступ до каналу зв'язку (КЗ). До зазначених каналів належать:

КВ – канал виклику БС → *М*С (DCH);

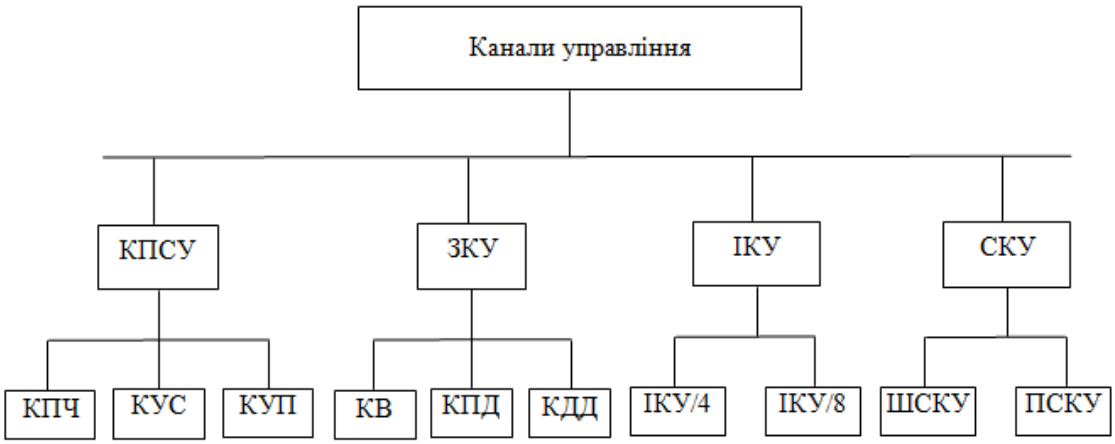


Рис. 4.1. **Види логічних каналів управління в стандарті GSM**

КПД – канал паралельного доступу МС → *Б*С (RACH);

КДД – канал дозволеного доступу (AGCH).

ІКУ використовуються для дуплексного зв'язку між БС → *М*С і призначені для встановлення необхідного виду обслуговування. По них проходить запит МС про необхідний вид обслуговування, контроль правильної відповіді і виділення вільного каналу зв'язку. Мають місце два види таких каналів:

ІКУ/4 – ІКУ, який складається з 4-х підканалів (SDCCH/4);

ІКУ/8 – ІКУ, який складається з 8-ми підканалів (SDCCH/8).

СКУ використовуються для дуплексного зв'язку між БС → *М*С. У напрямку «вниз» вони передають команди управління з БС на МС, а за напрямом «вгору» – інформацію про статус МС. СКУ служать для передачі команд під час переходу МС з одного стільника в інший та для встановлення вихідного рівня потужності передавача МС (TXPWR). СКУ поділяються на:

ШСКУ – швидкий суміщений КУ (FACCH);

ПСКУ – повільний суміщений КУ (SACCH);

За напрямом «вгору» МС відправляє дані, що стосуються рівня встановленої вихідної потужності (TXPWR), виміряної приймачем рівня радіосигналу (RXLEV) і якості його прийому (RXQUAL). У СКУ завжди міститься один із двох каналів: канал зв'язку (TCH) чи індивідуальний канал управління (SDCCH). СКУ завжди об'єднуються з каналами зв'язку або з ІКУ. При цьому розрізняють шість видів об'єднаних каналів управління:

ШСКУ – КУ, об'єднаний з КЗ, які мають швидкості 9.6; 4.8; 2.4 кбіт/с;

ШСКУ – КУ, об'єднаний з КЗ, які мають швидкості 4.8; 2.4 кбіт/с;

ПСКУ – КУ, об'єднаний з КЗ, які мають швидкості 9.6; 4.8; 2.4 кбіт/с;

ПСКУ – КУ, об'єднаний з КЗ, які мають швидкості 4.8; 2.4 кбіт/с;

ПСКУ/с4 – КУ, об'єднаний з ІКУ/4;

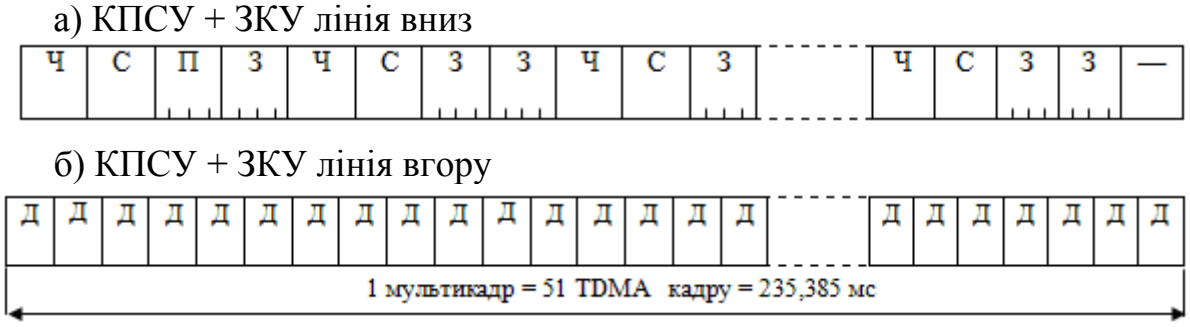
ПСКУ/с8 – КУ, об'єднаний з ІКУ/8.

