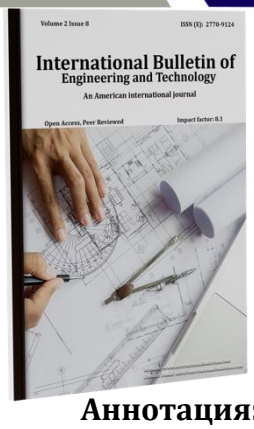

IDENTIFYING THE ORGANIZERS OF THE GSM STANDARD'S GENERAL NETWORK SCHEME

Shoxruh Erkin o'g'li Alimardonov
Military Institute of Information and Communication Technologies and Communications of the Ministry of Defense of the Republic of Uzbekistan
shohruhalimardonov1202@gmail.com
https://doi.org/10.5281/zenodo.14701273

Аннотация: В статье подробно рассматриваются основные компоненты сети мобильной связи GSM, принципы их взаимодействия, процессы аутентификации, а также функции различных центров (HLR, VLR, EIR, OMS, NMC). В статье представлен состав долгосрочных и временных данных, хранящихся в системах HLR (Home Location Register) и VLR (Visitor Location Register). В нем также рассматривается, как информация об абонентах хранится в сети, как она обновляется в зависимости от местоположения мобильных станций, а также процессы аутентификации и шифрования. В статье также представлен всесторонний обзор важных ролей, которые системы управления сетями, включая OMS и NMC, играют в обеспечении их эффективной работы. Объясняются принципы взаимодействия этих элементов и их влияние на другие элементы системы.

Ключевые слова: GSM, мобильная связь, аутентификация, HLR, VLR, EIR, IMEI, шифрование, управление сетью, OMS, NMC, мобильная станция, идентификация, протоколы, безопасность, сетевые центры, EIR, BSS, IWF.

ANNOTATION: This article explains in detail the main components of the GSM mobile communication network, their principles of interaction, authentication processes and the functions of various centers (HLR, VLR, EIR, OMS, NMC). The article presents the composition of long-term and temporary data stored in the HLR (Home Location Register) and VLR (Visitor Location Register) systems. It also covers how subscriber information is stored in the network, how it is updated depending on the location of mobile stations, and the authentication and encryption processes. The article also provides complete information on the important roles that network management systems, including OMS and NMC, play in ensuring their effective operation. The principles of interaction of these elements and their impact on other elements in the system are explained.

Keywords: GSM, mobile communication, authentication, HLR, VLR, EIR, IMEI, encryption, network management, OMS, NMC, mobile station, identification, protocols, security, network centers, EIR, BSS, IWF.

Стандарт GSM (глобальная система мобильной связи) — одна из современных цифровых сетей, тесно связанная, прежде всего, с ISDN и IN (интеллектуальная сеть). Глобальная система сотовой связи UMTS (Универсальная система мобильной связи) будет интегрирована в международный стандарт на основе развития основных функциональных элементов GSM. В 1990 году была опубликована первая фаза спецификаций GSM. К середине 1991 года была начата поддержка коммерческих услуг GSM, а к 1993 году в 22 странах действовало 36 сетей GSM, а 25 стран приняли решение о внедрении GSM или рассматривали возможность его внедрения. В июне 1992 года в России был принят стандарт GSM в качестве федерального стандарта подвижной цифровой спутниковой системы связи (МАСТ).

С января 1996 года началась коммерческая эксплуатация сети стандарта GSM (900 МГц) в Москве и области. Оператором сети GSM в Москве является компания «Мобильные ТелеСистемы» (МТС). В первые дни коммерческой работы МТС впервые в России был открыт автоматический роуминг подписок с абонентами MAST ее сетей стандарта GSM в Германии, Швейцарии, Финляндии и Англии. МТС совместно с операторами сетей GSM других регионов организовала создание федеральной сети GSM и ее интеграцию с глобальной сетью сотовой связи, охватывающей Европу, Азию, Австралию и Африку.

Согласно определениям МСЭ-Т (Международный союз электросвязи - Сектор стандартизации электросвязи), сеть GSM обеспечивает следующее: передачу информации (услуги канала связи); отображение информации (телеуслуги); могут предоставлять дополнительные услуги.

