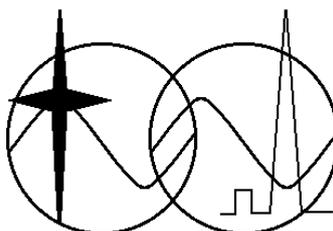


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**  
**ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**  
**СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ**  
**(ТУСУР)**

**Кафедра средств радиосвязи (СРС)**



**СТРУКТУРА ЛОГИЧЕСКИХ КАНАЛОВ УПРАВЛЕНИЯ**  
**И АЛГОРИТМЫ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ GSM-900**

**Учебно-методическое пособие по лабораторной работе**  
**для студентов радиотехнических специальностей**

**Составил:**  
**заведующий кафедрой СРС,**  
**профессор Мелихов С.В.**

**2012**

### **1. Цель работы**

Изучить структуру логических каналов управления и алгоритмы функционирования систем GSM по установлению исходящего и входящего соединений.

### **2. Задание**

1. Изучить структуру логических каналов управления.
2. Изучить алгоритм установления исходящего соединения (MS→BTS, ПС→БС).
3. Изучить алгоритм установления входящего соединения (BTS→MS, БС→ПС).
4. Изучить механизмы безопасности.
5. Составить отчет.

### **3. Краткая теория**

Физический канал в стандарте GSM представляет собой комбинацию временного и частотного разделения сигналов и определяется как последовательность радиочастотных каналов (с возможностью перескоков по частотам) и временных окон TDMA кадров.

Физический канал управления (ФКУ) предназначен для обеспечения установления соединения и образования логических каналов управления (ЛКУ). ФКУ передают служебные сообщения и данные, представленные в цифровой форме. В зависимости от функционального назначения служебной информации и данных служебные сообщения в определенном порядке объединяются в ЛКУ.

Основным назначением ЛКУ является обеспечение передачи подвижной станции (ПС) и БС сигналов управления служебных сообщений и сигналов синхронизации. В зависимости от сочетания служебных сообщений в одном ФКУ может быть размещено несколько ЛКУ.

В зависимости от выполняемых функций в стандарте GSM различают четыре вида логических каналов управления (рис. 1):

КПСУ – каналы передачи сигналов управления (Broadcast Control Channels - BCCH);

ОКУ – общие каналы управления (Common Control Channels - CCCH);

ИКУ – индивидуальные каналы управления (Stand-alone Dedicated Control Channels - SDCCCH);

СКУ – совмещенные каналы управления (Associated Control Channels - ACCH).



Рисунок 1 – Виды логических каналов управления в стандарте GSM

КПСУ используются только в направлении БС  $\rightarrow$  ПС и содержат информацию о подстройке частоты, кадровой (временной) синхронизации, а также обеспечивают передачу основных команд по управлению передачей (номера общих каналов управления, которые объединяются с другими каналами). К указанным каналам относятся:

КПЧ – канал подстройки частоты (Frequency Correction Channel - FCCH);

КУС – канал управления синхронизацией (Synchronisation Channel - SCH);

КУП – канал управления передачей (Broadcast Control Channel - BCCH).

ОКУ предназначены для вызова ПС, для запроса ПС о назначении индивидуального КУ, для выделения специального канала управления, обеспечивающего прямой доступ к каналу связи (КС). К указанным каналам относятся:

КВ – канал вызова (БС  $\rightarrow$  ПС) (Daging Channel - DCH);

КПД – канал параллельного доступа (ПС  $\rightarrow$  БС) (Random Access Channel - RACH);

КРД – канал разрешенного доступа (Access Grant Channel - AGCH).

ИКУ используются для дуплексной связи между БС  $\leftrightarrow$  ПС и предназначены для установки требуемого вида обслуживания.

По ним происходит запрос ПС о нужном виде обслуживания, контроль правильного ответа и выделение свободного канала связи. Имеют место два вида таких каналов:

ИКУ/4 – индивидуальный КУ, который состоит из четырех подканалов (Stand-alone Dedicated Control Channel – SDCCH/4);

ИКУ/8 – индивидуальный КУ, который состоит из восьми подканалов (Stand-alone Dedicated Control Channel – SDCCH/8).

СКУ используются для дуплексной связи между БС  $\longleftrightarrow$  ПС. В направлении «вниз» (DL) они передают команды управления с БС на ПС, а по направлению «вверх» (UL) – информацию о статусе ПС. Каналы АССН служат для передаче команд при переходе ПС из одной соты в другую (handover), а также для установки выходного уровня мощности передатчика ПС (TXPWR). Совмещенные каналы управления делятся на:

БСКУ – быстрый совмещенный КУ (Fast Associated Control Channel – FACCH);

МСКУ – медленный совмещенный КУ (Slow Associated Control Channel – SACCH);

По направлению «вверх» ПС посылает данные, касающиеся уровня установленной выходной мощности (TXPWR), измеренного приемником уровня радиосигнала (RXLEV) и качества его приема (RXQUAL). В совмещенном канале управления всегда содержится один из двух каналов: канал связи (ТСН) или индивидуальный канал управления (SDCCH). Совмещенные КУ всегда объединяются с каналами связи либо с индивидуальными КУ. При этом различают шесть видов объединенных каналов управления:

БСКУ – КУ, объединенный с КС, имеющими скорости 9.6; 4.8; 2.4 кбит/с;

БСКУ – КУ, объединенный с КС, имеющими скорости 4.8; 2.4 кбит/с;

МСКУ – КУ, объединенный с КС, имеющими скорости 9.6; 4.8; 2.4 кбит/с;

МСКУ – КУ, объединенный с КС, имеющими скорости 4.8; 2.4 кбит/с;

МСКУ/с4 – КУ, объединенный с ИКУ/4;

МСКУ/с8 – КУ, объединенный с ИКУ/8.

