**Введение**

GPRS (General Packet Radio Service) - это новая перспективная технология, стандартизация которой началась в 1993 году в European Telecommunication Standards Institute (http://www.etsi.org/), позволяющая работать в сети Internet, используя обычный мобильный телефон. С помощью GPRS, пользователи могут работать со своей электронной почтой, с обычными Web-серверами (а не со специальными WAP-версиями) и т.д. Основное достоинство GPRS-сетей состоит в том, что пользователь оплачивает только объем передаваемой/получаемой информации, а не время нахождения в сети. До разработки технологии GPRS, абонент оплачивал все время соединения независимо от того, использовал он установленный канал передачи данных. Иными словами, ресурсы сети задействованы только во время непосредственной передачи данных от телефона. Во время пауз (например, просмотр полученной электронной почты) ресурсы сети предоставляются в распоряжение других абонентов. Кроме того, технология GPRS является промежуточным этапом при переходе от сетей 2 поколения (GSM) к 3-му (UMTS). В GPRS максимально возможная скорость передачи данных составляет 171,2 Кбит/с - это почти в 12 раз быстрее работы передачи данных в обычных сетях GSM (9,6 Кбит/с). Однако на данный момент скорости не так высоки - обычно 30-40 Кбит/с. В настоящее время три крупнейших сотовых сети Таджикистана (Вавилон, Билайн, Мегафон) предлагают своим абонентам услуги GPRS. Реальное число желающих воспользоваться преимуществами этой технологии очень велико.

1. **Технология GPRS**
   1. **Общая характеристика технологии GPRS**

Одним из существенных недостатков сетей сотовой связи стандарта GSM на сегодняшний день является низкая скорость передачи данных (максимум 9.6 кбит/с). Да и сама организация этого процесса далека от совершенства - для передачи данных абоненту выделяется один голосовой канал, а биллинг осуществляется исходя из времени соединения (причем по тарифам, мало отличающимся от речевых).

Для высокоскоростной передачи данных посредством существующих GSM-сетей и была разработана GPRS (General Packet Radio Service - услуга пакетной передачи данных по радиоканалу). Необходимо отметить, что кроме повышения скорости (максимум составляет 171.2 кбит/с), новая система предполагает иную схему оплаты услуги передачи данных - при использовании GPRS расчеты будут производиться пропорционально объему переданной информации, а не времени, проведенному online. К тому же, введение GPRS будет способствовать более бережливому и рациональному распределению радиочастотного ресурса, можно сказать, что "пакеты" данных предполагается передавать одновременно по многим каналам (именно в одновременном использовании нескольких каналов и заключается выигрыш в скорости) в паузах между передачей речи. И только в паузах - голосовой трафик имеет безусловный приоритет перед данными, так что скорость передачи информации определяется не только возможностями сетевого и абонентского оборудования, но и загрузкой сети.

GPRS позволит ввести принципиально новые услуги, которые раньше не были доступны. Прежде всего это мобильный доступ к ресурсам Интернета с удовлетворяющей потребителя скоростью, мгновенным соединением и с очень выгодной системой тарификации. Например, при просмотре с помощью системы GPRS WEB-страницы в Интернете, мы можем изучать содержимое столько, сколько нам необходимо, поскольку платим только за принятую информацию и не платим за время нахождения в сети Интернет (не передавая данные, мы не занимаем каналы сети). При введении повременной оплаты на фиксированных телефонных линиях, тарифы на доступ в Интернет с мобильного GPRS-телефона будут еще более конкурентоспособны. Для тех абонентов, кто уже оценил удобство использования телефонов с WAP - броузером, внедрение технологии GPRS означает практически мгновенную загрузку WAP - страниц на экране телефона и более выгодную систему тарификации.

Для корпоративных пользователей система GPRS может послужить отличным инструментом для обеспечения безопасного и быстрого доступа сотрудников к корпоративным сетям предприятий, к почтовым, информационным серверам, удаленным базам данных. При этом появится возможность получать доступ к корпоративным сетям даже если абонент находится в сети другого GSM оператора, с которым организован GPRS-роуминг.

Технологии GPRS может применяться в системах телеметрии: устройство может быть все время подключено, не занимая при этом отдельный канал. Такая услуга может быть востребована службами охраны, банками для подключения банкоматов и в других областях, в том числе и промышленных. Технология GPRS позволит быстро передавать и получать большие объемы данных, видеоизображения, музыкальные файлы стандарта MP-3 и другую мультимедийную информацию.

В GPRS ни один канал не занимается под передачу данных целиком - и это основное качественное отличие новой технологии от используемых ныне. Разумеется, разработчики GPRS приложили все усилия для того, чтобы установка новой системы "поверх" существующих GSM-сетей оказалась как можно менее обременительной (и разорительной, что немаловажно) для операторов.

Рассмотрим подробнее, какие новые блоки и связи появляются в общей архитектуре системы сотовой связи стандарта GSM с внедрением GPRS, и пользовательское оборудование, способное работать с высокоскоростной пакетной передачей данных. Доработку GSM-сети для предоставления услуг высокоскоростной передачи данных GPRS можно условно разделить на две формы - программную и аппаратную. Если говорить о программном обеспечении, то оно нуждается в замене или обновлении практически всюду - начиная с реестров HLR-VLR и заканчивая базовыми станциями BTS. В частности, вводится режим многопользовательского доступа к временным кадрам каналов GSM, а в HLR, например, появляется новый параметр Mobile Station Multislot Capability (количество каналов, с которыми одновременно может работать мобильный телефон абонента).

**1.2 Структурная схема и состав GPRS технологии**

На рисунке 4 представлена структурная схема GPRS технологии, где изображены основные составляющие системы.