Для передачі вище перелічених КУ використовується 51-кадровий мультикадр, винятками є канали ШСКУ і ПСКУ, для їх передачі використовується 26-кадровий мультикадр.

Об'єднаний КУ КПСУ/ЗКУ призначений для всіх МС, які в один і той самий час знаходяться в одному стільнику. У каналі КУП *«мережа → МС»*

передається загальна інформація про стільник, в якій МС знаходяться в даний момент, і про сусідні стільники. У каналі КЗ (*«мережа → МС»*) передається інформація про циклову синхронізацію і пізнання прийомопередавача БС. Інформація для синхронізації несучої передається в каналі КПЧ (*«мережа → МС»*). Канал КПД *«МС → мережа»* використовується МС для доступу до мережі у разі необхідності проходження реєстрації при включенні або виклику.

КДД (*«мережа → МС»*) використовується для заняття спеціальних видів обслуговування (SDCCH або TCH) мобільною станцією, яка раніше не запрошувала через канал RACH. КВ (*«мережа → МС»*) використовується для виклику МС мережею або абонентом мережі. На рис. 4.2 подано відображення каналів, які розглядаються, на одному ФКУ в структурі 51-кадрового мультикадру.



Ч – TDMA кадр для підстроювання частоти, канал КПЧ;
С – TDMA кадр для синхронізації, канал КУС;
П – TDMA кадр для каналу КУП;
З – TDMA кадр для каналу ЗКУ;
Д – TDMA кадр для каналу КПД.

Рис. 4.2. **Відображення каналів, які розглядаються, на одному ФКУ в структурі 51-кадрового мультикадру**

На лінії «вгору» в мультикадрі здійснюється передача сигналів каналу виклику, який є єдиним КУ від МС до БС, причому для доступу до мережі МС може використовувати нульовий часовий інтервал в будь-якому з кадрів. На лінії «вниз» 51-кадровий мультикадр групується в 5 груп по 10 кадрів, причому один з кадрів залишається незайнятим. Кожна з груп починається з сигналів каналу КПЧ, за якими йдуть сигнали КУС. Інші 8 кадрів в кожній групі утворюють два блоки з чотирьох кадрів. Перший блок першої групи призначений для сигналів каналу ВССН, тоді як інші 9 блоків використовуються для передачі каналу виклику і каналу дозволеного доступу загального КУ СССН. МС може займати один з дев’яти блоків виклику, а сам блок може використовуватися для виклику декількох МС.

Встановлення вихідного з'єднання (МС → *БС* **)**

Можливість встановлення вихідного з'єднання забезпечується тим, що БС мережі на виділених ним частотах здійснюють передачу мультикадрів об'єднаного КУ (КПСУ+ЗКУ). Залежно від навантаження в мережі структура мультикадрів може змінюватися. При великому навантаженні в мережі передавальний мультикадр, має вигляд (рис. 4.3). Якщо навантаження в стільнику мале, КПСУ+ЗКУ об'єднується з 4ІКУ/4 (рис. 4.4).

а) 8 ІКУ/8 лінія вниз

I0	I1	I2	I3	I4	I5	I6	I7	A0	A1	A2	A3	—	—	—
I0	i1	I2	I3	I4	I5	I6	I7	A4	A5	A6	A7	—	—	—

б) 8 ІКУ/8 лінія вгору

A5	A6	A7	—	—	—	I0	I1	I2	I3	I4	I5	I6	I7	A0
A1	A2	A3	—	—	—	I0	I1	I2	I3	I4	I5	I6	I7	A0

1 мультикадр = 51 TDMA кадру = 235,385 мс

І – TDMA кадр для каналу ІКУ;
А – TDMA кадр для каналу ПСКУ.