Для передачи вышеперечисленных КУ используется 51-кадровый мультикадр, исключением являются каналы БСКУ и МСКУ, для их передачи используется 26-кадровый мультикадр.

Объединенный КУ КПСУ/ОКУ предназначен для всех ПС, которые в одно и то же время находятся в одной соте. В канале КУП «сеть  $\longrightarrow$  ПС» передается общая информация о соте, в которой ПС находятся в данный момент, и о соседних сотах.

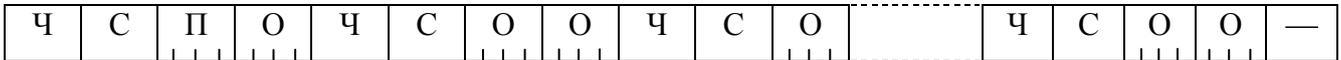
В канале КС («сеть  $\longrightarrow$  ПС») передается информация о цикловой синхронизации и опознавании приемопередатчика БС. Информация для синхронизации несущей передается в канале КПЧ («сеть  $\longrightarrow$  ПС»). Канал КПД «ПС  $\longrightarrow$  сеть» используется ПС для доступа к сети в случае необходимости прохождения регистрации при включении или вызове.

Канал разрешенного доступа (AGCH, «сеть  $\longrightarrow$  ПС») используется для занятия специальных видов обслуживания (SDCCH или ТСН) подвижной станцией, которая ранее не запрашивала через канал RACH.

Канал вызова (PCH, «сеть  $\longrightarrow$  ПС») используется для вызова ПС сетью либо абонентом сети.

На рис. 2 показано отображение рассматриваемых каналов на одном физическом канале управления в структуре 51-кадрового мультикадра.

а) КПСУ + ОКУ линия вниз



б) КПСУ + ОКУ линия вверх



Ч – TDMA кадр для подстройки частоты, канал КПЧ;

С - TDMA кадр для синхронизации, канал КУС;

П - TDMA кадр для канала КУП;

О - TDMA кадр для канала ОКУ;

Д - TDMA кадр для канала КПД.

Рисунок 2 – Отображение рассматриваемых каналов на одном ФКУ в структуре 51-кадрового мультикадра

На линии «вверх» (UpLink) в мультикадре осуществляется передача сигналов канала вызова, который является единственным КУ от ПС к БС, причем для доступа к сети ПС может использовать нулевой временной интервал в любом из кадров. На линии «вниз» 51-кадровый мультикадр группируется в 5 групп по 10 кадров, причем один из кадров остается незанятым. Каждая из групп начинается с сигналов канала КПЧ, за которыми следуют сигналы КУС. Остальные 8 кадров в каждой группе образуют два блока из четырех кадров. Первый блок первой группы предназначен для сигналов канала ВССН, тогда как другие 9 блоков (блоки передачи сигналов вызова) используются для передачи канала вызова и канала разрешенного доступа общего КУ СССН. ПС может занимать один из девяти блоков вызова, а сам блок может использоваться для вызова нескольких ПС.

**Установление исходящего соединения (ПС → БС).** Возможность установления исходящего соединения обеспечивается тем, что БС сети на выделенных им частотах осуществляют передачу мультикадров объединенного КУ (КПСУ + ОКУ). В зависимости от нагрузки в сети структура мультикадров может изменяться. При большой нагрузке в сети передаваемый мультикадр имеет вид, изображенный на рис. 3. Однако, если нагрузка в соте мала, КПСУ + ОКУ объединяется с индивидуальным каналом управления 4ИКУ/4 (рис. 4).

а) 8 ИКУ/8 линия вниз

|    |    |    |    |    |    |    |    |    |    |    |    |   |   |   |
|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|
| И0 | И1 | И2 | И3 | И4 | И5 | И6 | И7 | А0 | А1 | А2 | А3 | — | — | — |
| И0 | И1 | И2 | И3 | И4 | И5 | И6 | И7 | А4 | А5 | А6 | А7 | — | — | — |

б) 8 ИКУ/8 линия вверх

|    |    |    |   |   |   |    |    |    |    |    |    |    |    |    |
|----|----|----|---|---|---|----|----|----|----|----|----|----|----|----|
| А5 | А6 | А7 | — | — | — | И0 | И1 | И2 | И3 | И4 | И5 | И6 | И7 | А0 |
| А1 | А2 | А3 | — | — | — | И0 | И1 | И2 | И3 | И4 | И5 | И6 | И7 | А0 |

1 мультикадр = 51 TDMA кадр = 235,385 мс

И – TDMA кадр для канала ИКУ;

А – TDMA кадр для канала МСКУ.

Рисунок 3 – Передаваемый мультикадр при большой нагрузке в сети

а) КПСУ + ОКУ + 4ИКУ/4 линия вниз

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |    |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|---|
| 4 | С | П | 0 | 4 | С | 0 | 0 | 4 | С | И | И | 4 | С | И | И | 4 | С | М0 | М | — |
|   |   |   |   |   |   |   |   |   |   | 0 | 1 |   |   | 2 | 3 |   |   |    | 1 |   |
| 4 | С | П | 0 | 4 | С | 0 | 0 | 4 | С | И | И | 4 | С | И | И | 4 | С | М2 | М | — |
|   |   |   |   |   |   |   |   |   |   | 0 | 1 |   |   | 2 | 3 |   |   |    | 3 |   |

б) КПСУ + ОКУ + 4ИКУ/4 линия вверх

|    |   |   |    |    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |    |    |    |   |    |    |
|----|---|---|----|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|----|----|---|----|----|
| ИЗ | Д | Д | М2 | М3 | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | И0 | И1 | Д  | Д | И2 |    |
| ИЗ | Д | Д | М0 | М1 | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д | Д  | И0 | И1 | Д | Д  | И2 |

1 мультикадр = 51 TDMA кадр = 235,385 мс

М – TDMA кадр для канала МСКУ;

П – TDMA кадр для канала КУП;

О – TDMA кадр для канала ОКУ;

И – TDMA кадр для канала ИКУ;

Д – TDMA кадр для канала КПД.