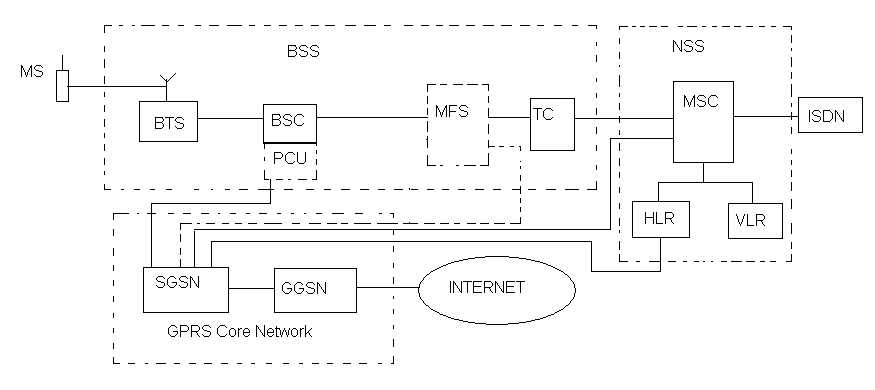


Рисунок 1 – Структурная схема модернизированной сети GSM под технологию GPRS

Ядро системы GPRS (GPRS Core Network) состоит (рис.4) из двух основных блоков - SGSN (Serving GPRS Support Node - узел поддержки GPRS) и GGPRS (Gateway GPRS Support Node - шлюзовой узел GPRS). Остановимся на их функциях более подробно.

SGSN является “мозгом” рассматриваемой системы. В некотором роде SGSN можно назвать аналогом MSC - коммутатора сети GSM. SGSN контролирует доставку пакетов данных пользователям, взаимодействует с реестром собственных абонентов сети HLR, проверяя, разрешены ли запрашиваемые пользователями услуги, ведет мониторинг находящихся online пользователей, организует регистрацию абонентов вновь "проявившихся" в зоне действия сети и т.п. Так же как и MSC, SGSN, в системе может быть и не один - в этом случае каждый узел отвечает за свой участок сети. Например, SGSN производства компании Motorola имеет следующие характеристики: каждый узел поддерживает передачу до 2000 пакетов в секунду, одновременно контролирует до 10000 находящихся online пользователей. Всего же в системе может быть до 18 SGSN Motorola.

Предназначение GGSN можно понять из его названия - это шлюз между сотовой сетью (вернее, ее частью для передачи данных GPRS) и внешними информационными магистралями (Internet, корпоративными интранет-сетями, другими GPRS системами и так далее). Основной задачей GGSN, таким образом, является роутинг (маршрутизация) данных, идущих от и к абоненту через SGSN. Вторичными функциями GGSN является адресация данных, динамическая выдача IP-адресов, а также отслеживание информации о внешних сетях и собственных абонентах (в том числе тарификация услуг).

В GPRS-систему заложена хорошая масштабируемость - при появлении новых абонентов оператор может увеличивать число SGSN, а при эскалации суммарного трафика - добавлять в систему новые GGSN. Внутри ядра GPRS-системы (между SGSN и GGSN) данные передаются с помощью специального туннельного протокола GTP (GPRS Tunneling Protocol).

Еще одной составной частью системы GPRS является PCU (Packet Control Unit - устройство контроля пакетной передачи). PCU стыкуется с контроллером базовых станций BSC и отвечает за направление трафика данных непосредственно от BSC к SGSN.

Но есть и альтернатива такой модернизации, без изменений в контролере (BSC) например компания Alcatel предлагает решение Alcatel EVOLIUM™ MFS 9135 Multi-BSS Fast packet Server (на рис.4 обозначен как MFS пунктирной линией) — это специальный сервер GPRS, предназначенный для поддержки существующих базовых станций Evolium BSS. Сервер располагается на площадке MSC или отдельным “рэком”, и поэтому его инсталляция требует только удаленной загрузки небольшого программного обеспечения без прерывания работы сети. Конструктивно сервер может состоять из одной или двух полок, вмещающих до 11 процессорных плат плюс 1 резервную каждая. В максимальной конфигурации сервер обслуживает 22 контроллера базовых станций (BSC) и обеспечивает одновременную обработку до 5280 каналов PDCH (Packet Data channels). В перспективе (при ориентации системы на мобильный Интернет) возможно добавление специального узла - IGSN (Internet GPRS Support Node - узел поддержки Интернет).

За управление и контроль GPRS-системы отвечает OMC-R/G (Operation and Maintenance Center - Radio/GSN - центр управления и обслуживания радио/узла GPRS. Это интерфейс между системой и обслуживающим ее персоналом.

Прежде чем приступить к работе с GPRS, мобильная станция, так же как и в обычном случае передачи голоса, должна зарегистрироваться в системе. Как уже было сказано, регистрацией ("прикреплением" (attachment) к сети) пользователей занимается SGSN. В случае успешного прохождения всех процедур (проверки доступности запрашиваемой услуги и копирования необходимых данных о пользователе из HLR в SGSN) абоненту выдается P-TMSI (Packet Temporary Mobile Subscriber Identity - временный номер мобильного абонента для пакетной передачи данных), аналогичный TMSI, который назначается мобильному телефону для передачи голоса (если абонентский терминал относится к классу А , то ему при регистрации выделяется как TMSI, так и P-TMSI).

Для быстрой маршрутизации информации к мобильному абоненту GPRS-система нуждается в данных о его месторасположении относительно сети, причем с большей точностью, нежели в случае передачи голосового трафика ( HLR и VLR хранят номер Location Area (LA), в которой находится абонент). Но как возрастет служебный трафик в сотовой сети и расход энергии мобильным аппаратом, если телефон будет информировать систему каждый раз при переходе от одной соты к другой! Чтобы найти разумный компромисс между объемом сигнального трафика в сети GPRS и необходимостью знать с высокой точностью местонахождение абонента принято деление терминалов на три класса:

1) IDLE (неработающий). Телефон отключен или находится вне зоны действия сети. Очевидно, что система не отслеживает перемещение подобных абонентов.