Рис. 4.3. **Передавальний мультикадр при великому навантаженні в мережі**

а) КПСУ + ЗКУ + 4ІКУ/4 лінія вниз

4	С	Пр	З	4	С	З	З	4	С	І0	І1	4	С	І2	І3	4	С	П0	П1	—
4	С	Пр	З	4	С	З	ОЗ	4	С	І0	І1	4	С	І2	І3	4	С	П2	П3	—

б) КПСУ + ЗКУ + 4ІКУ/4 лінія вгору

І3	Д	Д	П2	П3	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	І0	І1	Д	Д	І2
І3	Д	Д	П0	П1	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	І0	І1	Д	Д	І2

1 мультикадр = 51 TDMA кадру = 235,385 мс

П – TDMA кадр для каналу ПСКУ;
Пр – TDMA кадр для каналу КУП;
З – TDMA кадр для каналу ЗКУ;
І – TDMA кадр для каналу ІКУ;
Д – TDMA кадр для каналу КПД.

Рис. 4.4. **Передавальний мультикадр при малому навантаженні у стільнику (КПСУ + ЗКУ об'єднується з 4ІКУ/4)**

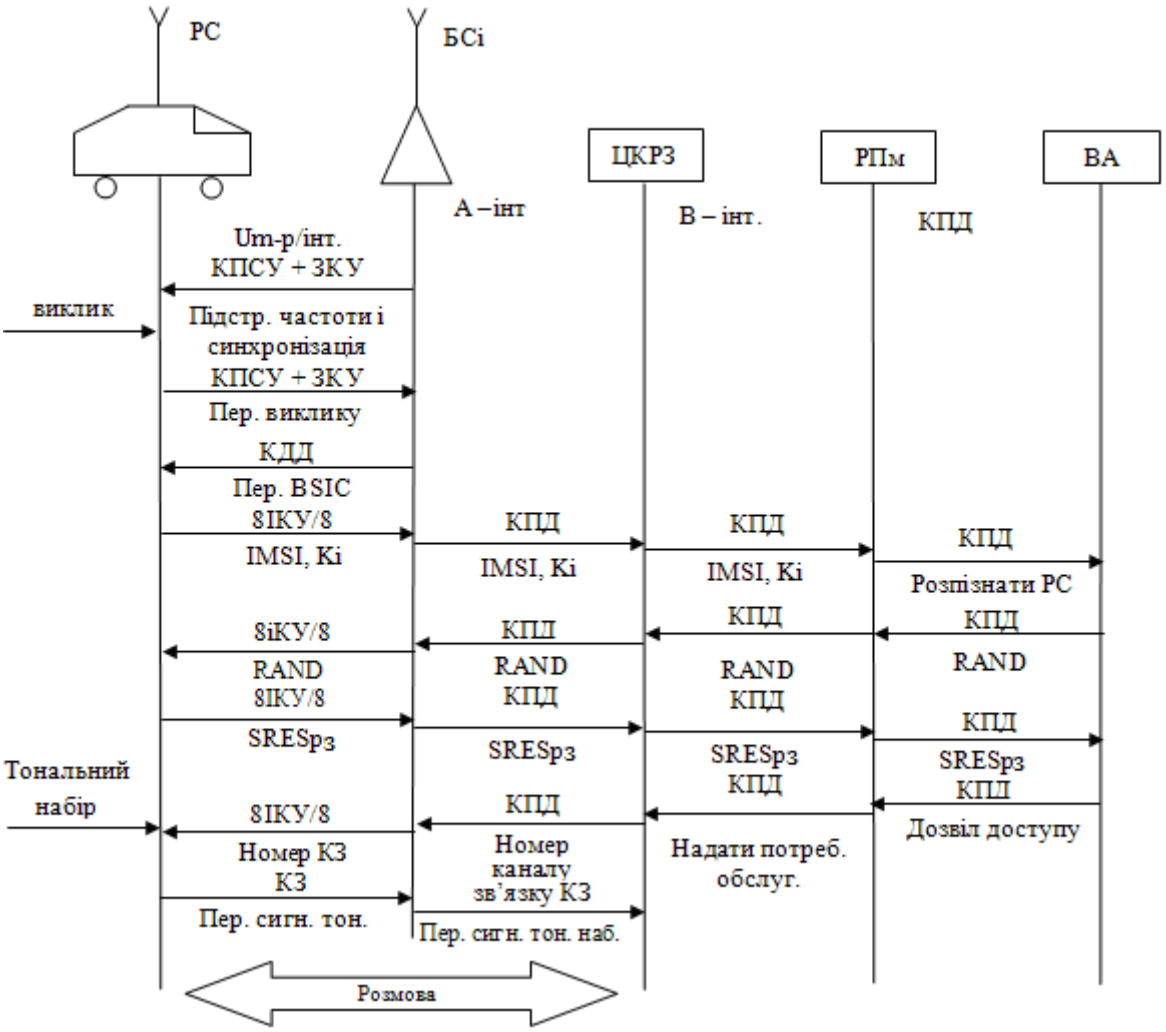


Рис. 4.5. **Алгоритм встановлення вихідного з'єднання (** МС → *БС* **)**

До надходження від користувача МС сигналу виклику приймач МС здійснює сканування по всіх 124 робочих частотах. На кожній робочій частоті МС проводить виміри прийнятого від БС сигналу, і обчислює оцінку якості прийнятого сигналу. Вибір обслуговуючої БС проводиться за низкою ознак: рівень приймаючого від БС сигналу має бути не меншим заданого (Zmp=9 дБ); обчислена оцінка якості має бути максимальна; відстань від МС до БС має бути мінімальна.