Рисунок 4 – Передаваемый мультикадр при малой нагрузке в соте (КПСУ + ОКУ объединяется с индивидуальным каналом управления 4 ИКУ/4)

До поступления от пользователя ПС сигнала вызова приемник ПС осуществляет сканирование по всем 124 рабочим частотам, так как априорно не известно, на какой из них работает доступная ему БС.

На каждой рабочей частоте ПС производит измерение принятого от БС сигнала (RXLEV), и вычисляет оценку качества принятого сигнала (RXQUAL). Выбор обслуживающей БС производится по ряду признаков, а именно:

- принимаемый от БС сигнал должен быть не менее определенного уровня, требуемого для обеспечения отношения сигнал/шум (SNR) не менее 9 дБ;
- вычисленная оценка качества должна быть максимальной;
- расстояние от БС до ПС должно быть минимально.

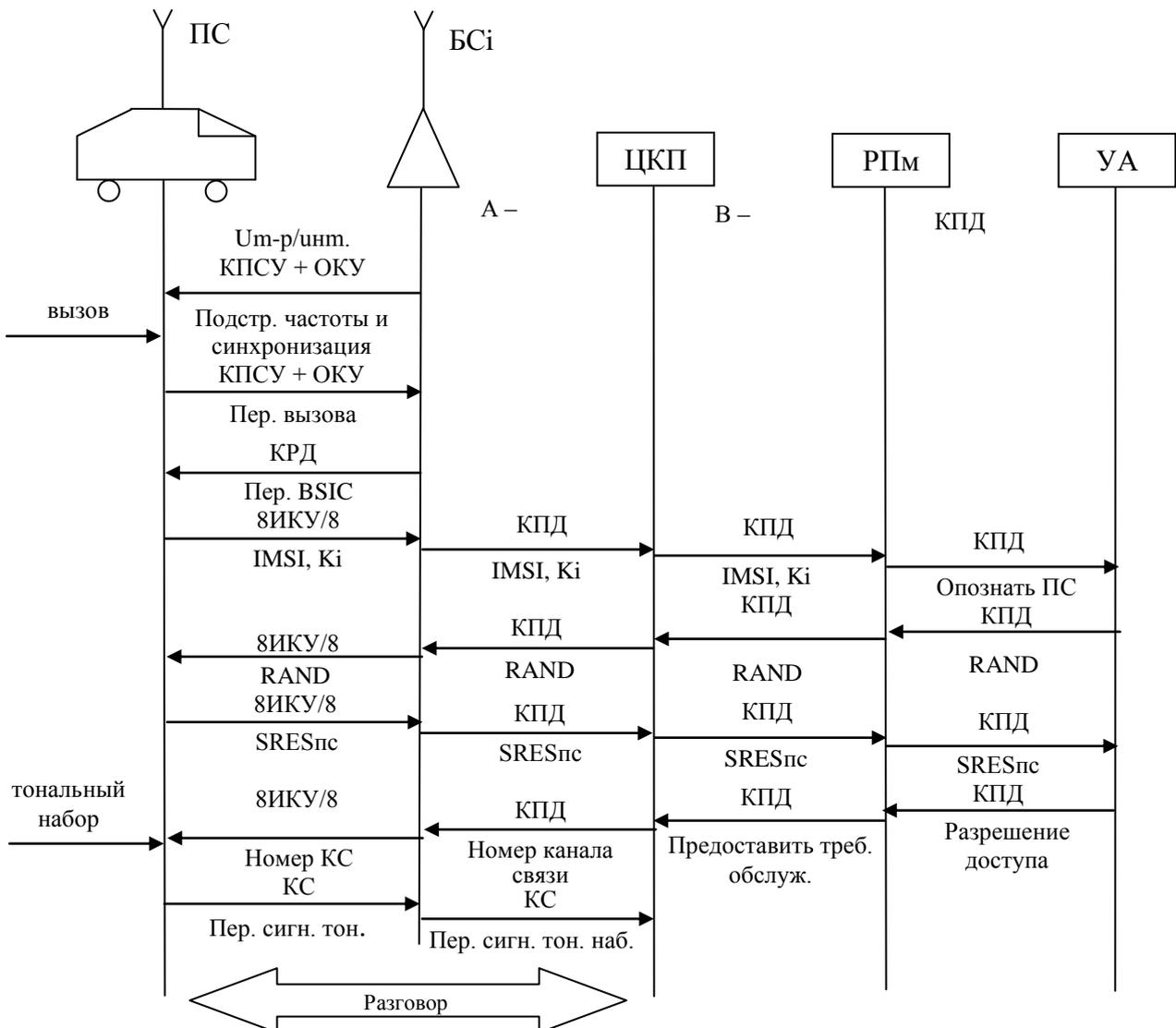


Рисунок 5 – Алгоритм установления исходящего соединения (ПС → БС)

При нажатии кнопки вызова (рис. 5) на ПС осуществляется передача сигналов объединенного КУ (KPCY + OKY). При этом на всех временных позициях мультикадра КУ