2) STANDBY (режим ожидания). Аппарат зарегистрирован (прикреплен) в GPRS-системе, но уже долгое время (определяемое специальным таймером) не работает с передачей данных. Местоположение STANDBY - абонентов известно с точностью до RA (Routing Area - область маршрутизации). RA мельче, чем LA (каждая LA разбивается на несколько RA, но, тем не менее, RA крупнее, чем сота, и состоит из нескольких элементарных ячеек).

3) READY (готовность). Абонентский терминал зарегистрирован в системе и находится в активной работе. Координаты телефонов, находящихся в режиме READY, известны системе (а, точнее, SGSN) с точностью до соты. Согласно этой идеологии, терминалы, находящиеся в STANDBY-режиме, при переходе из одного RA в другой посылают SGSN специальный сигнал о смене области маршрутизации (routing area update request). Если новая и старая RA контролируется одним SGSN, то смена RA приводит лишь к корректировке записи в SGSN. Если же абонент переходит в зону действия нового SGSN, то новый SGSN запрашивает у старого информацию о пользователе, а MSC, VLR, HLR и вовлеченные в работу GGSN ставятся в известность о смене SGSN. Когда телефон, работающий с GPRS-системой, перемещается в другую LA, то SGSN отправляет соответствующему VLR сообщение о необходимости смены записи о местонахождении абонента.

Интересно обстоят дела с маршрутизацией данных в случае роуминга GPRS-абонента. При этом возможны два варианта. SGSN в обоих случаях используется гостевой (VSGSN - Visited SGSN), а вот GGSN может использоваться либо гостевой (VGGSN - Visited GGSN), либо домашний (HGGSN - Home GGSN). В последнем случае между домашним и гостевым операторами должна существовать GPRS-магистраль (InterPLMN GPRS BackBone - GPRS-линия между разными мобильными сетями) для передачи трафика между HGGSN и мобильным абонентом. Кроме того, появляется необходимость в BG (Border Gateway - граничный шлюз) с обеих сторон с целью обеспечения защиты сетей от атак извне.

Следует отметить такой важный параметр, как QoS (Quality of Service - качество сервиса). Очевидно, что видеоконференция в режиме реального времени и отправка сообщения электронной почты предъявляют разные требования, например, к задержкам на пути пакетов данных. Поэтому в GPRS существует несколько классов QoS, подразделяющихся по следующим признакам:

* необходимому приоритету (существует высокий, средний и низкий приоритет данных);
* надежности (разделение на три класса по количеству возможных ошибок разного рода, потерянных пакетов и т.п.);
* задержкам (задержки информации вне GPRS-сети в расчет не принимаются);
* количественным характеристикам (пиковое и среднее значение скорости);

Класс QoS выбирается индивидуально для каждой новой сессии передачи данных. Кроме QoS, в характеристику сессии передачи данных входит тип протокола (PDP type - Packet Data Protocol type); PDP-адрес, выданный мобильной станции (выдача адресов бывает как статической, так и динамической); а также адрес GGSN, с которым идет работа. "Профиль" сессии (в англоязычной литературе принято обозначение "PDP context") записывается в телефон, а также в обслуживающие его SGSN и GGSN. Одновременно может поддерживаться несколько профилей передачи данных для каждого пользователя.

Пакетная передача данных предусматривает два режима "соединений":

* PTP (Point-To-Point - точка-точка);
* PTM (Point-To-Multipoint - точка-многоточие).

Широковещательный режим РТМ в свою очередь подразделяется на два класса:

1)PTM-M (PTM-Multicast) - передача необходимой информации всем пользователям, находящимся в определенной географической зоне;

2)PTM-G (PTM-Group Call) - данные направляются определенной группе пользователей.

Поддержка режима "многоточечной" передачи информации PTM ожидается в будущих спецификациях GPRS.

1.3 Абонентские терминалы для GPRS технологии

Для работы с системой пакетной передачи данных необходимо иметь специальный телефон, совместимый с GPRS. GPRS-терминалы подразделяются на три класса:

1) Устройства класса А способны одновременно работать как с передачей голоса, так и с передачей данных (они, говоря техническим языком, обладают возможностью функционировать как в режиме коммутации каналов (circuit switched), так и в режиме коммутации пакетов (packet switched). Подчеркну - речь идет об одновременной работе в разных режимах);

2)Устройства класса В могут осуществлять либо передачу голоса, либо передачу данных, но не одновременно;

3) Устройства класса С поддерживают только передачу данных и не могут быть использованы для голосовой связи. Как правило, это разного рода компьютерные платы для обеспечения беспроводного доступа к данным.

Максимальная скорость передачи данных определяется, в первую очередь, количеством каналов, с которыми одновременно может работать абонентский терминал. Один канал обеспечивает передачу данных со скоростью до 13.4 кбит/с.

Французская фирма SAGEM стала одним из первых производителей, представивших GPRS-совместимые телефоны. Модель Sagem MC-850, относится к классу В и имеет один канал для передачи данных и три - для приема, а чуть более современный Sagem MW-959, включает в себя уже четыре канала для входящего трафика (на передачу остался по-прежнему один канал, также не изменился класс устройства). Таким образом, максимальная скорость приема данных с помощью телефона Sagem MW-959 составляет 53.6 кбит/с, а передачи - 13.4 кбит/с.