При натисненні кнопки виклику (рис. 4.5) на МС здійснюється передача сигналів об'єднаного КУ (КПСУ+ЗКУ). При цьому на всіх тимчасових позиціях мультикадру КУ містяться сигнали КПД, що забезпечують можливість визначення БС потрібного користувачем виду обслуговування. Після визначення виду обслуговування БС по КПД передає МС свій код впізнання (BSIC). Отримавши код впізнання, МС по раніше призначеному ІКУ здійснює передачу свого міжнародного ідентифікаційного номера (IMSI) і ключа аутентифікації (Ki) для визначення повноважень користувача на надання вказаного виду обслуговування. Оскільки устаткування БС не дозволяє визначити повноваження користувача, то по каналу передачі даних (КПД) вона передає в ЦКРЗ вище вказані дані про МС, які надходять через регістри переміщення (РПм) і положення (РПл) у вузол аутентифікації (ВА). Реалізація про-

цедури аутентифікації абонента описана в лабораторній роботі №3. Отже, з'єднання між МС і БС встановлено.

Встановлення вхідного з'єднання (БС → *МС* **)**

При надходженні в ЦКРЗ заявки на встановлення з'єднання з однією з МС від ЦКРЗ по каналу передачі даних на мережу БС надходить сигнал виклику даної МС (рис. 4.6).