Система GSM — это цифровая система передачи данных, закодированных и переданных в виде цифрового потока. Он также предоставляет различные услуги по передаче данных. Абоненты GSM могут обмениваться информацией с сетями с коммутацией пакетов и сетями связи с коммутацией каналов, используя различные методы и протоколы, аналогичные тем, которые используются абонентами ISDN обычных телефонных сетей, например, X.25 или X.32. Возможна передача факсимильных сообщений, что осуществляется при использовании соответствующего адаптера для факсимильного аппарата. Уникальной особенностью GSM, отсутствующей в аналоговых системах, является двусторонняя передача коротких сообщений (до 160 байт) в виде SMS (Short Message Service), передаваемых в режиме буферизованных данных. Сообщение может быть отправлено получателю, являющемуся подписчиком SMS, а затем отправителю может быть отправлено подтверждение о получении. Короткие сообщения можно использовать в режиме широковещательной рассылки, например, для уведомления абонентов об изменениях дорожной обстановки в данном районе. В качестве дополнительных возможностей текущие функции описывают услуги по передаче информации и обеспечению связи (например, переадресация вызовов при невозможности соединения с мобильным абонентом). Ожидается появление новых возможностей, таких как идентификация вызывающего абонента, организация очереди вызовов, одновременный разговор с несколькими абонентами и многое другое.

В соответствии с рекомендациями SERT 1980 года по использованию спектра частот мобильной связи в диапазоне частот 862…960 МГц стандарт GSM для цифровой общеевропейской сотовой системы наземной подвижной связи базируется на двух диапазонах частот: 890…915 МГц. МГц (для передатчиков мобильных станций – MS), 935…960 МГц (для передатчиков мобильных станций – MS), и 940…960 МГц (для передатчиков мобильных станций – MS). Работа передатчиков МГ (для передатчиков базовых станций – BTS) предусмотрено.

Стандарт GSM использует узкополосный множественный доступ с временным разделением (NB-TDMA). Структура кадра TDMA включает 8 временных интервалов в каждой из 124 несущих.

Для защиты от ошибок в радиоканалах при передаче информационных сообщений применяется блочное и перемежающееся кодирование со смещением. Эффективное кодирование при низкой скорости перемещения мобильной станции и увеличенной скорости перемещения в 217 скачков в секунду обеспечивает медленное повторное подключение рабочих частот (SFH) во время сеанса связи.

Для борьбы с помеховым ослаблением принимаемых сигналов, вызванным многолучевым распространением радиоволн в городских условиях, в аппаратуре связи необходимо проводить коррекцию импульсных сигналов со среднеквадратичным отклонением времени задержки до 16 мкс. Для обеспечения

Система синхронизации рассчитана на компенсацию абсолютных задержек сигнала до 233 мкс, что соответствует максимальной дальности связи или максимальному радиусу соты 35 км.

Гауссовская манипуляция с минимальным отклонением (GMSK) в стандарте GSM; Индекс манипуляции установлен на уровне 0,3. Обработка речи осуществляется в рамках принятой системы дифференциальной передачи речи (DTX), которая обеспечивает включение передатчика при наличии речевого сигнала во время перерывов или по окончании разговора, а также выключение передатчика.

В качестве устройства преобразования речи был выбран речевой кодек с линейным предиктивным кодированием с регулярным импульсным возбуждением/долгосрочным предсказанием и прогнозированием (RPE/LTP – LPC – кодек). Общая скорость преобразования речевого сигнала составляет 13 кбит/с.

В стандарте GSM достигнут высокий уровень безопасности передачи сообщений; Сообщения были зашифрованы с использованием алгоритма шифрования с открытым ключом (RSA).