содержатся сигналы канала параллельного доступа, что обеспечивает возможность определения БС требуемого пользователем вида обслуживания. Следует отметить, что эта информация содержится в подканалах выделенного ПС индивидуального КУ. После определения вида обслуживания БС по КПД передает ПС свой код опознавания (BSIC). Получив код опознавания, ПС по ранее назначенному ИКУ осуществляет передачу своего международного идентификационного номера (IMSI) и ключа аутентификации (Ki) для определения полномочий пользователя на предоставление указанного вида обслуживания. Так как оборудование БС не позволяет определить полномочия пользователя, то по каналу передачи данных (КПД) она передает в центр коммутации подвижной связи (ЦКПС) указанные выше данные о ПС, которые поступают через регистры перемещения (РПм) и положения (РПл) в узел аутентификации (УА). Процедура аутентификации абонента реализуется следующим образом: из узла аутентификации в адрес ПС передается случайный номер (RAND) через выбранную БС. На ПС при помощи априорно известного ключа Ki и алгоритма аутентификации (A3) по формуле

$$SRES_{\text{пс}} = K_i \cdot \text{RAND}$$

определяется значение отклика, удовлетворяющее условию опознавания по принципу «свой-чужой». Далее вычисленное значение  $SRES_{\text{пс}}$  через БС и ЦКПС поступает в узел аутентификации, где происходит его сравнение со значением  $SRES_{\text{цкпс}}$ , содержащимся в УА. При совпадении этих значений из УА в ЦКПС поступаем сигнал разрешения доступа ПС к сети и закрепленные за ПС одного из логических каналов связи. После предоставления ПС канала TCH, соответствующего требуемому виду обслуживания, БС осуществляет контроль установленного соединения. В случае несовпадения значений, то есть  $SRES_{\text{пс}} \neq SRES_{\text{цкпс}}$ , пользователь получает отказ в обслуживании.

Соединение между ПС и БС с учетом требуемого вида обслуживания установлено.

**Установление входящего соединения (БС → ПС).** При поступлении в ЦКПС заявки (запроса) на установление соединения с одной из ПС от ЦКПС по каналу передачи данных на сеть БС поступает сигнал вызова данной ПС (рис. 6). Далее БС осуществляет передачу вызова в мультикадре объединенного КУ КПСУ/ОКУ в одном из блоков вызова AGCH/PCN на свободной в данный момент временной позиции. Получив вызов, ПС передает в КУ КПСУ/ОКУ сигнал подтверждения получения вызова, транслирующийся через БС на ЦКПС. В свою очередь, из регистров положения и перемещения ЦКПС получает информацию о расстоянии между ПС и БС и направлении перемещения подвижного абонента относительно сети базовых станций и передает на БС команду передать в адрес вызываемого абонента комбинацию «временного опережения» («timing advance» - «ТА») для

вычисления дистанции связи на интервале БС → ПС. Комбинация «ТА» имеет объем 6 бит и обеспечивает измерение абсолютной дистанции связи от 0 до почти 70 км с точностью  $\pm 1$  км. Максимальное значение «ТА» равно 232,6 мкс. Измеренное значение «ТА» от БС по каналу передачи данных через MSC поступает в регистры РПл и РПм. Отметим, что в зависимости от значений «ТА», содержащихся в этих регистрах, осуществляется передача ПС на обслуживание другой БС. После проведения алгоритма аутентификации вызываемой ПС происходит проключение разговорного тракта между ПС и ЦКПС. На протяжении всего сеанса связи между ПС или абонентом сети ISDN БС и ЦКПС осуществляют постоянное слежение за качеством передачи информации и данных.

Таким образом, соединение между БС и ПС с учетом требуемого вида обслуживания установлено.