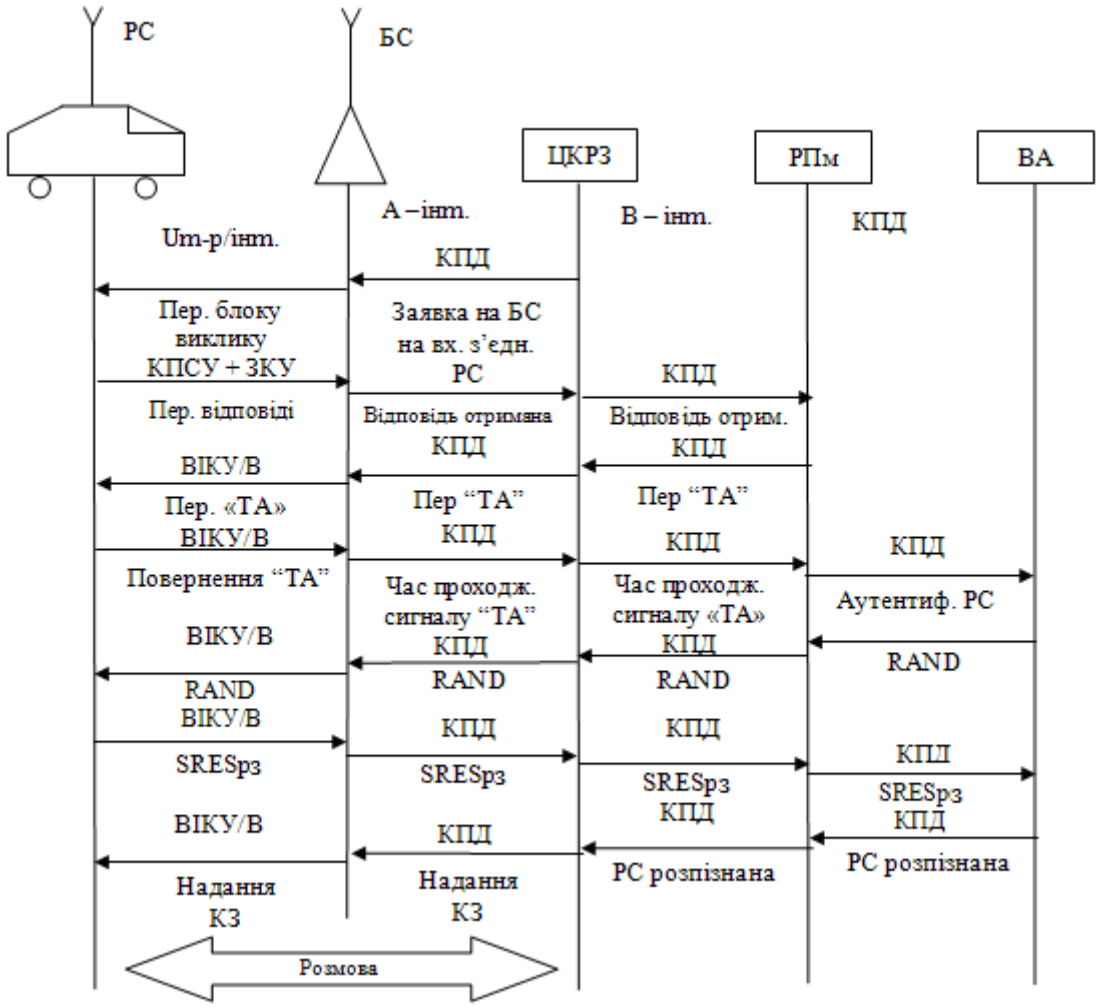


Рис. 4.6. **Алгоритм встановлення вхідного з'єднання (** БС → *МС* **)**

Далі БС здійснює передачу виклику в мультикадрі об'єднаного КУ КПСУ/ЗКУ в одному з блоків виклику AGCH/PCH на вільній в даний момент часу позиції. Отримавши виклик, МС передає в КУ КПСУ/ЗКУ сигнал підтвердження отримання виклику, що транслюється через БС на ЦКРЗ. А з РПм і РПл ЦКРЗ отримує інформацію про відстань між МС і БС та напрям переміщення рухомого абонента щодо мережі БС і передає на БС команду передати на адресу абонента, що викликається, комбінацію «тимчасового випередження» (ТА) для обчислення дистанції зв'язку на інтервалі БС → *МС* . Комбінація ТА має об'єм 6 біт і забезпечує вимірювання абсолютної дистанції зв'язку від 0 до майже 70 км з точністю ±1км. Максимальне значення ТА дорівнює 232,6 мкс. Виміряне значення ТА від БС по каналу передачі даних че-

рез MSC надходить в регістри РПл і РПм. Залежно від значень ТА, що містяться в цих регістрах, здійснюється передача МС на обслуговування іншої БС. Після проведення алгоритму аутентифікації викликаючою МС, відбувається проключення розмовного тракту між МС і ЦКРЗ. Впродовж всього сеансу зв'язку між МС або абонентом мережі ISDN БС і ЦКРЗ здійснюють стеження за якістю передачі інформації і даних. Отже, з'єднання між БС і МС з врахуванням виду обслуговування встановлено.

Естафетна передача (HandOver)

Під естафетною передачею мають на увазі супровід МС при переміщенні її з одного стільника в інший без перерв сеансу зв'язку. У періоди пікових навантажень кількість заявок на естафетну передачу різко збільшується і перевищує кількість вільних радіоканалів.