Таблица 1. Основные характеристики стандарта GSM

Mobile station transmission and support of the station acceptance to do Frequency, MHz	890…915
Mobile station acceptance to do and support of the station transmission Frequency, MHz	935…960
Reception to do and transmission frequency duplex dispersion, MGs	45
the radio channel messages transmission speed, kbit /s	270, 833
Spoken codec change speed, kbit /s	13
Contact channel of the street width, kgs	200
Maximum number of channels	124
Support at the stations organization to be done communication channels maximum number	16…20
Modulation type	M S K
VT modulation index	0.3
From modulation previous Gaussian filter band width, kgs	82.2
Frequency according to per second jumps number	217
Temporal distribution in intervals	2
Mobile station for frame (transmit / receive) to do)	
Speech codec type	RPE LTP
Maximum radius of the market, km	up to 35
Channels organization to do scheme (mixed)	TDMA/FDMA

Functional structure and interfaces adopted in the GSM standard Figure 1 shows the structure diagram: MSC (Mobile Switching Centre) - mobile communication switching centre; BSS (Base Station System) - base station equipment; OMS (Operations and Maintenance Centre) - management and service centre; MS (Mobile Stations) - mobile stations.

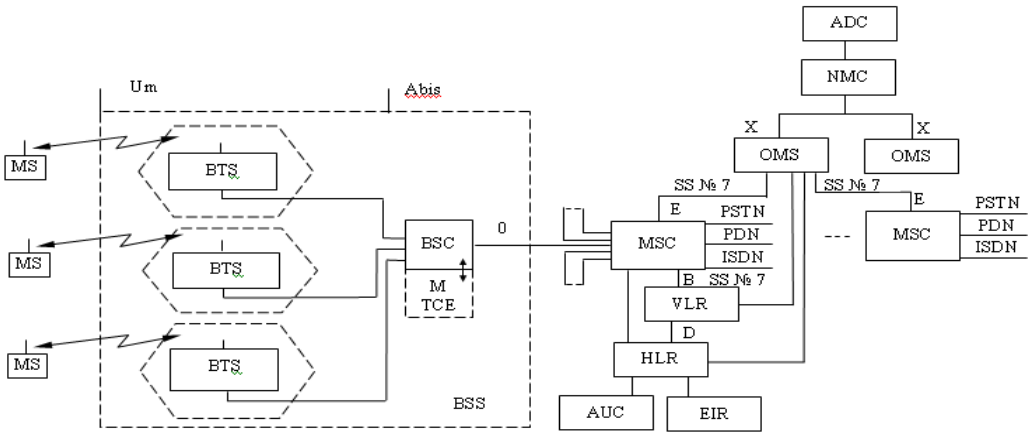

Figure 1. Structure diagram of the GSM standard.

The functional integration of the system is carried out at the interfaces. All network functional components of the GSM standard interact according to the signaling system MKKTT N7 (SSIT SS N7). SS N7 is internationally standardized and is designed for the exchange of signaling information in a digital network of communication with digital program-control stations. The system is optimized for operation on a digital channel with a speed of 64 kbit/s and allows you to control the communication process, as well as transmit maintenance and operational information. In addition, it can be used as a reliable transport system for transmitting other types of information between stations and specialized centers in telecommunication networks. SS N7 uses a method of transmitting signaling information on a special channel common to one or more bundles of information channels. Signal information must be transmitted in the correct sequence without losses, while terrestrial and satellite channels can interact. The SS N7 network is a prerequisite for creating a GSM standard network.

The mobile switching center serves a group of stations and provides all types of connections necessary for the operation of a mobile station. The MSC switching station is similar to ISDN and includes an interface between the fixed networks (PSTN, PDN, ISDN, etc.) and the mobile network. It provides call routing and call control functions. In addition to performing the usual ISDN functions of the switching station, the MSC is responsible for radio channel switching functions. These include relaying, which ensures the continuity of communication when the mobile station changes location from station to station and reconnects working channels in the station in the event of interference or malfunctions. Each MSC provides service to mobile subscribers located within the boundaries of a certain geographical area (for example, Moscow and the region). The MSC controls the call setup and routing procedures. Signaling for the public switched telephone network (PSTN) according to the MSC SS N7 protocol provides the function of transferring calls or other types of interfaces according to the requirements of a specific project.

MSC generates the data necessary for billing for services provided by the communication network, collects data on the conversations that have taken place and transmits them to the billing center (billing center). MSC contains statistical information necessary for monitoring and optimizing the operation of the network.

MSC provides security procedures used to control access to radio channels.