1. **Безопасность технологии GPRS**

**2.1 Безопасность мобильной станции**

Наибольший интерес вызывает безопасность мобильного телефона, который в терминах GPRS является мобильной станцией. Его безопасность складывается из двух составляющих: SIM-карта и сам телефон

SIM-карта (Subscriber Identity Module) - это модуль идентификации абонента. В SIM-карте содержится информация о сервисах, предоставляемых абоненту, независимая от типа используемого мобильного оборудования. Эта карта может вставляться в любой другой GSM терминал, при этом абонент получает возможность использовать этот терминал для получения всех сервисов системы, на которые он подписан. С точки зрения безопасности SIM-карта отвечает за идентификацию абонента и аутентификацию мобильного телефона в GPRS-сети. Она содержит идентификатор IMSI, индивидуальный ключ аутентификации абонента длиной 128 бит Ki, алгоритм генерации ключей шифрования A8 и алгоритм аутентификации A3 и разумеется PIN-код для доступа к функциям карты. Алгоритм A5 наряду с IMEI включен в состав программного обеспечения телефона и обеспечивает его защиту.

Каждый абонент в GPRS-сети имеет уникальный международный идентификатор мобильного абонента (IMSI, International Mobile Subscriber Identity), хранимый в SIM-карте. IMSI состоит из 3 элементов:

трехразрядный код страны, двухразрядный код сети, десятиразрядный код абонента (Mobile Subscriber Identity Number, MSIN).

Алгоритм A8 отвечает за генерацию ключей шифрования, который, используя случайное число, передаваемое на мобильный терминал в момент соединения с сетью, и ключ Ki генерит 64-битный ключ шифрования трафика. Так как индивидуальный ключ Ki имеется не только у абонента, но и хранится в реестрах HLR и VLR, то и абонент и оборудование сети создают одинаковый ключ шифрования, который и используется для защиты передаваемых данных.

Алгоритм A3, отвечающий за аутентификацию абонента, похож на алгоритм A8 и также использует случайное число, получаемое в момент подключения к сети и индивидуальный ключ абонента.

Для доступа к функциям SIM-карты необходимо использовать специальный персональный код (другими словами, пароль) PIN (Personal Identiёcation Number), после 3-х неправильных попыток ввода которого, SIM-карта блокируется.

Безопасность самого телефона, как уже было сказано выше, обеспечивается двумя механизмами:

алгоритмом шифрования A5, который обеспечивает защиту данных, циркулируемых между мобильной станцией и узлом SGSN.

Уникальным 14-тиразрядным международным идентификатором аппаратуры мобильной связи (International Mobile Equipment Identity, IMEI), который однозначно идентифицирует телефон. Узнать этот номер очень просто - достаточно набрать на телефоне комбинацию \*#06#. Если высвеченное число не совпадает с тем, что указано на задней крышке телефона, то вероятнее всего вы пользуетесь взломанным аппаратом. Именно эти номера хранятся в реестре EIR. Данный реестр ведет три типа списков IMEI:

- "белый" список, содержащий идентификаторы всех разрешенных аппаратов.

- "серый" список, содержащий идентификаторы всех незапрещенных аппаратов, но используемых для различных целей, например, тестирования и т.п.

- "черный" список, содержащий идентификаторы всех запрещенных аппаратов. Как заявил в одном из интервью вице-президент МТС (http://www.mts.ru/press/speech9.html) Михаил Сусов "Сейчас между операторами (в России - А.Л.) проводятся переговоры о создании единого "черного списка" краденых телефонов".

Надо понимать, что идентификаторы IMEI и IMSI - независимы между собой. Более того - они решают различные задачи: IMEI идентифицирует мобильный терминал, а IMSI - абонента.

**2.2 Безопасность соединения мобильной станции с узлом SGSN**

В процессе подключения мобильной станции, описываемом далее, между ней и узлом SGSN происходит выбор версии используемого в дальнейшем алгоритма шифрования GPRS-A5. В 3-м квартале 2002 года началось внедрение третьей версии этого алгоритма (A5/3), которая может использоваться не только в GSM-, но и в GPRS-, HSCSD- и EDGE-сетях. Данный алгоритм разработан на базе алгоритма "Казуми" (Kasumi), в свою очередь разработанного на базе алгоритма MISTY компании Мицубиси. Как утверждается в пресс-релизе Ассоциации GSM, A5/3 обеспечивает на сегодняшний день практически 100-процентную защиту передаваемых данных. Однако не стоить безоглядно, верить этому утверждению. Аналогичные заявления делались и для предыдущих версий алгоритма A5, история которого начинается с 1987 года, однако они были успешно взломаны.

В сетях GPRS используются алгоритмы семейства A5 - GEA1 и GEA2, а после разработки A5/3 - начинается внедрение созданного на его базе алгоритма GEA3.

**2.3 Безопасность данных в процессе их передачи по сети GPRS**

Все данные между узлами поддержки (SGSN и GGSN) передаются с помощью специального протокола GTP (GPRS Tunneling Protocol), который инкапсулирует в себя любые пользовательские протоколы, например, HTTP, Telnet, FTP и т.д. По умолчанию GTP-трафик не шифруется. Кроме того, опорная сеть строится на базе частных IP-адресов, описанных в RFC 1918 (http://www.ietf.org/rfc/rfc1918.txt), что обеспечивает невозможность прямого доступа к сетевому оборудованию из внешних сетей.

Безопасность в процессе взаимодействия с различными операторами GPRS-услуг

Безопасность возлагается на устройства, называемые пограничными шлюзами (border gateway, BG), которые очень похожи на обычные межсетевые экраны, защищающие корпоративные сети от посягательств злоумышленников. В частности, этот шлюз защищает оператора от атак, связанных с подменой адреса (IP Spooёng).

Настройка такого шлюза включает в себя создание правил, разрешающих входящий/исходящий пользовательский трафик, данные биллинговой системы, аутентификацию роуминговых абонентов и т.п. Дополнительно на пограничный шлюз может быть установлено программное обеспечение, организующее VPN между различными GPRS-операторами.

Помимо встроенных в пограничный шлюз защитных механизмов, существует возможность использования продуктов третьих фирм. Первым таким решением стал межсетевой экран Firewall-1 GX компании CheckPoint Software (http://www.checkpoint.com/products/solutions/ёrewall-1gx.html), который, будучи установлен на пограничном шлюзе или узле GGSN повышает защищенность сети GPRS-оператора от возможных несанкционированных действий.