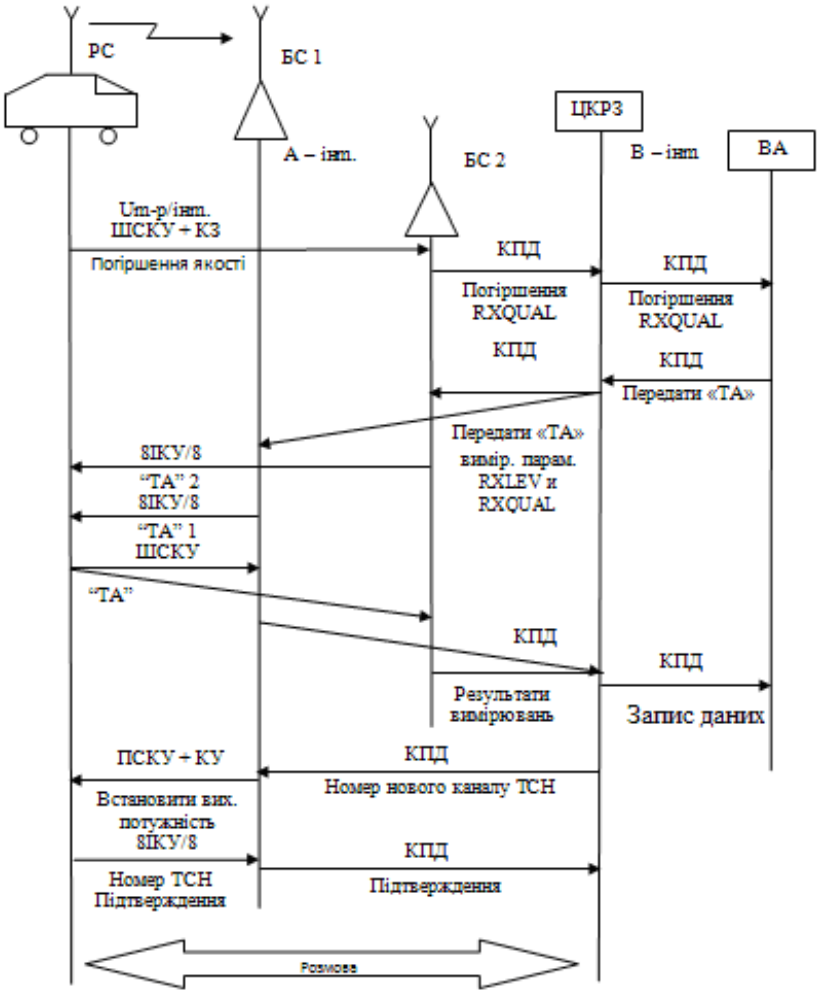


Рис. 4.7. **Алгоритм встановлення вхідного з'єднання при збільшенні відстані між МС і БС та впливу перешкод**

Ухвалення рішення про естафетну передачу здійснює ЦКРЗ, ґрунтуючись на результатах вимірів, виконаних БС і МС. Ці виміри сортує ЦКРЗ в такій послідовності: RXQUAL; RXLEV; DISTANCE; PBGT (бюджет випромінюваної потужності). БС вимірює RXLEV, RXQUAL і DISTANCE, тоді як

МС вимірює і передає на обслуговуючу БС в каналі ПСКУ значення RXLEV, RXQUAL і RXLEV для усіх сусідніх БС, які потім фіксуються в ЦКРЗ. При видаленні МС від обслуговуючої БС значення RXLEV і RXQUAL стають нижчими, тоді як RXLEV для однієї із сусідніх БС збільшується (рис. 4.7). Це може відбуватися з двох причин:

1) за рахунок збільшення відстані між МС і БС, а отже і зменшення бюджету випромінюваної потужності МС;

2) за рахунок перешкод від інших МС по основному каналу.

Перша вирішується шляхом передачі управління МС з однією БС на іншу при контролі з ЦКРЗ, коли зміна потужності, що випромінюється передавачем МС, неможлива або немає сенсу. Друга може вирішуватися як шляхом управління випромінюваної потужності, так і за рахунок надання МС іншого частотного радіоканалу по сигналу з БС, що передається в каналі ШСКУ.

У стандарті GSM вирішені питання безпеки зв'язку. Термін «безпека» розуміють як виняток несанкціонованого використання системи і забезпечення секретності переговорів рухомих абонентів. Визначені такі механізми безпеки: аутентифікація; секретність передачі даних; секретність абонента; секретність в процедурі коригування місця розташування. Захист сигналів управління і даних користувача здійснюється тільки по радіоканалу.

Секретність передачі даних

Усі конфіденційні повідомлення повинні передаватися в режимі захисту інформації. Алгоритм формування ключів шифрування (АВ) зберігається в модулі SIM. Після прийому випадкового номера RAND МС вичисляє відгук SRES і ключ шифрування (Кс), використовуючи RAND, Ki і алгоритм А8 (рис. 4.8). Ключ шифрування Кс не передається по радіоканалу. Як МС, так і мережа обчислюють Кс, який використовується іншими рухомими абонентами. Внаслідок секретності обчислення Кс відбувається в SIM. Крім випадкового числа RAND мережа посилає МС числову послідовність ключа шифрування. Число зберігається мобільною станцією і міститься в кожному першому повідомленні, що передається в мережу.

$$Kc = Ki[RAND]$$

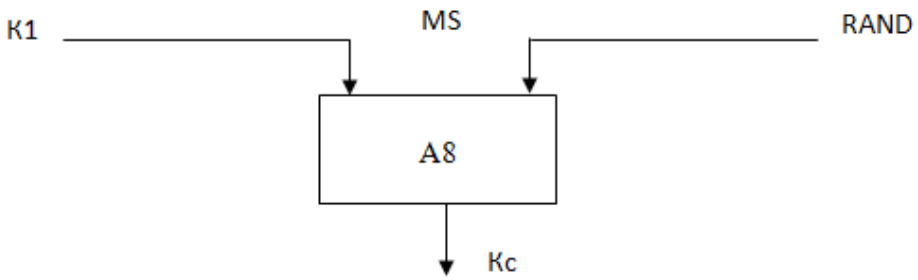


Рис. 4.8. **Визначення ключа шифрування Кс**

Деякі мережі приймають рішення про наявність числової послідовності діючого ключа шифрування у разі, якщо потрібно приступити до розпізнавання або, якщо виконується попереднє розпізнавання, використовуючи правильний

ключ шифрування. Для встановлення режиму шифрування (рис. 4.9) мережа передає МС команду СМС на перехід в режим шифрування. Після отримання команди СМС, МС, використовуючи наявний в ній ключ, приступає до шифрування і дешифрування повідомлень. Потік даних, що передаються шифруються біт за бітом або потоковим шифром, з використанням алгоритму шифрування А5 і ключа шифрування Кс.