MSC participates in call management, but also manages the control transfer procedures, in addition to location registration and control transfer in the base station subsystem (BSS). Location registration of mobile stations is necessary to ensure the delivery of calls from subscribers of the public telephone network or from other mobile subscribers to mobile subscribers. The call transfer procedure is capable of maintaining the connection and ensures the continuation of the conversation when mobile stations move from one service area to another. In the cells controlled by one base station controller (BSC), calls are transferred by

this BSC. When the call transfer is carried out between two networks controlled by different BSCs, the primary control is carried out by the MSC. The GSM standard provides procedures for transferring calls between networks (controllers) belonging to different MSCs. The switching center uses the Home Location Register (HLR) and the Location Location Register (VLR) to keep track of mobile stations. The HLR stores information about the location of any mobile station, which allows the switching center to transmit the station's call. The HLR contains the International Mobile Subscriber Identity Number (IMSI).

It is used to identify the mobile station in the Authentication Center (AUC) (Tables 2.3).

Table 2. Composition of long-term data stored in the HLR and VLR

Stored in HLR and VLR far term information composition	
HLR	VLR
1	IMSI – In Motion subscriber international identification number
2	ISDN international online mobile station number
3	Mobile station category
4	Authentication key
5	Type of support service provision
6	Index of closed user groups
7	Users closed of the group blocking code
8	Transmission possible was main calls composition
9	Notify the calling subscriber
10	Calling subscriber identification number
11	Work schedule
12	Notifying the called subscriber
13	Subscribers in binding signaling control
14	Users closed of the group features (tools)
15	Closed user group privileges
16	Outgoing calls are prohibited in a closed group of users.
17	Maximum number of subscribers
18	Password to use
HLR	
19	Priority access class i
20	Incoming calls are prohibited in a closed group of users

In practice, the HLR contains a reference database of information about subscribers that is constantly recorded in the network. It contains selected numbers and addresses, as well as special information about the authenticity of subscribers, the composition of communication services, routing. Information about the roaming (strangeness) of the subscriber is registered, including information about the temporary identification number (TMSI) of the mobile subscriber and the VLR.

If there are several HLRs in the network, all MSCs and VLRs of the network have remote access to the information in the HLR, there is one record about the subscriber in the database, therefore, each HLR contains a certain part of the general database of information about subscribers in the network. Access to the database of information about subscribers is carried

out by IMSI or MSISDN (mobile subscriber number of the ISDN network). The database can be used by MSCs or VLRs belonging to other networks to provide inter-network roaming for subscribers.

Table 3. Contents of time-based data stored in the HLR and VLR

Stored in HLR and VLR far term information composition	
HLR	VLR
Authentication and encryption settings	TMSI - user's timely international identification number
VLR is assigned mobile of the station timely number	Location zone identifier
VLR migration registry address	Home from services use according to instruction
Mobile station migration zone	Number of sales in "relay transmission"
Relay station number	Authentication and encryption settings
Registration status	
Answer when it wasn't timer (link) when turned off) is turned off	
Password this at the moment usable composition	
Communication activity	

The second main device that provides control over the migration of a mobile station from one zone to another is the VLR migration register. With its help, the functions of the operation of mobile stations outside the boundaries of the zones controlled by the HLR are achieved. When mobile stations move from the operating area of one base station controller BSC to the operating area of another BSC during the migration process, it is registered by the new BSC and information about the communication area number to which the mobile station calls will be forwarded is entered in the VLR. Since the data in the HLR and VLR are stored, protection of the memory device of these registers is provided in the event of a breakdown.

The VLR contains the same data as the HLR, but this data remains in the VLR until the subscriber is in the VLR controlled area.

In the GSM mobile communication network, it is grouped into geographical areas (LA), to which its own identification number (LAC) is assigned. Each VLR contains information about subscribers in several LAs. When a mobile subscriber moves from one LA to another, its location information is automatically updated in the VLR. If the old and new LAs are under different VLRs, the information in the old VLR is deleted after being copied to the new VLR. The subscriber's current VLR address in the HLR is also updated.

The VLR ensures that the mobile station's "stray" number (MSRN) is assigned. When a mobile station receives an incoming call, the VLR selects the MSRN and forwards it to the MSC, which routes the call to the base stations near the mobile subscriber.