**2.4 Безопасность в процессе взаимодействия с Internet**

Основные механизмы безопасности реализованы на узле GGSN, в состав которого входит межсетевой экран, который определяет тип входящего и исходящего GPRS-трафика. Задача межсетевого экрана, входящего в состав GGSN, защитить мобильную станцию от атак внешних (из Internet) хакеров. Защита от атак с других мобильных станций возлагается на узел SGSN. Для предотвращения доступа к сетевому оборудованию опорной сети от внешних злоумышленников используется трансляция адресов (network address translation). Все остальные механизмы защиты могут быть взяты из классической практики обеспечения информационной безопасности Internet-сетей и устройств, например, аутентификация при помощи серверов RADIUS или защита трафика с помощью IPSec.

Процедура подключения мобильной станции

Упрощенно процесс подключения абонента, желающего воспользоваться услугами GPRS, выглядит следующим образом:

Мобильная станция посылает запрос (Attach Request) на получение доступа к сети, который содержит ряд параметров, в т.ч. и IMSI.

Узел SGSN, получив такой запрос, проверяет наличие аутентифицирующей данного абонента информации в своей базе. Если такая информация отсутствует, то SGSN посылает запрос в реестр HLR, который возвращаетт.н. аутентификационный триплет, содержащий:

Случайное число, используемое в алгоритмах A3 и A8 для выработки ключа шифрования и аутентификации абонента.

32-хразрядный ключ аутентификации абонента, который вырабатывается на основе индивидуального ключа, хранящегося как на мобильной станции, так и в реестре HLR.

Ключ шифрования данных, получаемый также на базе индивидуального ключа абонента.

Полученное случайное число передается на мобильную станцию, которая на его основе вырабатывает ключ шифрования и ключ аутентификации. Т.к. индивидуальные ключи, хранящиеся в реестре HLR и на мобильной станции совпадают, то и ключи шифрования и аутентификации также должны совпадать, что и является фактом правомочности запроса данным абонентом оплаченных GPRS-услуг.

После идентификации абонента осуществляется идентификация оборудования, которое посылает на SGSN идентификатор IMEI. Узел SGSN в свою очередь проводит проверку данного оборудования по реестру EIR.

После аутентификации абонента и оборудования происходит процедура определения местоположения абонента (с использованием реестров HLR и VLR), после чего происходит завершение процедуры подключения мобильной станции к сети GPRS. В том случае, если мобильная станция не смогла пройти аутентификацию, то SGSN посылает на нее сообщение Attach Reject.

1. **Реализация защиты технологии GPRS**

**3.1 Применение процесса аутентификации**

Информация, имеющая отношение к безопасности, состоящая из триплетов RAND, ответ на подпись (SRES), и Kc, сохраняется в визитном регистре перемещения (VLR). Когда VLR использовал триплет для аутентификации мобильной станции, он или сбрасывает его, или отмечает как использованный. Если VLR необходимо использовать триплет, он использовает набор не помеченных триплетов предпочтительно тем, которые уже помечены как использованные.

Когда VLR успешно запрашивает триплет в регистре расположения дома (HLR) или в старом VLR, он сбрасывает все триплеты, которые помечены как использованные. Когда HLR получает запрос на триплеты, он посылает любые наборы, которые не помечены как использованные. Эти наборы затем уничтожаются или помечаются как использованные. Системный оператор, сколько раз набор может быть повторно использован до сброса. Когда в HLR нет триплетов, он пошлёт запрос на дополнительные триплеты в центр аутентификации.

Запрос на эстафетной основе может быть интегрирован в различные потоки вызовов (например, на регистрацию, переадресацию). Он описывается здесь отдельно для большей ясности. Рисунки показывают потоки вызовов запроса на эстафетной основе.

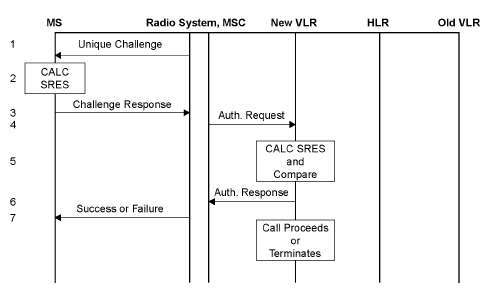


Рис 2. Уникальный запрос GSM на эстафетной основе.

1. Обслуживающая система посылает RAND мобильной станции.

2. Мобильная станция вычисляет SRES с использованием RAND и ключ аутентификации (K;) в алгоритме шифрования.

3. Мобильная станция передаёт SRES в обслуживающую систему.

4. Центр коммутации мобильной связи (MSC) посылает сообщение в VLR с запросом аутентификации.

5. VLR проверяет достоверность SRES.

6. VLR возвращает статус в MSC.

7. MSC посылает мобильной станции сообщение об успехе или неудаче операции.

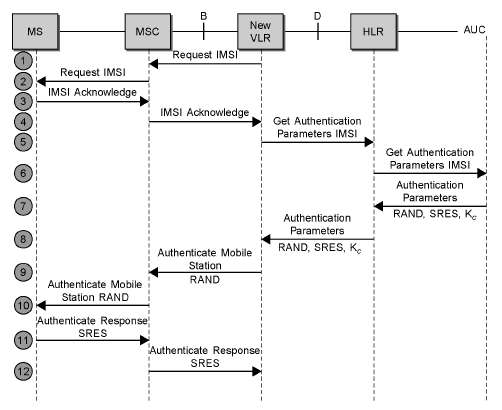


Рис.3 Уникальный запрос GSM на эстафетной основе с шифрованием.