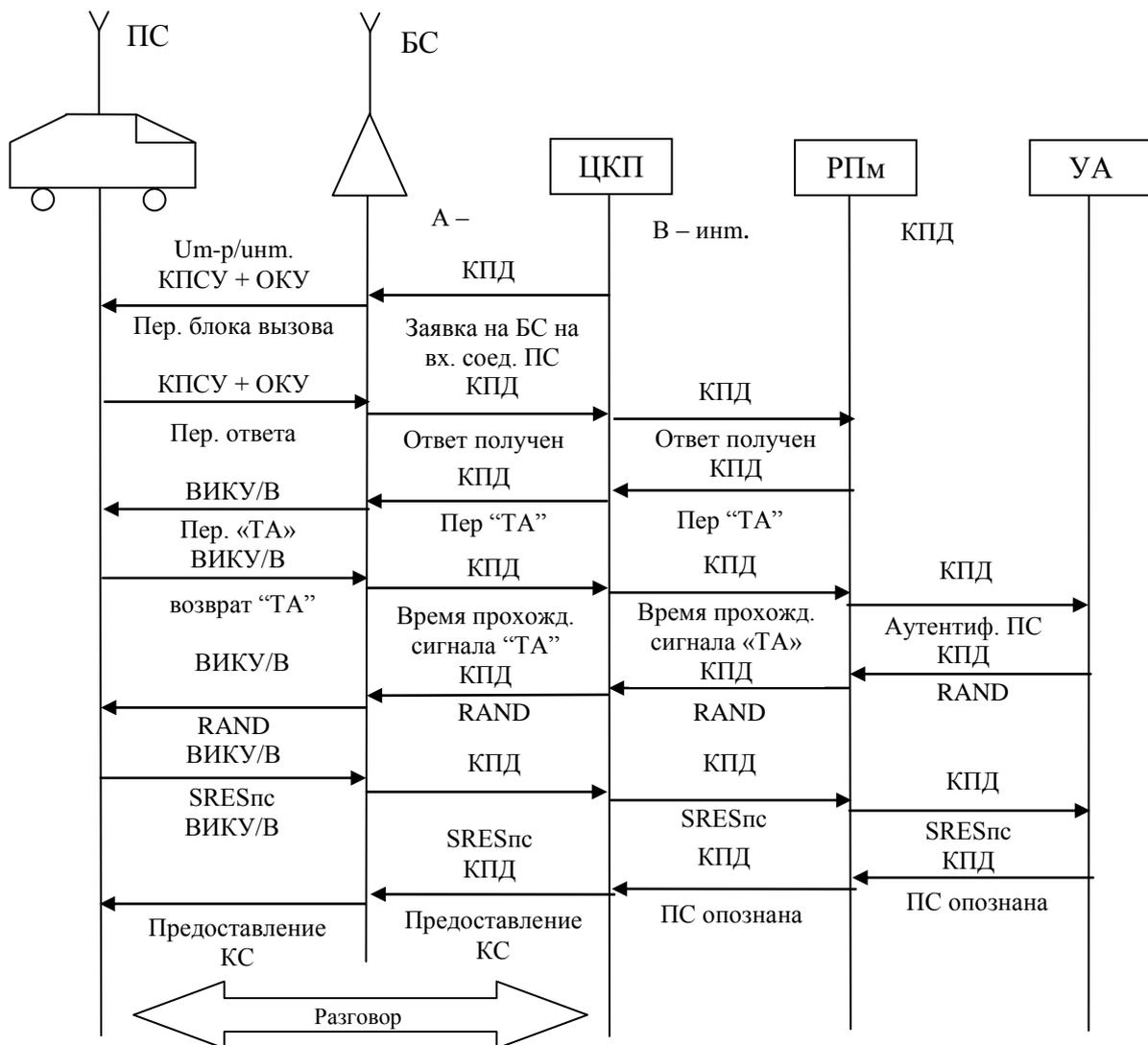


Рисунок 6 – Алгоритм установления входящего соединения (БС ↔ ПС)

**Эстафетная передача (HandOver).** Под эстафетной передачей понимается сопровождение ПС при перемещении ее из одной соты в другую без перерывов сеанса связи. В периоды пиковых нагрузок количество заявок на эстафетную передачу резко увеличивается и превышает количество свободных радиоканалов. Принятие решения о эстафетной передаче осуществляет центр коммутации подвижной связи, основываясь на результатах измерений, выполненных БС и ПС. Эти измерения сортирует ЦКПС в следующей последовательности:

RXQUAL;

RXLEV;

DISTANCE;

PBGT (бюджет излучаемой мощности).

БС измеряет RXLEV, RXQUAL и DISTANCE, в то время как ПС измеряет и передает на обслуживаемую БС в канале MCKY значения RXLEV, RXQUAL и RXLEV для всех соседних БС, которые затем фиксируются в ЦКПС. При удалении ПС от обслуживаемой БС значения RXLEV и RXQUAL становятся ниже, в то время как RXLEV для одной из соседних БС увеличивается (см. рис. 7). Это может происходить по двум основным причинам:

- 1) за счет увеличения расстояния между ПС и БС, а, следовательно, и уменьшения бюджета излучаемой мощности ПС;
- 2) за счет помех от других подвижных станций по основному каналу.

Первая решается только путем передачи управления ПС с одной БС на другую при контроле с ЦКПС, когда изменение мощности, излучаемой передатчиком ПС, невозможно или не имеет смысла. Напротив, вторая может решаться как путем управления излучаемой мощности, так и за счет предоставления ПС другого частотного радиоканала по сигналу с БС, передаваемому в канале БСКУ. Таким образом, если БС не может предоставить приемлемый для ПС радиоканал, она посылает запрос о невозможности связи в ЦКПС, который исходя из выполненных ПС и БС измерений принимает решение о эстафетной передаче на другую БС.

В стандарте GSM решены вопросы безопасности связи. Здесь термин «безопасность» понимается как исключение несанкционированного использования системы и обеспечение секретности переговоров подвижных абонентов. Определены следующие механизмы безопасности:

- аутентификация;
- секретность передачи данных;
- секретность абонента;
- секретность в процедуре корректировки местоположения.