The VLR verifies the transfer number when transferring calls from one MSC to another. In addition, the VLR manages the allocation of new TMSIs and forwards them to the MSC. It manages the authentication procedures during call processing. TMSI can be changed from time to time to complicate the procedure for identifying subscribers at the operator's discretion. Access to the database can be provided by the VLR via IMSI, TMSI or MSRN. In general, the VLR contains a local database of information about the subscriber in motion for

the area where the subscriber is located, which allows you to eliminate constant requests to the HLR and reduce the time for servicing calls. To prevent unauthorized use of communication system resources, authentication mechanisms are introduced - subscriber identity certificates. The authentication center includes several blocks and generates authentication keys and algorithms. With its help, the subscriber's authority is verified and his access to the communication network is carried out. The AUS makes a decision on the parameters of the authentication process and determines the encryption key for subscriber stations based on the database located in the Equipment Identification Register (EIR).

When using the communication system, each mobile subscriber receives a subscriber identity module (SIM), which consists of an international mobile identity number (IMSI), its own authentication key (Ki), and an authentication algorithm (A3).

As a result of the exchange of information between the mobile station and the network, a full authentication cycle is performed using the information entered into the SIM, and the subscriber is allowed to use the network.

The procedure for verifying the authenticity of the network subscriber is as follows. The network transmits a random number (RAND) to the mobile station. It determines the response value (SRES) using Ki and the authentication algorithm A3, i.e.

$$SRES = Ki * [RAND]$$

The mobile station sends the SRES value calculated in the network, which is compared with the SRES value calculated by the network. If both values match, the mobile station starts transmitting messages. Otherwise, the connection is disconnected and the mobile communication indicator shows that there is no delay. SRES calculation occurs in the SIM to ensure confidentiality. Non-confidential information (e.g. Ki) is not processed in the SIM module.

The authentication procedure is shown in the diagram in Figure 4.

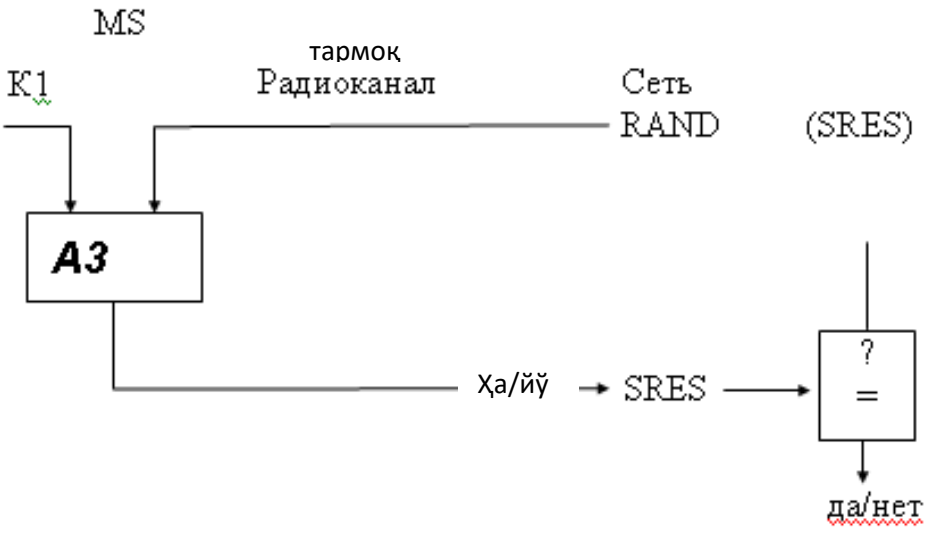

Figure 4. Authentication principle.

EIR – Equipment Identification Register contains a centralized database of data to verify the authenticity of the International Mobile Equipment Identity (IMEI) number of a mobile station. This database is exclusively related to the mobile station equipment. The EIR database consists of a list of IMEI numbers organized as follows.

WHITE LIST – contains IMEI numbers that are associated with authorized mobile stations.

BLACK LIST – contains IMEI numbers of mobile stations that have been stolen or otherwise refused service.