И GSM, и североамериканские системы используют международный идентификационный номер мобильного оборудования (IMEI), который сохраняется в регистре идентификационных номеров оборудования (EIR) для проверки неисправностей и поддельного оборудования. EIR содержит подлинный список (список подлинных мобильных устройств), подозрительный список (список мобильных устройств под наблюдением), и мошеннический список (список мобильных устройств, которым отказано в услугах).

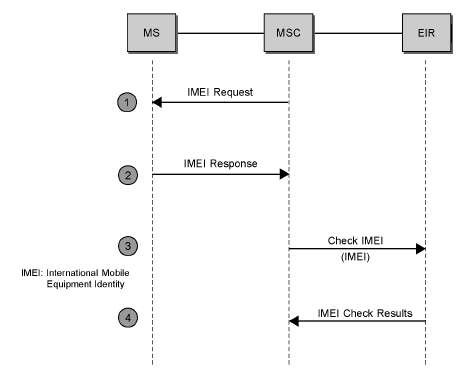


Рис.4 Проверка идентификационного номера оборудования.

**3.1.1 Алгоритм аутентификации**

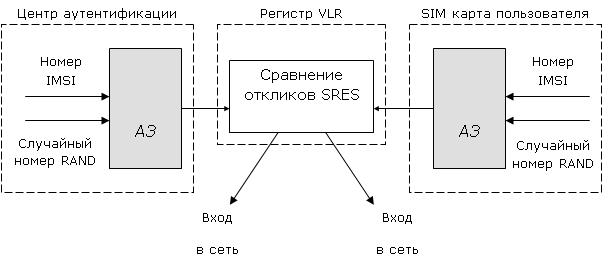


Рис. 5 Алгоритм аутентификации

Каждый подвижный абонент на время пользования системой связи получает стандартный модуль подлинности абонента (SIM), который содержит: международный идентификационный номер (IMSI), свой индивидуальный ключ аутентификации (Ki), алгоритм аутентификации (A3).

С помощью записанной в SIM информации в результате взаимного обмена данными между подвижной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети.

SGSN - Узел Обеспечения GPRS, который обрабатывает запросты от телефона, расшифровывая кадры и отсылая далее по назначению. Кадры шлются сразу параллельно на несколько базовых станции для увеличения скорости передачи данных, поэтому на одну конкретную BTS поступают последовательные кадры с непоследовательными номерами. До SGSN кадры поступают также в зашифрованным виде, что также затруднят ряд атак. Новый алгоритм A5 передачи данных по GPRS неизвестен на данный момент, поэтому данная область криптоанализа GSM станет доступной, когда станут известны новые алгориты шифрования GPRS, а это рано или поздно произойдет, так что работы криптоаналитакам на ближайщее будещее больше чем достаточно.

****

Рис.6 отправка кадров

**3.2 Специализированный межсетевой экран**

В качестве примера специализированного межсетевого экрана можно привести продукт Firewall-1 GX, разработанный компанией Check Point Software Technologies. Firewall-1 GX производит детальную инспекцию всех пакетов GTP и, в отличие от других систем, может осуществлять следующие ограничения:

1) выбор типа PDU (Protocol Data Unit) – продукт обладает возможностями настроек разрешенных и запрещенных типов пакетов GTP PDU;

2) контроль целостности туннеля – модуль Firewall-1 GX отслеживает все события, происходящие с туннелем, – создание, удаление или обновление туннеля – и осуществляет детальную фильтрацию трафика, так как имеет полный контроль над статусом туннеля;

3) контроль целостности запросов и ответов – все ответы сопоставляются с запросами на базе времени, типов запросов и номеров последовательностей;

4) контроль номеров последовательностей – специальный механизм T-PDU контролирует номера последовательностей пакетов и может осуществлять настройку их разброса (девиации);

5) предотвращение вмешательства злоумышленника в туннель – с помощью описания роуминговых областей и политик можно установить ограничения на разрешенные передачи и перенаправления туннелей;

6) контроль целостности и морфологии пакетов – все информационные элементы (IE) сканируются на корректность с учетом версии протокола и состояния флагов заголовка GTP-пакета;

7) блокирование анонимного доступа.

**3.3 Межсетевой экран Check Point Firewall-1 GX**

**3.3.1Основные функциональные особенности Firewall-1 GX**

Установка в качестве шлюза безопасности в GPRS-сети обычного IP-межсетевого экрана оставляет очень много уязвимостей в сети оператора из-за специфики используемых протоколов. В этом случае злоумышленник получает возможность осуществить множество сетевых атак. Firewall-1 GX учитывает все особенности протокола GTP и позволяет оператору надежно защитить свою сеть. Основные особенности такого решения перечислены ниже:

-Полное соответствие стандартам 3GPP GPRS

-Проверка целостности пакетов в протоколе GTP, а также внутренней морфологии

-Подробный анализ и управление туннелями

-Управление роуминговыми ограничениями, политиками перенаправления и переключения соединений на базовых станциях.

-Анализ информационных элементов GTP

-Генерация отчетов и предупреждений с указанием всей GTP-специфичной информации

-Не допускает перегрузок сети вредоносными пакетами

-Позволяет оператору создавать политику безопасности, учитывающую специфику GTP

Firewall-1 GX производит детальную инспекцию всех пакетов GTP и, в отличие от других систем, может осуществлять следующие ограничения:

-Выбор типа PDLJ - Продукт обладает полными возможностями настроек разрешенных и запрещенных типов пактов GTP PDLJ.

-Контроль целостности туннеля - Модуль Firewall-1 GX отслеживает все события, происходящие с туннелем с течением времени - создание, удаление или обновление туннеля, и может осуществлять детальную фильтрацию трафика, т.к. имеет полный контроль над статусом туннеля.

-Контроль целостности запросов и ответов - Все ответы сопоставляются с запросами на базе времени, типов запросов и номеров последовательностей.

-Контроль номеров последовательностей - Специальный механизм T-PDU контролирует номера последовательностей пакетов и имеет возможность настройки их разброса (девиации).