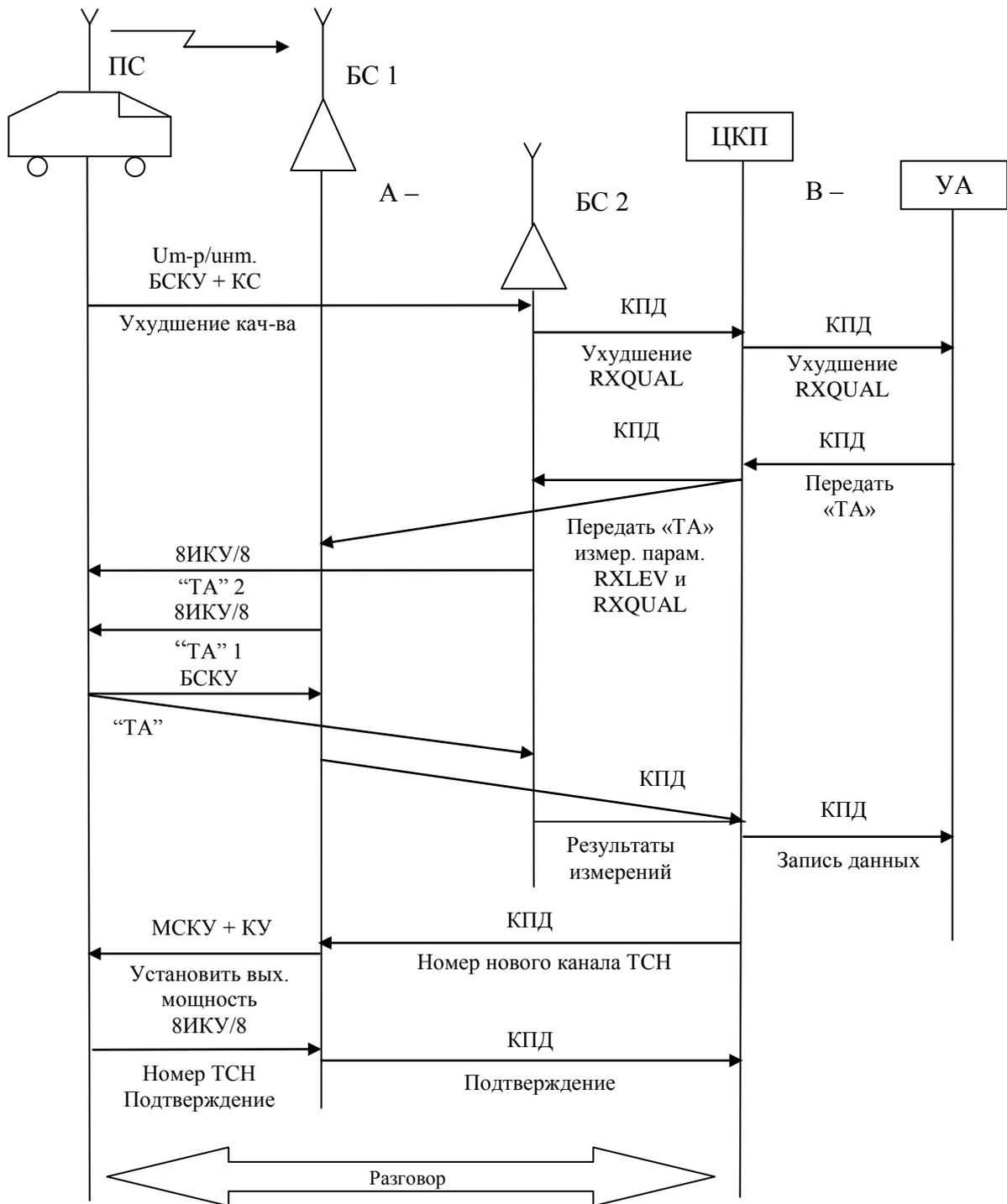


Рисунок 7 – Алгоритм установления входящего соединения при увеличении расстояния между ПС и БС и влиянии помех

Защита сигналов управления и данных пользователя осуществляется только по радиоканалу. Режимы секретности в стандарте GSM определяются рекомендациями, приведенными ниже.

GSM 02.09. Аспекты секретности. Определяет характеристики безопасности, применяемые в сетях GSM. Регламентируется их применение в подвижных станциях и сетях.

GSM 03. 20. Секретность, связанная с функциями сети. Определяет функции сети, необходимые для обеспечения характеристик безопасности, рассматриваемых в рекомендации GSM 02. 09.

GSM 03. 21. Алгоритмы секретности. Определяет криптографические алгоритмы в системе связи.

GSM 02. 17. Модули подлинности абонентов (SIM). Определяет основные характеристики модуля SIM.

Кратко рассмотрим механизмы безопасности.

**Секретность передачи данных.** Для обеспечения секретности передаваемой по радиоканалу информации вводится следующий механизм защиты. Все конфиденциальные сообщения должны передаваться в режиме защиты информации. Алгоритм формирования ключей шифрования (АВ) хранится в модуле SIM. После приема случайного номера RAND подвижная станция вычисляет кроме отклика SRES также и ключ шифрования (Kc), используя RAND, Ki и алгоритм A8 (рис. 8):

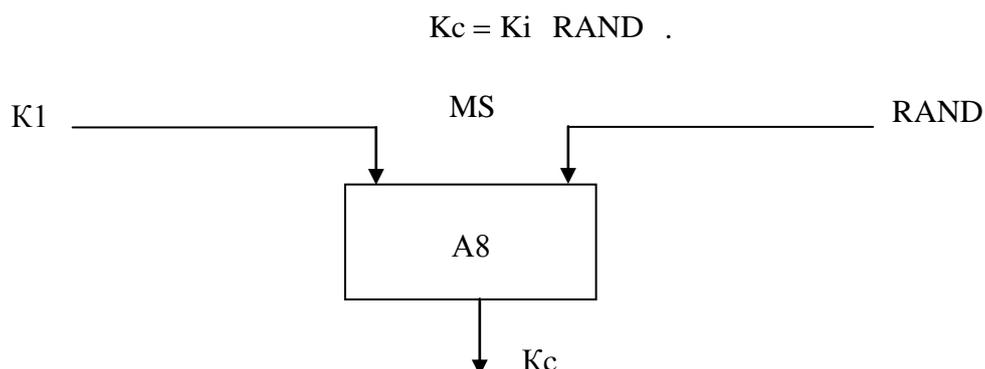


Рисунок 8 – Определение ключа шифрования Kc

Ключ шифрования Kc не передается по радиоканалу. Как подвижная станция, так и сеть вычисляют ключ шифрования, который используется другими подвижными абонентами. По причине секретности вычисление Kc происходит в SIM.

Кроме случайного числа RAND сеть посылает подвижной станции числовую последовательность ключа шифрования. Это число связано с действительным значением Kc и позволяет избежать формирования неправильного ключа. Число хранится подвижной станцией и содержится в каждом первом сообщении, передаваемом в сеть. Некоторые сети принимают решение о наличии числовой последовательности действующего ключа шифрования в случае, если необходимо приступить к опознаванию или если выполняется

предварительное опознавание, используя правильный ключ шифрования. В некоторых случаях это допущение реально не обеспечивается.

Для установки режима шифрования сеть передает подвижной станции команду СМС (Ciphering Mode Command) на переход в режим шифрования. После получения команды СМС подвижная станция, используя имеющийся у нее ключ, приступает к шифрованию и дешифрованию сообщений. Поток передаваемых данных шифруется бит за битом или поточным шифром, с использованием алгоритма шифрования А5 и ключа шифрования Кс. Процедура установки режима шифрования показана на рис. 9.