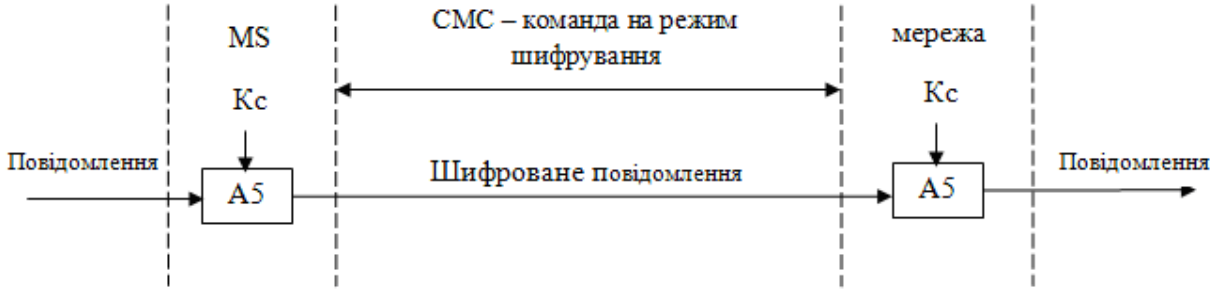


Рис. 4.9. **Процедура встановлення режиму шифрування**

Забезпечення секретності абонента

Для виключення визначення абонента шляхом перехоплення повідомлень, що передаються по радіоканалу, кожному абонентові системи зв'язку привласнюється «тимчасове посвідчення особи» – тимчасовий міжнародний ідентифікаційний номер користувача (TMSI), який дійсний тільки в межах зони розташування. У іншій зоні розташування йому привласнюється новий TMSI. Після закінчення процедури аутентифікації і початку дії режиму шифрування TMSI передається на МС тільки в зашифрованому вигляді. Якщо МС переходить в нову область розташування, то її TMSI повинен передаватися разом з ідентифікаційним номером зони (LAI), в якій TMSI був присвоєний абонентові.

Секретність в процесі коригування місця знаходження

При виконанні процедури коригування місця знаходження по КУ здійснюється двосторонній обмін між МС і БС службовими повідомленнями, що містять TMSI. Тому в радіоканалі треба забезпечити секретність перейменування TMSI і їх приналежність конкретному абонентові.

Розглянемо як забезпечується секретність в процедурі коригування місця знаходження у разі, коли абонент проводить сеанс зв'язку і при цьому здійснює переміщення з однієї зони розташування в іншу (рис. 4.10). В цьому випадку МС вже зареєстрована в регістрі переміщення VLR з тимчасовим номером TMSI, що відповідає колишній зоні розташування. При вході в нову зону розміщення здійснюється процедура розпізнавання, яка проводиться по старому, зашифрованому в радіоканалі TMSI, що передається одночасно з найменуванням зони розміщення LAI. LAI дає інформацію ЦК і центру управління про напрям переміщення МС і дозволяє запросити колишню зону розміщення про статус абонента і його дані, виключивши обмін цими службовими повідомленнями по радіоканалах управління. При цьому по КЗ пові-

домлення передається, як зашифрований інформаційний текст з перериванням повідомлення в процесі естафетної передачі на 100-150 мс.