-Предотвращение вмешательства злоумышленника в туннель - С помощью описания роуминговых областей и политик можно установить ограничения на разрешенные передачи и перенаправления туннелей.

-Контроль целостности и морфологии пакетов - Все информационные элементы (IE) сканируются на корректность с учетом версии протокола и состояния флагов заголовка GTP-пакета.

-Блокирование анонимного доступа - В зависимости от политики безопасности оператора, анонимные соединения могут быть разрешены или запрещены.

-Контроль использования статических IP-адресов - В зависимости от политики безопасности оператора, использование туннелей со статическими IP-адресами пользователей может быть разрешено или блокировано.

-Контроль количества открываемых соединений - Специальный механизм Anti-Flood ограничивает поток сигнализационных сообщений для каждого GGSN, чтобы избежать его перегрузки, а также блокирует атаки типа Signaling Flood, одновременно уведомляя администратора безопасности.

**3.3.2 Отчетность и сигнализация в Firewall-1 GX**

Отчетность с учетом GTP-специфики.

Процедура создания и работы туннеля регистрируется отдельно от обычных IP-сессий и содержит все необходимые PDP-пaраметры, такие как:

-IMSI

-MS-ISDN

-IP-адрес GSN

-АРМ

-Режим выбора

-IP-адрес пользователя

Все действия, связанные с обновлением или удалением туннелей регистрируются, а кроме этого, ведется подсчет объема переданной информации в байтах и PDLJ.

Предупреждения GTP.

Модуль инспекции GTP-трафика генерирует различные виды предупреждений и сигналов тревоги по всем случаям нарушения политики безопасности или корректной работы протокола.

Дополнительные возможности Firewall-1 GX.

Особенности работы с APN/IMSI.

Шлюз Firewall-1 GX может осуществлять детальную фильтрацию контекста PDP в зависимости от APNJMSI, MS-IDSN и Selection mode или используя комбинацию всех этих параметров.

Конфигурация GTP v.1 (1999).

GTP v.1 будет поддерживаться в следующих версиях Firewall-1 GX, но поведение GTP vl можно настраивать уже в текущей версии. Эти настройки включают в себя разрешенные типы PDU протокола GTP vl, и какие действия нужно предпринимать для остальных PDU GTP vl.

**3.3.3Описание и схема тестовой зоны Firewall-1 GX.**

Состав тестовой зоны:

-шлюз Check Point Firewall-1 GX, на котором установлено программное обеспечение станции управления и инспекционного модуля;

-рабочая станция с эмулятором одного из коммутаторов SGSN;

-рабочая станция с графическим интерфейсом управления Firewall-1 GX (GUI), и эмулятором второго коммутатора SGSN, для тестирования процедуры handover;

-рабочая станция с эмулятором шлюза во внешние сети GGSN.

Такой набор программного и аппаратного обеспечения позволит воссоздать работу типичной GPRS-сети и испытать функциональность межсетевого экрана Firewall-1 GX.

В процессе тестирования будет испытана следующая функциональность Firewall-1 GX:

-Проверка корректности пакетов с точки зрения протокола (Packet Sanity)

-Проверка работоспособности установленной политики безопасности (Security Enforcement Test)

-Проверка работы системы отчетности и сигнализации (Logs and Alerts)

-Проверка дополнительных возможностей политики безопасности (Advanced Security Enforcement)

-Проверка работы с процедурой передачи абонента между базовыми станциями - handover (Handovers)

-Проверка работоспособности механизма ограничения сигнализационных потоков (Rate Limiting)

-Проверка работоспособности механизма учета количества переданной информации (Accounting)

-Проверка работоспособности механизма контроля номеров последовательностей (Sequence Number Validation).

На следующем этапе тестирования можно задействовать программные и аппаратные средства реальной GPRS-сети оператора, в этом случае схема размещения оборудования будет соответствовать приведенной на рис.7.

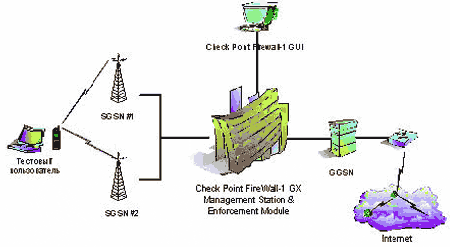


Рис. 7 Схема размещения оборудования

1. **Безопасность жизнедеятельности**

## 4.1. Анализ опасных и вредных факторов

Производственные факторы в зависимости от последствий, к которым может привести их действие, подразделяются на опасные и вредные. Фактор, воздействие которого на работающего в определенных условиях приводит к травме или другому резкому ухудшению здоровья, называется опасным производственным фактором. Фактор, воздействие которого на работающего в определенных условиях приводит к заболеванию или снижению работоспособности, называется вредным производственным фактором.

Специалисты по радиомонтажу сталкиваются с воздействием многих производственных вредных и опасных факторов согласно ГОСТ 12.0.003-74 ССБТ. К вредным и опасным факторам следует отнести следующие специфические для радиомонтажного производственного помещения факторы:

а) **Физические:**

повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека. При радиомонтаже применяются такие электроинструменты, как электродрель, электропаяльник, работающие при напряжении 220 В; при неисправности этих приборов рабочие подвергаются опасности поражения электрическим током.

повышенная запыленность и загазованность воздуха рабочей зоны. При пайке радиосхем применяется припой, содержащий свинец, который, испаряясь, загрязняет воздух рабочей зоны.

повышенная или пониженная температура воздуха рабочей зоны;

отсутствие или недостаток естественного света;

недостаточная освещённость рабочей зоны;

повышенный уровень шума (от систем вентиляции);

б) **Химические:**

повышенное содержание токсических веществ, вызывающих отравление организма. Мелкие частицы свинца при пайке, попадая в воздух рабочей зоны, загрязняют одежду и открытые части тела работающего, а также попадают в организм через органы дыхания, что приводит к отравлению и вызывает изменения в нервной системе, крови и сосудах.