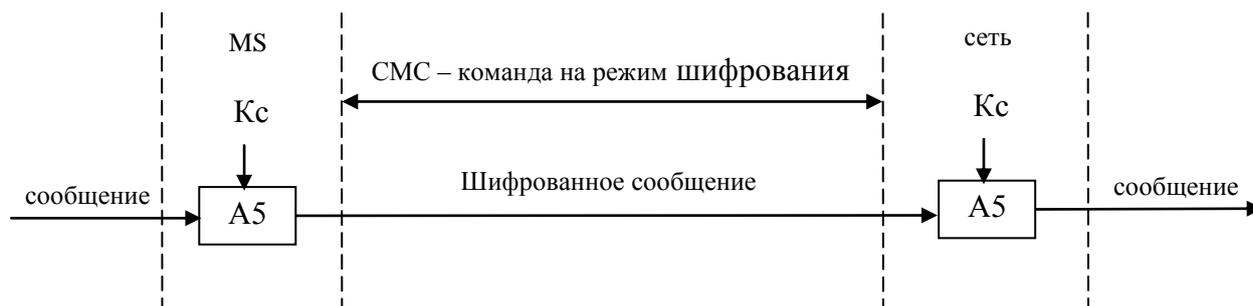


Рисунок 9 – Процедура установки режима шифрования

**Обеспечение секретности абонента.** Для исключения определения (идентификации) абонента путем перехвата сообщений, передаваемых по радиоканалу, каждому абоненту системы связи присваивается «временное удостоверение личности» – временный международный идентификационный номер пользователя (TMSI), который действителен только в пределах зоны расположения. В другой зоне расположения ему присваивается новый TMSI. Если абоненту еще не присвоен временный номер (например, при первом включении подвижной станции), идентификация проводится через международный идентификационный номер (TMSI). После окончания процедуры аутентификации и начала действия режима шифрования временный идентификационный номер TMSI передается на подвижную станцию только в зашифрованном виде. Этот TMSI будет использоваться при всех последующих доступах к системе. Если подвижная станция переходит в новую область расположения, то ее TMSI должен передаваться вместе с идентификационным номером зоны (LAI), в которой TMSI был присвоен абоненту.

**Секретность в процессе корректировки местоположения ПС.** При выполнении процедуры корректировки местоположения по каналам управления осуществляется двусторонний обмен между ПС и БС служебными сообщениями, содержащими временные номера абонентов TMSI. В этом случае в радиоканале необходимо обеспечить секретность переименования TMSI и их принадлежность конкретной ПС.

Рассмотрим, как обеспечивается секретность в процедуре корректировки местоположения в случае, когда абонент проводит сеанс связи и при этом осуществляет перемещение из одной зоны расположения в другую (рис. 10).

В этом случае подвижная станция уже зарегистрирована в регистре перемещения VLR с временным номером TMSI, соответствующим прежней зоне расположения. При входе в новую зону расположения осуществляется процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с наименованием зоны расположения LAI. LAI дает информацию центру коммутации и центру управления о направлении перемещения подвижной станции и позволяет запросить прежнюю зону расположения о статусе абонента и его данные, исключив обмен этими служебными сообщениями по радиоканалам управления. При этом по каналу связи сообщение передается как зашифрованный информационный текст с прерыванием сообщения в процессе эстафетной передачи на 100-150 мс.

Процедура корректировки местоположения, включающая характеристики секретности, показана на рис. 10.

**Общий состав секретной информации и ее распределение в аппаратных средствах GSM.** В соответствии с рассмотренными механизмами безопасности, действующими с стандарте GSM, секретной считается следующая информация:

RAND – случайное число, используемое для аутентификации ПС;

SRES – значение отклика (ответ ПС на полученное случайное число);

K<sub>i</sub> – индивидуальный ключ аутентификации пользователя, используемый для вычисления значения отклика и ключа шифрования;

K<sub>c</sub> – ключ шифрования, используемый для шифрования/дешифрования сигналов управления и данных пользователя в радиоканале;

A3 – алгоритм аутентификации, используемый для вычисления значения отклика из случайного числа с использованием ключа K<sub>i</sub> ;

A8 – алгоритм формирования ключа шифрования, используемый для вычисления ключа K<sub>c</sub> из случайного числа с использованием ключа K<sub>i</sub> ;

A5 – поточный алгоритм, используемый для шифрования/дешифрования сигналов управления и данных пользователя с использованием ключа K<sub>c</sub> ;

CKSN – номер ключевой последовательности шифрования (указывает на действительное число K<sub>c</sub>, чтобы избежать использования разных ключей на передающей и приемной сторонах);

TMSI – временный международный идентификационный номер пользователя.