GREY LIST – contains IMEI numbers of mobile stations with software problems that are not considered grounds for inclusion in the “black list”.

The EIR database can be accessed remotely by the MSC of this network, as well as MSCs of other mobile networks.

As in the case of the HLR, a network can have more than one EIR, where each EIR manages a specific group of IMEIs. The MSC includes a transmitter that returns the EIR address when receiving an IMEI number, and manages the appropriate part of the device database.

IWF - inter-network functional connection is one of the components of the MSC. It provides subscribers with the ability to use the means of changing the protocols and data transfer rates that can be used to transfer data between the terminal equipment (DIE) of the GSM network and the ordinary terminal equipment of the registered network. The inter-network functional connection "separates" the modem from the device's own bank to connect to the corresponding modem of the registered network. The IWF provides direct connection type interfaces for the device delivered to the customer, for example, for packet data transfer PAD according to the X.25 protocol.

ES - echo suppressor is used for all telephone channels (regardless of their length) due to physical delay in the distribution tracts, including the radio channel of GSM networks PSTN by MSC aa. A typical echo suppressor ES can provide a 68-millisecond interval in the section between the output of the registered telephone network and the telephone of the network. The total delay in the GSM channel during forward and reverse propagation due to signal processing, speech encoding/decoding, channel coding, etc. is approximately 180 ms. This delay may not be noticeable to the mobile subscriber unless the hybrid transformer is turned on, which is a necessary installation in the MSC, since the standard connection in the telephone channel PSTN is considered two-wire. When connecting two subscribers of the specified network, there will be no echo signals. Delays in the propagation of signals in the GSM path without ES activation annoy subscribers, interrupt conversations and distract attention. OMS - the operation and maintenance center is the central element of the GSM network, which provides control and management of other components of the network and monitoring the quality of its operation. OMS is integrated with other components of the GSM network via data transmission channels of the X.25 protocol. OMS provides the function of processing emergency signals intended for informing service personnel and registers information about emergency situations in other network components. Depending on the nature of the malfunction, OMS is able to eliminate it automatically or with the active intervention of an employee. OMS can provide verification of the state of network equipment and the passage of mobile station calls. OMS is able to control the load on the network. The effective management function includes collecting statistical data on the load from the components of the GSM network, writing them to disk files and displaying them on the display for visual analysis. OMS provides management of the database of software changes and network element configurations. Software loading into memory is carried out from OMS to other network elements or from them to OMS.

NMC - Network Management Center is able to provide rational hierarchical management of the GSM network. It provides operation and maintenance at all network levels, supported by OMS centers responsible for managing regional networks. NMC provides graphical management of the entire network and provides dispatching management of the network in complex emergency situations, such as failures or overloaded nodes. In addition, it monitors the status of the automatic control device implemented in the network equipment and displays the network status for NMC operators. This allows operators to monitor their regional problems, and if necessary, provide assistance to the OMS responsible for a specific region. Thus, the NMC employee knows the overall network status and instructs the OMS employee to change the strategy for solving the regional problem. NMC - focuses on signaling

routes and connections between nodes, since it does not allow conditions for overloading the network. To prevent the spread of congestion between networks, the NMC coordinates the routing of connections between the GSM and PSTN networks. In this case, the NMC employee coordinates the network management issues with another NMC employee. The NMC provides scheduling control for the network equipment of the base station subsystem (BSS). When subscribers can use the system with high priority (emergency services), the NMC operators can activate emergency procedures such as "priority access" in experimental situations.

If the local OMS is considered unserviceable, the NMC can take responsibility for any area, in which case the OMS acts as a transit point between the network NVC and the equipment. The NMC provides operators with functions similar to those of the OMS.

The NMC is an important network planning tool, since the NMC monitors the network and its operation at the network level, in particular, it provides network planning with information that determines its optimal development.

BSS is a base station equipment, which includes a base station controller (BSC) and base transceiver stations (BTS). The base station controller can control several transceiver units. The BSS manages the allocation of radio channels, controls connections, regulates their queuing, provides frequency hopping operation, signal modulation and demodulation, message encoding and decoding, speech encoding, speech, data and paging rate adaptation, and determines the queue for transmitting personal paging messages.