в) **Психофизиологические:**

перенапряжение анализаторов;

монотонность труда;

эмоциональные и нервно - психические перегрузки.

## 4.2 Схема пожароэвакуации и оснащение помещения средствами пожаропредупреждения и пожаротушения

При ведении радиомонтажных работ производится пайка, обслуживание припоем, применение ЛВЖ (этиловый спирт, скипидар). Поэтому данные работы являются пожароопасными. Электрические паяльники обеспечиваются специальными термостойкими диэлектрическими подставками. ЛВЖ хранится в посуде с герметическими крышками (пробками).

Схема пожароэвакуации представлена на рисунке 7.

Помещение оснащено:

Автоматический комбинированный извещатель типа КИ-1, реагирует как на возникновение дыма, так и на повышение температуры. Располагается в помещении и коридоре.

Ручной углекислотный огнетушитель типа ОУ-5 емкостью 5 л, предназначен для тушения радиоэлектронного оборудования. Время действия огнетушителя до 60 с, дальность струи 2 м.

Пожарный кран, предназначен для тушения пожара водой, устанавливается на высоте 1,35 м от пола, оборудован пожарным рукавом 10 - 20 м и пожарным стволом.

Ящик с песком объемом 1% от общего объема помещения; в нашем случае объем ящика с песком составляет 1,2 м3.

Рис. 8 - схема пожароэвакуации и оснастка помещения средствами пожаропредупреждения и пожаротушения.

2 м

0,8 м

0,8 м

1,4 м

1,2 м

1,2 м

1,2 м

2,5 м

## 4.3 Расчет одиночного заземления

Для предотвращения электрических травм, которые могут быть вызваны при касании металлических конструкций или корпусов электрооборудования, оказавшихся под напряжением вследствие повреждения изоляции, а также для защиты аппаратуры устраиваются защитные заземления, представляющие собой преднамеренное соединение с землей или ее эквивалентом металлических частей электроустановок, нормально не находящихся под напряжением.

Расчет заземляющего устройства осуществляют исходя из его максимально допустимого сопротивления, установленного для соответствующего оборудования.

В электроустановках напряжением выше 1000 В в сети с заземленной нейтралью сопротивление заземляющего устройства должно быть не более 0,5 Ом в любое время года, то есть  Ом (согласно ПУЭ).

Так как естественный заземлитель отсутствует (не предусмотрен заданием), то предусматривается искусственный заземлитель, сопротивление которого  Ом.

Определим расчетное удельное сопротивление , где  - удельное сопротивление грунта, Ом\*м,  - климатический коэффициент (выбирается из справочника в соответствии с климатическими условиями отдельных зон). Выбираем тип грунта - суглинок с сопротивлением  Ом\*м, а климатический коэффициент в соответствии с нашей зоной . Тогда расчетное удельное сопротивление будет определено:

 Ом\*м. (4.3.1)

Выберем тип заземлителя и его размеры. Искусственный заземлитель относится к типу трубчатый или стержневой длиной  м и диаметром  м. Расстояние от заземлителя до поверхности земли в расчетах примем равным  м.

Рассчитаем сопротивление растекания одиночного трубчатого заземлителя:

, (4.3.2)

где  (м) - расстояние от поверхности земли до средины заземлителя.

Используя выше приведенные данные, получим:

 (Ом)

Количество параллельно соединенных одиночных заземлителей, необходимых для получения допустимого значения сопротивления заземления, без учета сопротивления полосы соединения, будет составлять:

, (4.3.3)

где  - коэффициент использования группового заземлителя. Согласно справочным данным, количество параллельно соединенных одиночных заземлителей должно быть не меньше двух. Так как мы рассчитываем одиночное заземление, то из справочных таблиц выбираем .

Тогда .

Длина полосы соединения определяется как:

, (4.3.4)

где  м - расстояние между вертикальными заземлителями.

Соответственно  м. Рассчитаем сопротивление  полосы соединения, используя формулу:

, (4.3.5)

где  - эквивалентный диаметр соединительной полосы шириной . В расчетах примем  при  см.

Тогда

 (Ом).

Исходя из найденных значений, можно рассчитать сопротивление всего заземляющего устройства с учетом соединительной полосы:

, (4.3.6)

где  - коэффициент использования соединительной полосы, выбирается из справочника и в соответствии с заданными условиями имеет значение .

** (Ом).**

Таким образом, сопротивление растекания группового искусственного заземлителя несколько меньше заданного (0,5 Ом), что повышает безопасность.

**4.Разработка схемы применения**

**4.1 Типовые схемы применения**

**Заключение**

В заключение хочу добавить, что, при создании технологии GPRS (как и при создании многих современных сетевых технологий) вопросам безопасности внимания уделялось недостаточно. Многие аспекты не описаны и отданы на откуп операторам, которые далеко не всегда уделяет безопасности первостепенное внимание, что приводит к печальным последствиям. Специалистами найдено уже немало недостатков технологии GPRS, но это уже тема другого проекта.

**Список литературы**

1. Основыпостроения телекоммуникационных систем и сетей: учебник для вузов / В.В. Крухмалёв, Н.В. Гордиенко, А.Д. Моченов и др.; под. ред. В.Н. Гордиенко и В.В. Крухмалёва. - М.: Горячая линия - Телеком, 2004. - 510 с.: ил.
2. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. - СПб.: BHV - Санкт-Петербург, 2000.
3. Карташевский В.Г. Сети подвижной связи / В.Г. Карташевский, С.Н. Семенов, Т.В. Фирстова. - М.: Эко-Трендз, 2001.
4. Системы мобильной связи: учебное пособие для вузов / В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов; под ред.В.П. Ипатова. - М.: Горячая линия - Телеком, 2003. - 272 с., ил.