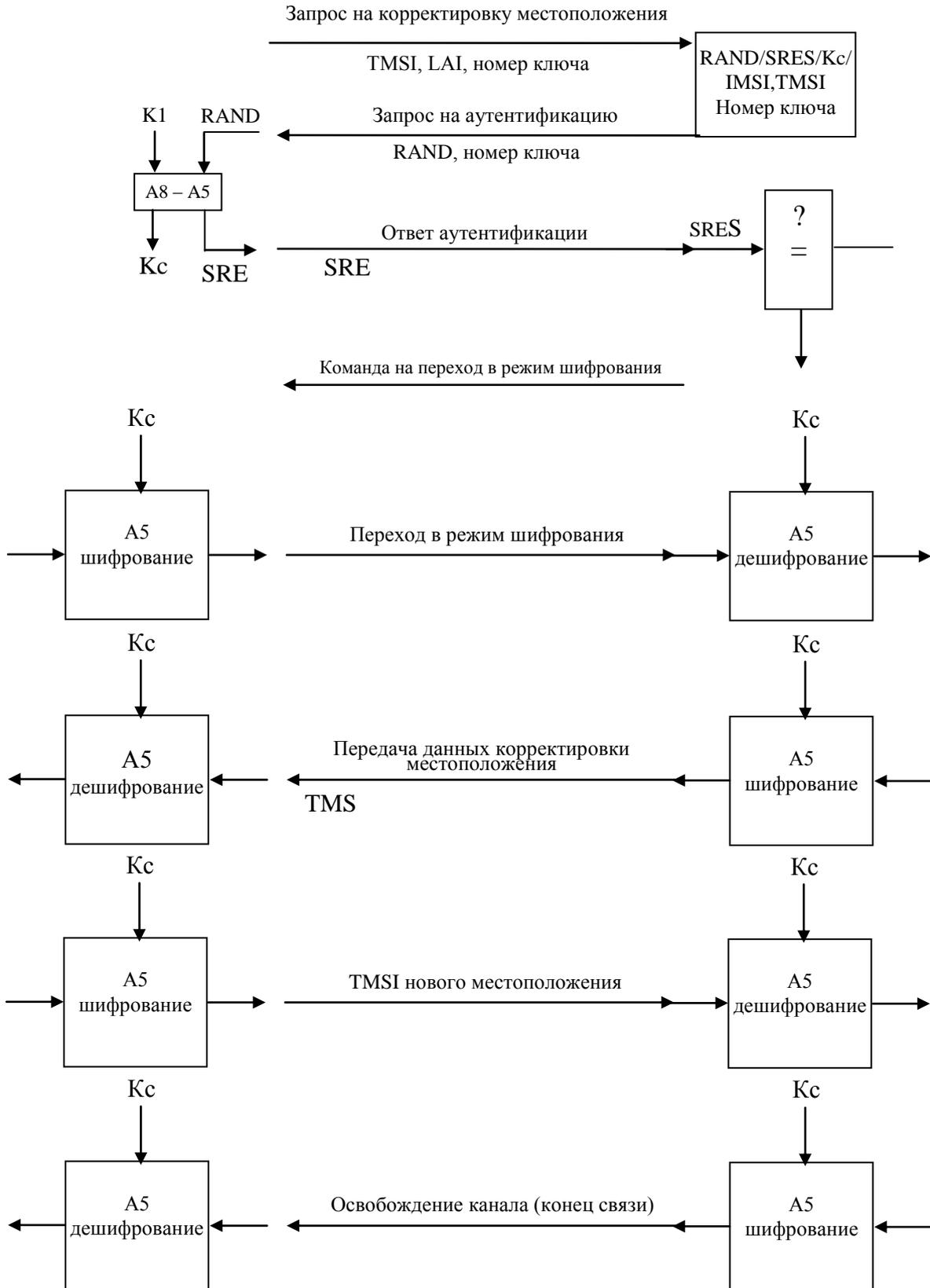


Рисунок 10 – Схема корректировки местоположения ПС

Таблица 1 иллюстрирует распределение секретной информации в аппаратных средствах системы связи GSM.

Таблица 1.

***Распределение секретной информации в аппаратных средствах***

| № п/п | Аппаратные средства                   | Вид секретной информации                            |
|-------|---------------------------------------|---|
| 1.    | Подвижная станция (без SIM)           | A5  |
| 2.    | Модуль подлинности пользователя (SIM) | A3, A8, IMSI, Ki, TMSI/LAI, Kc/CKSN                 |
| 3.    | Центр аутентификации (AUC)            | A3, A8, IMSI/Ki                                     |
| 4.    | Регистр местоположения (HLR)          | группы IMSI/RAND/SRES/Kc                            |
| 5.    | Регистр перемещения (VLR)             | группы IMSI/RAND/SRES/Kc,<br>IMSI/ TMSI/LAI/Kc/CKSN |
| 6.    | Центр коммутации (MSC)                | A5, временные TMSI/IMSI/Kc                          |
| 7.    | Контроллер базовой станции (BSC)      | A5, временные TMSI/IMSI/Kc                          |

**4. Контрольные вопросы**

1. Перечислите виды логических каналов управления в стандарте GSM.
2. Дайте краткую характеристику логических каналов управления.
3. Поясните структуру 51-кадрового мультикадра.
4. Поясните передаваемый мультикадр при большой нагрузке в сети.
5. Поясните передаваемый мультикадр при малой нагрузке в сети.
6. Поясните алгоритм установления исходящего соединения (ПС → БС).
7. Поясните алгоритм установления входящего соединения при увеличении расстояния между ПС и БС, а также за счет влияния помех.
8. Поясните механизм секретности передачи данных.
9. Поясните механизм обеспечения секретности абонента.
10. Поясните процедуру корректировки местоположения.
11. Поясните общий состав секретной информации.
12. Поясните распределение секретной информации в аппаратных средствах.

**5. Содержание отчета**

1. Название и цель работы.
2. Характеристика логических каналов управления.

## Литература

1. Громаков Ю.Я. Стандарты и системы подвижной радиосвязи. - М.: ЭКО-ТРЭНДЗ, 1998. – 239 с.
2. Попов В.И. Основы сотовой связи стандарта GSM. – М.: Эко-Трендз, 2005. – 292 с.
3. Маковеева М.М., Шинаков Ю.С. Системы связи с подвижными объектами: Учебное пособие для вузов. – М.: Радио и связь, 2002. – 440 с.
4. Цифровые и аналоговые системы передачи: Учебник для вузов / В.И. Иванов, В.Н. Гордиенко, Г.Н. Попов и др.; под ред. В.И. Иванова. – М.: Горячая линия-Телеком, 2005. – 231 с.