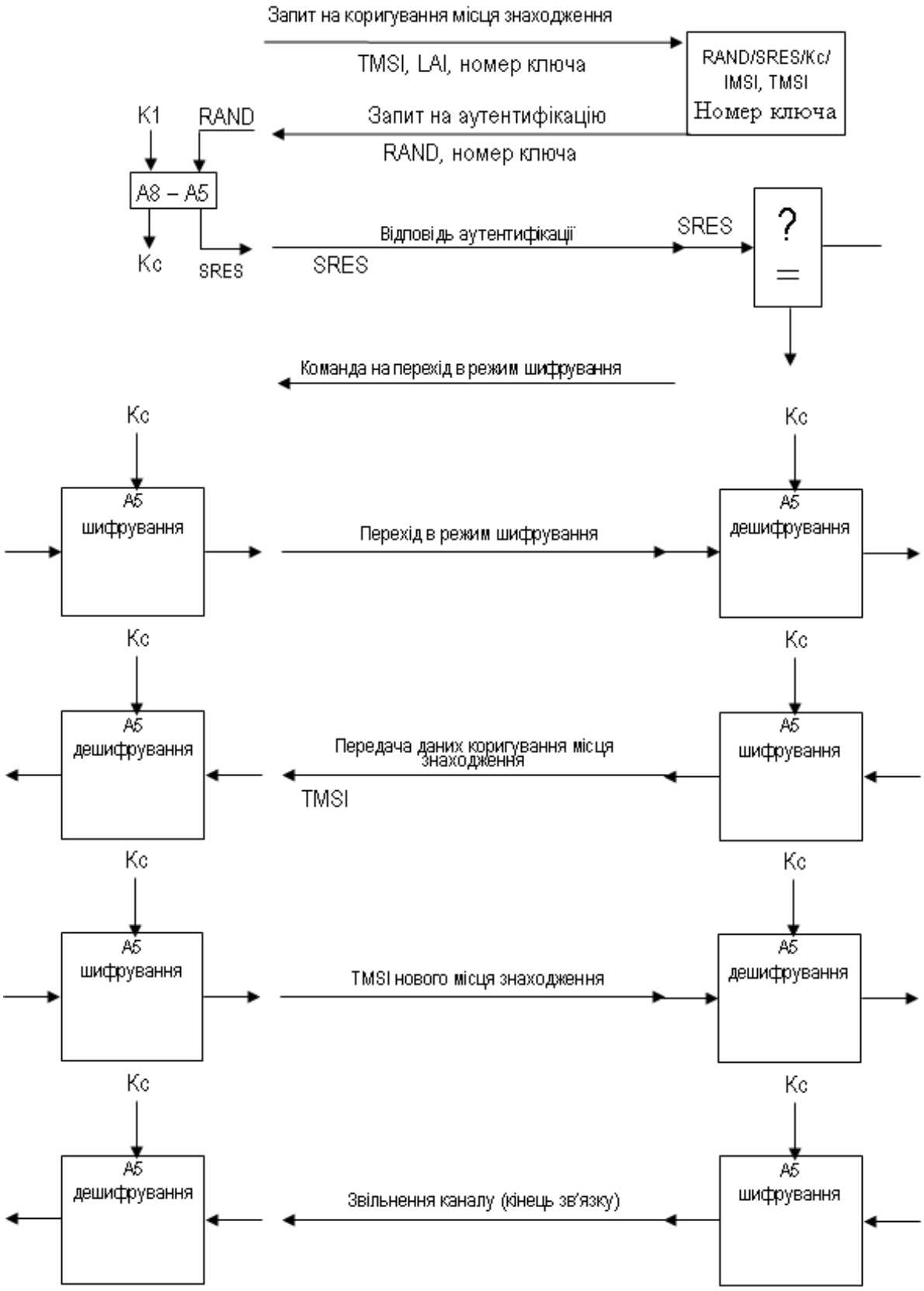


Рис. 4.10. **Схема коригування місця знаходження**

Відповідно до розглянутих механізмів безпеки, діючих в стандарті GSM, секретною вважається така інформація:

RAND – випадкове число, що використовується для аутентифікації рухомого абонента.

SRES – значення відгуку – відповідь МС на отримане випадкове число.

Ki – індивідуальний ключ аутентифікації користувача, що використовується для обчислення значення відгуку і ключа шифрування.

Кс – ключ шифрування, що використовується для шифрування/ дешифрування сигналів управління і даних користувача в радіоканалі.

A3 – алгоритм аутентифікації, що використовується для обчислення значення відгуку із випадкового числа з використанням ключа Ki.

A8 – алгоритм формування ключа шифрування, що використовується для обчислення ключа Кс із випадкового числа з використанням ключа Ki.

A5 – потоковий алгоритм, що використовується для шифрування/ дешифрування сигналів управління і даних користувача з використанням Кс.

CKSN – номер ключової послідовності шифрування, вказує на дійсне число Кс.

TMSI – тимчасовий міжнародний ідентифікаційний номер користувача.

5. Контрольні запитання

1. Види логічних каналів управління в стандарті GSM та їхня характеристика.
2. Поясніть структуру 51-кадрового мультикадру.
3. Поясніть алгоритм встановлення вихідного з'єднання (МС $\rightarrow$ БС).
4. Поясніть алгоритм встановлення вхідного з'єднання (БС $\rightarrow$ *М*С).
5. Поясніть механізм секретності передачі даних.
6. Поясніть механізм забезпечення секретності абонента.
7. Характеристика процедури коригування місця знаходження.
8. Яка інформація вважається секретною?

6. Зміст звіту

1. Призначення та мета роботи.
2. Характеристика логічних каналів управління.
3. Контрольні запитання та відповіді на них.
4. Висновок.