The BSS performs some functions in the operation of the MSC, HLR, VLR, for example: channel release under the control of the MSC, but the MSC can request the base station to provide channel release if the call is not received due to radio interference. The BSS and MSC together provide priority transmission of information for certain categories of mobile stations.

TSE is a transcoder that converts the outgoing signals of the MSC speech and data channel (64 kbit/s IKM) to the form of the corresponding GSM recommendations (GSM 04.08 recommendations) over the radio interface.

The transmission rate of speech presented in digital form in accordance with these requirements is 13 kbit/s. This digital speech signal transmission channel is called “full-rate”. The standard provides for the use of a half-rate speech channel in the future (transmission rate 6.5 kbit/s).

The transmission rate is reduced by using a special speech converter using linear predictive coding (LPC), long-term prediction (LTP), residual impulse excitation (RPE - sometimes called RELP).

The transcoder is usually located together with the MSS, in which the transmission of digital messages in the direction of the base stations - BSC controller is carried out by adding additional bits (staging) to the stream with a transmission rate of 13 kbit/s up to a data rate of 16 kbit/s. Then 4-fold compression is performed on the standard channel of 64 kbit/s. Thus, a 30-channel IKM line is formed, which provides the transmission of 120 speech channels defined by the GSM recommendations.

The sixteenth channel (64 kbit/s) is allocated separately for the transmission of “temporal window” signaling information and usually contains the SS N7 or LAPD graphic. On the other channel (64 kbit/s) a data packet compatible with the MKKTT X.25 protocol can be transmitted.

Thus, the resulting transmission rate for the specified interface is 30x64 kbit/s + 64 kbit/s + 64 kbit/s = 2048 kbit/s.

MS is a mobile station, which is a device that serves to organize the use of existing fixed networks of electrical communication by subscribers of GSM networks. Within the framework of the GSM standard, 5 classes of mobile stations are accepted, from the class 1 model with an

output power of 20 W installed in the transport model to the class 5 portable model with a maximum power of 0.8 W. Adaptive adjustment of the transmitter power is provided, which ensures the required communication quality when transmitting messages.

The mobile station and the mobile subscriber are independent of each other. Each subscriber has an international identification number (IMSI), which is recorded on its smart card. This approach allows installing radio telephones in taxis and cars for rent. Each mobile station is assigned an international identification number (IMEI). This number is used to prevent a stolen station or unauthorized station from being able to use GSM networks. In conclusion, the authentication and security systems of the GSM network, as well as the processes of identifying subscribers and verifying their authenticity in the network, are widely covered. Network components such as HLR and VLR play an important role in storing subscriber information and managing the network. Network security is ensured by the Authentication Center (AUC) and the Equipment Identification Registry (EIR). Also, the operation and maintenance centers (OMS) and the network management centers (NMC) monitor the optimal operation of the network. In general, the authentication system and security protocols of the GSM network serve to ensure the reliability and security of mobile communication services.

References:

1. Brown, T., & Davis, M. (2018). Emergency Protocols and Safety Management for UAV Operations. Journal of Aerospace Safety.
2. Garcia, R., & Martinez, J. (2021). Autonomous Control Systems in UAVs: Advances and Challenges. International Journal of Robotics and Automation.
3. Gonzalez, A., et al. (2020). Predictive Maintenance Techniques for Unmanned Aerial Vehicles. Journal of Mechanical Engineering.
4. Harris, K., et al. (2022). Optimizing Technical Maintenance for UAVs: Emerging Technologies and Methods. Aerospace Engineering Review.
5. Jones, P., et al. (2023). Real-Time Data Analysis in UAV Operations: Techniques and Applications. Data Science in Aerospace.
6. Khan, A., & Ali, R. (2022). Training and Certification for UAV Operators: Current Practices and Future Directions. Aviation Safety Journal.
7. Lee, S., et al. (2019). Flight Planning and Optimization for Unmanned Aerial Systems. Journal of Flight Management.
8. Miller, H., & Wilson, R. (2020). Software Solutions for UAV Flight Planning and Monitoring. Computing and Aerospace Systems.